جامعة البحرين

كلية الحقوق **قسم القانون العام**



الهجمات الإلكترونية
وسبل مواجهتها في القانون الدولي

أطروحة مقدمة لاستكمال متطلبات الحصول على درجة الدكتوراه

في القانون العام

إعـــــــداد

مريم خالد بوقحوص

الرقم الجامعي: 20052267

إشـــــــراف

أ.د. محمود السيد داوود

أستاذ العلاقات الدولية بجامعة البحرين

وأستاذ القانون الدولي العام بجامعة الأزهر سابقاً

مـــملكة البـــحرين

سبتمبر 2022

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

﴿وَقُل رَبِّ زِدني عِلمًا﴾

[طه: ١١٤]

جامعة البحرين
كلية الحقوق
قسم القانون العام
برنامج الدكتوراه

نموذج رقم (2)
صفحة الاعتماد من قبل لجنة التحكيم

ناقش الطالب/ مريم خالد أحمد بوقحوص رقم جامعي 20052267 الأطروحة التي استكمل بها متطلبات الحصول على درجة الدكتوراه في **(الفلسفة في القانون العام)** والمعنونة بـ **(الهجمات الإلكترونية وسبل مواجهتها في القانون الدولي)**
وذلك في يوم الثلاثاء الموافق 2022/12/13
وتوصي اللجنة بمنحه درجة الدكتوراه، بتقدير (A)

(لجنة المناقشة)

الاسم	التوقيع
أ.د. محمود السيد داوود – مشرفاً	
أ.د. وائل أحمد علام – ممتحناً خارجياً	
د. فؤاد عبدالكريم موسى – ممتحناً داخلياً	

الختم

كلية الحقوق
قسم القانون العام
COLLEGE OF LAW
PUBLIC LAW
DEPT.
UNIVERSITY OF BAHRAIN

ملخص الأطروحة

بدأ الحديث عن احتمال حدوث حرب ذات طبيعة سيبرانية في تسعينات القرن الماضي كضرب من الخيال العلمي وظل الأمر كذلك حتى استفاق العالم في 2007 على الهجمات السيبرانية التي وقعت على إستونيا وكانت كفيلة بأن تشل خدمات ومرافق الدولة لأسابيع. اليوم موضوع الهجمات السيبرانية الدولية من المواضيع الجادة التي تأخذ حيزا من سياسات الدفاع والأمن لدى جميع الدول. ذلك لأن قدرات الهجمات السيبرانية المحتملة تهدد بآثار غاية في الخطورة لا تقل عن أي سلاح ثقيل تقليدي. لذلك يجب الاستعداد لمواجهتها قانونيا. وذلك بتحريم استخدامها غير المشروع ووضع إطار قانوني للدولة الضحية للرد عليها.

تحاول هذه الدراسة معالجة الهجمات السيبرانية من منظور قانون اللجوء إلى الحرب Jus Ad Bellum وهو القانون الذي ينظم أموراً مثل: متى يحق للدولة اللجوء إلى الحرب، منع الحرب، ومبررات الحرب. وذلك بتطبيق قاعدة منع استخدام القوة على الهجمات السيبرانية وما ينتج عن مخالفتها من حق الدولة الضحية في الدفاع عن النفس ضد الهجوم السيبراني المسلح. كذلك تطبق هذه الدراسة قواعد مسؤولية الدولة على الهجمات السيبرانية وما ينتج عن ثبوت المسؤولية الدولية عن هجوم سيبراني غير مشروع من حق الدولة الضحية في اللجوء لسبل المساعدة الذاتية غير القسرية. لتخرج الدراسة بأربعة ردود متاحة للدولة الضحية على الهجمات السيبرانية العدوانية وهي الدفاع عن النفس– التدابير المضادة– التدابير القانونية– وتدابير حالة الضرورة.

إهداء

أمي

عسى أن تعبر كلمتي الفراق،

هذا بعض قطافك.

أبي

هذه واحدة من محاولات لن تتوقف في سبيل اقتدائي بدربك المشرف.

شكر وتقدير

الحمد لله أولاً وآخراً حمداً يليق بجلال وجهه وعظيم سلطانه، على توفيقه وتيسيره على إكمال هذا العمل.

أما بعد فهذه الأطروحة ليست مجهوداً فردياً، بل يقف خلفها فريق كبير يشاركني الإنجاز.

شكراً لأبي الأستاذ الدكتور خالد أحمد بوقحوص الذي أصبته من همي وتعبي ما أصبته ولم يفتأ يشد عزمي حتى اكتمال هذا المشروع، وشكراً للفاضلة الكريمة كالبحر نادية مراغي. أؤكد: لولا دعمكما اللامحدود لما رأت هذه الأطروحة النور.

شكراً لزوجي العزيز محمد بهزاد وأبنائي الثلاثة عبدالعزيز وسمية وسلمى على الصبر والتحمل والتماس العذر.

وعظيم الامتنان للأستاذ الدكتور علي المدني أستاذ العلوم اللغوية على تكرمه بالتدقيق اللغوي الذي بذل فيه الساعات الطِوال حتى انعكس ذلك في رقي اللغة وسلاسة الأسلوب وفي التخفيف من تعقيد الفكرة.

وأجل التقدير للأستاذ الدكتور محمود داوود مشرف الرسالة على مجهوده وصبره ومتابعته، حتى أينع ثمره وحان حصاده.

والثناء الصادق للعزيزة صفية إسحاق الكوهجي وعزيزتي الرائعة إيمان محمد ضيف لمساعدتهما في تنسيق البحث.

والشكر موصول لجميع منتسبي كلية الحقوق بجامعة البحرين على ما لاقيته منهم من دعم وتشجيع، وأخص بالذكر الدكتور مروان المدرس رئيس قسم القانون العام لما أحاطني به من رعاية ومتابعة واهتمام.

وأخيراً أتقدم بعظيم الامتنان لجامعة البحرين لابتعاثي وإتاحة هذه الفرصة لي. وشكراً لوطني البحرين الذي ما فتأت أرتع في خيره، وأسال الله أن يهديني لرد بعض جميله.

قائمة المحتويات (الفهرست)

اعتماد لجنة المناقشة ..... أ

ملخص الأطروحة ..... ب

إهداء ..... ج

شكر وتقدير ..... د

قائمة المحتويات (الفهرست) ..... ه

المقدمة 1

الفصل الأول 12

مدخل لفهم الهجمات الإلكترونية 12

المبحث الأول 13

ماهية الهجمات الإلكترونية في القانون الدولي 13

المطلب الأول 13

تعريف الهجمات الإلكترونية 13

الفرع الأول: تعريف الهجمات الإلكترونية 14

الفرع الثاني: تمييز مصطلح الهجمات الإلكترونية عن المصطلحات الأخرى المشابهة له 20

المطلب الثاني 26

خصائص الهجمات الإلكترونية 26

الفرع الأول: خاصية الفعالية 27

الفرع الثاني: خاصية تدني التكلفة 30

الفرع الثالث: خاصية السرعة 32

الفرع الرابع: خاصية كونها عابرة للحدود 34

الفرع الخامس: خاصية كونها مجهولة المصدر 36

الفرع السادس: خاصية قلب موازين القوة 38

المطلب الثالث 40

صور الهجمات الإلكترونية على الصعيد الدولي 40

الفرع الأول: طريقة العمل معياراً للتفرقة بين صور الهجمات 40
الفرع الثاني: أثر الهجمات معياراً للتفرقة بين صور الهجمات 43
المبحث الثاني.....50
أهم نماذج الهجمات الإلكترونية في العلاقات الدولية.....50
الفرع الأول.....51
الهجوم الإلكتروني على إستونيا 51
الفرع الثاني.....55
الهجمات الإلكترونية على جورجيا 55
الفرع الثالث.....59
الهجوم الإلكتروني على إيران.....59
الفرع الرابع.....63
عمليات التجسس الإلكتروني الصيني ــ الأمريكي 63
الفرع الخامس 68
عمليات التدخل الروسي الإلكتروني في الانتخابات الأمريكية عام 2016.....68
المبحث الثالث.....71
انطباق القانون الدولي على الهجمات السيبرانية.....71
الفصل الثاني.....80
تطبيق قاعدة منع استخدام القوة والاستثناءات الواردة عليها في الميثاق على الهجمات السيبرانية 80
المبحث الأول 81
قاعدة منع استخدام القوة في القانون الدولي ومدى انطباقها على الهجمات الإلكترونية 81
المطلب الأول.....83
التطور التاريخي لقاعدة منع استخدام القوة في القانون الدولي.....83
المطلب الثاني.....88
مدى خضوع الهجمات الإلكترونية لمبدأ حظر استخدام القوة.....88
الفرع الأول: مدى عد الهجمات السيبرانية في حكم القوة بالنظر إلى ذكر القوة في المواد المختلفة من الميثاق 89

الفرع الثاني: قياس الهجمات السيبرانية على القوة الاقتصادية والسياسية.....93
الفرع الثالث: معالجة الهجمات الإلكترونية في ظل قاعدة عدم التدخل في الشؤون الداخلية للدول الأخرى.....97
الفرع الرابع: قياس الهجمات السيبرانية على الأسلحة الكيميائية والبيولوجية.....101
المطلب الثالث.....102
التمييز بين ما يدخل في نطاق المادة (4)2 وغيره من الهجمات الإلكترونية 102
الفرع الأول: الهجمات الإلكترونية الداخلة في نطاق قاعدة منع استخدام القوة 103
أولا: الهجمات الإلكترونية التي تضاهي آثارها استخدام القوة.....104
ثانيا: الهجمات التعطيلية التي ذات النطاق الواسع والضرر الجسيم 107
ثالثا: الهجمات الصادرة من فاعل غير حكومي برعاية دولة 111
رابعا: التهديد باستخدام القوة السيبرانية 112
الفرع الثاني: الهجمات الإلكترونية التي لا تدخل في نطاق المادة (4)2.....116
أولا: مبدأ عدم التدخل.....118
ثانيا: مبدأ السيادة الإقليمية 121
ثالثا: مبدأ بذل العناية اللازمة DUE DILIGENCE 127
المبحث الثاني.....136
الدفاع عن النفس ضد الهجمات السيبرانية.....136
المطلب الأول.....137
الدفاع عن النفس ضد الهجمات السيبرانية في صورته التقليدية.....137
الفرع الأول: شروط الدفاع عن النفس في القانون الدولي العرفي (الضرورة والتناسب) 138
القسم الأول: الضرورة في الدفاع عن النفس ضد هجمات سيبرانية.....140
القسم الثاني: التناسب في الدفاع عن النفس ضد الهجمات السيبرانية 144
الفرع الثاني: شروط الدفاع عن النفس في ميثاق الأمم المتحدة (الهجوم المسلح).....149
القسم الأول: مدى عدِّ الهجوم السيبراني في حكم الهجوم المسلح 151
أ) الهجمات السيبرانية ذات الأثر الحركي المضاهي لآثار الهجوم المسلح:.....152
ب) الهجمات السيبرانية المسلحة ذات الأثر غير الحركي: 154
المطلب الثاني.....162

الأنواع التوسعية في الدفاع عن النفس وانطباقها على الهجوم السيبراني 162
الفرع الأول: الدفاع عن النفس ضد هجوم مسلح تراكمي 163
الفرع الثاني: الدفاع عن النفس الجماعي ضد الهجمات السيبرانية.....169
الفرع الثالث: الدفاع عن النفس ضد تهديد باستخدام القوة.....173
أولا: الدفاع عن النفس ردا على تهديد وشيك 174
ثانيا: الدفاع عن النفس ضد تهديد غير وشيك 181
الفرع الرابع: الدفاع عن النفس ضد الهجمات السيبرانية الصادرة من الفاعلين غير الحكوميين NON-STATE ACTOR.....182
أولا: الرد بالدفاع عن النفس ضد هجمات الجماعات غير الحكومية التي ترعاها دولة 186
ثانيا: الدفاع عن النفس ضد الهجمات السيبرانية الصادرة من جماعات غير حكومية مستقلة ولا ترعاها الدولة.....192

المبحث الثالث.....197
استخدام القوة من قبل مجلس الأمن.....197
الفصل الثالث.....202
سبل المواجهة الدولية للهجمات السيبرانية.....202
المبحث الأول 203
المسؤولية الدولية عن الهجمات السيبرانية.....203
المطلب الأول.....206
الركن الأول: أن تؤدي العمليات السيبرانية إلى خرق لالتزام دولي 206
أولا: مشكلة تجزء القوانين أو المعايير الدولية التي تحكم الهجمات السيبرانية 207
ثانيا: مشكلة التمييز بين القواعد القانونية الدولية الملزمة وغيرها.....212
ثالثا: الالتزامات المستحقة للمجتمع الدولي ككل أو OBLIGATION ERGA OMNES215
المطلب الثاني.....219
الركن الثاني: أن تكون نسبة العمليات السيبرانية غير المشروعة للدولة ممكنة 220
الفرع الأول: نسبة الهجمات السيبرانية للدولة قانوناً.....220
أولا: حالات نسبة الهجمات السيبرانية قانوناً إلى الدولة 221

المجموعة الأولى: العمليات السيبرانية التي تجريها أجهزة الدولة 221
المجموعة الثانية: العمليات السيبرانية التي يقوم بها بعض الأشخاص والكيانات في أثناء ممارستهم بعض اختصاصات الحكومة. 222
المجموعة الثالثة: الهجمات السيبرانية الصادرة من الأجهزة التي توضع تحت تصرف الدولة من قبل دولة أخرى. 223
المجموعة الرابعة: الهجمات السيبرانية المخالفة أو المتجاوزة للصلاحيات المعطاة من قبل الدولة. 225
المجموعة الخامسة: الهجمات السيبرانية الصادرة من الأفراد حال غياب السلطة الرسمية أو في حال انعدام قدرتها على القيام بمهامها. 226
المجموعة السادسة: الهجمات السيبرانية التي يتم القيام بها بناء على توجيهات الدولة أو تحت رقابتها. 227
ثانيا: مشكلة نسبة العملية السيبرانية قانوناً إلى الدولة 229
ثالثا: حل مشكلة نسبة العملية السيبرانية قانوناً إلى الدولة 229
الفرع الثاني 230
نسبة العملية السيبرانية إلى الدولة تقنياً 231
أولا: بعض أدوات الإثبات التقني 231
ثانيا: مشكلة الإثبات التقني في الفضاء السيبراني 235
ثالثا: الحل المتبع من الدول حالياً للتغلب على مشكلة الإسناد التقني 238
المطلب الثالث 243
بعض الحلول المستقبلية المقترحة للتصدي لمشكلة الإثبات وضعف الأدلة التقنية 243
الفرع الأول: القطاع الخاص 244
الفرع الثاني: لجان تقصي الحقائق الدولية 247
الفرع الثالث: جهاز دولي مستقل لإسناد العمليات السيبرانية 249
المطلب الرابع 252
آثار المسؤولية الدولية عن الهجمات السيبرانية 252
الفرع الأول: الكف عن الفعل غير المشروع 252
الفرع الثاني: تقديم التأكيدات والضمانات بعدم التكرار 253
الفرع الثالث: جبر الضرر 255

أولا: جبر الضرر بوصفه نتيجة قانونية للعمليات السيبرانية غير المشروعة.....256
ثانيا: أشكال جبر الضرر.....259
أولا: جبر ضرر الهجمات السيبرانية عن طريق الرد (إعادة الحالة إلى ما كانت عليه) 259
ثانيا: جبر ضرر الهجمات السيبرانية عن طريق التعويض المالي 261
ثالثا: جبر ضرر الهجمات السيبرانية عن طريق الترضية.....262
المبحث الثاني.....264
الاستجابة الدولية الممكنة رداً على الهجمات السيبرانية 264
(عدا الدفاع عن النفس) 264
المطلب الأول.....266
مواجهة الهجمات السيبرانية باتخاذ إجراءات المساعدة الذاتية.....266
الفرع الأول: التدابير القانونية غير الودية "RETORSION" 269
الفرع الثاني: التدابير المضادة 271
القسم الأول: شروط التدابير المضادة 275
القسم الثاني: التدابير المضادة ضد إخلال بالتزام يمس المجتمع الدولي ككلERGA OMNES
.....288
الفرع الثالث: تدابير بمقتضى حالة الضرورة 290
أولا: شروط حالة الضرورة.....290
ثانيا: تطبيق التصرف بناء على حالة الضرورة في النطاق السيبراني 293
المطلب الثاني.....296
المواجهة القضائية للهجمات السيبرانية أمام محكمة العدل الدولية.....296
الفرع الأول: معيار محكمة العدل الدولية في الإثبات 298
الفرع الثاني: متى تقبل محكمة العدل الدولية الدليل الظرفي؟ ومتى ترفضه؟ 300
الفرع الثالث: الأدلة الظرفية في سياق الهجمات السيبرانية 303
الخاتمة.....306
المصادر والمراجع 312
ABSTRACT 386

بسم الله الرحمن الرحيم

المقدمة

أولا: موضوع الدراسة:

غزا الحاسوب وعلومه جميع فروع المعرفة الإنسانية العامة والعلمية البحتة، فطفق وسيلة واسعة الشيوع، لا يمكن الاستغناء عنها بأي من أحوال الأفراد، والجماعات، أو المؤسسات العامة والخاصة، أو الدول بوجه عام، بل صار وسيلة لا تفارق الأطفال والطلاب في جدهم ولعبهم، بل صار ملازما لكل أمرئ في يده مخزونا في هاتفه، حتى طفقت منافع الحاسوب متعذرة الحصر. ولا يستغني القانون بمختلف فروعه عن الحاسوب وبرامجه المتعددة، وبخاصه في النظام القضائي وما يلزمه من قواعد بيانات.

بيد أن الحاسوب سلاح ذو حدين نافع وضار، ويكاد هذا يكون عاماً في جميع مناحي الحياة. ومازال نفعه وضرره يتسع، حتى استفحل خطر الضرر. وقد شغل القانون الدولي كثيرا بمخاطر الحاسوب في تدمير الدول والمؤسسات، مما حمل فقهاء القانون الدولي على دراسة ما عرف بالهجمات السيبرانية.

هذه الهجمات السيبرانية التي تستهدف الدولة ظاهرة ناشئة في العلاقات الدولية، تتم باستخدام جهاز حاسوب من قِبل دولة لمهاجمة شبكات وأجهزة دولة أخرى. هذه الظاهرة الناشئة في تصاعد كبير، وتطرح العديد من التحديات على القانون الدولي المعاصر، الذي وضعت قواعده قبل ظهور الاستخدام الضار للإنترنت. وتعالج هذه الدراسة موضوع الهجمات السيبرانية التي تقوم بها دولة، أو ترعاها دولة، أو تكون مسؤولة عنها دولة ضد دولة أخرى، في ظل قواعد القانون الدولي العرفية والمكتوبة في ميثاق الأمم المتحدة.

وهناك أمران مهمان يجب توجيه النظر إليهما في أثناء قراءة هذه الدراسة:

1- أن هذا البحث يعالج الهجمات الإلكترونية وفق قواعد اللجوء إلى الحرب Jus ad bellum فالقانون الدولي واسع في موضوعاته وفروعه القانونية، فلا يمكن تغطية موضوعات القانون الدولي كلها، فمثلا: لن يتطرق البحث إلى قانون النزاع المسلح، أو القانون الدولي الجنائي، أو حقوق الإنسان، أو غيرها.

بالرغم من أنه يمكن أن تُستَخدَم تلك المجموعات القانونية لتكييف سيناريو هجمات سيبرانية ذات صلة بها؛ لكن لأسباب تتعلق بمحدودية مساحة البحث، ولإتاحة المجال لتناول الموضوع تناولا عميقا، دفعا للمعالجات السطحية، ارتأت الباحثة أن تكون البداية من قانون اللجوء إلى الحرب؛ لأهميته وارتباط عدد كبير من القواعد القانونية به. لذلك فالدراسة تصبو إلى الإجابة عن سؤال: متى تعد الهجمات السيبرانية استخداما للقوة يؤهل للرد عليها بالدفاع عن النفس؟ فإن لم تصل إلى حد استخدام القوة المسلحة، فكيف يمكن مواجهتها؟

2-ولا مناص من الإشارة إلى أمر آخر وهو أن هذه الدراسة موجهة إلى مشكلة الهجمات السيبرانية في إطار غير مؤسسي. أو بعبارة أدق تبتعد عن صلاحيات وإجراءات أجهزة الأمم المتحدة. فموضوع قانون اللجوء إلى الحرب عادة ما يرتبط بمجلس الأمن، وبالفصل السابع من الميثاق وبعض صلاحيات الجمعية العمومية للأمم المتحدة. لكن هنا سيتم معالجته وفق منظور الدولة المنفردة أساساً. فهذا البحث يهدف إلى التوصل إلى ما يمكن أن تقوم به الدولة بنفسها من إجراءات مشروعة قانوناً رداً على هجوم سيبراني تعرضت له.

وليس ذلك تقليلا من أهمية وظيفة مجلس الأمن فمن الناحية القانونية يملك مجلس الأمن صلاحيات واسعة، يمكن أن يستخدمها لضبط الهجمات السيبرانية، لكن الحقيقة أن هذا الأمر مستبعد في الوقت الحالي لسببين: أولهما: حالة الانقسام في مجلس الأمن غنية عن التعريف، ثانياً: لاتزال الهجمات السيبرانية موضوعا يشوبه الغموض القانوني؛ ذلك أنه لم تستقر الآراء على الكثير من جوانبه. فمثلا لايزال التحدي قائما في تقرير متى تعد الهجمة السيبرانية استخداما للقوة! ناهيك عن متى تعد تهديدا للسلم والأمن الدوليين!! لذلك فإنه -في هذه المرحلة المبكرة وفي حالة غياب معاهدة دولية تتفق عليها الدول؛ لتقنين الهجمات الإلكترونية- يتوجب الاهتمام بضبط السلوك الفردي لكل دولة، وتحديد ما يمكنها، وما لا يمكنها القيام به.

وفضلاً عما تقدم فإن هذه الدراسة تحاول تجديد طرح قانون اللجوء إلى الحرب، مما يتطلب تغيير المعالجة الكلاسيكية في تناول قضايا القانون الدولي من خلال منظومة الأمم المتحدة. ولا يعني ذلك تغيير، أو تحريف القواعد الراسخة في القانون الدولي، لكنه يعني التحول من تتبع أثر الأجهزة الدولية إلى "آليات المساعدة الذاتية" التي يمكن أن تواجه بها الدولة الهجمات السيبرانية العدوانية وهي (الدفاع عن النفس، والتدابير القانونية غير الودية، والإجراءات المضادة، وتدابير حالة الضرورة). فاذا توافرت شروط كل حالة وأركانها، تكون التدابير مشروعة وفقا للقانون الدولي، وتوفر للدول مساحة جيدة للرد

على الهجمات السيبرانية. وإنه من باب تجديد طرح قانون اللجوء إلى الحرب سيعنى البحث بالمرور بآخر ما توصلت إليه الآراء الفقهية في كل قاعدة. فعادة ما يكون الأصل في القاعدة القانونية أنها في صورتها التقليدية، ثم تأتي محاولات الدول لتوسيع نطاقها أو تضييقه بما يتناسب مع مصالحها. فمثلا في الدفاع عن النفس هناك القاعدة التقليدية، كما جاءت في العرف الدولي والميثاق، وهناك دفاع عن النفس استباقي أو دفاع عن النفس ضد جماعات مسلحة مستقلة أو دفاع عن النفس ضد هجوم مسلح تم تجميعه تراكمياً، تلك الأنواع لم ترد في الميثاق، ومن المهم تناول كيفية انعكاسها في النطاق السيبراني والبت في شرعيتها من عدمه.

مع ذلك فلا بد من تأكيد أن توجه هذه الدراسة هو ضبط سلوك الدول في الفضاء الإلكتروني وفق ميثاق الأمم المتحدة. وبعبارة أخرى يناقش البحث أحدث القراءات لقانون اللجوء إلى الحرب حسب المدرسة التقليدية مدرسة الميثاق. فبعضهم يرى أن ممارسات الدول أدت إلى تغيير الميثاق وقواعد القانون الدولي بلا رجعة، وأن القوة النسبية للدول هي الحاكم وليس نص الميثاق[1] هذا البحث يخالف هذه المدرسة ويرفض أي سلوك لا يتماشى مع الميثاق، فالبحث يبحث عن الرد المشروع على الهجمات السيبرانية وفق نصوص الميثاق وأحكام محكمة العدل الدولية والعرف الدولي وبناء على ما جاء في هذه المصادر يتم تكييف العمليات السيبرانية وطرق الرد عليها.

ثانيا: أهمية الدراسة:

تكمن أهمية هذه الدراسة في سببين أولهما: زيادة الاعتماد على التكنولوجيا. والثاني تزايد قدرات الهجمات السيبرانية.

وأما تزايد أهمية الفضاء الإلكتروني بسبب تزايد اعتماد الدول على التكنولوجيا. لنأخذ عليه مثلاً: دولة مثل الولايات المتحدة يتكون فيها "الاقتصاد الرقمي" وحده من 6.9٪ من إجمالي الناتج المحلي للولايات المتحدة، و"تقنية المعلومات" تحوي 19.9٪، و"خدمات الاتصالات" 9 .9٪. وأما القطاع المالي فاعتماده على تكنولوجيا المعلومات 20.7% من الناتج القومي ولنتذكر. والحال أنه خلافا لمعظم الدول التي لا تزال السيولة النقدية طريقة الدفع السائدة فإن النقد لا يشكل سوى 33 ٪ من المدفوعات الحالية في الولايات المتحدة. ويصعب تقدير ما يمكن أن يفعله هجوم سيبراني في مثل هذه الحالات! لكنه

[1] Glennon, M. J. (2003). *Limits of Law, Prerogatives of Power: Interventionism after Kosovo* (2001st ed.), pp. 2-3. London, United Kingdom: Palgrave Macmillan.

حتما لن يقل عن تريليونات الدولارات من ثروات الأمم. لذلك تتأكد أهمية الدفاع عن البنية التحتية الإلكترونية التي تنمو باستمرار كما ينمو اعتمادنا على تكنولوجيا المعلومات[1].

أما تزايد القدرات السيبرانية الهجومية فإنها تأتي بديلاً جذاباً للعمليات العسكرية الحركية التقليدية. فلأسباب عديدة مثل وفرة الوسيلة السيبرانية حيث يستطيع أي شخص امتلاكها بالإضافة إلى مجهولية الفاعل، بالإضافة إلى انخفاض تكلفتها، كل ذلك سبب إقبالا ليس على مستوى الأفراد للجوء إلى الهجمات السيبرانية لتحقيق مصالح خاصة، بل حتى على صعيد الدول التي تحولت من استراتيجيات الاستهداف الحركي التقليدي إلى نهج متعدد الأوجه يحتل فيه البعد السيبراني اهتماما خاصا.

كل ذلك يؤكد بما لا يدع مجالا للشك أن الهجمات السيبرانية ستكون جزءا مهما من النزاعات الدولية المستقبلية. لذلك من المهم تشجيع استعداد القانون الدولي للتصدي لذلك. وبالرغم من أن هناك بعض المحاولات الجادة التي حصلت لتكييف الهجمات الإلكترونية فإنها لا تزال في بدايتها ومانزال محتاجة إلى التمحيص والتطوير، خصوصاً أننا مازلنا في المرحلة النظرية، أي لم يحدث أي تطبيق عملي قضائي أو تحكيمي للقانون الدولي على الهجمات الإلكترونية التي ما فتأت تحصل، وتعاني منها الدول.

ثالثا: منهجية الدراسة:

الاعتماد في هذه الدراسة على المنهج الوصفي لتَعَرُّف الهجمات الإلكترونية، وخصائصها وأنواعها والوقوف على الحوادث التي حدثت، إلى جانب المنهج التحليلي الذي يقوم على دراسة القواعد القانونية، ووصف الهجمات السيبرانية وشرح دلالاتها بغية مقاربتها بما يلائمها من القواعد الدولية العرفية أو المنصوص عليها في ميثاق الأمم المتحدة وغيره من المعاهدات والمواثيق الدولية، بقصد النظر في مدى إمكان أن تشملها تلك القواعد والمواثيق، مع عرض وبيان الآراء الفقهية التي طرحت حول المسألة وتحليلها ومقارنتها وتقرير مدى اتفاقها مع المبادئ المستقرة في القانون الدولي.

[1] Eaton, T. (2021). Self-Defense to Cyber Force: Combatting the Notion of 'Scale And Effect. *American University International Law Journal*, *36*(4), 697–771 [p. 702]. Retrieved from https://digitalcommons.wcl.american.edu/auilr/vol36/iss4/1/

رابعا: إشكاليات الدراسة:

1. إن أكبر الإشكاليات في هذا البحث هو دراسة مدى ملائمة القانون الدولي العرفي وميثاق الأمم المتحدة، للتصدي للتهديدات المرتبطة بالإنترنت وتكنولوجيا المعلومات والاتصالات. وكيفية تفسير قواعد القانون الدولي على الفضاء السيبراني والعمليات السيبرانية.
2. إشكالية تحديد ما يعد قوة في الهجمات السيبرانية، وهو أمر غاية في الأهمية؛ لأنه يترتب عليه تحريم استخدامها، وفقا لميثاق الأمم المتحدة، لكن لا يزال التحدي المتمثل في تحديد القوة في المجال السيبراني. وتحاول الدارسة الغوص في بعض المنافذ القانونية التي يمكن – من خلالها– رفع اللثام عما يدخل في مفهوم القوة في تلك الهجمات.
3. ويترتب على ما سبق إشكالية أخرى وهي الرد المطروح على الهجوم السيبراني حينما لا يكون هناك ضرر مادي (إصابة أو تدمير) كأن يتم إتلاف البيانات فقط، أو عندما يتوقف البريد الإلكتروني الحكومي عن العمل، أو عندما تفشل الأنظمة المصرفية، أو تنهار أسواق الأسهم، ولكن لا تقع إصابات في الأشخاص ولا تدمير مادي للممتلكات.
4. وينبثق من الإشكاليات السابقة إشكالية الدفاع عن النفس ضد الهجمات السيبرانية، هو الأساس الذي يباح فيه الدفاع عن النفس، خصوصا أن الدفاع عن النفس لا تقيده الوسيلة، فالدفاع عن النفس ضد الهجوم السيبراني يمكن أن يكون سيبرانياً، ويمكن أن يكون بالسلاح التقليدي العادي.
5. ومن الإشكاليات الكبرى التي تقف عليها الدراسة إشكالية الجماعات غير الحكومية التي تقوم بالهجمات السيبرانية ضد الدول. فإلى أي حد يمكن تحميل الدولة المسؤولية عن أفعال هذه الجماعات الموجودة على إقليمها. هل يمكن أن تستخدم الدولة ضحية الهجمات السيبرانية الدفاع عن النفس ضد تلك الجماعات، خصوصا إذا لم تثبت صلة بينها وبين الدولة التي توجد على إقليمها.
6. ولا مفر من دراسة مشكلة التنسيب في الهجمات السيبرانية وبخاصة حال عدم القطع في معرفة الفاعل. مع تكتيم الدول على الأدلة التي تبين الكيفية التي تم التوصل بها إلى نتيجة التنسيب المعلنة.

خامسا: تساؤلات الدراسة:

1. ما مخاطر حسبان الهجوم الإلكتروني خرقا لمبدأ "منع استخدام القوة" وما مزاياها؟
2. ما هو الهجوم السيبراني الذي يمثل انتهاكا لقاعدة منع استخدام القوة؟
3. ما هو الرد المشروع قانوناً على الهجمات السيبرانية؟
4. هل يمكن أن يصل هجوم سيبراني لدرجة الهجوم المسلح؟
5. متى يمكن أن يكون الدفاع عن النفس مشروعاً ضد هجوم سيبراني، وما هي حدوده وضوابطه في النطاق السيبراني؟
6. هل يمكن أن تعد الهجمات السيبرانية خرقا لمبدأ السيادة؟ وإن صح ذلك فما هو معيار عدم احترام السيادة في العمليات السيبرانية؟
7. هل يمكن أن تعد الهجمات السيبرانية خرقاً لمبدأ عدم التدخل في الشأن الداخلي؟ وإن كان ذلك صحيحا فما هو معيار التدخل غير المشروع في الشؤون الداخلية في الدول الأخرى في العمليات السيبرانية؟
8. التزام بذل العناية الذي يقضي بأن لا تسمح الدولة أن يكون إقليمها منطلقا للإضرار بالدول الأخرى، كيف يمكن تطبيقه في النطاق السيبراني؟ وهل يمكن جعل الدولة مسؤولة عن معرفة كل فعل سيبراني ضار يخرج من إقليمها؟
9. متى يمكن تحميل دولة ما مسؤولية هجوم سيبراني وما يترتب عليه من أضرار؟
10. ماذا حقق المجتمع الدولي للتصدي التشريعي للهجمات الإلكترونية حتى الآن؟
11. كيف يمكن معرفة أن دولة ما تقف خلف هجوم سيبراني؟ وهل هناك أي وسيلة لزيادة ثقة الرأي العام والمجتمع الدولي في نتيجة التنسيب؟
12. ما مدى إمكانية أن تنظر محكمة العدل الدولية في قضية هجمات سيبرانية؟ وهل هناك سوابق قضائية قبلت فيها أدلة ظرفية تناسب الطبيعة السيبرانية؟

سادسا: أهداف الدراسة:

تهدف الدراسة عامة –في كل قسم منها– إلى توفير سبيل قانوني للدولة؛ لتواجه ما قد تتعرض له من هجمات سيبرانية، وفي سبيل التوصل إلى هذا الهدف العام لابد من تحقيق الأهداف الفرعية التالية:

1. فهم معنى الهجوم الإلكتروني من منظور القانون الدولي وتَعَرُّف أنواعه وتقسيماته ودرجاته.
2. تطبيق قاعدة منع استخدام القوة على الهجمات السيبرانية؛ وذلك لتحريمها وفق ميثاق الأمم المتحدة.
3. التوصل إلى معايير مقبولة لنسبة الهجوم السيبراني إلى دولة معينة.
4. عرض المقترحات التي تعزز من الشفافية وتزيل الغموض حول عملية التحقيق التقني لتكون النتيجة المعلنة عن الدولة التي تقف خلف العملية السيبرانية أكثر قبولا.
5. تطبيق قواعد مسؤولية الدولة على الهجمات السيبرانية، للتوصل إلى معايير يمكن من خلالها تحميل الدولة مسؤولية الهجمات السيبرانية التي أصابت دولة أخرى، وما يتبع ذلك من آثار كالكف عن الهجمات السيبرانية غير المشروعة وجبر الضرر الناتج عنها.
6. حصر الردود الممكن اتخاذها من قبل الدول ضد الهجمات السيبرانية العدوانية، مع تحديد النطاق والوقت والحالة المشروعة لكل رد.

سابعا: الدراسات السابقة:

- دليل (تالين) 2.0 القانون الدولي المطبق على العمليات السيبرانية Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (2017)

تم نشر دليل (تالين) 2.0 هذا بواسطة مطبعة جامعة كامبريدج. في أوائل فبراير 2017. بقيادة مركز التميز للدفاع السيبراني التعاوني، التابع لحلف الناتو، شارك في كتابته ومراجعته عدد كبير من القانونين والخبراء في مجال الحاسوب، والعسكريين، تمثل الآراء فيه –أساساً– آراء 19 خبير في مجال القانون يطلقون على أنفسهم "فريق الخبراء القانونيين الدوليين". دليل (تالين) هو أهم المرجعيات في مجال الهجوم الإلكتروني والقانون الدولي على الإطلاق. وعلى الرغم من كونه دراسة أكاديمية غير ملزمة، فقد تم الاحتفاء بدليل (تالين) بوصفه دليلًا مهمًا للدول القومية، وللعلماء المدنيين والعسكريين. وقد صدرت طبعة أولى منه عام 2013 (Tallinn Manual0.1) لكنها انحصرت في مجال الحرب السيبرانية، ولم تتطرق للغالبية العظمى من الهجمات التي تهدف إلى التجسس أو سرقة البيانات الحساسة والملكية الفكرية. لذلك جاءت الطبعة الثانية من الدليل في 2017 بهدف سد النقص في الطبعة الأولى، فبالإضافة إلى كل قواعد الحرب السيبرانية التي

تم التوصل إليها في النسخة الأولى ركز دليل (تالين) 2.0 على التحليل القانوني للحوادث السيبرانية الأكثر شيوعًا، التي تواجهها الدول يومياً والتي لا تصل مستوى أعمال الحرب. فوضع 154 قاعدة قانونية تعالج موضوعات متنوعة، على سبيل المثال لا الحصر: السيادة على الفضاء السيبراني، قانون مسؤولية الدولة، وقانون الجو والفضاء والقانون الدبلوماسي والقنصلي وقانون حقوق الإنسان، من بين أمور أخرى. تجدر الإشارة أن دليل (تالين) مسبوق ببعض الأدلة قبله، مثل: دليل سان ريمو 1995 للقانون الدولي المطبق على الحرب البحرية، ودليل هارفرد 2009 للقانون الدولي المطبق على الحروب الجوية والصاروخية.

- كتاب فرانسوا ديليرو العمليات السيبرانية والقانون الدولي Cyber Operations and International Law (2020)

قدم فيه تحليلاً شاملاً للقانون الدولي المطبق على العمليات السيبرانية، بما في ذلك الفحص المنهجي للإسناد والشرعية، وسبل الانتصاف، ووضح أهمية التدابير المضادة بوصفها شكلا من أشكال العلاجات وأظهر حدود القانون الدولي وقدراته في حل القضايا المتعلقة بعمليات الفضاء السيبراني. فوفقا للكتاب هناك العديد من الحالات التي يترك فيها القانون الدولي الدولة ضحية عمليات السيبرانية لا حول لها ولا قوة. كالحال في العمليات الإلكترونية التي تجريها جهات فاعلة غير حكومية نيابة عن دولة. ويتبين في كتاب ديليرو أن قانون مسؤولية الدولة يقدم مجموعة من الحلول للاستجابة للعمليات السيبرانية، والسعي للحصول على تعويضات، لكنه لا يقدم إجابة في كل حالة لتبقى بعض الأسئلة مفتوحة وبانتظار الإجابة عنها.

- كتاب ماركو روسيني: العمليات السيبرانية واستخدام القوة في القانون الدولي Cyber Operations and the Use of Force in International Law (2015):

يستهل الفصل الأول بظهور التهديد السيبراني للأمن الدولي، ويشرح المنطقة التي يعمل فيها القانون الدولي ("الأنشطة الإلكترونية التي تقوم بها الدول ضد الدول الأخرى" خلافاً لتلك الأنشطة التي تعد جرائم إنترنت). فضلا عن مناقشة "مشكلات تحديد الهوية والإسناد". وينتهي بشرح نطاق الكتاب والغرض منه. يعرض الفصل الثاني تحليل قانون اللجوء للحرب (قانون يحدد متى يجوز للدول استخدام القوة في العلاقات الدولية) أما الفصلان الثالث والرابع فيعالجان الهجمات السيبرانية في نطاق قانون

النزاع المسلح (القانون الذي ينظم كيفية تنفيذ الأعمال العدائية في النزاعات المسلحة ويحمي المتضررين منها) فيعالجان المشكلات القانونية الناشئة من استخدام الهجمات الإلكترونية في النزاعات المسلحة، بما في ذلك "الوسائل والأساليب"، وقانون الاستهداف، والعمليات الإلكترونية التي لا تصل لعتبة الهجوم. ويقف الفصل الخامس على مبدأ الحياد في القانون الدولي، وكيف يمكن تطبيقه في النطاق السيبراني بخاصة؛ نظرا إلى الطبيعة العالمية للبنية التحتية لتكنولوجيا المعلومات والشركات العالمية التي تمتلكها.

- بحث دوروارد جونسون ومايكل شميت : الاستجابة للعمليات السيبرانية بالوكالة بموجب القانون الدولي Responding to Proxy Cyber Operations Under International Law(2021)

ورقة بحثية تتناول مشكلة استخدام وكلاء الإنترنت من قبل دول مثل روسيا والصين وكوريا الشمالية وإيران؛ فمثل هذه الدول تستخدم وكلاء غير حكوميين؛ للقيام بالعمليات السيبرانية الضارة ضد الدول نيابة عنها، وما ينشأ عن هذه الحالة من تعقيد قانوني أو "منطقة رمادية". يتوقف عند قضية التنسيب، لتحديد العلاقة الواقعية والقانونية بين الوكيل والدولة، ثم أنواع الردود المسموح بها، وفقا للقانون الدولي ضد العمليات السيبرانية بالوكالة.

- ورقة يوفال شانيو ومايكل شميت: آلية إسناد دولية للعمليات السيبرانية العدائية An International Attribution Mechanism for Hostile Cyber Operations (2020)

ورقة بحثية تتناول مشكلة الإسناد في القانون الدولي، فتعرض المنهج المتبع حاليا من قبل الدول، وتؤكد أن مدى قبول نتيجة إسناد العملية السيبرانية يعتمد على مدى المعقولية في التوصل إلى هذه النتيجة، وليس اليقين المطلق وتقترح بعض الأمور للتخفيف من السلطة التقديرية للدولة ضحية العملية السيبرانية، وزيادة ثقة المجتمع الدولي بالنتيجة. فتذكر بآلية موجودة واستخدمت عبر التاريخ، وهي لجان تقصي الحقائق المستقلة، كما وتدعو الورقة إلى إنشاء آلية تحقيق وإسناد دولية، لإسناد العمليات السيبرانية إلى فاعليها على غرار هيئة التفتيش في منظمة حظر الأسلحة الكيميائية.

ثامنا: خطة الدراسة:

بناء على ما تقدم تم تقسيم هذه الدراسة إلى ثلاثة فصول: **الفصل الأول**، بعنوان مدخل لفهم الهجمات السيبرانية وفيه يتم تَعَرُّف الهجمات السيبرانية، وخصائصها، وأنواعها بالإضافة إلى بعض حوادث الهجمات السيبرانية التي حدثت على صعيد العلاقات الدولية. و**الفصل الثاني**، بعنوان تطبيق قاعدة منع استخدام القوة، والاستثناءات الواردة عليها في الميثاق على الهجمات السيبرانية، فيعنى المبحث الأول منه بقاعدة منع استخدام القوة ومدى دخول الهجمات السيبرانية في نطاقها. أما المبحث الثاني فإنه يتناول استثناء الدفاع عن النفس فيفصل في كيفية الدفاع الشرعي عن النفس ضد هجوم سيبراني. ثم المبحث الثالث يتناول بإيجاز الاستثناء الثاني من قاعدة منع استخدام القوة، وهو استخدام القوة من قبل مجلس الأمن. وأما **الفصل الثالث**، فهو بعنوان المواجهة الدولية للهجمات السيبرانية، ولما كانت المواجهة تبدأ بتحميل الدولة المسؤولة مسؤولية الهجوم السيبراني؛ يعالج المبحث الأول المسؤولية الدولية عن الهجمات السيبرانية ليميز متى يعد الهجوم السيبراني فعلا غير مشروع؟ وكيف ينسب إلى دولة معينة؟ في المبحث الثاني يعرض الفصل أنواع الاستجابة الدولية الممكنة ردا على الهجمات السيبرانية –عدا الدفاع عن النفس– وهي تدابير قانونية، وتدابير مضادة، وتدابير حالة الضرورة، واللجوء إلى القضاء الدولي وبالأخص محكمة العدل الدولية. في كل ذلك تعرض القاعدة العامة من القانون الدولي ثم يتم تطبيقها على الحالة السيبرانية. وذلك بالاستعانة بأهم الآراء الفقهية في هذا المجال ومحاولة تحليلها وترجيح الأقرب إلى الصواب بينها.

الفصل الأول

مدخل لفهم الهجمات السيبرانية

المبحث الأول: ماهية الهجمات السيبرانية في القانون الدولي

المطلب الأول: تعريف الهجمات الإلكترونية

المطلب الثاني: خصائص الهجمات الإلكترونية

المطلب الثالث: صور الهجمات الإلكترونية على الصعيد الدولي

المبحث الثاني: أهم نماذج الهجمات الإلكترونية في العلاقات الدولية

المبحث الثالث: انطباق القانون الدولي على الهجمات السيبرانية

الفصل الأول

مدخل لفهم الهجمات الإلكترونية

يهدف هذا الفصل إلى تقديم مفهوم واضح للهجمات الإلكترونية على المستوى الدولي، وهذه الخطوة تعدُّ ضرورية، لأن المشكلة جديدة نوعا ما، والكتابات عنها (في مجال القانون الدولي) شحيحة في الفقه العربي، فقد شاب المشكلة بعض الغموض، وبات حجم المشكلة غير معروف أو على الأقل غير متفق عليه

إذ أنه لا يمكن البدء بالتأصيل القانوني للهجمات الإلكترونية دون توضيح ماهيتها أولا، وما الآثار التي تترتب عليها؟ فلا بد من الاتفاق على ماهية الشيء المراد تكييفه، ولن يكون ذلك إلا بتقديم صورة كاملة لمختلف جوانب المشكلة. الحقيقة أن هناك لبساً وتداخلا بين الهجمات الإلكترونية في المجال الدولي مع الجرائم الإلكترونية، تلك التي تقع على الأفراد أو الأشخاص الاعتباريين، مع أن كليهما يخضعان لفروع مختلفة من القانون؛ لذلك يجب تحديد الهجمات الإلكترونية الدولية التي تخضع للقانون الدولي دون سواه لتكون قاعدة يتم الانطلاق منها إلى تكييفها القانوني.

كذلك فإن هذا الفصل التعريفي ضروري للتعرف على مدى فداحة المشكلة وخطورتها وبالتالي آثارها. فمعرفة أثر الهجمات الإلكترونية ونطاقها ضروري لنعرف أين يقع الاعتداء في القانون الدولي؟ وأي القواعد تحديداً هي تلك التي يخالفها؟

بناء عليه يقسم هذا الفصل إلى ثلاثة مباحث. يعرف المبحث الأول "ماهية الهجمات السيبرانية" والهجمات السيبرانية جاءت في ثلاثة فروع أولا: تعريف الهجمات السيبرانية وتمييز الهجمات السيبرانية عن المصطلحات المشابهة لها. ثانيا: خصائص الهجمات السيبرانية وأخيرا صور الهجمات السيبرانية.

وبعد تَعَرُّف خصائص وصور الهجمات السيبرانية يأتي المبحث الثاني ليتناول بعض النماذج الجادة للهجمات السيبرانية بين الدول، وهي خمس وقائع للهجمات السيبرانية وقعت في إستونيا وجورجيا وإيران والولايات المتحدة في حادثة التدخل السيبراني في الانتخابات وأخيرا الولايات المتحدة في حادثة التجسس الصيني، كل واحدة من هذه الحوادث تستحق التوقف عندها بشيء من التفصيل بسبب التنوع بينها في الظروف المحيطة والأهداف.

أخيرا بعد الإلمام بأهم نماذج الهجمات السيبرانية وتمهيدا للفصل الثاني يطرح المبحث الثالث من هذا الفصل تساؤلاً مهماً حول مدى صلاحية تطبيق القانون الدولي على الهجمات السيبرانية.

المبحث الأول

ماهية الهجمات الإلكترونية في القانون الدولي

يهدف هذا المبحث إلى إعطاء صورة شاملة للهجمات الإلكترونية، وذلك بالإجابة عن ثلاثة أسئلة. أولا ماهي الهجمات الإلكترونية على الصعيد الدولي؟ ثانيا: ما هو الفرق بين الهجوم الإلكتروني والهجوم التقليدي؟ ثالثاً ماهي صور وأنواع الهجمات الإلكترونية؟ وسيتم تناول كل سؤال من هذه الأسئلة في مطلب مستقل.

المطلب الأول

تعريف الهجمات الإلكترونية

تجب الإشارة إلى أن هناك مشكلتين تعترضان تعريف الهجمات الإلكترونية. أولهما: عدم استقرار الفقه على تعريف للهجمات الإلكترونية حتى الآن فالتعريفات الموجودة كثيرة وتختلف في عناصرها باختلاف رؤية الجهة التي تقوم بالتعريف فالخبراء التقنيون يغلبون الجانب التقني والمؤسسات العسكرية تغلب الأمن العسكري والمؤسسات الثقافية تربط الهجمات بالجانب الثقافي، أما الجانب القانوني فهو ينقسم في تعريف الهجمات السيبرانية بين مدرستين: أولهما تعتمد على الهدف والأخرى تعتمد على الوسيلة.

والمشكلة الأخرى هي عدم الاستقرار على مصطلح لوصف الفعل السيبراني الضار في المجال الدولي. فالبعض يستخدم مصطلح هجوم إلكتروني أو سيبراني، البعض الآخر يستخدم مصطلح الحرب الإلكترونية أو الارهاب الإلكتروني، أو الجريمة الإلكترونية، بينما بعض الكتاب يستخدم كل هذه المصطلحات بمعنى واحد، وهناك كتاب آخرون يستخدمون كل مصطلح للدلالة على شيء مختلف؛ لذلك سيتم الوقوف عند مشكلة تعدد المصطلحات للتمييز بين كل منها وتأكيد أفضلية مصطلح الهجمات السيبرانية. لذلك يستعرض التعريفات القانونية المختلفة للهجمات السيبرانية ليستقر على

التعريف الأنسب ويعرض الفرع الثاني بعض المصطلحات التي تتشابه مع الهجمات السيبرانية ليسلط الضوء على أوجه الاختلاف بينها وبين الهجمات السيبرانية.

الفرع الأول: تعريف الهجمات الإلكترونية

إن الجدل الحالي الذي يقسم الدول بخصوص التعريف هو ما إذا كان ينبغي تبني النهج القائم على الوسائل أو النهج القائم على النتائج لتعريف الهجوم السيبراني؟[1]. يُعرّف النهج المستند إلى وسائل الهجمات الإلكترونية بالطرق التي يتم إجراؤها فيها، على سبيل المثال فايروس الضار[2]. أما النهج القائم على الآثار فأنه يحدد الهجمات الإلكترونية من خلال الهدف من الهجوم، كأن يستهدف الهجوم تقليل القدرات السيبرانية لدولة أخرى[3].

وهناك عدد من الأمور تزيد من تعقيد تعريف الهجوم السيبراني، ومنها: وجود الجهات الفاعلة غير الحكومية في الصورة، ومنها التساؤل عن مدى أهمية أن تؤدي الهجمات إلى أثر تدميري أو حركي، أو أهمية ان تؤدي الهجمات إلى تغيير المعلومات في الجهاز لتكوين هجوم مسلح.

ولسوف نبدأ بوجهات النظر التي اخذت بنهج الأثر في تحديد الهجمات السيبرانية ثم ننتقل للتعريفات التي اتبعت نهج الأداة المستخدمة.

أولا: التعريف القائم على نهج الأثر السيبراني:

بداية التعريفات التي تقوم على نهج الأثر عادة فيها تجاهل للوسيلة السيبرانية. والوسيلة السيبرانية هي الجانب الجديد الذي يحتاج إلى ضبط قانوني في العلاقات الدولية، لذلك من غير المستغرب أن يتجاوز الفقه هذا المنهج، وينتقل للمنهج الذي يعنى بالوسيلة. فمن أهم التعريفات للهجوم السيبراني القائم على اعتبار الأثر هو ما نشرته جامعة يال عام [4] 2012 وهو على النحو الآتي:

---

[1] Nguyen, R. (2013). Navigating "Jus Ad Bellum" in the Age of Cyber Warfare. *California Law Review*, *101*(4), 1079–1129. Retrieved from https://www.californialawreview.org/print/4navigating-jus-ad-bellum-in-the-age-of-cyber-warfare/

[2] المرجع السابق – ص1117

[3] المرجع السابق – ص1119

[4] A. Hathaway, O. et al. (2012). The Law of Cyber-Attack. *California Law Review*, *100*(4), 817–886. Retrieved from https://www.californialawreview.org/print/2the-law-of-cyber-attack/

"الهجوم السيبراني يتكون من أي إجراء يتم اتخاذه لتقويض الوظائف لشبكة كمبيوتر لأغراض سياسية أو أمنية وطنية"[1].

أي اجراء تعني أي نشاط، يعني يكفي أن يكون السلوك نشطًا، إما الهجوم أو الدفاع النشط كقرصنة تفجير تقطيع، فليس مهماً تحديد النشاط؛ لأننا نحدد الهجوم السيبراني وفقاً لهدفه "تقويض وظائف شبكة الكمبيوتر للأمن السياسي أو القومي" فيمكن استخدام أي أداة لاستهداف شبكة كمبيوتر،[2] فلابد وفقا لهذا التعريف أن يوجد جهاز كمبيوتر ويقع الهجوم السيبراني على الجهاز أو على الشبكة التي تربط أجهزة الكمبيوتر ببعضها البعض. غالبا ما تكون هذه الشبكة هي الانترنت، ولكن هناك أيضًا العديد من الشبكات المغلقة، مثل الشبكات الآمنة التي تستخدم داخل الشركة الخاصة، أو المؤسسة الحكومية الواحدة[3]. أما جهاز الكمبيوتر فلا يعني الجهاز المعروف، بل يمكن أن يكون الكمبيوتر في سيارة أو طائرة أو غسالة[4].

ووفقاً لهذا التعريف فإن استخدام شبكة كمبيوتر في الولايات المتحدة لتشغيل طائرة بدون طيار؛ من أجل تنفيذ هجوم مسلح في افغانستان ليس هجومًا إلكترونيا. بل هو تقنية متقدمة تستخدم في حرب تقليدية. أما استخدام مادة متفجرة عادية لقطع شبكة الكابلات تحت ــ سطح البحر التي تحمل حزم المعلومات بين القارات ــ فأنه يُعَدُّ هجومًا إلكترونيا[5]. بل إن قطعها يدويا سيكون هجوما إلكترونيا.

ويخرج من نطاق الهجمات الإلكترونية التجسس السيبراني، أو الاستغلال السيبراني، لأن هذه المفاهيم لا تنطوي على تغيير شبكات الكمبيوتر بطريقة تؤثر على قدرتها، فوفقاً لهذا التعريف يجب على الهجوم السيبراني أن يفعل أكثر من المراقبة السلبية لجهاز الكمبيوتر أو الشبكة أو نسخ البيانات، حتى لو كانت تلك البيانات سرية فهو غير كاف، بل يجب على الفاعل يؤثر على تشغيل النظام إما عن طريق إتلاف نظام التشغيل أو عن طريق إضافة معلومات خاطئة أو مضللة أو غير مرحب بها[6].

لقد سبقت الإشارة إلى أن معظم المراجع الحديثة تأخذ بالنهج القائم على الأدوات؛ وذلك للقصور الواضح في التعريف القائم على الهدف، والذي يمكن تلخيصه في الآتي:

---

[1] المرجع السابق – ص826
[2] المرجع السابق – ص830
[3] المرجع السابق – ص830
[4] المرجع السابق – ص827
[5] المرجع السابق – ص827
[6] المرجع السابق – ص829

- مشكلة تجاهل الوسيلة:

المشكلة في هذا التعريف أنه لا يعنى بخصوصية الهجمات السيبرانية، بل يعدها مجرد تقنية حرب، ويتعامل فقط مع آثارها. لا يمكن إنكار أن آثار الهجمات السيبرانية خصوصا غير الملموسة أنه جزء من المشكلة؛ احتار الفقه في تصنيفها، وكيفية الرد عليها، لكن ذلك لا يقارن بخصائص الأداة مثل المجهولية والسرعة والفاعلية والقدرة على عبور الحدود. كل تلك الخصائص تميز الأداة السيبرانية وتجعلها أكثر من مجرد تقنية حرب. لا ريب أن قواعد ومبادئ القانون الدولي الحالية تنطبق على هذه الظاهرة بيد أنها تحتاج إلى تكييف يراعي طبيعتها الخاصة، ويؤكد قابلية القانون الدولي للتطبيق، فإذا كانت الهجمات المجرد تقنية حرب فلماذا انطلقت دعوات العديد من الرؤساء والمنظمات وعلى رأسهم الأمين العام للأمم المتحدة[1] للتصدي القانوني لهذه الظاهرة.

- مشكلة التضييق من نطاق الهدف:

يخرج من نطاق هذا التعريف العمليات السيبرانية التجسسية التي تهدف إلى استخدام الدخول غير المشروع؛ لتحقيق أهداف معينة في الفضاء السيبراني، وإن كانت لا تغير ساكنا في الشبكة، لكنها تؤدي إلى أضرار حقيقية مثل الاطلاع على معلومات اقتصادية مهمة، أو معلومات سرية عن مشكلات تعاني منها الدولة ما يمكن استغلاله. وهذه العمليات تخرج من نطاق التعريف، وهي من أكثر الأنواع حدوثا. كذلك يخرج من نطاق هذا التعريف استخدام الدول للفضاء السيبراني للتدخل في الشؤن الداخلية للدول الأخرى، كتسخير وسائل التواصل الاجتماعي للتأثير على الرأي العام في انتخابات وطنية. وأسوء أن يفضي إليه هذا التعريف هو أن يحد من قدرات الظاهرة، ويجعلها بخلاف قدراتها الواقعية، لأن ذلك يؤدي إلى الفشل في ردع السلوك السيبراني الضار وإخراجه من نطاق التجريم.

ومع ذلك فإن هذا التعريف كان بداية جدية نحو رؤية موضوعية في تعريف الهجوم السيبراني، فهو يختلف عن التعريفات السابقة بأنه حررها من حصر الفاعل في دولة قومية، كما حرر الهجوم السيبراني من نطاق الحرب الإلكترونية [2]هذا المصطلح الذي أصبح غير مقبول ويؤخذ عليه عدم الواقعية. ويبدو أن مثل هذا التعريف جاء ليحاكي بعض الآراء التي لا ترى أثر قدرة الهجمات السيبرانية غير المادية

---

[1] انظر: "ناقوس الخطر الرابع: التكنولوجيا والفضاء الإلكتروني"
شؤون الأمم المتحدة. (يناير 25، 2022). الأمين العام يأمل في أن تقوم جميع البلدان بإخماد نيران عالمية مستعرة. استرجع من https://news.un.org/ar/story/2022/01/1092282

[2] Clarke, R. A., & Knake, R. (2010). *Cyber War: The Next Threat to National Security and What to Do About It*, p. 6. Harper Collins.

أي الآراء التي ترى أن الهجمات السيبرانية تنتج آثاراً تظل حبيسة الحاسوب، ولا تظهر في العالم المادي، وهذا أمر غير صحيح؛ لأن الهجمات السيبرانية تتطور في قدراتها، وتزداد تعقيدا يوما بعد يوم ويجب الاستعداد لها بأوسع تصور ممكن وليس بأضيق تصور ممكن[1].

ثانياً: التعريف القائم على نهج الأداة السيبرانية:

أما التعريف القائم على الوسيلة أو الأداة السيبرانية في تعريف الهجمات السيبرانية فهو كثير، لكن قبل البدء بالتعريف يجب التفرقة بين مصطلحين في موضوع تنظيم السلوك الدولي في الفضاء السيبراني. وهما (الهجمات السيبرانية) و(العمليات السيبرانية). نبدأ بالتفرقة بينهما من منظور دليل (تالين) (Tallinn)، ثم طرح تساؤل حول ما إذا كانت التفرقة بين المصطلحين مطلوبة أم لا.

"**الهجوم الإلكتروني** هو عملية إلكترونية، سواء أكانت هجومية أم دفاعية، ومن المتوقع بشكل معقول أن تتسبب في إصابة، أو وفاة الأشخاص، أو تلف، أو تدمير الأشياء"[2].

أولا: هذا التعريف جاء في سياق مناقشة انطباق الهجوم السيبراني في القانون الدولي الإنساني أو قانون النزاع المسلح وبالتالي فإنه يوضح حالة انطباق الهجوم السيبراني في أثناء النزاع المسلح. وتعريف الهجوم السيبراني هنا يحاكي تعريف الهجوم المسلح وفقا للقانون الدولي الإنساني.[3] يترتب على ذلك أن نتائج اعتبار هجوم سيبراني ــ وفقا للقانون الدولي الإنساني ــ تنطبق عليه قواعد النزاع المسلح مثل تمييز المدنيين وعدم استهدافهم، تناسب الميزة أو الفائدة العسكرية المرجوة من الهجوم مع الخسائر المدنية وغيرها. لكن هذا التعريف لا يناسب نطاق هذا البحث وهو قانون اللجوء إلى الحرب. فأكثر الأنشطة الإلكترونية الضارة لا تشكل فعلا حربيا.

---

[1] للمزيد من المشكلات المترتبة على اعتماد الهدف كمعيار
انظر: المرجع السابق – Nguyen, R. – ص 1086-1088

[2] Tallinn Manual 2.0, commentary to rule 92, p. 415
Schmitt, M.N. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd ed.). Cambridge University Press. https://doi.org/10.1017/9781316822524

[3] تنص المادة (49) في الفقرة (1): "تعني "الهجمات" أعمال العنف الهجومية والدفاعية ضد الخصم." وفي الفقرة (3): "تسري أحكام هذا القسم على كل عملية حربية أفي البر كانت أم في الجو أم في البحر قد تصيب السكان المدنيين أو الأفراد المدنيين أو الأعيان المدنية على البر. كما تنطبق على كافة الهجمات الموجهة من البحر أو من الجو ضد أهداف على البر، ولكنها لا تمس بطريقة أخرى قواعد القانون الدولي التي تطبق على النزاع المسلح في البحر أو في الجو"
الأمم المتحدة، الملحق (البروتوكول) الأول الإضافي إلى اتفاقيات جنيف (1977)

ثانياً: مع ذلك انتقد هذا التعريف وإن كان في نطاق قانون النزاع المسلح لأنه حدد نطاق مصطلح الهجوم السيبراني بالعنف فيرى دليل (تالين) بأن كلمة "هجوم" في نزاع مسلح تعني أنه يجب النظر في "العنف" بمعنى العواقب العنيفة.[1] بينما كان يمكن توسيع نطاق حماية المدنيين بتوسيع معنى الهجوم السيبراني. فالمصطلحات الواردة في التعريف مثل "الضرر" و "الإصابة" و "الخطر" لا تقتصر في الواقع على الأفراد والأشياء المادية، بل يمكن أن تقع على المعلومات[2]. فغالبًا ما تكون أنظمة الكمبيوتر والبيانات هي الأهداف الرئيسة للعملية الإلكترونية. لكن من الأبعد احتمالا أن تفي العمليات الإلكترونية بمتطلبات "الهجوم الإلكتروني" على النحو المعرف هنا.

أما الأفعال السيبرانية المدنية التي تتم خارج نطاق النزاع المسلح في أثناء النزاع المسلح لكنها لا تصل إلى مستوى الهجوم السيبراني فقد أسماها دليل (تالين) "العمليات السيبرانية" وعرفها كالآتي:

"**العمليات السيبرانية:** توظيف القدرات السيبرانية لتحقيق أهداف في الفضاء السيبراني[3] أو من خلاله"[4].

هنا في منهج التعريف من خلال الأداة نجد الهدف واسعاً جدا فهو "تحقيق أهداف داخل الفضاء السيبراني أو من خلاله" فهو يشمل كل أنواع الهجمات السيبرانية الممكنة، تلك التي تترك أثرا يمكن اكتشافه أو التي لا تترك أثرا يمكن اكتشافه، فالتعريف ينطبق على الوصول غير المصرح به إلى أجهزة الكمبيوتر، أو أنظمة الكمبيوتر، أو الشبكات، للحصول على المعلومات، ولكن دون التأثير بالضرورة على وظيفة النظام الذي يتم الوصول إليه أو تعديل البيانات الموجودة فيه أو إفسادها أو حذفها[5].

هذا بالإضافة إلى العمليات، سواء أكانت هجومية أم دفاعية، مما يهدف إلى تغيير، أو حذف، أو إفساد، أو منع الوصول إلى بيانات أو برامج الكمبيوتر؛ لأغراض الدعاية، أو الخداع، أو التعطيل

---

[1] Tallinn Manual 2.0, commentary to rule 92, para. 3, pp. 415-416

[2] Greenberg, A. (2019, August 23). What Is Cyberwar? The Complete WIRED Guide. Retrieved from https://www.wired.com/story/cyberwar-guide/

[3] يعرف دليل (تالين) "الفضاء الإلكتروني" بـ "مجال عالمي داخل بيئة المعلومات يتكون من شبكة مترابطة من البنى التحتية لتكنولوجيا المعلومات والبيانات المقيمة، بما في ذلك الإنترنت وشبكات الاتصالات وأنظمة الكمبيوتر والمعالجات ووحدات التحكم المدمجة".

Tallinn Manual 2.0, commentary to rule 92, para. 3, p. 564

[4] Tallinn Manual 2.0, glossary, definition of "Cyber Operation", p. 564

[5] Dinstein, Y., & Dahl, A. W. (2020c). Section II: Cyber Operations. In *Oslo Manual on Select Topics of the Law of Armed Conflict: Rules and Commentary* (pp. 19–29) [p. 20]. Springer, Cham. https://doi.org/10.1007/978-3-030-39169-0_2

الجزئي، أو الكلي لعمل الكمبيوتر المستهدف، أو نظام الكمبيوتر، أو الشبكة المستهدفة، والبنية التحتية المادية التي يتم تشغيلها بواسطة الكمبيوتر (إن وجدت)، أو إحداث ضرر مادي خارجي للكمبيوتر أو نظام الكمبيوتر أو الشبكة. لكن ولأنه سلك نهج الوسيلة وليس الأثر في تعريف العمليات السيبرانية بيد أن القصف الحركي بالسلاح التقليدي للبنى التحتية السيبرانية[1] المادية لا يعد عملية إلكترونية؛ لأنه سلك نهج الوسيلة في العمليات السيبرانية، وليس نهج الأثر.

كذلك فقد تمكن هذا التعريف من التغلب على مشكلة الفاعل غير الحكومي كالجماعات المسلحة، فلم يحصر معنى الهجمات السيبرانية – التي يعالجها القانون الدولي – في الهجمات التي تصدر من الدول، وهو بذلك تفوق على عدد من التعريفات السابقة التي عانت من هذه المشكلة.

لكن هل وفق دليل (تالين) في التفرقة بين **العملية** السيبرانية و**الهجوم** السيبراني؟ فكلمة هجوم لا تقتصر على قانون النزاع المسلح jus in bello (وهو ليس موضوع هذا البحث) بل هي أحد محاور قانون اللجوء إلى الحرب jus ad bellum (وهو محور هذا البحث) وإن كانت كلمة هجوم، وبالتالي هجوم سيبراني تختلف في تعريفها وحدودها في قانون النزاع المسلح عن قانون اللجوء إلى الحرب[2]. ففي الحالة الأولى يتم الاعتماد على اتفاقيات جنيف وفي الحالة الثانية يتم الاعتماد على معايير محكمة العدل الدولية في تعريف الهجوم المسلح. فإن دليل (تالين) وفر تعريفاً سيبرانياً للحالة الأولى أي أثناء النزاع، ولم يوفره للحالة الثانية وهي بداية الحرب التي تسمح بالدفاع عن النفس. ففي قانون اللجوء إلى الحرب اكتفى بالعملية السيبرانية بينما ظل الهجوم السيبراني في قانون اللجوء إلى الحرب دون تعريف واضح، والسبب في ذلك أنه في قانون اللجوء إلى الحرب فإن العمليات السيبرانية لن تختلف في تعريفها عن الهجمات السيبرانية؛ لأن الفعل هو نفسه، ويجب أن يكون على نطاق أكبر وآثار أكثر جسامة، لكن الفعل نفسه كما عرفته العمليات السيبرانية هو " توظيف القدرات السيبرانية لتحقيق أهداف في

---

[1] المرجع السابق – ص19

[2] للمزيد حول التفرقة بين معنى الهجوم السيبراني في نطاق القانون الدولي الإنساني وقانون اللجوء للحرب انظر:

Hyde, R., & Kolb, R. (2008). The Separation Between Jus Ad Bellum and Jus in Bello in Modern International Law: Equality of the Belligerents and Just War. *An introduction to the international law of armed conflicts* (pp. 21–28). Hart Publishing.

Schmitt, M. N. (2012). *"Attack" as a Term of Art in International Law: The Cyber Operations Context*. In C. Czosseck, R. Ottis, & K. Ziolkowski (Eds.). Presented at the 4th International Conference on Cyber Conflict, Tallinn, Estonia. Retrieved from https://ccdcoe.org/uploads/2012/01/5_2_Schmitt_AttackAsATermOfArt.pdf

الفضاء السيبراني أو من خلاله". هذا التعريف يمكن ان ينطبق على العملية السيبرانية، أو يمكن أن يصل إلى عتبة الهجوم السيبراني بحسب حجمه ونطاقة.

في رأي الباحثة: من الأنسب لأغراض هذا البحث عدم استبعاد مصطلح الهجوم السيبراني؛ لأنه أحد المحاور المهمة في الفصل الثاني حيث يناقش البحث فيه مدى اعتبار الأفعال السيبرانية قوة وإمكانية وصولها إلى مستوى الهجمات المسلحة السيبرانية. لذلك ولأهداف هذا البحث فإن العملية السيبرانية أو الهجوم السيبراني هما " توظيف القدرات السيبرانية لتحقيق أهداف في الفضاء السيبراني أو من خلاله" مع عدم الإخلال بنطاق وحجم الهجوم، كما سيتم تناوله بالدراسة في الفصل الثاني.

هذا وتجدر الإشارة إلى أن "دليل أوسلو حول موضوعات مختارة من قانون النزاع المسلح"[1] أخذ بنفس تعريف العمليات السيبرانية الذي أورده دليل (تالين) تماما، واستخدمه للمعنيين: العمليات والهجمات السيبرانية[2] مع تأكيد ضرورة عنصر العنف الذي يُحدِث اضرار مادية ليصل إلى مستوى هجوم سيبراني في نطاق نزاع مسلح. فهو اتفق مع دليل (تالين) في اشتراط الطبيعة المادية مثل تدمير متعمد للبنية التحتية المادية أو الأضرار المادية للممتلكات أو إصابة الأشخاص[3]، لكنه اختلف مع دليل (تالين) في التفرقة بين الهجوم والعملية الإلكترونية، فهو يراهما شيئا واحدا، لان الهجوم هو عملية إلكترونية لكنها "عنيفة"[4].

الفرع الثاني: تمييز مصطلح الهجمات الإلكترونية عن المصطلحات الأخرى المشابهة له

كما أشرنا هناك خلط بين الهجمات الإلكترونية بين الدول المقصودة في نطاق هذا البحث وغيرها من الأفعال الإلكترونية الضارة نعرض بعضها هنا:

1- الجريمة الإلكترونية أو السيبرانية:

[1] أعد الكتاب مجموعة من الخبراء بعد التشاور مع عدد من الحكومات الرئيسية. الغرض منه هو تقديم التوجيه للممارسين في مجال النزاعات المسلحة (الضباط بشكل اساسي) فيما يتعلق ببعض الاعمال العدائية في مجموعة من السياقات الجديدة أو الأقل وضوحا مثل الاسلحة التي يتم التحكم بها عن بعد الاسلحة الأوتوماتيكية الفضاء الخارجي والفضاء السيبراني وغيرها.
انظر: المرجع السابق – Dinstein, Y., & Dahl, A. W.

[2] المرجع السابق – Rule 20(a) – ص19

[3] المرجع السابق – Rule 24 – ص22

[4] المرجع السابق – Rule 24 – para. 2 – ص19

تعرف الجريمة السيبرانية أنها "أنشطة إجرامية تتم عن طريق أجهزة الكومبيوتر أو الانترنت".[1] يتبين من هذا أنه لكي تعد الجريمة جريمة إلكترونية، يجب استخدام التكنولوجيا لفعل شيء غير قانوني، مثل نشر الفيروسات، أو الممارسات الاحتيالية على الإنترنت، أو والقرصنة عبر الإنترنت، أو تخزين المواد الإباحية المتعلقة بالأطفال على جهاز الكومبيوتر ومشاركتها مع جهاز كمبيوتر آخر.[2]

ويظهر مما سبق أن الجريمة الإلكترونية تحمل مدلولا مختلفا عن الهجمة أو العملية الإلكترونية الدولية. فمن ناحية الفاعل فالجريمة الإلكترونية غالبا ما يقوم بها فرد أو مجموعة أفراد لمصلحة شخصية. بينما الهجمات الإلكترونية الدولية تقوم بها دولة أو شخص فاعل غير الدول، لمصلحة قومية أو أيديولوجية وتكون على نطاق واسع بحيث تكون ضحيتها دولة. لذلك فإن الجريمة الإلكترونية – وإن – كانت عابرة للحدود يحكمها القانون الجنائي، أما الهجمات الإلكترونية بين الدول فيحكمها القانون الدولي.

تجدر الإشارة هنا إلى اتفاقية بودابست بشأن الجرائم الإلكترونية، وهي معاهدة دولية تم اعتمادها تحت رعاية مجلس أوروبا في عام 2001 ودخلت حيز التنفيذ في 2004[3] وهي حتى الآن المعاهدة الدولية الرئيسة الوحيدة للتصدي للجرائم الإلكترونية التي صادقت عليها أكثر من 60 دولة[4]، صاغت الاتفاقية مجموعة من الأفعال وعدتها جرائم إلكترونية، وتسعى الاتفاقية إلى صياغة سياسات جنائية مشتركة بين دول الأطراف بشأن تلك الجرائم الإلكترونية، فضلا عن أنها تسعى إلى تسهيل التعاون بين الدول الأطراف في إنفاذ القانون عبر الحدود في قضايا الجرائم الإلكترونية. وبالرغم من أن اتفاقية بودابست

---

[1] "Definition of cybercrime: Criminal activities carried out by means of computers or the internet." cybercrime (n.d.). In *Lexico (Oxford Dictionary)*. Retrieved from https://www.lexico.com/definition/cybercrime

[2] "Definition of cybercrime: criminal activity (such as fraud, theft, or distribution of child pornography) committed using a computer especially to illegally access, transmit, or manipulate data cybercrime." (n.d.). In *Merriam-Webster*. Retrieved from https://www.merriam-webster.com/dictionary/cybercrime

للمزيد عن انواع الجرائم السيبرانية

Tietsort, J.R. (2022, June 5). 17 Types of Cyber Attacks & Examples (UPDATED FOR 2022). Aura. Retrieved from https://www.aura.com/learn/types-of-cyber-attacks

[3] Council of Europe (Budapest), *Convention on Cybercrime*, 23 November 2001, ETS No. 185. Available at: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185

[4] Council of Europe (Budapest), *Convention on Cybercrime*, Chart of signatures and ratifications of Treaty 185. Available at: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185

ذات اختصاص جنائي فإنه يمكن الاستفادة منها في نطاق قانون اللجوء إلى الحرب من ناحية بعض تعرف بعض المصطلحات التقنية، كتعريف النفاذ غير المشروع، والاعتراض غير المشروع، والتدخل في النظام وغيرها[1].

2- الحرب السيبرانية:

من أشهر المصطلحات التي استخدمت كمرادفاتٍ للهجمات السيبرانية هو مصطلح الحرب السيبرانية. وأكثر تعريف انتشارا للحرب السيبرانية كانت للخبير في الأمن السيبراني في البيت الأبيض Richard A. Clarke الذي عرف الحرب السيبرانية بوصفها:

"تصرفات تقوم بها دولة قومية لاختراق أجهزة كمبيوتر، أو شبكات دولة قومية أخرى لأغراض؛ التسبب في ضرر أو تعطيل"[2].

هذا التعريف أقرب إلى تعريف العملية السيبرانية منه للحرب السيبرانية، لأنه يقتصر على السلوك السيبراني الضار بينما تعريف الحرب السيبرانية يحتاج لدمج مفهوم الحرب وهي "ظاهرة العنف الجماعي المنظم التي تؤثر على العلاقات بين مجتمعين أو أكثر"[3] مع مفهوم القدرات السيبرانية وهي استخدام تكنلوجيا المعلومات والاتصالات؛ لتحقيق أغراض من خلال استخدام الفضاء السيبراني.

السبب في أن تعريف الحرب السيبرانية أعلاه يعبر أكثر عن عملية سيبرانية بدلا من أن يشرح وضع الحرب السيبرانية، هو أن مصطلح الحرب السيبرانية كان يستخدم للتعبير عن العملية السيبرانية بين الدول حتى تم هجره بالفعل لمصطلح العملية السيبرانية أو الهجوم السيبراني. بل وأصبح مصطلح الحرب السيبرانية يتهم بالتضليل والسطحية[4]. لأن الحرب السيبرانية توحي بحدوث حرب إلكترونية تعتمد على الجانب الرقمي فقط ، لكن الأغلب أن الجانب السيبراني هو أداة جديدة من أدوات الحرب

---

[1] مجلس أوروبا (بودابست)، *الاتفاقية المتعلقة بالجريمة الإلكترونية*، رقم 185 (23 سبتمبر 2001). استرجع من https://rm.coe.int/budapest-convention-in-arabic/1680739173

[2] المرجع السابق – Cyber War – Clarke, R. A., & Knake, R. – ص6

[3] Médecins Sans Frontières. (n.d.). القاموس العملي للقانون الإنساني. Retrieved from https://ar.guide-humanitarian-law.org/content/article/5/hrb/

[4] Roscini, M. (2016). Cyber Operations and the Use of Force in International Law (1st ed.), p. 77. https://doi.org/10.1093/acprof:oso/9780199655014.001.0001

التقليدية، أو بعد رابع (بعد الأرض والجو والبحر) تتنافس فيه الدول[1]؛ كذلك يعد استخدام الحرب السيبرانية بدلا من العملية السيبرانية خاطئاً؛ لأنه محصور في الاستخدامات العسكرية فقط والأهم من ذلك أنه محصور في وقت الحرب[2] وبالتالي سينظمها فقط قانون النزاع المسلح، وهذا الحصر خاطئ؛ لأن أكثر العمليات الإلكترونية بين الدول تكون في وقت السلم ولأغراض غير عسكرية وهي تحتاج لأن تنظم بقانون اللجوء إلى الحرب وحقوق الإنسان وغيرها.

3- حرب المعلومات:

يستخدم أحياناً مصطلح حرب المعلومات بديلا عن مصطلح الهجمات السيبرانية برغم الاختلاف الكبير في المعنيين.

مثلا منظمة شنغهاي للتعاون[3] عرفت حرب المعلومات على النحو الآتي:

"نزاع بين دولتين أو أكثر في مساحة المعلومات بهدف إحداث ضرر لنظم المعلومات والعمليات والموارد ذات الأهمية الحاسمة وغيرها من الهياكل ، وتخريب النظم السياسية والاقتصادية والاجتماعية، وغسل نفسي شامل، يهدف إلى زعزعة استقرار المجتمع والدولة، فضلاً عن إجبار الدولة على اتخاذ القرارات لصالح جهة معارضة.[4] "

---

[1] تجد الإشارة إلى ان تسمية وزارة الداخلية الأمريكية "البنتاجون" للفضاء السيبراني هي المجال الخامس بعد الأرض، والجو والبحر والفضاء. للمزيد انظر:

Clarke, R. A., & Knake, R. K. (2020). *The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats*. Penguin Random House.

[2] كما انتقدت ماري إلين أونيل إيديولوجية النزعة العسكرية المطبقة على الفضاء الإلكتروني من قبل الدول، وما قد يؤدي إليه ذلك من التهاون في الرد باستخدام القوة على الهجمات السيبرانية خصوصا تلك الصادرة من جماعات غير حكومية.

O'Connell, M. E. (2012). Cyber Security without Cyber War. Journal of Conflict & Security Law, 17(2), 187–209 [p. 191-209]. https://doi.org/10.1093/jcsl/krs017

[3] منظمة دولية حكومية دولية دائمة، تم الإعلان عن إنشائها في 15 يونيو 2001 في شنغهاي (الصين) لأغراض التعاون السياسي والعسكري والاقتصادي وهي تضم الآن ثمانية بلدان أعضاء (جمهورية الهند، جمهورية كازاخستان، جمهورية الصين الشعبية، جمهورية قيرغيزستان، جمهورية باكستان الإسلامية، الاتحاد الروسي، جمهورية طاجيكستان، وجمهورية أوزبكستان)

The Shanghai Cooperation Organization (SCO). (n.d.). About SCO. Retrieved from http://eng.sectsco.org/about_sco/

[4] The Shanghai Cooperation Organization (SCO). (n.d.). Annex 1 to the Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of Information Security, p. 209. Retrieved from https://ccdcoe.org/uploads/2018/10/SCO-090616-IISAgreement.pdf

نلاحظ من التعريف غياب البعد السيبراني تماما. فلا يوجد أي اشتراط للطبيعة السيبرانية سواء أمِنْ ناحية الوسيلة المستخدمة في حرب المعلومات أم من ناحية الهدف. كل ما هو مطلوب أن يتم التسويق لمعلومات معينة، بأي وسيلة كانت في مجتمع معين؛ لتحقيق أهداف ضد نظام تلك الدولة. ومع ذلك فمن غير المستغرب أن يقترن أو يختلط مصطلح حرب المعلومات بالهجمات السيبرانية بسبب ما يوفره الفضاء السيبراني من مجال مهم لحرب المعلومات. بعبارة أخرى الهجمات السيبرانية أداة مهمة من أدوات حرب المعلومات.

فقد تهدف الهجمات الإلكترونية إلى التحكم في مساحة المعلومات الخاصة بالفرد، أو تقييد أو منع الوصول لمعلومات محددة بتعطيل تدفق المعلومات، وهذا ما يسمى بالهجمات الإلكترونية الاجتماعية وتتم من خلال تكوين صورة معينة في أذهان الأشخاص بما يتفق مع أهداف حرب المعلومات التي تقوم بها دولة معينة[1].

لابد من التنويه أن مصطلح حرب المعلومات بهذه الطريقة يستخدم من روسيا والصين والدول ذات السلوك المشترك حيث يتم خلط مخاوف الهجمات السيبرانية بحرب المعلومات، وعادة ما يتم اتهامهم باستخدام مصطلح حرب المعلومات للتذرع بتقييد حرية الرأي في الانترنت[2].

يتبين ان حرب المعلومات والهجمات الإلكترونية أمران مختلفان تماماً ففي حرب المعلومات تكون الأهداف أيديولوجية غالبا وتكون الوسيلة المعلومات الضارة التي تهدد النواحي الاجتماعية والثقافية

---

[1] Defence Education Enhancement Program (DEEP) eAcademy. (2020, May). *MEDIA – (DIS)INFORMATION – SECURITY*. North Atlantic Treaty Organization (NATO). Retrieved from https://www.nato.int/nato_static_fl2014/assets/pdf/2020/5/pdf/2005-deepportal4-information-warfare.pdf

[2] Perkovich, G., & Levite, A. E. (Eds.). (2017). 5 Cyber War and Information War à la Russe. In *Understanding Cyber Conflict: 14 Analogies* (pp. 81–98). Washington, DC: Georgetown University Press;
Giles, K. (2012). Russia's Public Stance on Cyberspace Issues. In C. Czosseck, R. Ottis, & K. Ziolkowski (Eds.), *Chapter 2 Cyber Policy & Strategic Options*, 63–76 [pp. 67-69]. Tallinn, Estonia. Retrieved from https://ccdcoe.org/uploads/2015/04/CyCon_2012_book_web_sisu.indd_.pdf;
Sheraz, M. M., & Dayan, F. (2018). Cyber Warfare And Protection Of Civilian Under International Humanitarian Law. *Ilkogretim Online - Elementary Education Online*, *17*(3), 1790–1803 [pp. 1793-1795]. Retrieved from https://www.ilkogretim-online.org/fulltext/218-1638043863.pdf

والسياسية، أما الهجمات الإلكترونية – كما تم تعريفها أعلاه – فهي أكثر اتساعا؛ لأنها مجردة من أي هدف وهي فقط تركز على القدرات السيبرانية.

4- الإرهاب الإلكتروني:

ولا مناص من الوقوف على مصطلح الإرهاب الإلكتروني؛ لتكرار الإشكالية السابقة نفسها، فهناك تداخل بينه وبين الهجمات السيبرانية.[1] فحلف الناتو عرف الإرهاب السيبراني بأنه:

"هجوم إلكتروني يستخدم أو يستغل شبكات الكمبيوتر أو الاتصالات لإحداث "دمار أو تعطيل كاف لتوليد الخوف أو ترهيب المجتمع وتحويله إلى هدف أيديولوجي"[2].

تعريف آخر للإرهاب السيبراني:

"يُقصد بالإرهاب السيبراني الهجمات المتعمدة ذات الدوافع السياسية من قبل الجماعات دون الوطنية أو العملاء السريين، أو الأفراد ضد المعلومات وأنظمة الكمبيوتر وبرامج الكمبيوتر والبيانات التي تؤدي إلى العنف ضد أهداف غير قتالية."[3]

لا يوجد تعريف مجمع عليه للإرهاب حتى الآن، فمن الطبيعي ألا يتم الاتفاق على عناصر الإرهاب السيبراني، لكن مما تكررت الإشارة اليه في تعريفات الإرهاب هو انه الهدف أو الغاية التي عادة ما تكون سياسية أو ايديلوجية. ومن المضامين المتكررة في تعريف الإرهاب عامة هو عنصر التخويف أو الترهيب، فإذا ما جمع ذلك مع الطبيعة السيبرانية يكون الإرهاب السيبراني عبارة عن تخويف أو ترهيب باستخدام القدرات السيبرانية، لتحقيق أهداف سياسية أو أيديلوجية.

---

[1] الدكتور عادل عبد الصادق يعرف الإرهاب الالكتروني بأنه: "العدوان، أو التخويف أو التهديد مادياً أو معنوياً باستخدام الوسائل الالكترونية، الصادرة من الدول أو الجماعات، أو الأفراد عبر الفضاء الالكتروني، أو أن يكون هدفا لذلك العدوان بما يؤثر على الاستخدام السلمي له"
عبد الصادق، عادل .(2009) .*الارهاب الالكتروني: القوة في العلاقات الدولية نمط جديد وتحديات مختلفة* (الطبعة الأولى)، ص103. مركز الدراسات السياسية والاستراتيجية بالأهرام.

[2] NATO and Cyber Terrorism. (2008). In *Responses to Cyber Terrorism* (NATO Science for Peace and Security Series-E: Human and Societal Dynamics ed., pp. 118–126 [p. 119]). Ankara, Turkey: Centre of Excellence Defence Against Terrorism.

[3] Janczewski, L. J., & Colarik, A. M. (2007). *Cyber Warfare and Cyber Terrorism* (1st ed.), p. xiii. Hershey, Pennsylvania: IGI Global.

وخلافاً لمصطلح الحرب الإلكترونية فإن الارهاب الإلكتروني مشكلة حقيقية[1]، فسهولة الوصول إلى الإنترنت والحاسوب جعلت الجماعات الإرهابية، أو الجماعات الفاعلة من غير الدول تستفيد من الأداة السيبرانية؛ لتنفيذ أهداف إرهابية وهذا أمر يحتاج إلى الاهتمام والمعالجة القانونية؛ للتصدي وستعالج هذه الدراسة طرفاً من هذا الموضوع من منظور قانون اللجوء إلى الحرب في جزء الدفاع عن النفس ضد الهجمات السيبرانية الصادرة من جماعات مسلحة من غير الدول. مع ذلك فمعالجة القانون الدولي للإرهاب السيبراني لا تنحصر في قانون اللجوء إلى الحرب، بل في قانون النزاع المسلح والقانون الجنائي الدولي وقانون حقوق الانسان الدولي[2].

ومن المهم هنا التمييز بين مصطلح الهجوم السيبراني والإرهاب السيبراني، ذلك أن الهجوم السيبراني هو الأداة المستخدمة في الإرهاب السيبراني بينما الإرهاب السيبراني هو الذي يسخر الهجوم السيبراني لغايات إرهابية. لذلك فإن الهجمات أو لعمليات السيبرانية أوسع بكثير؛ لأنها تشمل كل الغايات والبواعث سواء أكانت سياسية أم اقتصادية أم أمنية.

المطلب الثاني

خصائص الهجمات الإلكترونية

تختلف خصائص الهجمات السيبرانية من حقل لآخر. مثلاً حقل تقنية المعلومات يقدم خصائص ذات طابع تقني مختلفة عن النظرة القانونية. وبما أن الهدف من معرفة خصائص الهجمات الإلكترونية هو تهيئة النقاش للانتقال إلى تكييفها في القانون الدولي كظاهرة جديدة، فالحاجة هنا هي تبيان تلك الخصائص التي تميزها عن الهجوم بالأسلحة التقليدية التي استقر تكييفها في قواعد استخدام القوة والدفاع عن النفس ولمعرفة إذا ما كانت القواعد التي تنطبق على هجمات التقليدية يمكن أن تنطبق

---

[1] قرار مجلس الأمن الذي يحث الدول الأعضاء على العمل بصورة تعاونية لمنع الإرهابيين من حيازة الأسلحة، بما في ذلك من خلال تكنولوجيات المعلومات والاتصالات.
انظر: قرار مجلس الأمن 2370، S/RES/2370 (2 أغسطس 2017). استرجع من (2017)https://undocs.org/ar/s/res/2370
للتعرف على جهود مكتب مكافحة الإرهاب التابع للأمم المتحدة لمواجهة الإرهاب السيبراني انظر "برنامج الأمن الالكتروني": الأمم المتحدة، مكتب مكافحة الإرهاب .(n.d.). أمن الفضاء الإلكتروني. استرجع من https://www.un.org/counterterrorism/ar/cct/programme-projects/cybersecurity

[2] "Frequently Asked Questions on International Law Aspects of Countering Terrorism", United Nations Office on Drugs and Crime (UNODC), (Vienna, 2009). Retrieved from https://www.unodc.org/documents/terrorism/Publications/FAQ/English.pdf

على الهجمات الإلكترونية، ستذكر خصائص الهجمات الإلكترونية التي تميزها عن الهجمات التقليدية[1]. ومن هذه الخصائص يمكن تَعَرُّف قدرات الهجمات الإلكترونية ومدى الضرر الذي يمكن أن تتسبب به. مما يسوغ كل تلك الدعوات المتزايدة لتقنين الهجمات الإلكترونية، فإنه يتبين في الفصل القادم أن ضررها يمكن أن يصل إلى تهديد السلم الدولي.

الفرع الأول: خاصية الفعالية

معنى فعالية الهجمة الإلكترونية القدرة العالية في الوصول إلى الهدف المحدد. تلك القدرة التي تساوي قدرة الأسلحة التقليدية أو حتى أدق منها[2]. فبالرغم من الصفة غير الملموسة بسبب أن الهجمة الإلكترونية تتم عبر الفضاء الإلكتروني، فإنها تتصف بقدرات تدميرية مادية عالية الدقة.

فالقدرات المحتملة للهجمات الإلكترونية على أرض الواقع هائلة. وفي ذلك قال الأمين العام للأمم المتحدة أنطونيو غوتيريش:

"أنا مقتنع تماما أن الحرب القادمة ستبدأ بهجوم إلكتروني ضخم ...لتدمير وشل البنية التحتية الأساسية"[3].

فلو حاولنا تخيل ذلك على أرض الواقع فماذا يمكن لهجمة إلكترونية على محطة توليد كهرباء مثلا أن تفعل؟ علما أن شبكة الكهرباء هي واحدة من أضعف أنظمة البنية التحتية عرضة للهجوم السيبراني؛ لأنها متصلة جزئيا بالإنترنت، ويتم تشغيلها بوساطة القطاع الخاص الذي لا يخضع للمعايير الأمنية

[1] National Research Council. (2009). *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*. (W. A. Owens, K. W. Dam, & H. S. Lin, Eds.) (Illustrated ed.), p. 80. Washington, DC: National Academies Press, https://doi.org/10.17226/12651

[2] Garrie, D. B. (2012). Cyber Warfare, What Are The Rules? *Journal of Law and Cyber Warfare* , *1*(1), 1–7. Retrieved from https://www.jstor.org/stable/26441232
Straub, J. (2019). A cyberattack could wreak destruction comparable to a nuclear weapon. *The Conversation*. Retrieved from https://theconversation.com/a-cyberattack-could-wreak-destruction-comparable-to-a-nuclear-weapon-112173

[3] Khalip, A. (2018, February 19). U.N. chief urges global rules for cyber warfare. Retrieved from https://www.reuters.com/article/us-un-guterres-cyber/u-n-chief-urges-global-rules-for-cyber-warfare-idUSKCN1G31Q4

الحكومية وإن هجمة على مولد كهرباء ذات مستوى عال من التعقيد يمكن أن تغلق المحطة لعدة أشهر.[1]

لهجمة إلكترونية على المولدات الكهربائية القدرة على التسبب بشلل في البلد المستهدف. فيصعب التنقل لغرق الشوارع في الظلام، ولتعطل المطارات والقطارات. لن يستطيع الأفراد سحب أموالهم من المصارف لتعطل أجهزة الصراف الآلي في جميع أنحاء البلاد، أو حتى القيام بعملية الشراء من المتاجر لتعطل صناديق الحساب. حتى المستشفيات ستكون مشلولة، ستغلق شركات الشحن، مصافي النفط، والمصانع. لن يتمكن الناس من معرفة ما يجري بسبب انقطاع وسائل التواصل الإعلامي وستسود حالة من الذعر التي تسبب بها هجوم إلكتروني على أجهزة محطة توليد الكهرباء تساوي حالة الذعر التي ستعم لو كانت بغطاء من القصف الجوي.

وفي المجال الجوي تظهر دقة الهجمات السيبرانية عبر التلاعب برادارات الملاحة الجوية وعندئذ فإنه يمكن أن تتسبب الهجمة السيبرانية بإسقاط الطائرات من الجو. وفقا للطرق التقليدية فإن استهداف طائرة معينة لإسقاطها يحتاج إلى ملاحقة ومناورات جوية. فاليوم عملية قرصنة تخضع الطائرة تحت سيطرة وتوجيه الجهة المعتدية. السبب أن اتصالات الملاحة الجوية تتم عن طريق الحاسوب، بل عملية الملاحة نفسها محوسبة[2]. كذلك سجلت حالات قرصنة على السيارات وصلت إلى حد الإطفاء الكامل لمحرك السيارة على الطريق[3] فبسبب تحول السيارات للرفاهية التكنلوجية وارتباطها بالإنترنت أصبحت تحت خطر القرصنة وتلاعب القراصنة. كل ذلك يبين الدقة العالية في الوصول إلى هدف محدد دون الحاجة لإصابة ما حوله.

---

[1] Olivier, M. (2012). Cyber Warfare: The Frontline of 21st Century Conflict. *LBJ Journal of Public Affairs*, *20*, 23–42 [p. 23-25]. Retrieved from https://repositories.lib.utexas.edu/handle/2152/17903

[2] Stokel-Walker, C. (2021, September 28). Planes can be remotely controlled by hackers. Retrieved from https://cybernews.com/security/planes-can-be-remotely-controlled-by-hackers/
Murphy, M. (2017, November 13). Boeing 757 controls HACKED remotely while on the runway, officials reveal. *The Sun*. Retrieved from https://www.thesun.co.uk/tech/4901413/boeing-757-controls-hacked-remotely-while-on-the-runway-officials-reveal/

[3] Applegate, S. D. (2013). *The Dawn of Kinetic Cyber*. In K. Podins, J. Stinissen, & M. Maybaum (Eds.). Presented at the 5th International Conference on Cyber Conflict, Tallinn, Estonia, p. 5-6. Retrieved from https://ccdcoe.org/uploads/2018/10/10_d2r1s4_applegate.pdf

ولا تقف قدرة الهجمات الإلكترونية عند ذلك الحد، بل تتخطاه، فقد وصلت إلى مرافق غاية في الحساسية كمحطات الطاقة النووية. فالتحكم في المفاعل النووي يتم عن طريق برامج حاسوب خاصة تتحكم في سير معدل الانشطار النووي بنمط منتظم ومستديم، فالخلل في تلك البرامج يؤدي إلى عدم السيطرة على معدل التفاعل النووي وبالتالي انصهار المفاعل النووي. هذه الحقيقة لم يغفل عنها القراصنة فالدول التي تملك مفاعلات نووية أكثر تعرضاً لهجمات إلكترونية هادفةَ الإخلال بعمل المفاعلات[1]. ونذكر ما حدث في إيران عام 2010 عندما عطل فايروس ستاكسنت عمل الحواسيب في محطة الطاقة النووية؛ مما سبب سلسة من الانفجارات في المفاعلات.

يقاس على ذلك كل الصناعات الحساسة والتي لا بد أن تعتمد في أحد مراحلها على برامج الحاسوب، ففي قطاع البتروكيماويات أنابيب النفط والغاز تواجه خطر الانفجار[2] إذا ما تم التلاعب بالبرامج التي تحرك المضخات، وفي مجال صناعة الأسلحة يمكن أن تؤدي القرصنة الإلكترونية إلى عطب في الأسلحة المصممة التي تعتمد صناعتها على برامج محوسبة، وهكذا في قطاعات مقاولات البنية التحتية، أو المقاولات العسكرية، أو قطاع العلوم، أو التكنلوجيا... إلخ[3].

ليس الدقة في الوصول للهدف فقط ما تجنيه الهجمات السيبرانية، بل الفرصة في انتقاء نوع الضرر المطلوب. فإذا كانت الأمثلة المذكورة تحمل هدفاً تخريبياً فهناك خيار التعطيل فقط، كأن يتم تعطيل شبكة القطارات في البلاد، أو تعطيل عمل المواقع الرسمية، وأخيرا هناك خيار التجسس وجمع المعلومات سواء أفي المجال الصناعي كسرقة التصميمات وبراءات الاختراع أم في المجال السياسي كالتجسس على البريد الإلكتروني لصناع القرار السياسي أوقادة الأحزاب لمعرفة المزاج العام. فالهدف الذي تقدمه الهجمة يتنوع بين تخريب أو تعطيل أو تجسس.

هذا وأهم من الدقة في الوصول إلى الهدف واختيار نوع الضرر هو اتساع نطاق القابلية للاستهداف. ولا ريب أن ذلك نتيجة طبيعية لهذا العصر الرقمي الذي يعتمد على الحوسبة في كل شيء، فلا تعمل

---

[1] Kesler, B. (2011). The Vulnerability of Nuclear Facilities to Cyber Attack. *Strategic Insights*, *10*(1), 15–25. Retrieved from https://core.ac.uk/download/pdf/36718376.pdf

[2] Stergiopoulos, G., Gritzalis, D. A., & Limnaios, E. (2020). Cyber-Attacks on the Oil & Gas Sector: A Survey on Incident Assessment and Attack Patterns. *IEEE Access*, *8*, 128440–128475. https://doi.org/10.1109/access.2020.3007960

[3] إيهاب، خليفة. (2020). هجمات حرجة: الاستهداف السيبراني للأقمار الصناعية والمنشآت النووية *اتجاهات الأحداث* - مركز *المستقبل للأبحاث والدراسات المتقدمة*. استرجع من https://platform.almanhal.com/Details/Article/241951

أي مؤسسة خاصة أو حكومية دون أن تعتمد في بياناتها على الحاسوب معرضة بذلك نفسها للخطر، ولا صناعة في هذا الوقت إلا كان للآلات التي تعمل عن طريق الحاسوب أثر فيها. حتى الحروب أصبح الإنترنت آلة رئيسة في إدارتها فالاتصالات العسكرية تتم إلكترونيا، والطائرات بدون طيار يتم التحكم بها إلكترونيا، والصواريخ توجه إلكترونيا[1]. كل ذلك أوجد حاجة قوية إلى الاتصال الدائم بالشبكة العنكبوتية أي بمعنى آخر البقاء الدائم بدائرة الاستهداف.

وبالرغم من البرامج المخصصة للحماية من الهجمات الإلكترونية فإنه من المستحيل (حتى يومنا هذا) أن يكون الشخص أو المؤسسة المتصلة بالإنترنت (أي الموجودة في دائرة الاستهداف) بمأمن تام من خطر التعرض للهجمات السيبرانية[2]. فالأمن الكامل غير موجود في نطاق الفضاء السيبراني، فإما العودة إلى التعامل الورقي، أو قبول الخطر الإلكتروني المتربص في كل عملية يدخل فيها الحاسوب.

الفرع الثاني: خاصية تدني التكلفة

تتسم العمليات السيبرانية بتدني التكلفة. فيكفي أن يتوافر جهاز كومبيوتر متصل بالإنترنت مدعوما ببعض البرامج الخاصة لتنفيذ هجمة إلكترونية على دولة ما، فبالإضافة إلى تدني تكلفة تلك الأدوات فهي متوافرة على نطاق واسع ومنتشرة بما لا يمكن السيطرة عليه[3].

تدني تكلفة العمليات السيبرانية مقارنه بفعاليتها المرتفعة يجعلها مغرية جدا للدول، خصوصا إذا ما قورنت بارتفاع تكلفة الإنفاق العسكري الذي يلتهم ما يقدر بـ 5–10% من الدخل القومي للدول[4]. فلا جَرَمَ أن الدخول في الحروب التقليدية يستنزف ميزانيات الدول واقتصادها بين تدريب القوات وتسليحهم وتوفير معدات الحرب. كل ذلك غير وارد في المجال السيبراني الذي يتخطى ساحة المعركة والمواجهات

---

[1] للمزيد عن استخدام الانترنت في القطاع العسكري، انظر:
Cameron, L. (2022, May 24). IoT Meets the Military. Retrieved from https://www.computer.org/publications/tech-news/research/internet-of-military-battlefield-things-iomt-iobt

[2] Lauterbach, A. (2017, April 10). Cyber-security: Full Prevention is not possible. Retrieved from https://www.internationalairportreview.com/article/75245/cyber-security/

[3] Schreier, F. (2014, May). *On Cyberwarfare: DCAF Horizon 2015 Working Paper No. 7*, p. 31. The Geneva Centre for the Democratic Control of Armed Forces (DCAF). Retrieved from https://www.dcaf.ch/sites/default/files/publications/documents/OnCyberwarfare-Schreier.pdf

[4] البنك الدولي. (n.d.). الإنفاق العسكري (% من إجمالي الناتج المحلي) - معهد ستوكهولم الدولي لبحوث السلام، الكتاب السنوي: الأسلحة، ونزع السلاح، والأمن الدولي. استرجع من https://data.albankaldawli.org/indicator/MS.MIL.XPND.GD.ZS

المباشرة، لذلك قرار الدخول في حرب إلكترونيا غير مقتصر على الدول الغنية، بل إن أفقر الدول تستطيع إطلاق عملياتها في الفضاء السيبراني.

ليس رخص المعدات فقط، بل وفرتها. فليس هناك حاجة لجيوش جرارة لتحقيق الغلبة إلكترونيا فبضعة خبراء في القرصنة مع أجهزة حاسوب قادرين على إصابة أهداف دقيقة أكثر من الهجمات التقليدية. جيش الناتو الإلكتروني مثلا يتكون من 200 خبير فقط[1] بينما قوات الناتو العسكرية تصل إلى عشرات الآلاف؛ لذلك مما يدخل في انخفاض التكلفة هو انخفاض التكلفة البشرية من ناحية منفذ العملية السيبرانية. وأما من ناحية ضحايا الهجمات، فإنه حتى الآن يتم الحديث نظرياً عن إمكانات الهجمات السيبرانية في حصد أرواح المدنيين، لكن واقعياً يبدو أن خسائر الهجمات السيبرانية تصب بشكل أساسي على الأضرار الاقتصادية دون البشرية فحتى اليوم لم يمت شخص واحد بسبب هجوم إلكتروني[2] بالرغم من إمكان ذلك من الناحية النظرية، لكن قد يكون لخاصية الفعالية فضل في طبيعة الخسائر غير القاتلة وخلافاً للعشوائية أو الأخطاء في الاستهداف في الأسلحة التقليدية فإن الهجمات السيبرانية أدق في إصابة الشبكة أو الجهاز المطلوب وبالتالي تجنب الأضرار البشرية.

تجدر الإشارة بهذا الخصوص أن العمليات السيبرانية ليست منخفضة التكلفة فحسب، بل من الممكن تحصيل الأموال من خلالها سواء أكان بطريق غير مباشر كعمليات التجسس ذي الأهداف الاقتصادية، أم بطريق مباشر كسرقة الأموال من البنوك الوطنية. كوريا الشمالية مثلا لديها أبرع طاقم لسرقة البنوك إلكترونيا، فلقد نفذ منذ 2014 وحتى اليوم عمليات قرصنة على أكثر من 100 بنك منتشرة في 30 دولة، وقد نجحوا في الحصول على ما مجموعة 650 مليون دولار[3]. وهناك طرق أخرى لنهب الأموال عبر الهجمات الإلكترونية كالاستيلاء على العملات الرقمية المزورة (البتكوين) حتى أن تقريرا للأمم

---

[1] المرجع السابق – NATO Cyber Defence – NATO

[2] هناك حالة لهجوم سيبراني على سيرفرات مستشفى في المانيا تسبب في عدم القدرة على قبول المرضى مما تسبب بوفاة مريضة كانت في حالة حرجة. مع ذلك يصعب القول انها توفيت بسبب الهجوم السيبراني وحده لأن الهجوم "هجوم الفدية" فإنه يسطر المهاجمون على النظام ويطلبون مبلغا ماليا لإعادته. انظر:

Eddy, M., & Perlroth, N. (2020, September 19). Cyber Attack Suspected in German Woman's Death. Retrieved from https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html

[3] Winn, P. (2018, June 21). How North Korean hackers became the world's greatest bank robbers. Retrieved from https://gpinvestigations.pri.org/how-north-korean-hackers-became-the-worlds-greatest-bank-robbers-492a323732a6

المتحدة يزعم حصول كوريا الشمالية من هجمات على بورصات العملات المشفرة مبلغ 2 بليون دولار تستخدمها في تطوير أسلحة الدمار الشامل.[1]

والغريب في معادلة انخفاض التكلفة في العمليات السيبرانية أن الهجوم قليل التكلفة، بينما جانب الأمن الإلكتروني مكلف جدا[2]. فكل ما ذكر من جانب تدني التكلفة هو في الحقيقة مقصور على الهجمة الإلكترونية، لكن التحصين الإلكتروني يكلف دولة كالولايات المتحدة مثلاً أكثر من 16 بليون دولار سنويا[3]. ولمثل هذا الفارق أسبابه المنطقية فجانب الهجوم يكفيه شخص واحد، ملم بالجوانب الفنية وحاسوب وشبكة إنترنت، لكن جهة الدفاع التي لا تعلم من أين يمكن أن تأتيها الهجمة؟ تحتاج لتوظيف فرق فنية خاصة بالبحث عن الثغرات في الأنظمة. وذلك مما حمل بعض الشركات الخاصة كأبل وسامسونج أن تعرض مكافآت تصل إلى ملايين الدولارات على الجمهور لمن يستطيع أن يأتيهم بثغرة. فإذا تم فعلا اكتشاف ثغرات فهناك فرق أخرى مدربة وغاية في التخصص؛ لتطوير البرامج وسد تلك الثغرات[4].

الفرع الثالث: خاصية السرعة[5]

عامل السرعة يتكون من شقين: أولهما: هو الوقت من بداية إطلاقها وحتى الوصول إلى الهدف المطلوب، والثاني هو الوقت المتطلب لصد تلك الهجمة. فكلما كانت الهجمة الإلكترونية متطورة قل الوقت الأول وزاد الوقت الثاني. فالسرعة عامل مهم جدا؛ لأن العملية السيبرانية كلها بمثابة السباق

---

[1] Nichols, M. (2019, August 6). North Korea took $2 billion in cyberattacks to fund weapons program: U.N. report. Retrieved from https://www.reuters.com/article/us-northkorea-cyber-un/north-korea-took-2-billion-in-cyberattacks-to-fund-weapons-program-u-n-report-idUSKCN1UV1ZX

[2] Swinhoe, D. (2020, May 1). How much does it cost to launch a cyberattack? Retrieved from https://www.csoonline.com/article/3340049/how-much-does-it-cost-to-launch-a-cyberattack.html

[3] Statista Research Department. (2022, July 7). U.S. government: proposed cyber security spending in FY 2017–2021. Retrieved from https://www.statista.com/statistics/675399/us-government-spending-cyber-security/

[4] Winder, D. (2020, May 6). Microsoft Offers $100,000 If You Can Hack This Linux Operating System. Retrieved from https://www.forbes.com/sites/daveywinder/2020/05/06/microsoft-offers-100000-if-you-can-hack-this-linux-operating-system/?sh=4bc19fa819e4

انظر أيضا:

Koetsier, J. (2022, July 8). Apple Offers $2M To Hackers Who Can Break Its New Lockdown Mode. Retrieved from https://www.forbes.com/sites/johnkoetsier/2022/07/07/apple-offers-2m-to-hackers-who-can-break-its-new-lockdown-mode/?sh=ad2ac1a3e591

[5] المرجع السابق – Cyber War – Clarke, R. A., & Knake, R. – ص31

بين فريقين أولهما يحاول الدخول إلى أنظمة المعلومات والسيطرة عليها، والثاني يحاول إحباط الهجمة مدافعا. إلا أن ذلك ليس الحال دائما فقد يستغرق اكتشاف الاختراق الإلكتروني أشهرا، خصوصا إذا كان ذا طابع غير تخريبي كالهادف للتجسس. فوفقا لتقرير شركة CrowdStrike للأمن الإلكتروني للعام 2019: أصبحت الهجمات (الروسية) تتم في أقل من 19 دقيقة[1]، ونظرا لسرعة الهجمات وتطورها فإن وقت صدها وإحباط أثرها يجب ألا يتعدى 18 دقيقة و49، ثانية وإلا نجحت الهجمة في إحداث الضرر المطلوب.[2]

خاصية السرعة تلك ذات قيمية عالية في الهجمات الإلكترونية بين الدول. فقبل ظهور الأسلحة النووية كان الوقت اللازم لتكوين جيش بحجم مناسب ونقله إلى دولة العدو يستغرق مدة تمتد من أيام إلى أشهر، تلك المدة الزمنية تعطي وقتا كافيا لاكتشاف مؤشرات تحرك الطرف المهاجم، والاستعداد للرد عليها، أما في الهجمة الإلكترونية فعنصر السرعة عادة ما يقترن بعنصر المفاجأة، والمباغتة بدون سابق إنذار مما يسبب حالة من الشلل، وصعوبة في تحديد نوع الهجمة، وصعوبة في تقييم الضرر الواقع وبالتالي التأخر في تداركه، وبمعنى آخر المباغتة سبب لنجاح الهجمة وتحقيق المطلوب منها.

بالإضافة إلى ذلك فمن المنطقي القول إن الهجمة الإلكترونية أسرع من الأسلحة التقليدية في تحقيق الهدف، فإذا كان إسقاط طائرة بدون طيار ممكناً بهجوم سيبراني أو هجوم إلكتروني فإن خيار العملية السيبرانية أسرع من القيام بمناورات جوية لإسقاطها أو توجيه الأسلحة عليها من الأرض.

المشكلة أن هناك فجوة بين سرعة تطور الهجمات وتأخر تطور المنظومات الدفاعية. فالأمن الإلكتروني لا يستطيع مواكبة سرعة تطور الفيروسات والبرامج الضارة[3]. فالهجمات السيبرانية تتطور باستمرار؛ لوجود ذلك النوع من العقول البشرية الذي يهوى التحدي ويشعر بالرضا في تحقيق اختراق المنظومات الدفاعية. ومن المتنبئ ونحن على أعتاب عصر الذكاء الاصطناعي أن تزاد الهجمات الإلكترونية

---

[1] وفقا للتقرير المذكور تستغرق الهجمة الروسية حوالي 19 دقيقة والهجمة القادمة من كوريا الشمالية 2-3 ساعات والهجمة القادمة من إيران حوالي خمس ساعات أما الهجمات الفردية فإنها تستغرق حوالي التسع ونص ساعة

[2] CrowdStrike. (2019). *The Global Threat Report: Adversary Tradecraft and the Importance of Speed*. Retrieved from https://www.africacybersecurityconference.com/document/CrowdStrike_GTR_2019.pdf

[3] Williamson, D. (2021, June 1). Cyberattacks are getting faster as prevention stays slow. Retrieved from https://www.americanbanker.com/payments/opinion/cyberattacks-are-getting-faster-as-prevention-stays-slow

سرعة وفعالية.[1] فإذا كان اليوم قبل القيام بالهجوم الإلكتروني يحتاج إلى الفنيين المهرة؛ لإجراء البحوث ومراقبة كيفية تفاعل الهدف مع المنصات الرقمية، في عالم الغد، سيتمكن الذكاء الاصطناعي الهجومي من الوصول لنفس المستوى من النتائج في جزء صغير من الوقت، وستكون الضوابط الأمنية التقليدية عاجزة أمام هذا التهديد الجديد – اكتشاف هذا النشاط الاختراقي –[2]. ولذلك تتزايد التحذيرات والدعوات لتأسيس شبكة عالمية يتم من خلالها الإبلاغ عن الهجمات حيث تتضافر جهود خبراء فنيين من كل الدول لتحقيق نوع من الرقابة والسيطرة على الأفعال الضارة في الفضاء الإلكتروني.

الفرع الرابع: خاصية كونها عابرة للحدود

المسافات الجغرافية والحدود السياسية موضوع غير ذي صلة هنا بالهجمات الإلكترونية فالأهداف يمكنها القيام بالضربة من الطرف الآخر في العالم خلال ثوان معدودة؛[3] لأن المؤسسات التي يعتمد عليها الناس في حياتهم كالبنوك أو محطات توليد الكهرباء أو رادارات الملاحة الجوية كلها قابلة للاختراق من أي مكان في العالم[4].

ما توفره الهجمات الإلكترونية من (القدرة على الهجوم من موقعك) يغير الكثير من المفاهيم المتعلقة بانتشار القوات، والتجهيزات العسكرية، والنفقات والخسائر البشرية، وحتى في سمات الشخص المهاجم فتخطي ساحة المعركة يغير تماما من الشخص خلف الهجمة ذلك الذي لن يضطر للمواجهة الفعلية لكنه سيضرب من خلف الشاشات، ليس مهما أن تتوافر فيه القوة والانضباط والتدريب العسكري، كل ما هو مطلوب أن يمتلك بعض المهارات الرقمية، لذلك نجد أن بعض الهجمات كان وراءها مراهقون لم يبلغوا السن القانونية[5].

---

[1] Dixon, W., & Eagan, N. (2019, June). *3 ways AI will change the nature of cyber-attacks*. Article presented at the Annual Meeting of the New Champions 2019, Dalian, People's Republic of China. Retrieved from https://www.weforum.org/agenda/2019/06/ai-is-powering-a-new-generation-of-cyberattack-its-also-our-best-defence/

[2] المرجع السابق

[3] المرجع السابق – Roscini, M. – Cyber Operations and the Use of Force – ص2

[4] المرجع السابق

[5] Svabensky, V., & Vykopal, J. (2018). Gathering Insights from Teenagers' Hacking Experience with Authentic Cybersecurity Tools. *2018 IEEE Frontiers in Education Conference (FIE)*, 1–4. https://doi.org/10.1109/fie.2018.8658840

ولما كانت الهجمة الإلكترونية لا تحترم الحدود التقليدية (البر والبحر والجو) طفق الموضوع ضبابياً؛ بسبب طبيعة الإنترنت، فهو شيء كالفضاء لا بداية ولا نهاية له، أو كمستعمرات البكتيريا تنتشر متوسعةً دون أن توقفها حدود، يصعب السيطرة عليها. وأمام تلك الخاصية تظهر الكثير من التعقيدات القانونية. لأن الحديث هنا عن بعد رابع للحروب غير مادي لا تنطبق عليه قواعد المكان والزمان. ولهذا السبب عندما شرع الفقه القانوني الدولي في تناول الفعل الإلكتروني الضار كان الجدال الأول هل ينطبق القانون الدولي القائم على هذه الظاهرة الجديدة؟ أم ان تلك الطبيعة الخاصة بالإنترنت تحتاج إلى قوانين أخرى تتناسب معه. وسنعرض كيف استقرت آراء الفقهاء على أن مبادئ القانون الدولي الحالي قادرة على معالجة موضوع الهجمات الإلكترونية؟ وقد بدأت مرحلة جديدة من النقاش بسؤال كيف تنطبق قواعد القانون الدولي على الفضاء السيبراني؟

تجدر الإشارة هنا إلى أن بعض الدول تسعى إلى تحقيق ما يعرف بـ "سيادة الإنترنت"، وهو محاولة لفصل شبكة الأنترنت في إقليمها عن بقية العالم. ويحدث ذلك إما بإنشاء شبة إنترنت خاصة بالبلاد بأن تملك البلاد سيرفرات (خوادم انترنت) خاصة بها ومنفصله عن السيرفرات العالمية ومن ثم إمكان السيطرة على محتوى الشبكة، كما هو حاصل في الصين، وكما هو التوجه الروسي[1]. وإما عن طريق محاولة السيطرة على تدفق المعلومات للبلاد عن طريق منع مواقع معينة باسم السيادة الوطنية. كأن يكون كل من يملك عنوان انترنت IP صيني مثلا لا يمكنه الدخول على مواقع كفيس بوك ويوتيوب واستخدام محرك البحث قوقل. سواء كان ذلك دائماً أم مؤقتاً. تلك العملية من "رسم حدود على شبكة الإنترنت ثم محاولة التحكم بمحتوى تلك الحدود"[2] تتعارض مع طبيعته التي تقرب الحضارات بعضها من بعض، وتتنافى مع الاستخدام الأمثل الذي يضع العالم أمام المستخدم ليتصفحه بسعة، لذلك تلقى فكرة سيادة الانترنت معارضة من جماعات الضغط وتقابل بشعارات مضادة "كحرية الإنترنت"[3].

---

[1] صحيفة العرب" (2019, February 16). .الإنترنت ذات السيادة": موسكو تغلق حدودها الرقمية. استرجع من https://alarab.app/الإنترنت-ذات-السيادة-موسكو-تغلق-حدودها-الرقمية

[2] Budnitsky, S., & Jia, L. (2018). Branding Internet sovereignty: Digital media and the Chinese–Russian cyberalliance. *European Journal of Cultural Studies*, *21*(5), 594–613. https://doi.org/10.1177/1367549417751151

Jiang, M. (2010). Authoritarian Informationalism: China's Approach to Internet Sovereignty. *SAIS Review of International Affairs*, *30*(2), 71–89. https://doi.org/10.1353/sais.2010.0006

[3] Kolton, M. (2017). Interpreting China's Pursuit of Cyber Sovereignty and its Views on Cyber Deterrence. *The Cyber Defense Review*, *2*(1), 119–145. Retrieved from https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/1588940/interpreting-chinas-pursuit-of-cyber-sovereignty-and-its-views-on-cyber-deterre/

الفرع الخامس: خاصية كونها مجهولة المصدر[1]

يمكن القول: إن أهم ما يميز الهجمة الإلكترونية هو كونها مجهولة المصدر. فالهجمة الإلكترونية – دائما – فعل يحيط به الغموض من أين أتت ومن يقف خلفها؟ وإن نجحت التحقيقات بنسبة فعل الهجوم إلى دولة معينة فإن النتائج دائما ما تقابل بالتشكيك والإنكار.

غياب الشفافية معضلة من المعضلات من الناحية القانونية لسببين: أولهما: أنه يؤدي إلى عدم التقيد بأي قانون، فإن نجح القانون الدولي في وضع بعض القواعد والإجراءات في مجال مكافحة العدوان السيبراني فما الذي سيدفع الدول للالتزام إذا كانت تستطيع ارتكاب مخالفات في العتمة حيث لا مخاطرة بسمعتها واعتبارها معتدية وخارج إطار الشرعية الدولية؟ والثاني: عدم المقدرة على فرض العقوبات، فكيف تفرض العقوبات على فاعل غير معلوم أو حتى مشكوك بقيامة بالجريمة؟[2] يمكن القول إنَّ الهوية المجهولة تشجع على التمادي في الفعل الضار الإلكتروني لثلاثة أسباب:

أولا: صعوبة معرفة الفاعل إلا باستخدام تقنيات عالية[3]

فالأمر يتطلب إجراء تحقيقات دقيقة ليس من الجانب الفني فقط، بل والسياسي كذلك؛ وذلك لدراسة الدوافع التي تقف خلفها، وبالتالي ترجيح نسبتها إلى جهة محددة. والحقيقة أنه ليس بالأمر السهل على الحكومات أن تمتلك فنيين ملمين بكل ما يمكن أن يستجد في أنواع الهجمات الإلكترونية فهي تتجدد وتتطور باستمرار في حين أن شركات الأمن السيبراني التابعة للقطاع الخاص أصبحت تنافس الوكالات الحكومية، لتطويرها قدرات تمكنها من إسناد نشاط سيبراني ضار إلى الدول أو الجهات التي قد ترعاها الدولة حتى. على سبيل المثال، في الولايات المتحدة كانت الحكومة الفدرالية فقط قادرة على ربط الأعمال العدائية بالجهات الفاعلة الأجنبية، لكن في قضية التجسس الصيني الأمريكي كان القطاع الخاص هو الذي كشف عن هذا الاختراق للرأي العام وليس الحكومة، كما استخدمت الحكومة قدرات

---

[1] Rosenzweig, P. (2013). Chapter 6: The Fundamental Problem of Identity. In *Cyber Warfare: How Conflicts in Cyberspace Are Challenging America and Changing the World* (Illustrated, pp. 75–84). Praeger. Retrieved from http://publisher.abc-clio.com/A3670E

[2] Lotrionte, C., Corcoran, T., Lewis, J., & Rosenzweig, P. (2018, April). *Bringing Order to Chaos: The Development of Nation-State Cyber-Norms*. Presentation presented at the RSA Conference, San Francisco, California. Retrieved from https://youtu.be/nMJLjy2Y1T4

[3] الجمل، حازم (2015). الحماية الجنائية للأمن الإلكتروني (الطبعة الأولى). المنصورة، جمهورية مصر: دار الفكر والقانون للنشر والتوزيع، ص 78-81.

القطاع الخاص لإسناد عدد من الهجمات إلى فاعليها بعد أن عجز عن ذلك القطاع الحكومي[1]. وسيتم الحديث باستفاضة عن دور القطاع الخاص في تعقب الهجمات الدولية ومزايا وعيوب هذا الاتجاه المتنامي[2].

ثانيا: سهولة محو آثار الهجمة وإخفاء أدلة ارتكابها

طمس مَعالم الجريمة في العالم الرقمي أسهل بكثير مما هو عليه في العالم المادي. فالمهاجمون يملكون خيارات متعددة ومتجدده باستمرار لاختيار كيفية إخفاء آثارهم الرقمية التي تقود لمواقعهم وهوياتهم، فمثلا من الممارسات الشائعة التي يستخدمها المهاجمون للتهرب من الاكتشاف اقتحام أجهزة الكمبيوتر غير الآمنة واستخدام تلك الأجهزة "المختطفة" كوكلاء يمكنهم من خلالها شن وتوجيه الهجمات في جميع أنحاء العالم[3].

المشكلة الأصعب في العثور على هذه الهجمات هي عندما يتم التلاعب بعنوان المصدر. فكل ما يتم إرساله عبر الإنترنت يحتوي على معلومات حول مصدر البيانات ووجهتها. ويمكن للمهاجمين تغيير حقل المصدر [تزييفه] لجعله يبدو كما لو أنه آتٍ من مكان آخر.[4]

ثالثا: انعدم وجود رقابة دولية

بالرغم من أن مثل هذه الهجمات تمثل مشكلة دولية فإنه لا يوجد تعاون دولي للتصدي لها. فالهجمات الإلكترونية تعد من الجرائم المنظمة أي أنها جريمة عابرة للحدود، تحتاج إلى تعاون دولي؛ للتصدي لها فليس هناك دولة واحدة قادرة على مراقبة الفضاء السيبراني والتصدي لتعقيد عملية الإسناد والمعاقبة

---

[1] Eichensehr, K. (2020, July 24). Cyberattack Attribution and International Law. Retrieved from https://www.justsecurity.org/71640/cyberattack-attribution-and-international-law/

[2] Menn, J. (2022, April 7). Leading security companies Mandiant and CrowdStrike vow to collaborate. *The Washington Post*. Retrieved from https://www.washingtonpost.com/technology/2022/04/07/mandiant-crowdstrike-cybersecurity-cooperation/

[3] Greenemeier, L. (2011, June 11). Seeking Address: Why Cyber Attacks Are So Difficult to Trace Back to Hackers. *Scientific American*. Retrieved from https://www.scientificamerican.com/article/tracking-cyber-hackers/

[4] هناك أيضا طريقة أخرى حيث يستخدم المهاجمون عبر الإنترنت الفيروسات والديدان والبرامج الضارة الأخرى للسيطرة على خوادم الإنترنت أو حتى أجهزة الكمبيوتر الشخصية، وإنشاء شبكة من أجهزة الكمبيوتر "الزومبي" (وتسمى أيضًا الروبوتات) التي يمكنهم التحكم بها لشن هجماتهم. ونتيجة لذلك، قد يبدو أن الهجوم يأتي من خادم أو كمبيوتر معين، لكن هذا لا يعني أن الهجوم نشأ في ذلك الجهاز. انظر: المرجع السابق.

على الفعل الضار إن لم يكن ذلك بسبب التعقيدات الفنية فبسبب التعقيدات القانونية في هذه الظاهرة الجديدة نسبيا. وعلى الرغم من بعض الدعوات لإنشاء منظمة أو وكالة محايدة تعمل بشفافية لمراقبة الفضاء السيبراني وتكون رادعا فإن تلك الدعوات لم تلق استجابة إلى الآن[1]. وحتى ينشأ ذلك الكيان الدولي الجاد فالوضع مازال مشجعا للتمادي.

وتجدر الإشارة إلى أن التعقب يكون أكثر نجاحا وأكثر مصداقية إذا تبنته شركة خاصة بالأمن الإلكتروني، لأن نتائج التحقيقات الحكومية تقابل بالتشكيك في مصداقيتها كونها اتهامات مبنية على مواقف سياسية وعادة ما تكون دون تقديم أدلة للجمهور.[2]

الفرع السادس: خاصية قلب موازين القوة[3]

الفضاء الإلكتروني يعطي الدول الصغيرة وغير الفاعلة في الساحة الدولية مقداراً كبيراً من القوة غير متناسب مع حجمها في الحقيقة، تلك القوة تكمن في القدرة على التسبب بأذى هائل للدول الكبرى.

وضع القوة هنا مختلف تماما عنها في الحروب التقليدية، فمقاييس القوة المعروفة كالقوة الاقتصادية، والتفوق العسكري، والمساحة الجغرافية، وعدد السكان، كل ذلك يتلاشى في الحروب الرقمية، فالقوي فيها هو الذي يستطيع أن ينفذ عمليات سيبرانية متطورة تخترق أنظمة الطرف الآخر. لذلك تتسابق الدول في الاهتمام بهذا الجانب، الجانب الهجومي وليس التحصين الأمني فقط[4]. هنا مجال جديد للتسابق أو أداة أخرى للدول لتستخدمها بعضها ضد البعض.

---

[1] انظر على سبيل المثال:
Mueller, M., Grindal, K., Kuerbis, B., & Badiei, F. (2019). Cyber Attribution: Can a New Institution Achieve Transnational Credibility? *The Cyber Defense Review*, *4*(1), 107–122. Retrieved from https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/1830029/cyber-attribution-can-a-new-institution-achieve-transnational-credibility/

[2] ديفيس الثاني، جون إس، وآخرون (2017). تهديدات مجهولة المصدر: نحو مسائلة قانونية في الفضاء الإلكتروني. سانتا مونيكا، كاليفورنيا: مؤسسة RAND. ص29. استرجع من https://www.rand.org/content/dam/rand/pubs/research_reports/RR2000/RR2081/RAND_RR2081z1.arabic.pdf

[3] Olivier, M. – المرجع السابق

[4] ينظر تقرير الحملات الإلكترونية الهجومية ذات القوة العظمى: تجارب في الإستراتيجية
Austin, G., Tay, K. L., & Sharma, M. (2022, February). *Great-Power Offensive Cyber Campaigns: Experiments in Strategy*. International Institute for Strategic Studies (IISS). Retrieved from https://www.iiss.org/blogs/research-paper/2022/02/great-power-offensive-cyber-campaigns

في عام 2016 صوت مجلس حقوق الإنسان على قرار يقضي بأن الأنترنت حق من حقوق الانسان الأساسية،[1] هذا يبين أن هناك قناعة أو توجهاً عالمياً أن الإنترنت لم يعد رفاهية، بل أصبح حقاً وضرورة للحياة في القرن الحادي والعشرين. لذلك أصبحت الدول تهتم بتوفيره على نطاق واسع، فهو يعد أحد مؤشرات تقدم البلد. هذا وإن خطورة التحديات الأمنية التي تفرضها الحرب الإلكترونية مرتبطة بمدى اعتماد الدولة على تكنولوجيا المعلومات والاتصالات الحديثة.

لقد وصل الاعتماد على الإنترنت في بعض البلدان أن معظم الخدمات الحكومية تقدم إلكترونيا، حتى التصويت في الانتخابات يتم إلكترونيا من المنزل، كذلك عمليات التبادل التجاري والأعمال المصرفية تتم بالأنترنت[2]. وليس الاعتماد على الإنترنت في المعاملات وحدها هو ما يحدد مدى رقمية البلد، بل المقياس هو إمكان الوصول إلى الإنترنت فكلما كان الإنترنت أكثر إتاحة كانت البلد أكثر تقدما، وهنا يكون الحديث عن قلب موازين القوة فكلما تقدم البلد أكثر يصبح أضعف لأنه أكثر عرضة للخطر.

وفي الوقت الحالي تجتاح ثقافة الواي فاي المجاني العالم بحيث لا يتوفر الأنترنت المجاني داخل المرافق العامة والخاصة فحسب، بل حتى في شوارع المدن، والحدائق، والشواطئ، فمدن كنيويورك وغيرها يجد الشخص نفسه متصلا بالشبكة على الدوام[3]. هذه البلدان التي تنافس نحو التحول للرقمية تتمتع بمزيد من نقاط الضعف أمام البلدان ذات الاعتماد المحدود على تكنولوجيا المعلومات.

إذن فالهجمات السيبرانية وضعها غريب، فتلك البلدان المتطورة هي الحلقة الأضعف والأكثر قابلية للهجوم، وعلى العكس من ذلك فالبلدان غير المتطورة والتي لا تعتمد على التكنلوجيا ونظم المعلومات بسعة هي الأقوى والأقل عرضة للخطر. وإن حدثت بالفعل هجمات سيبرانية على كلا النوعين من البلدان سيكون تأثيرها على الأولى مدمرا، لأنها تعتمد على التكنلوجيا ونظم المعلومات في كل شيء

---

[1] قرار الجمعية العامة رقم 13/32، *تعزيز وحماية حقوق الإنسان على الإنترنت والتمتع بها*، A / HRC/RES/32/13 (1 يوليو 2016). استرجع من https://undocs.org/A/HRC/RES/32/13

[2] في ذلك يمكن الاطلاع على تقرير التنافسية الرقمية لعام 2021، انظر:

International Institute for Management Development (IMD). (n.d.). World Competitiveness Rankings - IMD. Retrieved from https://wwwcontent.imd.org/centers/world-competitiveness-center/rankings/world-competitiveness/

[3] Strachan, D. (2014, February 14). 9 Cities With The Best Free Wifi. Retrieved from https://www.businessinsider.com/9-cities-with-the-best-free-wifi-2014-2?international=true&r=US&IR=T

فكل شيء سيتوقف. أما النوع الثاني الذي لا يعتمد على التكنلوجيا فلن يتغير عليه شيء. وهذا هو المقصود بقلب موازين القوة[1].

المطلب الثالث

صور الهجمات الإلكترونية على الصعيد الدولي

الهجمات الإلكترونية كثيرة وهي في ازدياد عدداً وتعقيداً. وعامة يمكن عرض أنواع الهجمات الإلكترونية من خلال تقسيمها إلى مجموعتين. أولا: طريقة العمل، وفيه ينظر إلى الطريقة التي تعمل بها الهجمة أو التكنيك الذي يتم استخدامه؛ لإحداث الاختراق في الفضاء السيبراني أو من خلاله. ثانيا: الضرر، وفيه ينظر إلى الآثار التي أنتجها الهجوم السيبراني، ويتم فرزها في مجموعات بحسب آثارها.

الفرع الأول: طريقة العمل معياراً للتفرقة بين صور الهجمات

طريقة العمل قائمة على دراسة خط سير الهجمات من انطلاقها حتى وصولها لمبتغاها، وهي من اهتمامات علم الحاسوب، حيث يطغى الجانب التقني في البحث عن الثغرات التي يتمكن من خلالها المهاجمون من إحداث الاختراق.

يقدم علم الحاسوب قائمة طويلة من طرق عمل الهجمات الإلكترونية، وهي في ازدياد حيث تظهر سنويا طرق جديدة يتحدى بها القراصنة أنظمة الأمن السيبراني[2]. من أشهر الهجمات الإلكترونية الرئيسة من ناحية طريقة عملها:

---

[1] United Nations, UN News, *Developing countries most vulnerable to cyberattacks*, 9 December 2011. Retrieved from https://news.un.org/en/story/2011/12/397922-developing-countries-most-vulnerable-cyberattacks-un

[2] لأبرز الهجمات لعام 2020، انظر:

Whitney, L. (2020, March 2). Most common cyberattacks we'll see in 2020, and how to defend against them. Retrieved from https://www.zdnet.com/article/most-common-cyberattacks-well-see-in-2020-and-how-to-defend-against-them/

هجمات البرامج الضارة (Malware):

وهي أسلوب البرامج الضارة التي تخدع المستخدم لتثبيت برامج ضارة على نظامه، وتتسبب في تلفه[1]. هذه الطريقة الرئيسة يتفرع منها الكثير من الطرق الفرعية مثل برامج الفدية التي تمنع من الوصول إلى الملفات أو البيانات ما لم يتم دفع الفدية المطلوبة. وكذلك برامج التجسس هي أمثلة على البرامج الضارة. وبرامج الفيروسات التي تسبب تلف الأنظمة.[2]

هجمات رفض الخدمة (DDoS Attacks):

هجوم رفض الخدمة يطغى على موارد النظام أي الخدمات التي يوفرها برنامج أو موقع معين بحيث لا يمكنه الاستجابة لطلبات الخدمة[3]. على عكس الهجمات المصممة لتمكين المهاجم من الوصول، فإن هجوم رفض الخدمة لا يوفر فوائد مباشرة للمهاجمين. إلا إذا كان المهاجم راضيا عن مجرد التسبب برفض الخدمة للطرف الآخر. ومع ذلك، إذا كان المصدر المهاجم ينتمي إلى منافس تجاري مثلا فقد تكون فائدة تعطيل الخدمة حقيقية وكافية[4].

هجمات التَصَيُد (Phishing Attacks):

أسلوب الهجمات يركز على استخدام الحيل والخداع، وبه يتم خداع الأشخاص لمشاركة المعلومات الشخصية أو المالية من خلال التظاهر كشخص موثوق به مثل الشرطة أو البنك الذي تتعامل معه[5]. عادة ما تحدث هجمات التصيد الاحتيالي عبر البريد الإلكتروني متنكّرة في شكل مستند أو رابط مرفق. يمكن أن تحدث أيضًا عن طريق الهاتف (المعروف باسم vishing) أو الرسائل النصية أو وسائل التواصل الاجتماعي[6].

---

[1] The Law Society. (2019, August 28). How to identify a cyber attack. Retrieved from https://www.lawsociety.org.uk/topics/cybersecurity/how-to-identify-a-cyber-attack

[2] المرجع السابق

[3] Melnick, J. (2018, May 15). Top 10 Most Common Types of Cyber Attacks. Retrieved from https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/

[4] للمزيد عن أثار هجمات رفض الخدمة انظر:
Kohout, J. (2017, February 7). TeskaLabs Blog · How DDoS Attacks Can Sink Your Business. Retrieved from https://teskalabs.com/blog/how-ddos-can-sink-your-business

[5] المرجع السابق – The Law Society

[6] المرجع السابق

هجوم الرجل في المنتصف (Men in The Middle Attacks) :

طريقة ينجح بها المهاجمون في إقحام أنفسهم سرا بين المستخدم وخدمة الويب التي يحاول الوصول إليها. على سبيل المثال شبكات Wi-Fi من أكثر مداخل هجمات منتصف الطريق من خلال قيام المهاجم بتصميم نافذة تسجيل توهم المستخدم أن الشبكة المتوافرة تخص فندقاً، أو مجمعاً تجارياً، وبمجرد أن تتم عملية التسجيل يحصل المهاجم على دخول لجهاز المستخدم.[1]

هجمات اختراق كلمة المرور (Password Attacks):

في الهجمات المستندة إلى كلمة المرور، يستخدم المخترقون برامج للوصول إلى الحسابات الآمنة، تلك البرامج تكشف كلمة المرور التي حيث يمكنها اختبار آلاف كلمات المرور المحتملة. هذه البرامج ناجحة لأن القواعد المطلوبة في كلمة المرور جعلت المهمة أسهل لبرامج الكشف[2]. فغالبًا ما يتبع المستخدمون الإرشادات التي تخبرهم بان كلمات المرور الخاصة بهم تحتاج إلى احتواء حرف كبير وعلامة ترقيم. والنتيجة هي أنه من الأسهل على البرامج الخاصة والمتسللين تخمين كلمة المرور واقتحام الحسابات[3].

هذه بعض أنواع الهجمات الإلكترونية القائمة على النمط الذي تتم به، وهي رئيسة جدا، فإنه تتفرع عن كل واحدة منها عدة هجمات فرعية. الملاحظ على أنواع هذه الهجمات أنها تصف طريقة العمل، بغض النظر عن الهدف الذي ستصل إليه. فواحدة من الهجمات المذكورة يمكنها أن تتسبب بنتائج مختلفة.

مثلا هجمات البرامج الضارة Malware المذكورة سابقاً يمكن أن تكون نتيجتها تلفاً في الجهاز الذي تمت مهاجمته، أو تأتي الهجمة على شكل برنامج تجسسي يكشف المعلومات الموجودة في الجهاز المستهدف، كذلك من الممكن أن تأتي على شكل برامج الفدية التي تمنع من الوصول إلى الملفات أو البيانات ما لم تدفع فدية[4]. هذه ثلاث نتائج مختلفة تتحقق بأسلوب واحد من الهجمات وهو البرامج

---

[1] Yasar, K., & Cobb, M. (2022, April 28). man-in-the-middle attack (MitM). Retrieved from https://www.techtarget.com/iotagenda/definition/man-in-the-middle-attack-MitM

[2] وهو مرجع مستخدم أعلاه، انظر: المرجع السابق – Melnick, J.

[3] المرجع السابق

[4] المرجع السابق – The Law Society

الضارة. كذلك الأمر في بقية أنواع الهجمات، فكل واحدة منها يمكنها أن تحقق أهدافاً مختلفة. والعكس صحيح؛ فأحياناً للوصول إلى نتيجة معينة يستخدم المهاجم أحياناً أكثر من نمط في الهجوم.

فإذا ما أردنا تناول تلك الهجمات الإلكترونية من منظور قانوني فلن تكون الطريقة التي تتم بها الهجمة أمراً ذا اعتبار؛ لأنها لا تدل على حجم الضرر، فمعرفة القاعدة القانونية الواجبة التطبيق تستلزم معرفة الحق المعتدى عليه. أي علامَ وقعت الهجمة؟ وما الضرر الذي أحدثته؟ أما نمط الهجمات المذكورة أعلاه فهي بمنزلة الأداة التي تمت بها الجريمة وهي لا تؤثر في تجريم الفعل.

الفرع الثاني: أثر الهجمات معياراً للتفرقة بين صور الهجمات

تقسيم الهجمات من ناحية أثرها أحد الجوانب المهمة التي يُعتمد عليها في تكييفها القانوني، فالأثر متصل بالحق المعتدى عليه وبالضرر الذي يتحمل مسؤوليته من أحدثه، وهذه مداخل مهمة لتطبيق قواعد القانون الدولي على المجال السيبراني.

وقد يتداخل أثر الهجمة مع هدفها، فمن الممكن أن تقسم الهجمات بحسب الهدف الذي توجه صوبه، كأن تكون هجمات معلوماتية، أو هجمات مالية، أو هجمات تخريبية، لكن الحقيقة أن اعتماد الأثر الذي حدث بالفعل معياراً للتفريق أدق من الهدف الذي قد لا يحدث؛ لأنه من الممكن أن تبدأ الهجمة وتحبط دون أن تصل إلى هدفها الكامل، والعكس صحيح، فإنه يمكن أن تتعدى الهجمة هدفها، وتسبب ضرراً أكثر مما كان مقصوداً. لذلك فالأهداف أو النوايا الأولية لا تصلح معياراً للتفرقة بين أنواع الهجمات بين الدول.

ففي القانون الدولي لا يعتد – عملياً – بمحاولات الاختراق الفاشلة، التي تتم على مدار الساعة دون توقف[1]. فمسألة المحاسبة على محاولات الهجمات، أو الشروع في الهجمات تفوق قدرة القانون الدولي؛ نظراً لطبيعة الفضاء السيبراني غير القابل للضبط، وانتفاء جهة رقابية عليا تتحكم به، ناهيك عن مجهولية الفاعل. فالقانون الدولي يتعامل مع ما حدث بالفعل وهو الأثر.

[1] يصل عدد الهجمات الإلكترونية ــ سواء أكانت بين افراد عاديين أم دول ــ إلى ملايين الهجمات يومياً، ويمكن رصد الهجمات الإلكترونية التي تحدث الآن مباشرة من خلال الاطلاع على موقع:
Check Point. (n.d.). Live Cyber Threat Map. Retrieved from https://threatmap.checkpoint.com/

هناك عدة تقسيمات تعتمد على آثار الهجمات الإلكترونية. فبإعادة النظر إلى حوادث الهجمات الإلكترونية الدولية التي تم التفصيل فيها أعلاه، يتبين أن الهجمات إما أن تقع على **معلومات** مثل أن يتم سرقتها أو إخفاؤها، أو أن تقع على **معدات** كأن يتضرر جهاز الحاسوب من الفيروس ولا يعمل، أو تتضرر المولدات الكهربائية أو أجهزة الطرد المركزي في محطات الطاقة النووية.

بيد أن هناك تقسيماً آخر لأثر الهجمات، أكثر تفصيلاً، وفيه يقسم الضرر إلى ثلاثة أنواع من الخسائر: أولها: خسارة السرية ومثالها الهجمات التجسسية، وثانيها: خسارة السلامة وتحدث عندما تتمكن الهجمة من اتلاف الجهاز في ابسط الحالات او أحداث إصابة أو وفاة في اشد الحالات، وثالثها: خسارة التوفر ومثالها ان تتمكن الهجمة السيبرانية من ايقاف الخدمات الإلكترونية وسببت شللاً في مختلف قطاعات الدولة[1].

أما التقسيم الذي سيتم اعتماده هنا هو تقسيم ثلاثي يقسم آثار الهجمات الإلكترونية من ناحية جسامتها ثلاث مجموعات: الهجمات الحركية، والهجمات التعطيلية، وهجمات الدخول غير المشروع. هذا التقسيم الذي يفرق بين درجة جسامة أثر الهجمات ذو أهمية عالية عند تقرير كيفية الرد على الهجمات أو الجانب الدفاعي في الهجمات السيبرانية بين الدول. وسنتناول كل فئة بشيء من التفصيل.

أولا: الصورة الأولى: الهجمات الحركية (Kinetic):

المقصود بالهجمات الإلكترونية الحركية هو أن يؤدي الهجوم الإلكتروني إلى ضرر مادي Physical على الأشخاص أو الأشياء وهي أكثر صور الهجمات تطرفا وفيها يتجاوز تهديد القرصنة الإزعاج الإلكتروني، والربح الإجرامي، وحتى التجسس، ليشمل نوعًا من اضطراب العالم المادي الذي لم يكن ممكناً تحقيقه إلا بالهجمات العسكرية.

[1] Finnemore, M., & Hollis, D. B. (2016). Constructing Norms for Global Cybersecurity. *American Journal of International Law*, *110*(3), 425–479 [p. 443]. https://doi.org/10.1017/s0002930000016894

انظر أيضا:

Forcepoint. (2021, May 5). What is the CIA Triad? Retrieved from https://www.forcepoint.com/cyber-edu/cia-triad

تستهدف الهجمات السيبرانية الحركية أنظمة تسمى بالأنظمة الفيزيائية السيبرانية Cyber Physical Systems وهو النظام الذي يجمع بين الآلة والحاسوب حيث يتحكم الحاسوب بعمل الآلة[1]. وكلما كان المهاجم يجمع بين خبرة نظم المعلومات مع خبرة فيزيائية بالآلة التي سيوجه الهجوم نحوها ستتضاعف فرص نجاح الهجمة.

صممت "الأنظمة الفيزيائية السيبرانية" بحيث يكون لها تأثير حركي على أرض الواقع. وهي تستخدم في المراقبة والتحكم في العمليات الفيزيائية من خلال استخدام أجهزة الكمبيوتر وتقنية المعلومات. ومجرد حقيقة وجودها وترابطها مع الفضاء الإلكتروني يعني ضمناً أنها يمكن أن تكون محل التلاعب بها واستخدامها لأغراض غير تلك التي كانت مخصصة لها[2].

تدخل "الأنظمة الفيزيائية السيبرانية" في مجموعة واسعة من قطاعات الصناعة كأنظمة السيارات المتقدمة، والإلكترونيات الطيران، كما أن توجد على هذه الأنظمة في الأجهزة الطبية، ومراقبة الحركة والسلامة، والمراقبة والتحكم البيئي، والتحكم في البنية التحتية الحيوية (الطاقة الكهربائية والموارد المائية والاتصالات)[3]. ولما أصبحت الأنظمة السيبرانية الفيزيائية تدخل في معظم القطاعات، طفق تهديد الهجمات السيبرانية الحركية يهدد معظم جوانب الحياة.

يقسم الخبراء الهجمات الإلكترونية الحركية إلى نوعين: أولهما: هو النوع التجريبي الذي يحدث في المختبرات والمرافق البحثية في جميع أنحاء العالم، ويحاول المختصون استباق المهاجمين السيبرانيين، واكتشاف الثغرات، وحجم الأضرار التي يمكن أن تسببها[4]. إن الاهتمام بمثل هذه التجارب مهم للدول؛ لتكون أكثر استعدادا للأخطار السيبرانية. ومن أمثلة ما توصلت إليه تجارب الهجمات الإلكترونية الحركية، تعطيل فرامل السيارات في المجال الصناعي، والتلاعب بضربات القلب في القطاع الصحي، وتخريب مولدات الكهرباء في البنية التحتية، وغيرها.

أما النوع الثاني فهو الهجمات السيبرانية الحركية الواقعية التي حدثت على أرض الواقع. وهي كثيرة على مستوى الأفراد والمؤسسات، أما على الصعيد الدولي فما زالت الحوادث تعتبر محدودة، وهي اقل

---

[1] المرجع السابق – Applegate, S. D. – ص2

[2] المرجع السابق – ص3

[3] National Institute of Standards and Technology (NIST). (2022, May 13). IoT Devices and Infrastructures Group. Retrieved from https://www.nist.gov/ctl/smart-connected-systems-division/iot-devices-and-infrastructures-group

المرجع السابق – Applegate, S. D. – ص4-5

[4] المرجع السابق – Applegate, S. D. – ص3-6

صورة من الصور الثلاث حدوثاً. ولا يزال أظهر مثال على ذلك هو هجوم Stuxnet 2010 في محطة الطاقة النووية في إيران.

لكن هناك هجمات حركية دولية أخرى، بعضها حصل قبل هجمات إيران 2010، لكنها لم تأخذ نفس الزخم لقلة المعلومات المصرحة عنها. مثل انفجار خط أنابيب النفط الذي يمتد عبر ثلاث دول (تركيا–جورجيا–أذربيجان) عام 2008. الانفجار الكبير حصل في شرق تركيا، وخلف أضرار بيئية و واقتصادية وجسدية برجال الإطفاء كان سببه في الأساس هجوم سيبراني. حيث تمكن المهاجمين السيبرانيين من اختراق نظام التحكم في خط الأنابيب والتلاعب بالصمامات لزيادة الضغط داخل الأنبوب من ناحية وقمع الإنذارات التي كانت ستنبه المشغلين إلى حدوث خطأ من الناحية الأخرى[1]. بعد بضع سنوات، أصبح الهجوم ينسب إلى روسيا[2].

وقد أظهر التقرير السنوي للمكتب الاتحادي الألماني لأمن المعلومات (BSI) في عام 2014، تعرض مصنع للصلب في ألمانيا لأضرار جسيمة، بعد أن اخترق المتسللون شبكة الكمبيوتر بالمصنع عبر بريد إلكتروني، من نوع التصيد، استهدف أفراداً معينين في الشركة لخداعهم لفتح الرسائل التي بحثت عن أسماء تسجيل الدخول، وكلمات المرور، واستولت عليها، مما مكن المهاجمين من الوصول إلى أنظمة التحكم في المصنع. أدى الهجوم إلى الإضرار بالنظام بحيث لا يمكن إغلاق فرن الانفجار[3]. ولا يوجد دليل نهائي ينسب الهجوم لدولة أو منظمة أو حتى أشخاص معينين[4].

---

[1] Lee, R. M., Assante, M., & Conway, T. (2014, November). *ICS CP/PE (Cyber-to-Physical or Process Effects) case study paper – Media report of the Baku-Tbilisi-Ceyhan (BTC) pipeline Cyber Attack*. SANS Industrial Control Systems, p. 2. Retrieved from https://www.yumpu.com/en/document/view/36490959/media-report-of-the-btc-pipeline-cyber-attack

[2] Lee, R. M., Assante, M. J., & Conway, T. (2014b, December). *ICS CP/PE (Cyber-to-Physical or Process Effects) case study paper – German Steel Mill Cyber Attack*. SANS Industrial Control Systems, p. 3. Retrieved from https://dokumen.tips/documents/ics-cppe-case-study-2-german-steelworks-facility.html

انظر أيضا:

Kucera, J. (2014, December 11). U.S. Intelligence: Russia Sabotaged BTC Pipeline Ahead Of 2008 Georgia War. Retrieved from https://eurasianet.org/us-intelligence-russia-sabotaged-btc-pipeline-ahead-of-2008-georgia-war

[3] المرجع السابق – Lee, R. M., Assante, M. J., & Conway, T. – German Steel Mill Cyber Attack – ص3

[4] المرجع السابق – ص5

ثانيا: الصورة الثانية: الهجمات التعطيلية (Disruptive):

تحدث الصورة الثانية عندما يؤدي الهجوم الإلكتروني إلى ضرر، لكنه يظل حبيس العالم الإلكتروني فلا يسبب تخريبا ماديا ملموسا على أرض الواقع، لكن يسبب ضررا رقميا يعطل السير الطبيعي للعمليات السيبرانية[1] فالصورة الأولى والثانية يشتركان في وجود ضرر تشعر به الجهة المتعرضة للهجوم، لكن طبيعة الضرر هي التي تختلف؛ فالضرر الأول ينتهي إلى حدوث تحرك في العالم المادي والضرر الثاني يبدأ وينتهي في العالم الرقمي. وهو الصورة التقليدية للهجمات السيبرانية التي تصدر من حاسوب إلى حاسوب.

تتصف الهجمات السيبرانية غير الحركية أنها تتسبب بضرر ذي طبيعة إلكترونية سواء أكان ذلك الضرر واقعا على الحواسيب أم على الشبكات. فالضرر على الحواسيب مثاله فقدان التحكم في جهاز الحاسوب، أو عدم إمكان الوصول إلى بعض الملفات، أو مسح بعض الملفات، أو تدمير البرمجة فلا يعمل. أما الضرر على الشبكات فمثاله منع الوصول إلى الخدمات الإلكترونية أو تشويه المواقع الحكومية بدعاية معادية لنظام الدولة. فإذا وجد الضرر فليست الطريقة أو نوع الهجمات الإلكترونية المستخدمة مهمة، فيستوي أن تستخدم هجمات منع الخدمة DDoS، أو هجمات الرجل في منتصف الطريق على الشبكات، أو هجمات البرامج الضارة كالفيروسات على الحواسيب الحكومية.

كما لا يشترط لتمام الهجوم التعطيلي تحكم المهاجم في النظام أو حتى الدخول إليه، فبعض الفيروسات تدمر برمجة الحاسوب دون أن يكون هناك تواصل، أو سيطرة من المهاجم على الجهاز المستهدف، كتلك البرامج الضارة التي تنتقل بالمعدات كأقراص التخزين ونحوها. فأي تلاعب مباشر أو غير مباشر بهدف إحداث – تغيير في المنطق الذي تستخدمه أجهزة الكمبيوتر أو بروتوكولات الشبكة[2]– يشعر به المستخدم الأصلي هو هجوم إلكتروني تعطيلي.

---

[1] King, A., & Gallagher, M. (2020, March). *CSC Report*. Cyberspace Solarium Commission (CSC), p. 132. Retrieved from https://cybersolarium.org/wp-content/uploads/2022/05/CSC-Final-Report.pdf

[2] Subramaniam, T. K., & Deepa, B. (2015). A Review Towards DDoS Prevention and Detection Methodology. *International Journal of Computational Science and Information Technology*, *3*(1/2/3), 1–9. https://doi.org/10.5121/ijcsity.2015.3301

إن الهجمات الإلكترونية غير الحركية أو التعطيلية طريقة غير مكلفة للدول؛ لتعطيل عمل جهات معادية[1]. يمكن أن تكون مدمرة في نواح كثيرة إذا ما تم شنها على مستوى الدولة القومية، وإن لم ينتج عنها تدمير مادي، وحَسْبُ ذلك تعطيل البنية التحتية، والخسائر الاقتصادية.

ثالثا: الصورة الثالثة: هجمات الدخول غير المصرح به (Unauthorized Access):

تحدث هذه الصورة عندما لا يؤدي الهجوم الإلكتروني أي ضرر سواء أفي العالم المادي أم الرقمي، فكل ما يحدث هو دخول غير مشروع على بيانات الدولة. أي بعبارة أخرى الهجمات التجسسية. التجسس وجمع المعلومات الاستخبارية جزء من جهاز الأمن في كل الدول عبر التاريخ[2] وقد تحولت عمليات المراقبة والتجسس التي ترعاها الدول من الطرق التقليدية إلى الأنشطة السيبرانية التي تتسابق فيها شركات التكنولوجيا الفائقة.

يهدف الهجوم السيبراني التجسسي إلى استخراج البيانات الاستخباراتية وجمعها، ويحدث عند اختراق غير قانوني لأجهزة الكمبيوتر، أو شبكات الكمبيوتر لدولة معينة؛ من أجل جمع أي بيانات حساسة أو سرية عادة ما يتم إخفاؤها وحمايتها من عامة الناس[3]. ويفرق البعض بين التجسس الإلكتروني والمراقبة الإلكترونية، فالتجسس يكشف معلومات مخزنه أما المراقبة فهي اعتراض الاتصال بين طرفين أو أكثر[4]. والمراقبة كالتجسس يمكن أن تعطي نظرة ثاقبة لما يخطط له الطرف الآخر.

تتصف الهجمات التجسسية السيبرانية بأمرين: أولهما: الدخول غير المصرح على بيانات دولة وثانيهما ألا يكون ضرر الهجمات فوريا بحيث تلمسه الجهة الأخرى في أثناء الهجمة. فالهجمات يجب أن تتناسب مع طبيعة التجسس الصامتة، ولا تفاجئ الطرف الآخر بالعدوان، فمتى ما حصل ضرر مباشر، كأن يفقد الطرف الآخر القدرة على التحكم في نظام الحاسوب، أو يفقد المعلومات، أو تتعذر القدرة على الوصول إليها كان ذلك من النوع الثاني من الهجمات (التعطيلي). لكن من الطبيعي أن

---

[1] المرجع السابق – Cyber Operations and the Use of Force – Roscini, M. – ص55-63

[2] عثمان، محمد. (يناير، 2015). دور القانون الدولي في مواجهة التجسس الدبلوماسي (رسالة دكتوراه). جامعة الشرق الأوسط، ص-23-28. استرجع من https://meu.edu.jo/libraryTheses/5879f716c1346_1.pdf

[3] Harry, C. (2015, July). *A Framework for Categorizing Disruptive Cyber Activity and Assessing Its Impact*. University of Maryland, p. 4-5. Retrieved from https://spp.umd.edu/research-impact/publications/framework-categorizing-disruptive-cyber-activity-and-assessing-its

[4] Banks, W. C. (2017). Cyber Espionage and Electronic Surveillance: Beyond the Media Coverage. *Emory Law Journal*, *66*(3), 513–525, [p. 514]. Retrieved from https://scholarlycommons.law.emory.edu/elj/vol66/iss3/3/

يكون هناك ضرر غير حال فالتجسس الدولي مدفوع بمصلحة قومية، ومن الطبيعي أن تغليب مصلحة الدولة المهاجمة يترتب عليه ضرر للدولة المتلقية للهجوم.

من الممكن أن تكون الهجمة التجسسية قصيرة، كالعملية التي تهدف إلى الحصول على معلومة محددة، فتبدأ وتنتهي في جلسة واحدة، أو تكون عبارة عن عدة هجمات مستمرة لمدة زمنية طويلة، تصل إلى سنوات مثل سلسة هجمات Titan Rain الصينية على الولايات المتحدة التي استمرت 2003-2005.[1]

القصد من التجسس قد يكون مشروعا إذا تم بدوافع أمنية مثل توقع الهجمات الإرهابية، لكنه في كثير من الأحيان غير ضروري، أو غير مشروع كأن يهدف تعرف خطط السياسة الخارجية للدول الأخرى، واكتساب ميزة في مفاوضات العلاقات الخارجية[2]. كذلك، فإن قدرًا كبيرًا من التجسس السيبراني ينطوي على مسائل اقتصادية، تمتد في بعض الأحيان لتشمل سرقة الملكية الفكرية[3]، ويتم القيام بها من قبل الدول أو وكلائها؛ لضمان الميزة الاقتصادية النسبية في المفاوضات التجارية أو الصفقات الأخرى أو على وجه الخصوص الشركات.[4]

الحقيقة أن موقف القانون الدولي ضعيف تجاه التجسس عامة، فليس هناك اتفاق بين الدول على عدم شرعيته في زمن السلم. وإن محاولة تطبيق القواعد العامة – مثل سيادة الدولة، وعدم التدخل في الشأن الداخلي للدول – لا يكفي لردعه. قد يعزى ذلك إلى كون أغلب الدول ترتكبه وتستفيد منه لذلك لم تتلاق الإرادات على التعاون للتخلص منه. ولذلك فمن غير المستغرب أن تكون 94% من الهجمات الإلكترونية بين الدول ذات دوافع تجسسية[5].

ورغم ذلك فمن المهم – في مجال الهجمات الإلكترونية الدولية – أن يعالج التجسس بوصفه صورة مستقلة إن لم يكن من أجل تجريمه فمن أجل تحديد الرد المتناسب معه قانوناً. فإن كان التجسس يشترك مع الهجمات الإلكترونية الحركية والتعطيلية – في مشكلات انتهاك السيادة وصعوبة معرفة

---

[1] للمزيد عن التجسس الصيني الأمريكي، انظر:
Council on Foreign Relations. (2005, August). Connect the Dots on State-Sponsored Cyber Incidents - Titan Rain. Retrieved from https://www.cfr.org/cyber-operations/titan-rain

[2] المرجع السابق – Banks, W. C. – ص514

[3] المرجع السابق – ص514-516

[4] المرجع السابق

[5] Swedish Security and Defense Industry Association (SOFF). (2018, March). *State sponsored cyber attacks*, p. 10. Retrieved from https://soff.se/wp-content/uploads/2018/03/Cybersecurity_statsunderst%C3%B6dda-akt%C3%B6rer.pdf

الفاعل، لكنه يختلف في إمكانية قياس الضرر الذي سببه – فمعرفة كمية المعلومات المخترقة، ومعرفة متى بدأت الهجمات؟ وهل انتهت بالفعل؟ أصعب في هذا النوع. التجسس يوجد وضعا جديدا يتمثل في عدم القدرة على تحديد الضرر خلافا للهجمات الحركية والتعطيلية لذلك فالرد عليه سيختلف أيضا.

بالرغم من انتشار هذا التقسيم للصور التي تأتي عليها الهجمات الإلكترونية فإن هناك بعض العيوب أهمها: أن هناك آثارا لا تدخل في هذا التصنيف كالأضرار المالية، فالصور الثلاث غالبا ما تحتوي في مرحلة ما على خسارة مالية. هذا وليس من السهل دائما الفصل بين الضرر الحركي والتعطيلي والتجسسي. فلو حصلت هجمات تعطيلية على سوق البورصة ستكون من حاسوب إلى حاسوب، لكن نتائجها الأكبر ستكون على أرض الواقع متمثلة في خسارة ملايين الدولارات! فهل تعد هذه هجمات تعطيلية أم انها حركية؟ غالبا ما يترافق الضرر الحركي مع التعطيلي، أو التعطيلي مع التجسسي فالمهاجم الذي يتمكن من السيطرة على جهاز غالبا لن يفوت فرصة أخذ ما فيه من معلومات.

كذلك ليس صحيحا أن جسامة الضرر تعتمد على قدرة الهجمة السيبرانية على حدوث تحريك فيزيائي على أرض الواقع. الهجمات السيبرانية على إستونيا 2007 التي سببت شللا على نطاق الدولة كانت أضرارها الاقتصادية والاجتماعية أكبر من الهجوم على تركيا عام 2014 والذي سبب انفجارا في أنبوب النفط، وربما تكلف الهجمات التجسسية وسرقة براءات الاختراع أكثر من الهجمات الصورتين السابقتين.

إن نتائج الهجمات أو مدى الضرر الذي يمكن أن تسببه تتحكم فيها عوامل أخرى مثل ماهي الأدوات المستخدمة في الهجوم؟ أهي برامج ضارة معتادة؟ أم هي أدوات تخصصية فائقة التكنلوجيا مصممة خصيصاً لتلك المهمة؟ هذا فضلا عن مدى خبرة الشخص المهاجم.

المبحث الثاني

أهم نماذج الهجمات الإلكترونية في العلاقات الدولية

لا مناص من الوقوف على أهم الحوادث المسجلة في الهجمات الإلكترونية بين الدول، ليس ذلك من باب النسق التاريخي وحسب، بل لاستكمال الصورة وتوضيح أن الموضوع صدد البحث مشكلة حقيقية تسبب معاناة حقيقية حدثت، ومازالت تحدث، وستستمر في الحدوث والاستفحال. كذلك يجب المرور

بهذه الحوادث لإثبات أن عصر الحروب الرقمية قد بدأ بالفعل فالحديث عن التصدي القانوني لهذه الظاهرة يجب أن ينتقل من مناقشة الفرضيات إلى الحوادث التي حصلت بالفعل، لذلك حوادث الهجمات الإلكترونية الدولية المطروحة هنا سيتم الاستشهاد بها في مواقع الفصول اللاحقة من هذا البحث.

تُعد دودة موريس التي أطلقت عبر الانترنت في عام 1988 شرارة الفعل السيبراني الضار؛ فإنها أول من أثر على أداء البنية التحتية للأنترنت[1]. اليوم، زادت الهجمات الإلكترونية وتنوعت وأصبح من الصعب معالجتها جميعها بالتحليل! لكن هناك حوادث من الهجمات الإلكترونية الأولية التي صدمت العالم، والتي شدت الانتباه إلى خطورة هذه الظاهرة ودفعت لأخذ المشكلة على محمل الجد. ولتجنب التكرار سيقتصر هذا المبحث على خمسة أمثلة دون غيرها؛ لثلاثة أسباب. أولها: أهميتها، فالهجمات الإلكترونية تحدث يومياً على مدار الساعة! لكن الأمثلة التي ستذكر أخذت حيزا كبيرا من اهتمام العالم. والسبب الثاني كونها انتهت أي أنها قضايا مكتملة، تم التحقيق فيها، والوصول إلى مصدرها فلن تتغير نتائجها غالباً. وأما السبب الثالث فهو أن كل واحد من هذه الأمثلة أتى بوضع جديد أي صورة مختلفة عن صور العدوان الإلكتروني على الدول.

الفرع الأول

الهجوم الإلكتروني على إستونيا

لا بد أن يذكر اسم إستونيا في أي محاولة لعرض الهجمات السيبرانية الدولية، فهي أول دولة تتعرض لهجوم سيبراني على نطاق واسع، وهي أول من وقع عليها نقل فكرة الحرب الإلكترونية من الخيال العلمي إلى الواقع، لم يكن الأمر مفاجأ لإستونيا فقط، بل للعالم أجمع!!

[1] في العام 1988 أطلق أول الفيروسات التي انتشرت عبر الإنترنت وهو ما يعرف بدودة مورييس Morris worm . وقد أطلق الفايروس إثناء تجربة الهدف منها معرفة عدد مستخدمين الإنترنت، لكن لاحقا تم تغيير البرمجة من مهمة إحصائية إلى مهمة تنسخ نسخ الفايروس نفسه على آلاف أجهزة الحاسوب بطريقة ضارة بعمل الحاسوب. كان ذلك أول برمجة ضارة أثرت على البنية التحتية لشبكة الإنترنت الناشئة آنذاك وكان روبرت موريس صانع الفايروس أول شخص يحاكم بموجب قانون الاحتيال الأمريكي. للمزيد عن دودة موريس ينظر:
Sulek, D., & Moran, N. (2009). What Analogies Can Tell Us About the Future of Cybersecurity. *Cryptology and Information Security Series, Volume 3: The Virtual Battlefield: Perspectives on Cyber Warfare*, 118–131 [p. 118]. Retrieved from http://195.222.11.251/uploads/2018/10/08_SULEK_What-Cyber-Analogies-Can-Tell-Us.pdf

أولا: خلفية الهجوم

المفتاح لفهم سبب الهجمات الإلكترونية التي حصلت هو فهم التراكمات من التوترات الاجتماعية بين الإستونيين والأقلية الإثنية الروسية في إستونيا. تتألف إستونيا من 1.3 مليون نسمة حوالي ربعهم من الروس[1]. في عام 1918، حصل الإستونيون على استقلالهم من روسيا، وفي عام 1940 تم إجبارهم على الانضمام إلى الاتحاد السوفيتي. ومن عام 1940 حتى استعادوا استقلالهم في عام 1991، نظرت إستونيا إلى وجود روسيا كاحتلال غير قانوني. ومن ناحية أخرى، ينظر الروس إلى الإستونيين على أنهم غير ممتنين؛ لأن الروس أنقذوهم من الألمان النازيين[2].

تفاقم التوتر عندما انضمت إستونيا إلى حلف الناتو في 2004، ووصل التوتر بين إستونيا وروسيا إلى نقطة حرجة في يناير 2007، عندما أعلنت الحكومة الإستونية أنها ستنقل نصب تذكاري للحرب العالمية الثانية من وسط العاصمة (تالين) إلى مقبرة عسكرية على مشارف المدينة، والنصب هو تمثال برونزي لجندي روسي خلال الحرب العالمية، هذا الأمر أثار حفيظة القوميين الروس في إستونيا؛ فقد كان التمثال رمزا لوجود القومية الروسية في البلد وكانوا يجتمعون عنده باستمرار. ورداً على ذلك، قام المتمردون من – أصل روسي – في البلاد بأعمال شغب في أسوأ اضطرابات شهدتها إستونيا منذ حرب استقلالها عام 1944. ثم حدثت مظاهرات في روسيا مؤيدة لموقف للإثنية الروسية في إستونيا. لكن الحكومة الإستونية لم تستجب للأقلية الروسية ونقلت التمثال في 26 أبريل لتبدأ بعد ذلك سلسلة من الهجمات الإلكترونية على إستونيا.

ثانيا: الهجمات الإلكترونية

قبل الحديث عن الهجمات الإلكترونية وما سببته من ضرر يجب التنبيه على أمر غاية في الأهمية، وهو أنه في عام 2007 ، كانت إستونيا واحدة من أكثر الدول الرقمية على وجه الأرض كان كل جانب تقريبا من جوانب حكومة إستونيا وتجارتها يعتمد على الإنترنت والفضاء الإلكتروني فجميع الخدمات والمعاملات الحكومية من دفع الضرائب، والتصويت في الانتخابات الوطنية وتقدم الأجانب

[1] Central Intelligence Agency (CIA). (2011). The World Factbook. Retrieved from https://www.cia.gov/the-world-factbook/

[2] Ashmore, W. C. (2009, May). *Impact of Alleged Russian Cyber Attacks* (Monograph). School of Advanced Military Studies, United States Army Command and General Staff College. Retrieved from https://apps.dtic.mil/sti/citations/ADA504991

للحصول على الإقامة كلها كانت تتم عن طريق الإنترنت فمثلا في قطاع الصحة لا تستخدم الأوراق، فالوصفات الطبية للأدوية، أو الاطلاع على نتائج الفحوصات المخبرية كان يتم إلكترونياً، كذلك المعاملات غير الحكومية في قطاعات البنوك والاتصالات جميعها تتم عن طريق الانترنت. [1]

في اليوم التالي لنقل التمثال، تعرضت إستونيا لهجمات إلكترونية واسعة النطاق. ويقسم الخبراء الهجمات مرحلتين: أولاهما دعائية، تتمثل في استخدام المواقع الحكومية لنشر اعتذارات مزيفة صادرة عن مسؤولين إستونيين عن نقل التمثال، والمرحلة الثانية الأكثر تقدما كانت تهدف إلى التخريب والحرمان من الوصول لخدمة الإنترنت[2].

تباينت الهجمات الإلكترونية ضد إستونيا في تطورها فالهجمات الأقل تعقيدا كانت عبارة عن الاختراقات لمواقع الويب والبريد الإلكتروني. استهدفت الهجمات عدداً من المواقع الإلكترونية الحكومية مثل الموقع الخاص برئيس الوزراء، والبرلمان، ومعظم وزارات الحكومة، كما استهدفت أحزابا سياسية في الدولة[3].

أما الهجمات الأكثر تأثيرا فقد كثرت على الأنظمة المصرفية والبنوك، فضلا عن تعطيل أنظمة قنوات التواصل مع الحكومة وخطوط الطوارئ، ومزودي الأخبار من قنوات إعلامية وإذاعية كلها تعرضت للهجوم وتوقفت عن العمل. وكانت الشركات المزودة بخدمات الإنترنت أول المتضررين[4].

طلبت إستونيا المساعدة من دول العالم، وبسبب خطورة الهجمات الإلكترونية، لقيت إستونيا استجابة دولية سريعة. ورغم أنه كان لدى إستونيا بعض الاستعدادات الرسمية للدفاع الإلكتروني فإنها استضافت خبراء أمن الحاسوب من الناتو والاتحاد الأوروبي والولايات المتحدة وإسرائيل وألمانيا وسلوفينيا؛ لتقديم

---

[1] Davis, J. (2007, August 21). Hackers Take Down the Most Wired Country in Europe. *Wired*. Retrieved from https://www.wired.com/2007/08/ff-estonia/

BBC News عربي (27 أكتوبر، 2017) هل تصبح إستونيا أول دولة "رقمية" في العالم. استرجع من https://www.bbc.com/arabic/vert-fut-41771226

[2] Tikk, E., Kaska, K., & Vihul, L. (2010). *International Cyber Incidents: Legal Considerations*. Tallinn, Estonia: Cooperative Cyber Defence Centre of Excellence (CCD COE). Retrieved from https://ccdcoe.org/uploads/2018/10/legalconsiderations_0.pdf

[3] Ottis, R. (2018, October). *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective*. Cooperative Cyber Defence Centre of Excellence (CCD COE), p. 2. Retrieved from https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf

[4] المرجع السابق – ص2-3

المساعدة، فضلا عن هدف تحسين فهمهم "للحرب الإلكترونية[1]." وقال الأمين العام لحلف الناتو: إن الهجمات كانت مسألة أمنية تتعلق بحلف الناتو أجمع وليس إستونيا فقط. وإن القضية "ستبقى على جدول الأعمال السياسي لأوقات طويلة قادمة"[2].

ولقد استمرت موجات الهجمات 3 أسابيع قبل أن يتم احتواؤها بالكامل. وكان الهدف الأساسي هو التخريب والتعطيل. ولم تتسبب الهجمات بحد ذاتها في أي ضرر حركي ملموس، لكنها أسفرت عن خسارة ملايين الدولارات. فقدرت الخسائر التي سببتها هذه المشاغبات الإلكترونية بـ 27 إلى 40[3] مليون دولار للحكومة وغيرها من الصناعات، وقد كان ذلك بسبب تطور البلد واعتمادها التام في المعاملات الحكومية والبنكية وحتى الشركات الخاصة على الأنترنت.

ثالثا: الإسناد الفني

التحقيق الفني توصل إلى أن الهجمات جاءت من عدة أماكن في العالم من ضمنها روسيا[4]. على الرغم من ذلك، أنكرت الحكومة الروسية ذلك، مشيرة إلى أنه على الرغم من إمكانية تتبع الهجمات لروسيا، فإنه لا يمكن نسبتها إلى عملاء الحكومة. وأعطت تفاسير كأن يكون المهاجمون ربما قاموا بتزوير عناوين بروتوكول الإنترنت الروسي الخاصة بالهجوم (أي تلاعب القراصنة بالعنوان لجعله كأنه قادم من روسيا)، أو أن يكون الهجوم من مواطنين روس غيورين، لكنها نفت أي تدخل حكومي رسمي[5]. حتى اليوم مازال تبادل الاتهامات قائما دون إثبات قطعي.

رابعا: النتائج

---

[1] Herzog, S. (2011). Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. *Journal of Strategic Security*, *4*(2), 49–60. https://doi.org/10.5038/1944-0472.4.2.3

[2] Sullivan, C. (2016). The 2014 Sony Hack and the Role of International Law. *Journal of National Security Law and Policy*, *8*(3), 437–468. Retrieved from https://jnslp.com/wp-content/uploads/2017/10/The-2014-Sony-Hack-and-the-Role-of-International-Law_2.pdf

[3] Haataja, S. (2017). The 2007 cyber attacks against Estonia and international law on the use of force: an informational approach. *Law, Innovation and Technology*, *9*(2), 159–189 [p. 161]. https://doi.org/10.1080/17579961.2017.1377914

[4] المرجع السابق – ص161

[5] المرجع السابق – Herzog, S.

انظر أيضا:

The Baltic Times. (2007, May 18). Kremlin denies involvement in cyber attacks on Estonia. Retrieved from https://www.baltictimes.com/news/articles/17908/

النتائج أظهرت قدرات إستونيا على التعامل مع الهجمات الإلكترونية بجودة؛ فقد استطاعت احتواء الموضوع وإيقافه دون أن يكون هناك ضرر على المدى الطويل[1]. فضلا عن أن إستونيا تعافت من الهجمات بنجاح في العالم الرقمي، فإنه بعد تلك الهجمات أصبحت إستونيا الرائدة في مجال السايبر تكنولوجي، مسيطرة على السوق. لكن أيضا من النتائج سوء العلاقات الروسية الاستونية إلى اليوم[2].

أما أكثر الدروس المستفادة من هذا الحدث فهو اقتناع العالم بخطورة الهجمات الإلكترونية؛ فقد أظهرت حادثة إستونيا شدة آثار الهجمات الإلكترونية على المجتمعات المتقدمة، التي تكون غاية في الضعف بسبب تقدمها الرقمي. فأي بلد لديه بنية تحتية لشبكة متطورة بما فيه الكفاية عرضة لهذه الهجمات. وقد تبين كيف أن الهجمات الإلكترونية البدائية تستغرق القليل من الوقت والجهد للتنظيم، في حين أن الدفاع ضدها أصبح أكثر صعوبة وتعقيدا.

بسبب إدراك خطورة الأمر على الدول المتقدمة أنشأ الناتو مركز الامتياز للدفاع السيبراني CCDCOE [3] ومقره (تالين) إستونيا. كما شرع حلف شمال الأطلسي والدول الأعضاء في الاتحاد الأوروبي في مناقشة الاتجاهات الجديدة للأمن السيبراني، والعقوبات المناسبة للدول التي وجدت أنها شاركت في الحرب الرقمية. كذلك أوصى الناتو النظر في تمديد الضمانات الأمنية بموجب المادة 5 من معاهدة حلف شمال الأطلسي إلى عالم الفضاء الإلكتروني، تبنى الناتو سياسات موحدة حول الإنترنت[54].

الفرع الثاني

الهجمات الإلكترونية على جورجيا

---

[1] المرجع السابق – Ashmore, W. C. – ص6

[2] المرجع السابق – Ashmore, W. C. – ص6

[3] CCDCOE هو مركز دفاع إلكتروني معتمد من الناتو يركز على البحث والتدريب والتمارين. إنه يمثل مجتمعًا من 29 دولة يقدم نظرة شاملة لموضوع الدفاع السيبراني في مجالات التكنولوجيا، والاستراتيجية، والعمليات، والقانون. لا تعد مراكز الامتياز المعتمدة من الناتو جزءًا من هيكل قيادة الناتو. يعمل المركز ويمول من قبل الدول الأعضاء فيه حاليًا هم: النمسا وبلجيكا وبلغاريا وكرواتيا والتشيك والدنمارك وإستونيا وفنلندا وفرنسا وألمانيا واليونان والمجر وإيطاليا ولاتفيا وليتوانيا والجبل الأسود وهولندا والنرويج وبولندا والبرتغال ورومانيا وسلوفاكيا وسلوفينيا وإسبانيا والسويد وسويسرا وتركيا والمملكة المتحدة والولايات المتحدة.
CCDCOE - The NATO Cooperative Cyber Defence Centre of Excellence is a multinational and interdisciplinary hub of cyber defence expertise. (n.d.). Retrieved from https://ccdcoe.org/

[4] ملخص عن الهجمات الالكترونية على إستونيا عام 2007، انظر:
Main Page. (2022, July 5). *International cyber law: interactive toolkit*. Retrieved from https://cyberlaw.ccdcoe.org/w/index.php?title=Main_Page&oldid=3465.

[5] المرجع السابق – Herzog, S. – ص55

تتشابه الهجمات على إستونيا وجورجيا في كونهما جمهوريتين سابقتين في الاتحاد السوفييتي، والجهة التي يشتبه في قيامها بالاعتداء هي روسيا. لكن المختلف أن هذه هي المرة الأولى التي يتم فيها الهجوم السيبراني بالتزامن مع معركة برية مسلحة. كما أن الهجمات كانت أكثر تطورا وتعقيدا وتنظيما من تلك التي حدثت في إستونيا[1]، بيد أن ضررها أقل؛ لأن جورجيا غير معتمدة على التعامل الإلكتروني بقدر إستونيا.

أولا: خلفية الهجوم

حصلت جمهورية جورجيا على استقلالها من الاتحاد السوفيتي في عام 1991، وكعادة الدول المستقلة عن الاتحاد السوفييتي، كانت على علاقة مضطربة مع روسيا بسبب رغبتها في ترسيخ هويتها الأوروبية الجديدة عامة، فجورجيا واحدة من أوائل الجمهوريات السوفيتية السابقة التي حاولت الانضمام إلى حلف شمال الأطلسي[2]. لكن بشكل خاص كانت العلاقات الجورجية الروسية أكثر اضطرابا؛ بسبب النزاع المستمر بين الدولتين حول السيطرة على منطقتين تتمتعان بحكم شبة ذاتي هما أوسيتا الجنوبية وأبخازيا. تحول هذا الخلاف إلى نزاع مسلح في أغسطس 2008 عندما اجتاحت القوات الجورجية أوسيتا الجنوبية وأبخازيا، وتدخلت روسيا لطرد القوات الجورجية[3]. وسبقت الهجمات البرية التي قامت بها روسيا هجمات عبر الإنترنت واسعة النطاق ضد الحكومة الجورجية وبنيتها التحتية المدنية.

ثانيا: الهجوم الإلكتروني

بدأت الهجمات السيبرانية قبل ثلاثة أسابيع على الأقل من العمليات العسكرية التي قامت بها روسيا[4]، إلا أن تطور الهجمات السيبرانية نما في وقت متزامن مع الهجوم الحركي الذي قامت به روسيا.

---

[1] للمزيد حول المقارنة بين إستونيا وجورجيا، انظر:
Kozlowski, A. (2014). Comparative analysis of cyberattacks on Estonia, Georgia and Kyrgyzstan. *European Scientific Journal (ESJ)*, *3*, 237–245. Retrieved from https://eujournal.org/index.php/esj/article/view/2941

[2] North Atlantic Treaty Organization (NATO). (2022, July 14). Relations with Georgia. Retrieved from https://www.nato.int/cps/en/natohq/topics_38988.htm

[3] Independent International Fact-Finding Mission on the Conflict in Georgia (IIFFMCG). (2009, September). *Report of the Independent International Fact-Finding Mission on the Conflict in Georgia* (Volume II), p. 4. Retrieved from https://www.mpil.de/files/pdf4/IIFFMCG_Volume_II1.pdf

[4] Gazula, M. B. (2017, May). *Cyber Warfare Conflict Analysis and Case Studies*. Cybersecurity Interdisciplinary Systems Laboratory (CISL), Massachusetts Institute of Technology (MIT), p. 38. Retrieved from https://web.mit.edu/smadnick/www/wp/2017-10.pdf

في 8 آب (أغسطس) 2008 تم شن هجوم منسق برفض الخدمة DDoS على مواقع الحكومة الجورجية على الإنترنت في الوقت نفسه الذي كانت فيه القوات الروسية تخوض معارك مع القوات الجورجية، وازدادت الهجمات الإلكترونية ضد جورجيا مع ازدياد الهجمات البرية.

هذه الهجمات السيبرانية ضد جورجيا هي أول حالات الإبلاغ عن الهجمات السيبرانية التي يتم استخدامها قبل النزاع العسكري وبالتزامن معه. وقد استخدمت الهجمات السيبرانية بوصفها عنصرا مساعدا للهجمات البرية؛ فسببت تدهور أنظمة الاتصالات الجورجية، مما منع القيادة العسكرية من التنسيق مع قواتها. كان هناك أيضا جزء من أنشطة التسلل المعلوماتي التي تم تصميمها لسرقة وتجميع المعلومات العسكرية والسياسية من الشبكات الجورجية[1].بالإضافة إلى ذلك، تم تصميم هذه الهجمات للسيطرة على تدفق المعلومات، والتأثير على تصور الناس فيما يتعلق بالصراع بين جورجيا وروسيا.

لم تكن البنية التحتية لتكنولوجيا المعلومات في جورجيا متطورة للغاية، لذلك لم يكن انقطاع الخدمة معقدًا كما كان الحال في إستونيا. تم تخريب بعض المواقع الإلكترونية الرسمية كوزارة الخارجية، والبنك الوطني. كما تم حظر المواقع المصرفية الحكومية، وحظر المواقع الإعلامية مما أدى إلى تعطيل وصول المعلومات للجمهور في جميع أنحاء جورجيا فضلا عن وصولها العالم الخارجي[2] فقد ركزت الحرب الإلكترونية بين جورجيا وروسيا على تكوين الرأي العام على شبكة الإنترنت.

تلقت جورجيا الكثير من المساعدة لمواجهة الهجمات الإلكترونية داخليًا ودوليًا. على سبيل المثال لا الحصر وفرت Google مساحة لحماية المواقع الإلكترونية لوزارة الشؤون الخارجية[3]. كما ساعد رئيس بولندا الحكومة الجورجية من خلال نشر البيانات الصحفية الرسمية على موقعه على الإنترنت[4]. وأرسلت إستونيا اختصاصي أمن المعلومات من فريق الاستجابة لحالات الطوارئ في الكمبيوتر؛ لمساعدة جورجيا في مواجهة الهجمات الإلكترونية[5].

[1] White, S. P. (2018, March 19). Understanding Cyberwarfare: Lessons from the Russia-Georgia War. Retrieved from https://mwi.usma.edu/understanding-cyberwarfare-lessons-russia-georgia-war/

[2] المرجع السابق – Ashmore, W. C. – ص11

[3] المرجع السابق – ص11

[4] المرجع السابق – ص12

[5] المرجع السابق

ثالثا: الإسناد التقني

الهجمات السيبرانية ضد جورجيا، مثلها مثل الهجمات ضد إستونيا، لم تُنَسَب من الناحية القانونية إلى جهة معينة، ولم تُحمّل أي دولة المسؤولية مطلقًا. ومع ذلك ربط العديد من خبراء الأمن السيبراني بين الهجمات وعناوين IP الروسية[1]، وبعبارة أخرى فإن التحقيقات تؤكد أن الهجمات كانت قد أتت من إقليم روسيا. أما روسيا فتنفي أي تورط في الهجمات السيبرانية، مدعيه مرة أخرى أن المتسللين لا يمتون للحكومة الروسية بصله وقد يكون مواطنون روس غيورون أو جماعات القرصنة المتنوعة هي المسؤولة[2].

إن توقيت الهجمات وتنسيقهما من شأنه أن يتعارض مع مزاعم الحكومة الروسية. ومع ذلك لا يمكن تحميل روسيا المسؤولية؛ فإنه لا يوجد دليل مباشر على تورط الحكومة الروسية في الهجمات الإلكترونية. لكن ما لا يمكن إنكاره هو أنه حتى بدون تدخل الحكومة الروسية، أنه ما فتأ واضحا أن الحكومة الروسية استفادت من تلك الهجمات الإلكترونية.

وتجدر الإشارة أنه كان في الوقت نفسه هجومان آخران مشابهان. أولهما في ليتوانيا التي تعرضت لهجمات إلكترونية في يونيو 2008 وذلك بعد ثلاثة أيام من إصدارها قانونًا يحظر استخدام الرموز السوفيتية والشيوعية[3]. والثاني في قيرغيزستان التي تعرضت لهجمات في يناير 2009 ووقعت الهجمات في اليوم نفسه الذي كانت فيه الحكومة الروسية تضغط على قيرغيزستان لوقف وصول الولايات المتحدة إلى القاعدة الجوية في شمال بيشكيك عاصمة قيرغيزستان! وهذه القاعدة الجوية هي مركز لوجستي رئيس يدعم جهود الحرب الأمريكية في أفغانستان[4].

هذا وإن للهجمات السيبرانية على جورجيا وليتوانيا وقيرغيزستان خصائص مشتركة منها: أنها بدأت بسبب معارضة الحكومة الروسية ومنها أنه لا يوجد دليل على تورط الحكومة الروسية في الهجمات

---

[1] المرجع السابق – IIFFMCG Report – ص12-14

[2] مع ذلك يؤكد الخبراء أن تلك الهجمات إن لم تكن صنيعة الحكومة الروسية فإنها لا بد وأنها برعاية وتشجيع منها، للمزيد انظر:
Gotsiridze, A. (2019, August 9). The Cyber Dimension of the 2008 Russia-Georgia War. Retrieved from https://gfsis.org.ge/blog/view/970

[3] المرجع السابق – Tikk, E., Kaska, K., & Vihul, L. – ص51

[4] Keizer, G. (2009, January 28). Russian "cybermilitia" knocks Kyrgyzstan offline. Retrieved from https://www.computerworld.com/article/2530572/russian--cybermilitia--knocks-kyrgyzstan-offline.html

السيبرانية. هذا ما يؤكد أن معارضة الحكومة الروسية يمكن أن تؤدي إلى هجوم سيبراني يعطل البنية التحتية الحكومية المهمة[1].

رابعا: النتائج

لم تختلف الدروس المستفادة من الهجمات الإلكترونية على إستونيا عن الهجمات الإلكترونية على جورجيا، فالأخيرة أيضاً سلطت الضوء على جدية مشكلة الهجمات السيبرانية، والصعوبات التي تنطوي عليها قضايا الإسناد ومسؤولية الدولة. لكن المختلف أن الهجمات الإلكترونية على جورجيا أظهرت تحدياً جديدًا وهو أنه يمكن استخدام الهجمات الإلكترونية أداةً في الحروب والنزاعات المسلحة، وذلك يعني ان الهجمات السيبرانية تُفَعِل فرعاً آخر من فروع القانون الدولي وهو القانون الدولي الإنساني.

الفرع الثالث

الهجوم الإلكتروني على إيران

الهجمات الإلكترونية على إيران تسمى كذلك بحادثة ستاكسنت Stuxnet نسبة إلى دودة كمبيوتر خبيثة. تلك الدودة ينظر إليها على أنها سلاح إلكتروني، تم بناؤه بتعاون مشترك بين الولايات المتحدة وإسرائيل. رغم عدم تبني الدولتين للهجمات رسميا لكن المراجع تتفق على ربط Stuxnet بهما. الأمر الجديد في هجمات إيران هو كونه أول هجوم إلكتروني يسبب ضرراً مادياً ملموساً على أرض الواقع؛ فقد تسبب في حدوث انفجارات محدودة في محطة نطنز للطاقة النووية في إيران.

أولا: خلفية الهجوم

من الصعب وضع اليد على سبب مباشر للهجمات الإلكترونية على إيران، فالعداء بين إيران من جهة والولايات المتحدة وإسرائيل من الجهة الأخرى قديم قد تعود أصوله إلى عام 1953 عندما أسقط رئيس

[1] للمزيد حول حوادث الهجمات الإلكترونية الروسية المشابهة، انظر:
Windrem, R. (2016, December 18). Timeline: Ten Years of Russian Cyber Attacks on Other Nations. Retrieved from https://www.nbcnews.com/storyline/hacking-in-america/timeline-ten-years-russian-cyber-attacks-other-nations-n697111

الوزراء الإيراني المنتخب ديموقراطيا من قبل وكالات الاستخبارات الأمريكية والبريطانية. لكن يمكن القول: إن السبب الرئيس الذي يمكن وضع اليد عليه لهجمات 2010 الإلكترونية على إيران هو برنامج إيران النووي[1]. البرنامج بدأ سلمياً وبالتعاون مع الولايات المتحدة في خمسينيات القرن العشرين، لكن بدأت المخاوف تظهر من طموح إيران بامتلاك أسلحة دمار شامل خصوصاً بعد الثورة الإيرانية 1979؛ فلقد تزايدت الاتهامات بوجود برنامج أسلحة نووية سري؛ ولذلك فرض مجلس الأمن عليها عدة عقوبات[2].

ثانيا: الهجوم الإلكتروني

طبيعة الهجوم هنا Stuxnet مختلفة جدا؛ لأن الفايروس لم يرسل عبر الإنترنت، بل عبر أدوات صلبة USB وبرامج إلكترونية مصابة بالفايروس تم إدخالها إلى المنشأة النووية قبل حدوث الضرر بسنة! فكانت تعمل بصمت لتستهدف أنظمة التحكم في أجهزة الطرد المركزي، وهي المسؤولة عن الأضرار الجسيمة التي لحقت بالبرنامج النووي لإيران[3].

فيروس Stuxnet عبارة عن برنامج متطور للغاية، فهو مصمم لاستهداف نوع معين من أجهزة الكمبيوتر وهو (Symantec, 2010) وحسب. تنتشر هذه الحواسيب الألمانية الصنع بشكل محدود

---

[1] Cyber Conflict Studies Association. (2012, June). *The History of Stuxnet: Key Takeaways for Cyber Decision Makers*. AFCEA International. Retrieved from https://www.afcea.org/committees/cyber/documents/TheHistoryofStuxnet.pdf

[2] قرارات الأمم المتحدة الملغية:

قرار مجلس الأمن 1737، S/RES/1737 (23 ديسمبر 2006). استرجع من https://www.un.org/securitycouncil/ar/node/45690

قرار مجلس الأمن 1747، S/RES/1747 (24 مارس 2007). استرجع من https://www.un.org/securitycouncil/ar/node/45693

قرار مجلس الأمن 1803، S/RES/1803 (3 مارس 2008). استرجع من https://www.un.org/securitycouncil/ar/node/45696

قرار مجلس الأمن 1929، S/RES/1929 (9 يونيو 2010). استرجع من https://www.un.org/securitycouncil/ar/s/res/1929-%282010%29

لكن تجدر الإشارة إلى أن القرارات السابقة ألغيت بالقرار 2231، وذلك بعد التوصل إلى ما يعرف بالاتفاق النووي مع إيران، والذي انسحبت منه الولايات المتحدة عام 2018:

قرار مجلس الأمن 2231، S/RES/2231 (20 يوليو 2015). استرجع من https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/225/25/PDF/N1522525.pdf?OpenElement

[3] Zetter, K. (2014, November 3). An Unprecedented Look at Stuxnet, the World's First Digital Weapon. *Wired*. Retrieved from https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

في بلدان معينة منها إيران[1]. ووفقًا للرأي الشائع بين الباحثين، فإن الهدف من إدخال الفايروس لإيران هو إيصاله إلى المنشأة النووية في مدينة نطنز الإيرانية ثم إلى الأجهزة المتحكمة بأجهزة الطرد المركزي. نظرًا لأن أنظمة التحكم في المنشأة النووية غير متصلة بالإنترنت، فقد كان Stuxnet يحتاج إلى السفر على محرك أقراص USB قابل للإزالة من جهاز كمبيوتر مصاب إلى نظام التحكم في المنشأة النووية[2]. ويبدو أنه أنتقل من أفراد يعملون في المنشاة دون علمهم بعد استخدام أجهزة كمبيوتر شخصية مصابة. ربما استهدف المهاجمون أولاً أجهزة الكمبيوتر الشخصية للطاقم العامل في محطة نطنز النووية[3].

بعد أن تمكن الفايروس من الانتشار والوصول للمنشاة النووية تَفَعَّلْ. من الناحية العملية، كانت له القدرة على التأثير على حركة أجهزة الطرد المركزي (المسؤولة عن فصل المواد النووية) بحيث يجعلها تدور أسرع أو أبطأ من الوتيرة المطلوبة بمقدار قليل وغير ملحوظ، لكنه بعد مدة من الزمن أخل بأجهزة الطرد المركزي، مما جعلها تدمر نفسها. كان التخريب مفاجأ لأن الفايروس غاية في التعقيد فهو أولا موجه إلى نوع معين من الحواسيب تستخدم في المنشآت النووية الإيرانية. ثانيا يظل خاملا حتى يصل إلى أجهزة التحكم بأجهزة الطرد المركزي ثم يبدأ التخريب ببطء شديد. ثالثا فايروس Stuxnet مصمم بطريقة يستطيع أن يخفي فيها نفسه إلى درجة أن التخريب حدث دون إظهار أي علامات على وجود مشاكلات في أنظمة المراقبة التي يستخدمها العاملون في المنشأة الإيرانية!! وبعبارة أخرى لديه القدرة على إظهار قراءة لا تعكس الواقع فقد كانت أجهزة الطرد المركزي تعمل بشكل صحيح أمام الإيرانيين[4]!

دمر الهجوم ما يقدر بـ 1000 جهاز طرد من أصل 9000 تعمل في المنشأة النووية الإيرانية[5]. حيث قامت إيران في العام 2010 باستبدال حوالي 1000 جهاز طرد مركزي من طراز IR-1 في محطة

---

[1] Kuru, H. (2018). Evolution of War and Cyber Attacks in the Concept of Conventional Warfare. *Journal of Learning and Teaching in Digital Age*, *3*(1), 12–20 [p. 16]. Retrieved from https://www.learntechlib.org/p/209516/

[2] المرجع السابق – ص16-17

[3] المرجع السابق – Zetter, K.

[4] للاطلاع على المزيد من آثار هجمات Stuxnet على المنشأة النووية الإيرانية من الناحية التقنية، انظر:
Albright, D., Brannan, P., & Walrond, C. (2010, December). *Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?* Institute for Science and International Security [p. 2]. Retrieved from https://isis-online.org/uploads/isis-reports/documents/stuxnet_FEP_22Dec2010.pdf

[5] Healey, J., & Grindal, K. (Eds.). (2013). A Fierce Domain: Conflict in Cyberspace, 1986 to 2012 (Illustrated ed.), p. 213. Vienna, Virginia: Cyber Conflict Studies Association (CCSA).

تخصيب الوقود في نطنز، مما يعني أن هذه الأجهزة دمرت بفعل الهجوم. لكن لا تزال الخسائر الدقيقة التي سببها الهجوم غير معلومة[1].

ثالثا: الإسناد الفني

التعقب في هجمات Stuxnet مختلف عما سبقه من ناحية أن الفايروس انتقل للمنشاة يدويا أو بريا إن جاز التعبير فمن الصعب جدا تتبع مصدره. فالهجمات التي سبقت على إستونيا وجورجيا كان من الممكن تتبع عنوان الـ IP على الأقل. لكن هنا التعقب يعتمد تماما على تحليل شفرة الفايروس وجنسية التكنولوجيا المستخدمة فيه[2]. ومن ناحية أخرى عزلة إيران الدولية صعبت عملية الإسناد أكثر في ظل غياب الشفافية، وغياب التعاون الدولي المطلوب لإجراء تحقيق فعال على صعيد خبراء الأمن الإلكتروني.

ومع ذلك هناك إجماع (من الحقلين القانوني والتقني) أن الفايروس هو نتيجة التعاون الأمريكي والإسرائيلي لسببين: أولهما: أن الفايروس – في وقت لاحق من الحادثة – خرج من محطة نطنز للطاقة النووية إلى العامة، غالبا عن طريق بطاقة تخزين USB مصابه، ووقع في يد الباحثين والشركات الخاصة في مجال الأمن السيبراني الذين قاموا بتحليله وبينت أنه صناعة أمريكية إسرائيلية (صنعته أمريكا وقامت إسرائيل بإضافة بعض التعديلات عليه)[3]. والسبب الثاني – وإن لم تصرح أيا من الدولتين رسميا مسؤوليتها عن Stuxnet تحديدا – فإن وكالة الأمن القومي الأمريكية تعترف بقيامها بهجمات إلكترونية على إيران بشكل عام إيران[4].

---

[1] المرجع السابق – ص1

[2] Lachow, I. (2011). The Stuxnet Enigma: Implications for the Future of Cybersecurity. *Georgetown Journal of International Affairs*, 118–126. Retrieved from http://www.jstor.org/stable/43133820.

[3] Anderson, N. (2012, June 1). Confirmed: US and Israel created Stuxnet, lost control of it. Retrieved from https://arstechnica.com/tech-policy/2012/06/confirmed-us-israel-created-stuxnet-lost-control-of-it/

[4] في عام 2012 اعترف مسؤول أمريكي ــ لم يذكر اسمه ــ مشاركة الولايات المتحدة ضمن برنامج "الألعاب الأولمبية" المصنف الذي بدأه الرئيس جورج دبليو بوش وتابعه الرئيس باراك أوباما. الولايات المتحدة. لم تصدر الحكومة أي تصريح رسمي حول هذا الموضوع. للمزيد انظر:

Iasiello, E. (2013). *Cyber Attack: A Dull Tool to Shape Foreign Policy*. In K. Podins, J. Stinissen, & M. Maybaum (Eds.) (p. 8). Presented at the 5th International Conference on Cyber Conflict, Tallinn, Estonia. Retrieved from https://ccdcoe.org/uploads/2018/10/24_d3r1s3_Iasiello.pdf

رابعا: النتائج

هناك عدد من السوابق التي جاء بها Stuxnet. فلقد كان جديدا على العالم أن رمزا رقميا مسلحا يهدف إلى تدمير هدف معين. في حين أن الهجمات على إستونيا وجورجيا كانت تهدف إلى تعطيل البنية التحتية الرقمية، ولم يكن الغرض منها أن يكون لها تأثير حركي. كما كان جديدا أن يتم اعتماد الإسناد الفني والإسناد القانوني لهجمات Stuxnet بشكل كامل على التحليل الجنائي لشفرة الكمبيوتر المستخدمة داخل الهجمات. فلم يكن هناك دليل مباشر على تورط الدولة[1].

وأخيرا كان Stuxnet على مستوى تقني لم يسبق له مثيل في البرامج الضارة، واستلزم إنتاجه استثمارًا كبيرًا في المال والمعرفة التقنية، مما أظهر – ولأول مرة – خطة طويلة الأجل نيابة عن دولة متوجهة للاعتماد على السلاح الرقمي.

الفرع الرابع

عمليات التجسس الإلكتروني الصيني ـ الأمريكي

التجسس بين أعضاء المجتمع الدولي قديم، منذ قيام الدول إلى اليوم. تختلف أهدافه باختلاف الأزمنة والظروف، لكن التجسس الإلكتروني بمعنى إحداث اختراق عبر الإنترنت؛ للحصول على أسرار دولة ما[2] حديث نسبيا يعود إلى بدايات القرن الواحد والعشرين وتعد الصين رائدة في التجسس الإلكتروني

سرّعت إدارة ترامب العمليات السيبرانية ردًا على الهجمات الإيرانية في الخليج العربي. في يونيو 2019، فشنت الولايات المتحدة هجومًا إلكترونيًا على إيران بعد أن أسقطت طائرة أمريكية بدون طيار بالقرب من مضيق هرمز. وقد أدى الهجوم إلى مسح قاعدة بيانات الحرس الثوري الإيراني المستخدمة للتخطيط لهجمات ضد ناقلات النفط في الخليج العربي
Hanna, A. (2021, December 16). The Invisible U.S.-Iran Cyber War. Retrieved from https://iranprimer.usip.org/blog/2019/oct/25/invisible-us-iran-cyber-war

في سبتمبر 2019، نفذت الولايات المتحدة هجومًا إلكترونيًا على "معدات مادية" إيرانية غير محددة - معدات تستخدم لنشر الدعاية - بعد هجمات إيران على منشأتين نفطيتين سعوديتين. وأشار التأكيد الأمريكي غير المعتاد لهجماتها في أكتوبر / تشرين الأول إلى أن الهدف كان ردع إيران دون اللجوء إلى الضربات الحركية. انظر: المرجع السابق
وفي أكتوبر 2020، صادرت الولايات المتحدة 92 نطاقًا مملوكًا للحرس الثوري. تظاهرت أربعة مواقع على الإنترنت بأنها مؤسسات إخبارية مرموقة، ولكنها كانت "دعاية إيرانية للتأثير على السياسة الداخلية والخارجية للولايات المتحدة". عمل مكتب التحقيقات الفيدرالي مع Google و Facebook و Twitter لتحديد المواقع الإلكترونية وإزالتها. انظر: المرجع السابق

[1] Jolley, J. D. (2017). Attribution, State Responsibility, and the Duty to Prevent Malicious Cyber-Attacks in International Law. (PhD Thesis), p. 25. University of Glasgow. https://doi.org/10.2139/ssrn.3056832

[2] Buchan, R., & Navarrete, I. (2020). Cyber Espionage. *Oxford Bibliographies in International Law*. https://doi.org/10.1093/obo/9780199796953-0212

فالاتهامات الموجهة إليها متكررة من قبل الدول بالتجسس وسرقة المعلومات، لكن أكثر العلاقات توترا بسبب كثرة التجسس الإلكتروني هي التي بين الصين والولايات المتحدة.

أولا: خلفية الهجوم

لا يمكن حصر سبب التجسس الإلكتروني بين الصين والولايات المتحدة في حادثة واحدة أو سبب ضيق. لكن يمكن القول إن الدافع العام للصين هو المصلحة الوطنية والرغبة في التفوق، فسرقة الأهداف الصناعية سببها الرغبة في التفوق الصناعي، وسرقة أسرار صناعات الأسلحة هدفها التفوق العسكري كذلك وسرقة بعض التقارير الاقتصادية هدفها تحقيق الامتياز الاقتصادي وهكذا.

ثانيا: الهجوم الإلكتروني

يصعب حصر حوادث التجسس الإلكتروني بسبب طبيعتها الصامتة بعكس الهجمات الإلكترونية ذات الأهداف التخريبية. أما التجسس فلا يكتشف فور حدوثه ويصعب تقييم ضرره؛ ذلك لأن التجسس الناجح لا يشعر الضحية بوجوده، ولا كمية المعلومات التي تم الحصول عليها. هذا ينطبق على التجسس الصيني السيبراني الذي تشتكي منه كثير من الدول المتقدمة[1]. ولا يمكن حصر عدد حوادث

[1] مثل ألمانيا، والمملكة المتحدة، وفرنسا، وكندا، وأستراليا، والاحتلال الإسرائيلي، وتايوان، واليابان، ورابطة أمم جنوب شرق آسيا، والهند. انظر:

Xinhua News Agency. (2022, January 17). *Full Text: Special Address by Chinese President Xi Jinping at the World Economic Forum Virtual Event of the Davos Agenda* [Press release]. Retrieved from http://www.xinhuanet.com/english/2021-01/25/c_139696610.htm

Connor, R. (2022, January 26). Chinese hackers targeting companies, says Germany. DW. Retrieved from https://www.dw.com/en/chinese-apt-27-hackers-targeting-companies-says-germany/a-60564091

UK condemns Chinese cyber attacks against governments and businesses. (2020, September 16). *National Cyber Security Centre (NCSC)*. Retrieved from https://www.ncsc.gov.uk/news/uk-condemns-chinese-cyber-attacks-against-businesses-governments

Reuters. (2021, July 21). French cybersecurity agency warns of China-linked APT31 attacks on French organizations. Retrieved September 6, 2022, from https://www.reuters.com/technology/french-cybersecurity-agency-warns-china-linked-apt31-attacks-french-2021-07-21/

Berthiaume, L. (2021, December 20). Canada blames China for widespread attack on email servers. Retrieved September 6, 2022, from https://www.nationalobserver.com/2021/07/19/news/canada-blames-china-widespread-attack-email-servers

Hurst, D. (2021, July 20). Australia joins allies in accusing China of 'malicious cyber activities.' Retrieved September 6, 2022, from https://www.theguardian.com/world/2021/jul/19/australia-joins-allies-in-accusing-china-of-malicious-cyber-activities

التجسس ولا معرفة متى بدأت بالتحديد؟ ولا الجزم بانتهائها من عدمه. لكن الأمر الذي يؤكده التقنيون أن الصين تتجسس بكثرة حتى أن شون هنري، الرئيس السابق لقسم الأمن السيبراني بمكتب التحقيقات الفيدرالية ، صرح بأن "هناك نوعين من الشركات: الشركات التي تم اختراقها والشركات التي لا تعرف أنها قد تم اختراقها[1]. لذلك ما سيتم ذكره هو بعض الأمثلة – التي لا حصر لها في الوقت الحالي – على التجسس السيبراني الصيني الأمريكي.

تصاعدت مشكلة الولايات المتحدة مع أنشطة الصين في الفضاء السيبراني على مدى سنوات. ففي العام 2003 بدأ هجوم Titan Rain الإلكتروني وهي تسمية أعطتها الحكومة الفيدرالية لسلسلة من الهجمات المنسقة على أنظمة الكومبيوتر الأمريكية، استمرت لمدة ثلاث سنوات على الأقل[2]. هذا الهجوم الصيني المنشأ يعتقد أنه كان برعاية الدولة[3]، واستهدف مرافق متعددة منها بهدف الوصول إلى المعلومات. مثلا مختبرات وزارة الطاقة، بالإضافة إلى مؤسسات تعليمية عسكرية مثل كلية الحرب البحرية وجامعة الدفاع الوطني. الهجمات على وزارة التجارة الأمريكية للحصول على بعض المعلومات المتعلقة بالصادرات والواردات. وقد أدت مثل هذه الهجمات إلى عمليات إغلاق ممتدة فتأكد ضبط

Miller, B. J. (2014, July 31). Israeli Iron Dome firms "infiltrated by Chinese hackers." *BBC News*. Retrieved from https://www.bbc.com/news/technology-28583283

Davidson, H., & Ni, V. (2022, August 6). Taiwan says China making simulated attack on main island. Retrieved September 6, 2022, from https://www.theguardian.com/world/2022/aug/06/taiwan-says-china-making-simulated-attack-main-island-military-drills

Yui , M., & Kawamoto, S. (2014, December 18). Chinese Criminals Blamed for Record Japan Bank Cybertheft. *Bloomberg*. Retrieved from https://www.bloomberg.com/news/articles/2014-12-17/chinese-criminals-blamed-for-record-japan-bank-cybertheft

Culpan, T. (2015, April 13). Decade-Long Cyberspy Attack Hacked Southeast Asian Targets. *Bloomberg*. Retrieved from https://www.bloomberg.com/news/articles/2015-04-12/decade-long-cyber-spying-campaign-hacked-southeast-asia-targets

Rising, D. (2022, April 7). Chinese hackers reportedly target India's power grid. Retrieved September 6, 2022, from https://abcnews.go.com/Technology/wireStory/chinese-hackers-reportedly-target-indias-power-grid-83928423

[1] Lowry, A. (2018, March 7). "There are only two types of companies: those that have been hacked, and those that will be." Retrieved from https://wecyberup.org/there-are-only-two-types-of-companies-those-that-have-been-hacked-and-those-that-will-be/

[2] Harold, S. W., Libicki, M. C., & Cevallos, A. S. (2016). *Getting to Yes with China in Cyberspace*, p. 36. RAND Corporation. https://doi.org/10.7249/RR1335

[3] Winkler, I. (2005, October 20). Guard against Titan Rain hackers. Retrieved from https://www.computerworld.com/article/2559195/guard-against-titan-rain-hackers.html

الرقابة، وأن جميع الأنظمة قد تم تنظيفها تمامًا، وأنه لا توجد بيانات سرية معرضة للخطر. كما نتج عن تلك العمليات السيبرانية استبدال المسؤولين أجهزتهم لتكون أكثر أمنا وإحكاماً.

في منتصف العام 2009 بدأت سلسلة هجمات على Google تم تسمية هذه الهجمات باسم "عملية Aurora"[1] وصفت جوجل في مدونتها الهجوم بأن المهاجمين كانوا يحاولون اختراق حسابات Gmail لمناصري حقوق الإنسان الصينيين[2]. لكن بعد ثلاث سنوات صرح كبير مديري معهد Microsoft للتكنولوجيا أن هناك سببا آخر للهجمات أكثر اقناعا للمحللين. فمناصرو حقوق الإنسان لم يكونوا هم الهدف. لأن حسابات النشطاء الصينيين Gmail تم وضع علامة عليها تسمح بالتنصت بأوامر القضاء الأمريكي. لذلك تم إنشاء ثغرات هي بمثابة أبواب خلفية بواسطة Google نفسها، حتى تتمكن الحكومة من مراقبة بيانات النشطاء. تم استغلال الأبواب الخلفية نفسها من قبل المتسللين الصينيين للدخول إلى حسابات Gmail[3]. وليس الناشطون أنفسهم هم المستهدفون لكن حساباتهم تحتوي على معلومات عن هويات العملاء الصينيين السريين الذين يعملون لمصلحة الولايات المتحدة وهو ما كانت الصين تسعى إلى الوصول إليه[4].

في عام 2011، تم شن هجوم إلكتروني ضد شركات النفط الأمريكية؛ لتحديد كيفية تقييمها لبعض بقع النفط، وماهي العطاءات التي كانت مستعدة لتقديمها للحصول على حقوق الحفر[5]. هذه المعلومات ذات قيمة هائلة لشركات النفط المنافسة؛ لأنها تمكنها – وبفارق ضئيل في العرض – من أن تحصل على مكاسب كبيرة.

أخيراً، نهج الصين في التجسس السيبراني وجمع المعلومات الاستخبارية نجح في كثير من الأحيان في اكتساب الملكية الفكرية ذات القيمة الاستراتيجية[6]. فضلا عن الحصول على معلومات التقنيات

---

[1] صرح ديمتري ألبير وفيتش نائب رئيس قسم أبحاث التهديدات في شركة الأمن السيبراني McAfee بعد الجزء من مسار الملف على جهاز المهاجم الذي تم تضمينه في اثنين من ثنائيات البرامج الضارة المرتبطة بالهجوم. بعبارات بسيطة، استخدم القراصنة حصان طروادة المسمى "Aurora".

[2] Anderlini, J. (2010, January 15). The Chinese dissident's 'unknown visitors.' Retrieved from https://www.ft.com/content/c590cdd0-016a-11df-8c54-00144feabdc0

[3] Everything You Need to Know About Operation Aurora. (2016, August 8). Retrieved from https://cyware.com/news/everything-you-need-to-know-about-operation-aurora-5c5f5b99

[4] المرجع السابق

[5] المرجع السابق – Harold, S. W., Libicki, M. C., & Cevallos, A. S. – ص38-39

[6] Hannas, W. C., Mulvenon, J., & Puglisi, A. B. (2013). *Chinese Industrial Espionage: Technology Acquisition and Military Modernisation (Asian Security Studies)* (1st ed.), p. 4-20. Retrieved from

الصناعية والعسكرية، وتصدر السبق في صناعتها، وامتلاك براءات اختراعها، وإعطاء الشركات الصينية السبق في اختراق الأسواق الأجنبية. ومن أمثلة ذلك أنه سرق قراصنة صينيون معلومات عن نظام صواريخ باتريوت وسفينة القوات البحرية الجديدة Littoral[1]، كانت عبارة عن مخططات للولايات المتحدة تمت سرقتها واستخدامها من أجل تطوير الأسلحة الصينية.

ثالثا: النتائج

توترت العلاقات الصينية الأمريكية بسبب السلوك الصيني في الفضاء السيبراني، وقد لوحت الولايات المتحدة بفرض عقوبات على الشركات الصينية[2]، وكان مجرد التلويح بالعقوبات كافياً لدفع الصين لتوقيع اتفاق بين الرئيس الأمريكي باراك أوباما والصيني شي جين بينغ عام 2015 بشأن التعاون في الفضاء السيبراني يقضي بالامتناع عن إجراء أو دعم سرقة الملكية الفكرية (عن علم) عبر الإنترنت[3]. بالرغم من التشكيك في فعالية مثل هذه الاتفاقية في قمع التجسس السيبراني الصيني[4] فإنها خطوة في الاتجاه الصحيح لتقنين سلوك الدول في الفضاء السيبراني.

كذلك بعد أن كانت الفكرة عن العدوان الإلكتروني متركزة حول كلمات مثل هجمات إلكترونية أو حرب إلكترونية جاءت فكرة التجسس الإلكتروني كنوع جديد من الخطر. وهذا غَيَرَ التعامل مع خطورة الإنترنت. فبعد أن كان الخطر هو حرب سيبرانية مكونة من هجمات قادمة من الأعداء يراد بها تخريب الدولة وتعطيل مرافقها أصبح الخطر هذا النوع من الهجوم الذي يُمَكِن المرء أن يسرق المعلومات التي تشكل سر الدولة وهو أكثر انتشار.

---

https://www.routledge.com/Chinese-Industrial-Espionage-Technology-Acquisition-and-Military-Modernisation/Hannas-Mulvenon-Puglisi/p/book/9780415821421

[1] Abad-Santos, A. (2022, May 12). China Is Winning the Cyber War Because They Hacked U.S. Plans for Real War. Retrieved from https://www.theatlantic.com/international/archive/2013/05/china-hackers-pentagon/314849/

[2] المرجع السابق – Harold, S. W., Libicki, M. C., & Cevallos, A. S. – ص11-12

[3] Rollins, J. W., Lawrence, S. V., Rennack, D. E., & Theohary, C. A. (2015, October). *U.S.-China Cyber Agreement*. Library of Congress, Congressional Research Service. Retrieved from https://digital.library.unt.edu/ark:/67531/metadc795686/m1/1/high_res_d/IN10376_2015Oct16.pdf

[4] Segal, A. (2016, October 15). The US-China Cyber Agreement: New Beginning or Tactical Pause? Retrieved from https://www.orfonline.org/expert-speak/the-us-china-cyber-agreement-new-beginning-or-tactical-pause/

التجسس الإلكتروني علم المؤسسات الحكومية والخاصة الحرص على المعلومة، فالهجمات الصينية التي استهدفت القطاعين العام والخاص زادت من تحصين المعلومات الرقمية وتضييق دائرة القادرين للوصول إليها. وقد ثبت أن مكاتب المحاماة أهداف سهلة لمثل هذه الاختراقات لأنها تحتفظ ببيانات ذات امتيازات عالية عن الشركات التي تمثلها ولكنها لم تكن كفؤا من ناحية التحصين السيبراني لأنها ليست كبيرة بما يكفي لتتحمل تكلفة موظفي تكنولوجيا الأمن الإلكتروني.[1]

أخيرا أن الخطر الإلكتروني متربص في حياتنا اليومية أكثر مما نعتقد، ولذلك أصبح الإنفاق في الحماية السيبرانية أكبر بكثير من الاقتصار على الأهداف العسكرية أو الحساسة[2].

الفرع الخامس

عمليات التدخل الروسي الإلكتروني في الانتخابات الأمريكية عام 2016

التدخل في الانتخابات الوطنية للدول هو التدخل في الشئون الداخلية الذي نهى عنه ميثاق الأمم المتحدة في المادة (7) 2، لكن برغم وسمها بعدم الشرعية – وحتى بعد ميثاق الأمم المتحدة – مازالت هذه الممارسة موجودة، فنجد الدول تتدخل في الشئون التي تعد من صميم السلطان الداخلي للدول الأخرى بما تمليه عليها مصالحها. لكن الشيء الجديد أن تلك الممارسة تحولت نحو السيبرانية. مثالها أنه أصبحت عرقلة انتخابات البدان الأخرى والتأثير على الرأي العام فيها تتم عن بعد إلكترونيا. وأول تدخل إلكتروني في انتخابات دولة أخرى هو ذلك الذي قامت به روسيا في أوكرانيا عام 2014[3]، ثم تلاه التدخل الروسي في الانتخابات الأمريكية عام 2016. سيتم هنا في هذا الفرع تناول المثال الأمريكي لعام 2016 الذي كانت أصداؤه أكبر في العالم وكان أكثر إثارة لاهتمام الباحثين في المجالين التكنولوجي والقانوني.

---

[1] المرجع السابق – Harold, S. W., Libicki, M. C., & Cevallos, A. S.

[1] المرجع السابق – ص39

[2] المرجع السابق – ص11-12

[3] Atlantic Council. (2019, May). *Ukrainian Election Task Force Foreign Interference in Ukraine's Democracy - Ukrainian Election Task Force Report*. Retrieved from https://www.atlanticcouncil.org/wp-content/uploads/2019/05/Foreign_Interference_in_Ukraines_Election.pdf

أولا: خلفية الهجوم

كان مهما لروسيا أن تدعم مرشحًا لرئاسة الولايات المتحدة أقل عداء لها مما كان عليه الرئيس أوباما، وبما أن المؤشرات الأولية كانت ترجح فوز المرشحة الرئاسية هيلاري كلينتون (من الحزب الديموقراطي نفسه ووزيرة الخارجية السابقة في عهد أوباما)، وضعت روسيا استراتيجية عمل لتقويض ثقة الناخبين الأمريكيين في نظامهم الانتخابي من جهة وفي نزاهة كلينتون من جهة اخرى[1].

كانت أهداف روسيا تتلخص في تقويض ثقة الجمهور في العملية الديمقراطية الأمريكية، وتشكيكهم في وجود تزوير في الأصوات، وتشويه سمعة الوزيرة كلينتون، وإلحاق الضرر بقابليتها للانتخاب ورئاستها المحتملة، وأخيراً تفضيل إعلامي واضح للرئيس المنتخب ترامب الذي كان يبشر في حملته بفكرة التطبيع مع روسيا.[2]

تشير التقارير إلى أن حساسية الأهداف تؤكد أن العمليات السيبرانية تمت بأمر الرئيس فلاديمير بوتين شخصياً[3]. هذا غير مستغرب إذا أخذ في عين الاعتبار أن مع وجود كلينتون في البيت الأبيض سيكون من شبه المستحيل رفع العقوبات عن روسيا، لذا فإن المسألة من مسائل الأمن القومي بالنسبة لروسيا.

ثانيا: الهجوم الإلكتروني

يمكن القول: إن أفضل مرجع لفهم الهجمات الإلكترونية المستخدمة في عرقلة الانتخابات الأمريكية هو التقرير الرسمي الذي قام به المحقق الخاص روبرت مولر بتكليف من مكتب الادعاء العام الأمريكي الذي كان بعنوان " التحقيق في التدخل الروسي في الانتخابات الرئاسية لعام 2016"[4].

---

[1] تقرير مكتب الاستخبارات القومية الأمريكي، انظر:
U.S. Office of the Director of National Intelligence (ODNI). (2017, January). *Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution*. Retrieved from https://www.dni.gov/files/documents/ICA_2017_01.pdf

[2] في يناير 2017، قدم مكتب مدير المخابرات الوطنية تقريرًا خاليًا من السرية (يمثل عمل مكتب التحقيقات الفدرالي ووكالة المخابرات المركزية ووكالة الأمن القومي) مع استنتاج مماثل. انظر المرجع السابق.

[3] United States Office of the Director of National Intelligence – المرجع السابق – ص11

[4] Mueller, R. S. (2019a, March). *Report On the Investigation Into Russian Interference In The 2016 Presidential Election* (Volume I of II). U.S. Department of Justice. Retrieved from https://www.justice.gov/archives/sco/file/1373816/download

برغم أنه برء الرئيس المنتخب دونالد ترامب من التواطء مع الروس[1]، خلص التقرير أن التدخل الروسي في الانتخابات الأمريكية 2016 كان شاملا وممنهجا. وذلك بطريقتين رئيستين:

الطريقة الأولى: حرب معلومات شنتها وكالة أبحاث الإنترنت الروسية على مواقع التواصل الاجتماعي[2]:

في العام 2016 كان لدى وكالة أبحاث الإنترنت الروسية القدرة على الوصول إلى ملايين الأشخاص الأمريكيين من خلال حساباتهم على وسائل التواصل الاجتماعي من خلال منصات Facebook وInstagram وTwitter.[3] فقد قامت وكالة أبحاث الإنترنت الروسية بإنشاء تجمعات تحمل عناوين محافظة مثل العدالة الاجتماعية للسود، أو المجموعات الدينية المختلفة ثم نشرت مئات المحتويات التي تثير الخلاف السياسي والاجتماعي وتضخمه في المجتمع الأمريكي[4]. وفي الوقت نفسه كانت تسوِّق لأفضلية دونالد ترامب وتهاجم الحزب الديموقراطي.

الطريقة الثانية: اختراق حساب المرشحة الديموقراطية هيلاري كلينتون:[5]

كذلك قام فريق تجسس إلكتروني روسي، يُعرف باسم "Cozy Bear"[6] باختراق قواعد البيانات لحملة المنافسة هيلاري كلينتون وكذلك اختراق بريدها الإلكتروني الخاص والحصول على بعض المعلومات التي تشكك في نزاهتها، ثم إطلاق تلك المواد المسروقة للعامة عن طريق كيانات مثل منظمة ويكيليكس المتخصصة في نشر التسريبات التي من هذا النوع[7].

هذا بالإضافة إلى حوادث أخرى من الهجمات الروسية، كتلك الهجمات التي استهدفت نظام آلات التصويت[8]، وهجمات أخرى قامت بسرقة بيانات قاعدة عريضة من الناخبين.

---

[1] Mueller, R. S. (2019b, March). *Report On the Investigation Into Russian Interference In The 2016 Presidential Election* (Volume II of II), p. 156-181. U.S. Department of Justice. Retrieved from https://www.justice.gov/storage/report_volume2.pdf

[2] المرجع السابق – ص22-23

[3] المرجع السابق – ص23-24 وص26

[4] المرجع السابق – ص22

[5] المرجع السابق – ص40-60

[6] Sanger, D. E., & Shane, S. (2016, December 10). Russian Hackers Acted to Aid Trump in Election, U.S. Says. *NY Times*. Retrieved from https://www.nytimes.com/2016/12/09/us/obama-russia-election-hack.html

[7] المرجع السابق – Mueller, R. S. – Volume II of II – ص59-60

[8] المرجع السابق – ص58-59

ثالثا: النتائج

قد تكون نتيجة التدخل الروسي في الانتخابات هو فوز المرشح الرئاسي دونالد ترامب الذي فاز بالفعل بعد أن كانت فرصه للفوز ضعيفة في بداية ترشحه. ولقد سبقت الإشارة إلى أنه أكدت التقارير أن التدخل الروسي حدث بالفعل، لكن ما هو مقدار تأثير تلك التدخلات السيبرانية في تحويل نتيجة الانتخابات؟ هذا سؤال يبقى محل نقاش.

مع التأكيد أن هذا ليس النموذج الأول للتدخل السيبراني في الشأن الداخلي، فقد حدث قبل ذلك في انتخابات أوكرانيا. لكن أكد هذا الهجوم للعالم أن هناك أخطاراً مختلفة للعدوان السيبراني على الدول. فبين التجسس الذي لا يغير ساكنا وبين الهجمات التخريبية أو التعطيلية التي تعيق سير الحياة الطبيعي يأتي هذه النوع من الهجمات الذي يخترق العقول[1] ليشكل خطرا على سيادة الدولة وسير العدالة والعملية الديموقراطية.

ولما كانت هذه الهجمات مختلفة في صورتها كانت آثارها القانونية مختلفة أيضا. هناك حاجة جديدة لدراسة ظاهرة التدخل السيبراني دولياً، وتحديد الحق الذي تم الاعتداء عليه والضرر الذي سببته، والرد المتناسب معها. وقد يكون الموضوع هنا أصعب من الصور السابقة. فأدوات العولمة والإعلام المفتوح قد سببت ضبابية في ترسيم الحدود بين ما يعد تدخلا في الشأن الداخلي وبين الإعلام الحر.

المبحث الثالث

انطباق القانون الدولي على الهجمات السيبرانية

القانون الدولي بقواعده العرفية والمكتوبة ينطبق على الهجمات السيبرانية. ولربما كان بالإمكان تخطي هذا النقاش لولا بعض الأصوات القليلة تجادل في هذه الفكرة. الآراء المعارضة لانطباق القانون الدولي على الفضاء السيبرانية: إما أنها تدعو إلى التوصل إلى اتفاقية جديدة مخصصة تماما للسلوك السيبراني بين الدول، وإما أنها تدعو إلى تخصيص القانون الدولي الحالي ليتماشى مع الطبيعة السيبرانية، لأنها ترى أن فكرة الفضاء الإلكتروني "مجال (افتراضي) جديد"، أو مجال نشاط، وعلى هذا النحو فهو مثل المجالات المادية للجو والأرض والبحر والفضاء الخارجي، يتطلب قواعد مصممة خصيصًا.

[1] المرجع السابق – ONDI – ص10-12

ويحسن البدء بالرأي الأخير للكاتب Michael P. Fischerkeller الذي يرى في مقاله المعنون بـ "القانون الدولي الحالي غير مناسب للأنشطة السيبرانية" أن ميثاق الأمم المتحدة يعكس تحيزا لما أسماه البيئات الاستراتيجية الكلاسيكية، فقد تطورت قواعد القانون الدولي المكتوبة أو العرفية في ظل كل من البيئات التقليدية (ويقصد الأسلحة التقليدية) والنووية[1]. هذه البيئات الكلاسيكية تهدد الاستقرار الدولي من خلال السعي لتحقيق مكاسب استراتيجية، إما بالقهر وإما باستخدام القوة الغاشمة. أما البيئة الاستراتيجية الإلكترونية فهي تختلف عن التقليدية أو النووية من حيثية أن التهديدات التي يتعرض لها الاستقرار الدولي تنبع من عنصر **الاستغلال** (أي أن الدول تستخدم الرمز بشكل أحادي للاستفادة من نقاط الضعف السيبرانية لدى الآخرين، بغرض تحقيق مكاسب استراتيجية.) وإن اختلاف البيئة الاستراتيجية للفضاء السيبراني عن البيئات النووية والتقليدية، يشكل تحديًا لانطباق قواعد القانون الدولي بسبب اختلاف السمات في كل بيئة.

فإن السمات الأساسية للبيئة النووية هي التكاليف التي لا جدال فيها (أي، لا يوجد دفاع صالح ضد الأسلحة النووية)، مما يؤدي إلى سلوك إكراه مهيمن (دائم) في شكل استراتيجية ردع دائم (أي التدمير المؤكد المتبادل)[2].

أما البيئة الاستراتيجية التقليدية فهي تقترن بتكاليف قابلة للجدل (يمكن الدفاع ضد القدرات التقليدية، على عكس الأسلحة النووية). يؤدي هذا إلى سلوكيات من القوة الغاشمة أو الإكراه عرضية (متقطعة) فتتكون استراتيجية الردع بالتهديد الذي تفرضه تكاليف الحرب التقليدية.[3]

أما في للبيئة الاستراتيجية السيبرانية فسنجد سمات جديده تماماً مثل ظروف الاتصال المستمر (لذلك احتمال السلوك مستمر وليس عرضي أو متقطع)، ووفرة من نقاط ضعف الأطراف الأخرى، والمرونة الكلية (القدرة على التعافي من استغلال تلك الثغرات يحول دون احداث ضرر ثقيل بالبيئة). وبالتالي يصعب الحديث عن ردع، بل على العكس هناك حتمية أمنية تتمثل في الاستمرار في اقتناص المبادرة لتحقيق ميزة استراتيجية والحفاظ عليها[4].

---

[1] Fischerkeller, M. P. (2021, August 31). Current International Law Is Not an Adequate Regime for Cyberspace. Retrieved from https://www.lawfareblog.com/current-international-law-not-adequate-regime-cyberspace

[2] المرجع السابق

[3] المرجع السابق

[4] المرجع السابق

وبعبارة أخرى لا يمكن تصور الردع أو أن تضحي الدول أمام فرصة –تحويل التوزيع الدولي للقوة – من خلال العمليات الإلكترونية المستمرة ذات الآثار التراكمية غير المكلفة ليس ماديا فحسب، بل حتى في مجال انتهاك القانون؛ لأنها ذات طبيعة غير قسرية، ولا تمثل انتهاكًا للحظر المفروض على استخدام القوة ولا تعادل هجومًا مسلحًا بموجب المادة 51 من ميثاق الأمم المتحدة. وتحقق الدول ميزة استراتيجية من خلال الاستغلال، وليس من خلال القوة الغاشمة أو الإكراه[1].

لذلك ونظراً للاختلافات الكبيرة بين السمات الأساسية للبيئات الاستراتيجية النووية والتقليدية مقابل البيئة الاستراتيجية السيبرانية يرى Fischerkeller أنه يجب على الدول قبول عدم كفاية القواعد الحالية كما هي لتنطبق في البيئة الاستراتيجية الإلكترونية، بل يدعو إلى إعادة صياغة القواعد مع التركيز على عنصر الاستغلال، وهذا ما قام بتطبيقه على قاعدة عدم التدخل في الشأن الداخلي. فإذا طبقناها على التدخل في الانتخابات الأمريكية 2016 فلن تنطبق القاعدة؛ بسبب عدم وجود عنصر الإكراه، وهو شرط في تعريف التدخل في الشأن الداخلي كما سيأتي الحديث عنه في الفصل الثاني. لكن قام الكاتب بتعريف الاستغلال ودمج عناصر الاستغلال الإلكتروني مع قاعدة عدم التدخل في هجمات التدخل في الانتخابات ليخرج بنتيجة مؤداها أن الذي حصل هو تدخل في الشأن الداخلي.[2]

في رأي مشابه في خطاب حول "التقنيات التخريبية والقانون الدولي" عرض نائب المدعي العام للاحتلال الإسرائيلي موقف الاحتلال من انطباق القانون الدولي على العمليات السيبرانية عندما قال:

"لا يمكن الافتراض تلقائياً أن القاعدة العرفية المطبقة في أي من المجالات المادية تنطبق أيضًا على المجال السيبراني. بل يجب دائما طرح سؤال رئيس هل الممارسة التي نشأت في مجالات أخرى مرتبطة ارتباطًا وثيقًا بالنشاط المتوخى في المجال السيبراني. بالإضافة إلى ذلك، يجب التأكد من أن الرأي القانوني الذي أدى إلى القواعد العرفية المطبقة في المجالات الأخرى لم يكن خاصًا بمجال معين. ونظرًا للخصائص الفريدة للمجال السيبراني، يجب إجراء مثل هذا التحليل بحكمة خاصة، فإنه توجد اختلافات ذات صلة في كثير من الأحيان"[3].

---

[1] المرجع السابق

[2] المرجع السابق

[3] Schondorf, R. (2020, December 9). Israel's perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations. Retrieved from https://www.ejiltalk.org/israels-perspective-on-key-legal-and-practical-issues-concerning-the-application-of-international-law-to-cyber-operations/

وبعبارة أخرى يجب تقسيم القانون الدولي إلى مجالات، والتحقق من أن القاعدة التي ستطبق على المجال السيبراني ليست مخصصة لمجال معين. ربما يكون صحيحا أن بعض القواعد (وهو الاستثناء) تخص مجالا معينا مثل القانون الدولي الإنساني الذي يطبق في وقت معين، وهو وقت النزاع المسلح أو قانون أعالي البحار الذي يفرض التزام الدول باحترام حرية الملاحة في أعالي البحار مما يقتصر على أعالي البحار وليس البحار الإقليمية الأخرى. لكن في حالة عدم وجود قيود على مجال معين أو نوع معين من النشاط، أو عندما يكون التعبير المستخدم لوصف القاعدة القانونية الدولية عاماً، فإن القاعدة تنطبق في كل وقت وفي كل مكان وعلى كل سلوك. فلا يوجد في القانون الدولي ما يشير إلى أنه يجب التأكد مما إذا كانت القاعدة تنطبق عبر "المجالات" كما يدعو نائب المدعي العام[1].

ثم إن الأنشطة عبر الإنترنت ليست غاية في حد ذاتها، ولكنها أداة لتحقيق أهداف، أو تأثيرات مختلفة تظهر عادة بطرق مختلفة، في واحد، أو أكثر من المجالات المادية التقليدية. مثلا القانون الدولي الإنساني يطبق وقت النزاع المسلح، وهو يحظر على الدول من أن توجه هجمات ضد المدنيين. بصرف النظر من أي فريق هم؟ واين موقعهم؟ ولا ماهية السلاح المستخدم، المهم ألا يتعرض المدنيين للأذى. فقد يتم تنفيذ التفجير بطرق القصف التقليدية وذلك غير مشروع، أو عن بعد بالطرق السيبرانية وسيظل الفعل غير مشروع بموجب قواعد القانون الدولي الإنساني. الوسيلة السيبرانية لا تحدث مجالاً جديداً، فهي أداة قادرة على تحقيق أضرار عسكرية، أو اقتصادية، أو حتى أدبية، والعبرة بنهاية الفعل السيبراني، وما تفضي إليه من خرق لأحد قواعد القانون الدولي وليس العبرة بالبداية، وإن كانت البداية باستغلال نقاط الضعف السيبراني بدلا من الإكراه أو القسر كما أشار Michael P. Fischerkeller فحتى الاستغلال ممنوع في القانون الدولي فهو غالباً ما يكون اعتداء على سيادة الدول، واحترام السيادة هو التزام قانوني مساو للالتزام بعدم التدخل في الشأن الداخلي. وهذا ما يمكن تطبيقه على التدخل في الانتخابات الأمريكية. في عام 2020. وقد أكدت الدول الأعضاء في الأمم المتحدة المشاركة في الفريق العامل المفتوح العضوية صراحةً أن التدابير الرامية إلى تعزيز سلوك الدولة المسئولة يجب أن

[1] Akande, D., Coco, A., & Dias, T. (2021, January 5). Old Habits Die Hard: Applying Existing International Law in Cyberspace and Beyond. Retrieved from https://www.ejiltalk.org/old-habits-die-hard-applying-existing-international-law-in-cyberspace-and-beyond/

تظل محايدة من الناحية التكنولوجية، أي تستوعب أي تكنولوجيا واي تقنيات مؤكدة القلق من إساءة الاستخدام، وليس التقنيات نفسها مما يوكد أن العبرة بالنتيجة التي تحققها الأدوات السيبرانية.[1]

لا ريب أنه لا يمكن إنكار أنه عند تطبيق القواعد العامة للقانون الدولي الحالي على الهجمات السيبرانية، قد يلزم بعض الربط والتعديل؛ لمراعاة بعض الميزات السيبرانية المحددة مثل السرعة والطبيعة العابرة للحدود ومجهولية المصدر. (وهذا ما سيم معالجته في الفصلين القادمين) ولا يمكن إنكار أن تخصيص قواعد قانونية للهجمات السيبرانية بشكل خاص قد ينطوي على بعض الفوائد، لكن حتى يحدث ذلك فإن نقطة البداية هي انطباق القانون الدولي القائم، وليس فراغ قانوني في هذه الظاهرة.

الحقيقة أن إطلاق كلمة "مجال" أو "بيئة استراتيجية" على الفضاء الإلكتروني، والتعامل معه على أنه جزء منفصل عن العالم المادي، وأنه يحتاج إلى قواعد قانونية منفصلة لتنظيمه أمر مستغرب. فالهجمات السيبرانية سواء أتم تنفيذها من قبل الدول أم الكيانات غير الحكومية؟ لا تحدث في فضاء افتراضي جديد. فهي تتكون بالضرورة من مكونات أو أجهزة مادية، مثل الكابلات، والأقمار الصناعية، وموجات الراديو، وأجهزة الكمبيوتر، وملايين دوائر السيليكون، بالإضافة إلى الأفراد الذين يبنون ويتحكمون ويستخدمون البرامج والأجهزة والبيانات[2]. بقدر ما تلعب المكونات غير المادية مثل البرامج والكود والبيانات من تأثير مهم في كيفية عمل المكونات المادية وتظل العمليات والأنشطة السيبرانية متأصلة إلى حد كبير في البنية التحتية المادية الملموسة حتى وإن عبرت الحدود الوطنية لإنشاء "مساحة معلومات عالمية" خيالية ، وإن تم تغليفها بمصطلحات مثل "السحابة" أو "شبكة الويب العالمية" أو "الواقع الافتراضي" "أو الفضاء السيبراني" فإن ذلك لا يفصلها عن حضورها المادي الموجود على إقليم معين تحت مسؤولية دولة معينة. لذلك قد يكون من الأفضل في المجال القانوني استخدام مصطلحات أكثر واقعية وأقل جدلا من الفضاء الإلكتروني مثل تكنولوجيا المعلومات والاتصالات[3].

في القانون الدولي – كما في القانون المحلي – حقيقة أن البشر قد طوروا تقنيات جديدة بمرور الوقت، مثل القطارات والسيارات وأجهزة التلفزيون والهواتف المحمولة[4] لا تعني أن هؤلاء ينشئون "مجالات" أو

---

[1] Open-ended Working Group (OWEG). (n.d.). *Second "Pre-draft" of the report of the OEWG on developments in the field of information and telecommunications in the context of international security*, para. 21, p. 4. Retrieved from https://front.un-arm.org/wp-content/uploads/2020/05/200527-oewg-ict-revised-pre-draft.pdf

[2] المرجع السابق – Akande, D., Coco, A., & Dias, T.

[3] المرجع السابق

[4] المرجع السابق

"بيئات استراتيجية" لا تخضع للقواعد أو المبادئ القانونية القائمة. وقد اعترفت محكمة العدل الدولية بهذا الأمر في فتواها بشأن الأسلحة النووية[1]. وبالمثل، أشارت لجنة القانون الدولي – في مشروع موادها بشأن منع الضرر العابر للحدود الناجم عن الأنشطة الخطرة – إلى أن التقنيات الجديدة تخضع أيضًا لواجبات إيجابية لمنع الضرر العابر للحدود[2]. إن تقرير فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي لعام 2013 أكد انطباق قواعد القانون الدولي الحالي على الفضاء السيبراني.[3] وتبنت الدول ذلك التقرير بقرار للجمعية العامة مما أعطاه قوة عرفية[4]. كل ذلك يؤكد أن القانون الدولي بصورته الحالية ينظم سلوك الدولة الذي يتم تنفيذه من خلال تكنولوجيا المعلومات والاتصالات، ويقع على عاتق أولئك الذين يدافعون عن استبعاد تكنولوجيا المعلومات والاتصالات من نطاقهم عبء تقديم أدلة على أن الدول في ممارساتها العامة بوصفها قانونا، قد نجحت في استنباط تكنولوجيا المعلومات والاتصالات[5].

أما الرأي القائل بالحاجة لاتفاقية خاصة تنصاع لها الدول بالرضا فلا يمكن مقابلته بالرفض – على حد سواء – للرأي القائل بعدم انطباق القانون الدولي على الهجمات السيبرانية. حتما إن وجود اتفاقية دولة تنظم سلوك الدول في الفضاء السيبراني هو الوضع المثالي؛ لأن المجتمع الدولي سوف يستفيد من تعريف واضح للهجوم السيبراني، وكذلك سوف يتم الاتفاق بشأن القضايا الحاسمة كإسناد الفعل السيبراني، وإمكانية الدفاع عن النفس ضد الفعل السيبراني، والالتزام باحترام القواعد السيبرانية. والأهم من ذلك آليات العمل الجماعي المتوقع أن تنتجها الاتفاقية لمواجهة الهجمات السيبرانية وهي بالفعل تحتاج إلى تعاون دولي. ولسوف تتعرض الدول لضغوط شديدة؛ لتنسيق أي آليات دفاع مع استجابة

---

[1] Legality of the Threat or Use of nuclear weapons, Advisory Opinion, I.C.J. Reports 1996, p. 226 [para. 39, p. 244; para. 86, p. 259]

[2] الأمم المتحدة، لجنة القانون الدولي، تقرير لجنة القانون الدولي إلى الجمعية العامة للأمم المتحدة عن أعمال دورتها الثالثة والخمسين، المجلد الثاني الجزء الثاني ((A/CN.4/SER.A/2001/Add.1 (Part 2)). https://legal.un.org/ilc/publications/yearbooks/arabic/ilc_2001_v2_p2.pdf
المسؤولية الدولية عن النتائج الضارة الناجمة عن أفعال لا يحظرها القانون الدولي (منع الضرر العابر للحدود الناجم عن أنشطة خطرة)، التعليق على المادة 3، الفقرة 4، ص197 والفقرة 11، ص199

[3] الأمم المتحدة، الجمعية العامة، *تقرير فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي: مذكرة من الأمين العام*، A/68/98 (24 يونيو 2013). استرجع من https://undocs.org/A/68/98
انظر: الفقرة 4 (ص6)، والفقرة 11 (ص8)، والفقرة 16 (ص9)، والفقرة 19 (ص9)

[4] قرار الجمعية العامة 68/243، *التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي*، A/RES/68/243 (27 ديسمبر 2013). استرجع من https://undocs.org/A/RES/68/243

[5] المرجع السابق – Akande, D., Coco, A., & Dias, T.

حقيقية متعددة الجنسيات[1]. كل تلك الأمور تعني مزيدا من الأمن في وجه التهديد السيبراني والاقتراب من احتواء هذه الظاهرة، لكن قبل ذلك لابد من توافر الإرادة السياسية؛ لإزالة العقبات.

إن روسيا من أكبر المؤيدين لوجود اتفاقية دولية تنظم سباق التسلح في الفضاء السيبراني، فمثلا في مناقشات فريق الأمم المتحدة العامل المفتوح العضوية لعام 2020 عبر ممثل روسيا أنه بدلاً من نفي انطباق أو كفاية القانون الدولي، المعاهدة هي الوسيلة الحاسمة لتوضيح كيفية تطبيق القانون الدولي الحالي على الفضاء السيبراني[2]. إلا أن مبادرات روسيا تقابل بالرفض من الدول الغربية؛ لأن لديهم مخاوف من إضافة قواعد قانونية لا تتماشى مع قواعد القانون الدولي، أو قواعد تغير من طبيعة الانترنت، وعلى وجه الخصوص المخاوف بشأن فرض قيود على التدفق الحر للمعلومات، أو المحتوى من خلال سيطرة حكومية أكبر[3] والحقيقة إن هذه المخاوف تتماشى مع توجه روسيا[4] الذي دائما ما يعطي أولوية للسيادة، حتى أن روسيا رفضت الانضمام إلى اتفاقية بودابست للجريمة السيبرانية لمخاوف متعلقة بالسيادة كما رفضت اعتبار القانون الدولي ينطبق بشكل تلقائي على الفضاء السيبراني؛ لمخاوف متعلقة بالسيادة والمساواة بين الدول[5].

---

[1] Moore, S. (2013). Cyber Attacks and the Beginnings of an International Cyber Treaty. *North Carolina Journal of International Law*, *39*(1), 223-257. Retrieved from https://scholarship.law.unc.edu/ncilj/vol39/iss1/7

[2] انظر بيان ممثل الاتحاد الروسي في المناقشة عبر الإنترنت بشأن "المسودة الأولية" الثانية للتقرير النهائي للفريق العامل المفتوح العضوية التابع للأمم المتحدة بشأن التطورات في مجال المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي (موسكو، 15 يونيو 2020)، انظر:

Open-Ended Working Group (OEWG). (2020, June). *Statement by the representative of the Russian Federation at the online discussion of the second "pre-draft" of the final report of the UN Open-ended Working Group on developments in the field of information and telecommunications in the context of international security* (Unofficial translation), pp. 3-4. Retrieved from https://front.un-arm.org/wp-content/uploads/2020/09/oewg-informal-virtual-meetings-statement-by-the-russian-federation-15-june-2020.pdf

[3] Korzak, E. (2021). Russia's Cyber Policy Efforts in the United Nations. *NATO Cooperative Cyber Defence Centre of Excellence, Tallinn Paper No. 11*. Retrieved from https://ccdcoe.org/uploads/2021/06/Elaine_Korzak_Russia_UN.docx.pdf

[4] المرجع السابق – ص17

الفهم الروسي لثورة المعلومات هو أنها تشكل في نهاية المطاف أداة تخريبية فيما يتعلق باستقرار النظام" فيمكن استخدام تدفق المعلومات كوسيلة للتأثير وتقويض النظام السياسي والاجتماعي للدولة. انظر:

Kurowska, X. (2019, December). *What does Russia want in cyber diplomacy? A primer*. Central European University, p. 12. Retrieved from https://eucd.s3.eu-central-1.amazonaws.com/eucd/assets/a4jdTSQp/13-kurowska_rif-final.pdf

[5] لم تكتف روسيا بعدم الانضمام لاتفاقية بودابست بسبب مخاوف متعلقة بالسيادة، بل تقود حاليا جهود دولية لصياغة اتفاقية جديدة تنظم نفس القضايا التي نظمتها اتفاقية بودابيست انظر:

ليس التوافق السياسي وحسب ما يشكل عقبة في التوصل لاتفاق سيبراني دولي، لكن هناك بعض الدول – وتوافقهم في ذلك الباحثة – ترى أن موضوع تكنلوجي متجدد كالهجمات السيبرانية لا يمكن أن يحصر في اتفاقية دولية لدواع عملية صرفه. مثلا، جمهورية التشيك تعارض التفاوض على صك قانوني جديد لمبدأين رئيسين:

أولهما: إن القانون الدولي القائم ينطبق على الفضاء السيبراني بأكمله. في الواقع، القانون الدولي الحالي يوفر لنا كل الأدوات اللازمة لمنع الصراعات الفعلية في المجال السيبراني. القضية على المحك ليست فجوة في القانون الحالي، ولكن الشأن هو الامتثال للقانون الحالي، والتوصل إلى فهم مشترك حول كيفية القيام بذلك لتطبيق القانون على بيئة اليوم[1].

ثانيهما: تعارض جمهورية التشيك التفاوض على صك قانوني جديد؛ لأن التطورات في تكنولوجيا المعلومات والاتصالات سريعة وديناميكية للغاية بحيث إن أي نتيجة محتملة لمثل هذا الجهد سيعفو عنها الزمن، وربما حتى قبل أن نصادق جميعًا على النتيجة. بدلا من ذلك، تفضل جمهورية التشيك تحقيق توافق قوي في الآراء بشأن تطبيق ديناميكي للقانون الدولي قادر على التكيف مع التطورات الجديدة[2] وفي ضوء عدم التوافق السياسي بخصوص صياغة اتفاقية دولية، فإنه يمكن القول إن أقوى مشروع قانون لتنظيم العمليات السيبرانية هو سلوك الدول وآراؤها وتصريحاتها عن كيفية تفسير القانون الدولي الحالي وتطبيقه في السياق السيبراني. فكلما توافقت الآراء وتكرر السلوك اقتربنا من قاعدة قانونية خاصة بالمجال السيبراني. فإذا كانت فكرة الاتفاقية الدولية سابقة لأوانها، يجب أن يتم التركيز على عملية تفسير المعايير الحالية للقانون الدولي على الهجمات السيبرانية.

Page, M. (2022, March 7). The hypocrisy of Russia's push for a new global cybercrime treaty. Retrieved from https://www.lowyinstitute.org/the-interpreter/hypocrisy-russia-s-push-new-global-cybercrime-treaty

[1] Mr. Richard Kadlčák Special Envoy for Cyberspace Director of Cybersecurity Department. (2020, February). *Czech Republic at the 2nd substantive session of the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security of the First Committee of the General Assembly of the United Nations*, p. 2. Retrieved from https://www.nukib.cz/download/publications_en/CZ%20Statement%20-%20OEWG%20-%20International%20Law%2011.02.2020.pdf

[2] المرجع السابق

الفصل الثاني

تطبيق قاعدة منع استخدام القوة والاستثناءات الواردة عليها في الميثاق على الهجمات السيبرانية

المبحث الأول: قاعدة منع استخدام القوة في القانون الدولي ومدى انطباقها على الهجمات الإلكترونية:

المطلب الأول: التطور التاريخي لقاعدة منع استخدام القوة في القانون الدولي.

المطلب الثاني: مدى خضوع الهجمات الإلكترونية لمبدأ حظر استخدام القوة.

المطلب الثالث: التمييز بين ما يدخل في نطاق المادة (4)2 وغيره من الهجمات الإلكترونية

المبحث الثاني: الدفاع عن النفس ضد الهجمات السيبرانية:

المطلب الأول: الدفاع عن النفس ضد الهجمات السيبرانية في صورته التقليدية.

المطلب الثاني: الأنواع التوسعية في الدفاع عن النفس، وانطباقها على الهجوم السيبراني.

المبحث الثالث: استخدام القوة من قبل مجلس الأمن.

الفصل الثاني

تطبيق قاعدة منع استخدام القوة والاستثناءات الواردة عليها في الميثاق على الهجمات السيبرانية

يهدف هذا الفصل إلى مناقشة قاعدة منع استخدام القوة واستثناءاتها في النطاق السيبراني. هذه القاعدة التي تمنع الدول من استخدام القوة في العلاقات الدولية ورد عليها استثناءان في ميثاق الأمم المتحدة. بمعنى أن هناك حالتين يمكن أن تُستَخدَم فيهما القوة في نطاق العلاقات الدولية بشكل مشروع وهما: الدفاع عن النفس، والقوة التي يستخدمها مجلس الأمن بموجب الفصل السابع من الميثاق.

تطبيق قاعدة منع استخدام القوة على الهجمات السيبرانية يعطي نتيجتين مهمتين: أولاهما: أن تكييف قاعدة منع استخدام القوة على الهجمات السيبرانية يعني عدَّها قوة محرمة بموجب ميثاق الأمم المتحدة. والثانية: إذا عدت الهجمات السيبرانية قوة محرمة وفق الميثاق فيترتب على استخدامها قيام الحق في الدفاع عن النفس ضدها. وهذه من أكثر الجوانب أهمية في عملية تقنين الهجمات السيبرانية في القانون الدولي. لأننا نتحدث عن إمكان الدفاع عن النفس تقليدياً كالقصف بالطائرات رداً على هجوم إلكتروني وقع على أجهزة الدولة.

سيناريو التصعيد هذا هو أكثر أمر مقلق في الهجمات السيبرانية الدولية؛ فإنه لا يمكن أن ينشأ الحق في الدفاع عن النفس ضد أي هجوم سيبراني يسير. لذلك لابد من الاتفاق على ما تعنيه القوة المحرمة المحركة لحق الدفاع عن النفس في نطاق الهجمات السيبرانية. كما ينبغي الاتفاق على طريقة الدفاع عن النفس وفق ضوابط الضرورة والتناسب بما يتلاءم مع طبيعة الهجمات السيبرانية.

لذلك يتكون هذا الفصل من ثلاثة مباحث **المبحث الأول** منها: قاعدة منع استخدام القوة المسلحة في القانون الدولي ومدى انطباقها على الهجمات الإلكترونية. و**المبحث الثاني:** الدفاع عن النفس ضد الهجمات السيبرانية المسلحة **وأما الثالث** فهو استخدام القوة من قبل مجلس الأمن. سيتم التوسع في المبحثين الأول والثاني، ومناقشة المبحث الأخير بإيجاز كما تمت الإشارة إليه في مقدمة البحث، فإن الهدف معالجة الهجمات السيبرانية خارج نطاق الأجهزة الدولية، ومن منظور الدولة، وتحديدا الدولة ضحية الهجوم السيبراني.

ينبغي تذكر أننا لا نُحْدِث قانونا خاصا للهجوم السيبراني، بل نسقط القانون الدولي الموجود على الحالة السيبرانية، وهذان امران مختلفان تماما. فإحداث قانون خاص بالهجمات السيبرانية يعني أن يتم تفصيل قواعد تتناسب مع خصائص الفضاء الإلكتروني. بينما تكييف الهجمات السيبرانية على القانون الموجود يعني الاكتفاء بالقواعد القانونية والالتزام بها كما هي؛ لضبط كل قدرات الهجمات السيبرانية واحتمالاتها. ولما كان الوضع الأول مستبعداً، لأنه يحتاج إلى معاهدة جديدة، تتفق عليها إرادة الدول، وهو أمر غاية في الصعوبة حاليا، فالخيار الوحيد هو تطبيق القانون الموجود على الهجمات السيبرانية، وهذا يعني الحذر من محاولة تغيير عناصر قاعدة قانونية لتتناسب مع الوضع السيبراني، والحذر من فرض معايير غير ملزمة وعدها ملزمة، والحذر من التقليل من شأن قاعدة ملزمة وإعطائها صفة تكميلية.

المبحث الأول

قاعدة منع استخدام القوة في القانون الدولي

ومدى انطباقها على الهجمات الإلكترونية

يؤكد Matthew C. Waxman أنه بالنظر إلى كفاية القانون الدولي الحالي؛ لتكييف الهجمات السيبرانية فإن المادة 2(4) من الميثاق هي مكان جيد للبدء؛ لأنه يؤسس أو يعكس المبادئ الأساسية التي يقوم عليها معظم القانون الدولي عامة[1]. المادة 2(4) هي التي تنص على قاعدة منع استخدام القوة في العلاقات الدولية.

يسعى مبدأ منع استخدام القوة إلى الحفاظ على العلاقات السلمية داخل مجتمع الدول من خلال وضع معايير صارمة فيما يتعلق بالوقت الذي قد تتجاوز فيه الدول التدابير غير العنيفة مثل الدبلوماسية والعقوبات الاقتصادية والتدابير المضادة. وتجدر الإشارة – خاصة – إلى الحق في القيام بذلك دفاعًا عن النفس عند مواجهة هجوم مسلح.

[1] Waxman, M. C. (2011). Cyber Attacks as "Force" under UN Charter Article 2(4). *International Law Studies, 87,* 43–57 [p. 43]. Retrieved from https://digital-commons.usnwc.edu/ils/vol87/iss1/5/

الحقيقة أن هذا البحث يتفق تماما مع هذه الفكرة، فكرة أهمية قاعدة منع استخدام القوة، وأنها البداية لتكييف أي ظاهرة جديدة يمكن أن تطرأ؛ لأنها الأساس والسبب الذي أنشأ من أجله النظام الدولي المعاصر. فالنظام الدولي الحالي أنشأ بوصفه نظاما بين الدول؛ لضمان عدم التصادم العنيف بين أصحاب السيادات ذات المصالح المختلفة[1]، فبعد أن كانت الدول تدخل حروبا طويلة؛ بسبب منطقة أو حدود متنازع عليها، جاء القانون الدولي بقاعدة منع استخدام القوة لترسي قاعدة قوية للسلم والأمن الدولي.

القول بأهمية قاعدة منع استخدام القوة وعدها نقطة البداية، لا ينفي أنها جزء من منظومة قواعد أخرى مثل تسوية المنازعات بالطرق السلمية، واحترام السيادة، وعدم التدخل في الشأن الداخلي. كل تلك القواعد وغيرها مرتبطة بعضها ببعض، وتؤدي جزءا مهما في النظام الدولي الحالي. لذلك تغطية الهجمات السيبرانية من ناحية قاعدة منع استخدام القوة يغطي جزءا من لغز تكييف الهجمات السيبرانية في القانون الدولي وليس كله[2]، لكن – كما تمت الإشارة إليه – هو الجزء الأهم، أو على الأقل هو نقطة البداية. وهذا المبحث وإن كان يعنى بقاعدة منع استخدام القوة بشكل أساسي، لكنه سيسقط بعض الضوء على القواعد الأخرى كقاعدة احترام السيادة، وقاعدة عدم التدخل في الشأن الداخلي، وواجب بذل العناية، وكيفية تطبيق تلك القواعد في نطاق الهجمات السيبرانية.

يبدأ المبحث بالتعريج على التطور التاريخي لقاعدة منع استخدام القوة في المطلب الأول منه، ثم يناقش مدى انطباق قاعدة منع استخدام القوة على الهجمات السيبرانية في المطلب الثاني، ثم التمييز بين ما يدخل في نطاق قاعدة منع استخدام القوة وغيره من الهجمات الإلكترونية في المطلب الثالث.

---

[1] London School of Economics. (2010, December 9). *Can International Law Change the World?* 32:00 [Video file]. Retrieved from https://youtu.be/gH8yIqcG13c?t=1920

[2] المرجع السابق

المطلب الأول

التطور التاريخي لقاعدة منع استخدام القوة في القانون الدولي

يهدف هذا المطلب إلى التعريف بقاعدة منع استخدام القوة قبل اسقاطها على الهجمات السيبرانية، وذلك عن طريق المرور بالجذور التاريخية لقاعدة منع استخدام القوة ثم تبلورها أكثر في عهد عصبة الأمم وصولا لصيغتها الحالية في ميثاق الأمم المتحدة.

أولى المحاولات التي وضعت لتنظيم اللجوء إلى الحرب ارتبطت بظهور مصطلح الحرب العادلة والحرب غير العادلة. ويعود أول ظهور لمصطلح الحرب العادلة إلى حقبة روما القديمة. إن تمييز الحرب العادلة هي محاولة دينية قام بها مجموعة كهنة يعرفون باسم "الأجنة"، وهم مجموعة من الكهنة الذين كانوا مسؤولين عن الحفاظ على العلاقات الداخلية والخارجية السلمية في روما القديمة، وأدى نشاطهم هذا إلى ظهور قانون الجنين (Ius Fetiale) وهو القانون الديني المتعلق بعملية إنشاء المعاهدات وتفسيرها وتطبيقها، فضلا عن اللوائح المتعلقة بإعلان الحرب. وكان من المتوقع أن تمر المداولات حول الحرب المحتملة من خلال هؤلاء الكهنة، الذين سيسعون أولا لمعرفة حكم الآلهة على عدالة الحرب[1]. ومعرفة ما إذا كان هناك خرق جسيم للسلام، قد حدث بالفعل، وهو المسوغ الوحيد لشن الحرب العادلة، ثم يحاولون التواصل مع الدولة أو المدينة المذنبة للمطالبة بالتعويض. فإذا لم يتم التوصل إلى حل مرضٍ بعد مدة زمنية معينة، فإنه يمكن أن تبدأ الحرب؛ تبعاً لما يصدره الكهنة في قرار عدالة الحرب من عدمها، وذلك على هيئة حكم قضائي، وهو لا يعني قيام الحرب، فوظيفة الحكم الوحيدة هي الفصل في مسألة ما إذا كان شن الحرب قراراً سليما أو غير صحيح، أما إعلان قيام الحرب (تنفيذ الحكم) فإنه سيكون عندئذ مسألة قرار جديد ، يصدره الملك أو مجلس الشيوخ.

ثم مع ظهور المسيحية تأثرت فكرة الحرب العادلة بعلماء اللاهوت المسيحيين مثل القديس أوغسطينوس والقديس توما الأكويني 1225 – 1274 ، فقد وضع الأخير ثلاثة معايير للحرب العادلة وهي[2]:

---

[1] Reichberg, G. M., Syse, H., & Begby, E. (Eds.). (2008). *The Ethics of War: Classic and Contemporary Readings* (1st ed.).

[2] رياحي، الطاهر. (2014). حظر استخدام القوة في العلاقات الدولية: بين شرعية النص ومشروعية الضرورة. التواصل في العلوم الإنسانية والاجتماعية، 38، 193–212. استرجع من https://www.asjp.cerist.dz/en/article/41790

- يجب أن تشن من قبل سلطة ذات سيادة بأمر من الملك. والمقصود هنا هو حظر شن حرب خاصة.
- يجب أن يكون لها سبب عادل مثل معاقبة المخالفين.
- يجب أن تكون القضية العادلة مصحوبة بالنية الصحيحة خدمةً الخير ودرءاً للشر.

لكن بعد قرابة أربعة قرون أخذ منهج الحرب العادلة يتراجع في أوروبا خصوصا بعد اتفاقية وستفاليا (Westphalia)[1] 1648 الذي ركز بقوة على فكرة السيادة، وكان سببا في ظهور مفهوم الدولة الوطنية[2]. وعلى ضوء الزيادة في ظهور الدول المستقلة في أوروبا تراجع المعيار الأخلاقي للحرب! فلم تعد الدول تجد نفسها في وضع يمكنها من الحكم على ما إذا كان سبب لجوء دولة أخرى إلى القوة عادلاً أم لا[3]. وقد دعم هذا النهج صعود المنهج الوضعي في القانون الدولي Positivism[4]، الذي يهمش النظرة الأخلاقية والدينية! ولا يعنى قانونياً إلا بالقرارات التي تصدر من سيادة، فإذا قررت دولة ذات سيادة اعلان الحرب، فذلك أمر قانوني! وهو المهم، أما الناحية الأخلاقية المتمثلة في كون الحرب عادلة أم لا فهي أمر غير ذي بال.

وبعد الحرب العالمية الأولى كان الهدف الرئيس من إنشاء عصبة الأمم تجنب حدوث[5] حرب عالمية ثانية، فقد أنشأ ميثاق عصبة الأمم بعض الالتزامات التي من شأنها أن تقلل من اللجوء إلى الحرب، وهي سابقة تاريخية أن تلتقي إرادة هذا العدد من الدول على التنازل عن حق اللجوء إلى الحرب، لكن ميثاق عصبة الأمم لم يستطع أن يمنع اللجوء إلى الحرب مطلقاً، بل كان في نصوصه ما يجعل اللجوء

---

[1] جلال يحي (2014) التاريخ الأوروبي الحديث والمعاصر حتى الحرب العالمية الأولى (الطبعة الثالثة). الإسكندرية: جمهورية مصر: المكتب الجامعي الحديث، ص32.

Kampmann, C. (2021). The Treaty of Westphalia as Peace Settlement and Political Concept: From a German Security System to the Constitution of International Law. In Marc Weller, M. Retter, & A. Varga (Eds.), *International Law and Peace Settlements* (pp. 64–85). Cambridge University Press. https://doi.org/10.1017/9781108627856.005

[2] The Open University. (2017). The use of force in international law. *University course*. Retrieved from https://www.open.edu/openlearn/society-politics-law/the-use-force-international-law/altformat-word

[3] المرجع السابق

[4] المرجع السابق

[5] والسبب في فشل عصبة الأمم في النص على قاعدة عامة صريحة بتحريم استخدام القوة مطلقاً بالرغم من آلام تجربة الحرب العالمية الأولى هو أن مسعى عصبة الأمم دائما ما يذكر بعيوبه الكثيرة فيما يتعلق بانعدام الإرادة الدولية الصادقة في تحقيق السلم الدولي، ومعاقبة الدول المنتصرة للدول المهزومة. كذلك فإن العصبة لم تكن عالمية بالقدر المطلوب؛ فأقصى ما وصل إليه عدد الدول الاعضاء هو ثمانية وخمسين، ثم بدأت بالانكماش بانسحاب دول مهمة كألمانيا وإيطاليا ناهيك عن روسيا والولايات المتحدة اللتين لم تنضمان للعصبة منذ البداية. وكان نتيجة ذلك أن دول المحور بدأت بتحدي قرارات العصبة، فكانت الحرب العالمية الثانية الدليل القاطع على فشل العصبة.

إلى الحرب حقا مشروعاً للدول، رغم أنه أخضع هذا الحكم لبعض القيود التي تعد جذوراً تأسيسية لقاعدة منع استخدام القوة الحالية[1].

كانت الحرب العالمية الأولى بعيدة عن بدء توظيف العمليات السيبرانية في الحروب، وبالتالي لم يتطرق ميثاق عصبة الأمم إلى أي ذكر لمثل تلك الظاهرة يسهم في تقنين الحرب السيبرانية. مع ذلك فإن الأسلحة المستخدمة في الحرب العالمية الأولى – وإن كانت تعد تقليدية في عالم اليوم – كانت في ذلك الوقت بمنزلة ثورات تكنلوجية فلأول مرة تستخدم الطائرات كأسلحة في الحروب[2] ولأول مرة تستخدم الأسلحة الكيميائية والغاز السام[3]. ولما كان القادة العسكريون كانوا بطيئين في تكييف استراتيجياتهم وتكتيكاتهم القديمة مع الأسلحة الجديدة لعام 1914 قتل الملايين من المدنيين دون ضرورة أو دون أن يكون موتهم مؤثرا في النصر أو الخسارة[4]! فما كان يعد تكنولوجيا جديدة في ذلك الوقت جعلت الحرب أكثر فظاعة وأكثر تعقيدًا من أي وقت مضى. مما جعل المزاج العام لميثاق عصبة الأمم هو تقييد اللجوء إلى الحرب.

وبرغم فشل عصبة الأمم في منع اللجوء إلى استخدام القوة مطلقا فإنه يعد أحد المحطات المهمة في تقنين اللجوء إلى القوة؛ فقد جاء بفلسفة جديدة في العلاقات الدولية تحد من السيادة المطلقة وترسم اطاراً من الشرعية حول اللجوء إلى القوة بعد أن كان حقا مطلقاً. وإن كان ميثاق العصبة لم يمنع الحرب فإنه يمكن القول إنه وضع خطوات غير مباشرة تساعد على حفظ السلم الدولي في نهاية المطاف وأظهر الامثلة على لمبادئ التي تطرق إليها ميثاق عصبة الأمم تمهيداً لتأسيس قاعدة منع

---

[1] يتجلى ذلك بوضوح في المادة 12 من ميثاق عصبة الأمم التي تنص على أنه: "يتفق أعضاء العصبة على أنه في حالة نشوء أي نزاع بينهم ــ من المحتمل أن يؤدي إلى القطيعة ــ فإنهم يعرضون الأمر إما للتحكيم، وإما إلى التسوية القضائية، أو للتحقيق من قبل المجلس، ولا يتفقون بأي حال من الأحوال على اللجوء إلى الحرب. إلى ما بعد ثلاثة أشهر من صدور الحكم من المحكمين أو الحكم القضائي أو تقرير المجلس. في أي حالة بموجب هذه المادة، يجب أن يصدر حكم المحكمين أو القرار القضائي في غضون مدة زمنية معقولة، ويجب أن يصدر المجلس قراره في غضون ستة أشهر بعد تقديم النزاع"
انظر: عصبة الأمم (1938) ميثاق عصبة الأمم، بما في ذلك التعديلات التي دخلت حيز النفاذ بتاريخ 1 فبراير 1938. استرجع من https://www.ungeneva.org/en/covenant-lon

[2] McLean, A. T. (1993). WWI: Technology and the weapons of war. In *Tar heel junior historian* (Vols. 32, No. 2, pp. 25–30). Raleigh, North Carolina: North Carolina Museum of History. Retrieved from https://digital.ncdcr.gov/digital/collection/p16062coll9/id/521069

انظر أيضا:

National Air and Space Museum. (2017, April 6). The Technology of World War I. Retrieved from https://airandspace.si.edu/stories/editorial/240-artist-soldiers-technology

[3] المرجع السابق

[4] المرجع السابق

استخدام القوة هي: عدم اللجوء إلى الحرب[1]ونزع السلاح[2]وتسوية المنازعات الدولية بالطرق السلمية[3] والأمن الجماعي.[4]

وبعد الحرب العالمية الثانية اكتشفت الإنسانية أبعادا جديدة لبشاعة الحرب!! وكانت إرادة الدول أكثر جدية لتجنب ويلات الحرب؛ لذلك نجحت الدول أخيراً في وضع مبدأ عدم اللجوء إلى القوة في العلاقات الدولية بوصفها قاعدة ملزمة في ميثاق الأمم المتحدة، إن الميثاق لم ينص على هذا المبدأ فحسب، بل وضع آلية للعمل به ولحمايته من أي خرق من قبل الدول.

ومن الواضح ميثاق أن الأمم المتحدة جعل من عدم اللجوء إلى الحرب هدفاً عاماً يحكم عمل جميع أجهزة الأمم المتحدة[5]. أما أهم ما يرسخ منع اللجوء إلى الحرب فهو قاعدة منع استخدام القوة المنصوص عليها في المادة 2(4) من الميثاق على النحو الآتي:

---

[1] انظر ديباجة ميثاق العصبة الذي ينص على أنه: "تتعهد الأطراف الموقعة في هذا الميثاق بالالتزام بعدم اللجوء إلى الحرب في حل المنازعات الدولية."
وانظر المادة 10 من ميثاق عصبة الأمم أن: "يتعهد أعضاء العصبة، باحترام سلامة أقاليم جميع أعضاء العصبة واستقلالها السياسي القائم والمحافظة عليه ضد أي عدوان خارجي وفي حالة وقوع عدوان من هذا النوع، أو في حالة وقوع تهديد، أو حلول خطر من هذا العدوان يشير المجلس بالوسائل التي يتم بها تنفيذ هذا الالتزام".

[2] انظر المادة 8 من ميثاق عصبة الأمم التي تحدثت عن خطة عمل لخفض التسلح الوطني إلى أدنى نقطة بوصفها عاملا مؤثرا في حفظ الأمن ونبذ إلى الجوء إلى الحرب، بالإضافة إلى آلية رقابة العصبة على صناعة الأسلحة، وتبادل الدول الأعضاء المعلومات الكاملة والصريحة حول حجم تسليحهم.

[3] انظر المواد 14 و15 من ميثاق العصبة، ويذكر أن آلية حل المنازعات تلك كانت فعالة للغاية في بعض الحالات. على سبيل المثال، في عام 1926 ، تفاوضت العصبة على حل سلمي للصراع بين العراق وتركيا حول محافظة الموصل، وفي أوائل الثلاثينات توسطت بنجاح في حل النزاع الحدودي بين كولومبيا وبيرو.
Getchell, M. (n.d.). The League of Nations (article). Retrieved from https://www.khanacademy.org/humanities/us-history/rise-to-world-power/us-in-wwi/a/the-league-of-nations

[4] انظر المادة 11 والمادة 16 من ميثاق عصبة الأمم:
Article 11: "Any war or threat of war, whether immediately affecting any of the Members of the League or not, is hereby declared a matter of concern to the whole League, and the League shall take any action that may be deemed wise and effectual to safeguard the peace of nations …"
Article 16: "Should any Member of the League resort to war in disregard of its covenants under Articles 12, 13 or 15, it shall ipso facto be deemed to have committed an act of war against all other Members of the League …"

[5] ويتجلى ذلك بوضوح من خلال أول عبارة كتبت في ديباجته وهي "نحن شعوب الأمم المتحدة وقد آلينا على أنفسنا أن ننقذ الأجيال المقبلة من ويلات الحرب". كذلك فقد ورد لفظ "حفظ السلم والأمن الدولي" أكثر من 25 مرة في فصولة المختلفة؛ فإنه لم يورده هدفاً عاماً فحسب، بل أدخله في وظائف أجهزتها المختلفة. ومن مؤشرات نهج تجنب الحروب نص الميثاق على آلية فض المنازعات بالطرق السلمية كما نص الميثاق على نزع السلاح.

"يمتنع أعضاء الهيئة جميعاً في علاقاتهم الدولية عن التهديد باستعمال القوة، أو استخدامها ضد سلامة الأراضي، أو الاستقلال السياسي، لأية دولة أو على أي وجه آخر لا يتفق ومقاصد الأمم المتحدة".

ومن هذا يتبين أن الميثاق نص صراحة على مبدأ حظر استخدام القوة، وبهذا أصبحت قوة المبدأ من قوة الميثاق الذي يسمو على ما عداه من التزامات دولية، كما أصبح التهديد بالقوة أو استخدامها أحد أهم مبادئ القانون الدولي المعاصر، والأهم من ذلك كله أنها اكتسبت قوة القاعدة القانونية الدولية الآمرة[1] Jus Cogen وهذا ينشئ التزامات قانونية غير عادية على الدول تجاه هذه القاعدة، وأهما أنه لا يمكن التذرع بأي ظرف لانتهاكها.

كذلك لم يكتف النص بتحريم استعمال القوة، بل حرم التهديد باستعمال القوة، فالتهديد باللجوء إلى القوة وإن كان مجرد تهديد فإنه يمكن أن يقوض السلم والأمن في العلاقات الدولية، وبالتالي فإنه من الجيد أن الميثاق تطرق إلى منع التهديد باستعمال القوة بين الدول. فإن كان من الجيد أن كلاً من التهديد والاستخدام يدخلان في مبدأ المنع فإنه – في الواقع العملي – الدول تهدد بعضها باستمرار، وتثار مسألة خرق المادة 2(4) عند الاستخدام الفعلي للقوة أكثر من التهديد بالقوة؛ مما يجعل بعض الكتاب يقللون من أهمية التهديد باستخدام القوة، برغم مساواته مع استخدام القوة من الناحية القانونية نظرياً[2]. ورغم ذلك – ومع ظهور الدفاع عن النفس الاستباقي – فإن منع التهديد في المادة 2(4) له قيمة مهمة وهي عدم إعطاء العذر لهذا النوع من الدفاع عن النفس.

وبالرغم من أن قاعدة منع استخدام القوة – التي تعد أهم ما بني عليه القانون الدولي وربما يعود إليها أكثر الفضل في استقرار النظام الدولي الحالي – فأنها ليست بالصلابة المطلوبة بسبب عدم التفصيل في أمور غاية في الأهمية في الواقع العملي أهمها:

أولاً: أنه يحرِّم استخدام القوة بين الدول الأعضاء في الأمم المتحدة، ولم يتطرق إلى مشروعية استخدام القوة داخل الحدود الوطنية. وربما يكون التحول الذي يشهده العالم من استخدام القوة في الحروب بين

[1] Helmersen, S. T. (2014). The Prohibition of the Use of Force as Jus Cogens: Explaining Apparent Derogations. *Netherlands International Law Review*, *61*(02), 167–193. https://doi.org/10.1017/s0165070x14001168

[2] Brownlie, I. (1991). *International Law and the Use of Force by States* (1st ed.), p. 250. Oxford, England: Clarendon Press.

الدول إلى استخدام القوة داخل الحدود الوطنية في الدولة الواحدة هو نتيجة النقص في تحريم توجيه القوة داخل الحدود الوطنية وفق ضوابط محددة.

ثانياً: أن النص جاء بلفظ القوة مطلقاً ولم يحدد ما المقصود بها؟ فهناك القوة المسلحة بمفهومها التقليدي، وهناك أنواع أخرى من القوة، كالقوة الاقتصادية والتي تشمل المقاطعة والعقوبات الاقتصادية، وهناك القوة السياسية، وتشمل قطع العلاقات الدبلوماسية، وحملات الدعاية السياسة الموجهة ضد دولة ما، فأي نوع هو الممنوع على الدول؟ ولا شك أن هذا قصور كبير في قاعدة منع استخدام القوة وهو وثيق الارتباط بموضوع الدراسة، فأكثر سؤال يتكرر في جوهر نقاشات الهجمات الإلكترونية هو ما معنى القوة المقصودة في المادة 2(4)؟ وهل الهجمات الإلكترونية العدوانية يمكن أن تدخل في نطاق هذا المعنى؟

فلو عُرِّفَت القوة الممنوعة بوسيلتها أو بهدفها أو بأثرها لكانت حدود السلوك العدواني الدولي أكثر وضوحاً، ولربما أدى ذلك إلى استقرار أكبر في العلاقات الدولية، ولو تم التوسع في بيان نوع القوة الممنوعة لتشمل كل ما يمكن أن يستجد من مسببات عدم الاستقرار بين الدول ومنها الهجمات الإلكترونية، لكان أجدر.

المطلب الثاني

مدى خضوع الهجمات الإلكترونية لمبدأ حظر استخدام القوة.

بعد أن تم عرض قاعدة منع استخدام القوة وصولاً لصورتها الحالية في ميثاق الأمم المتحدة، وتأكيد أن قاعدة منع استخدام القوة هي حجر الأساس الذي يستند عليه القانون الدولي، فإنه من المنطقي يليه الكلام على تكييف الهجمات الإلكترونية بربطها بمنظومة منع استخدام القوة في ميثاق الأمم المتحدة، والنظر في مدى خضوعها له. ولمعرفة هل يسمح الميثاق أن يُرتكب ضررٌ جسيمٌ في الفضاء الإلكتروني دون أن تكون له القدرة على التدخل لتجريمه جب معرفة ما إذا كانت السلطات التأسيسية لميثاق الأمم المتحدة صاغت الميثاق مراعاةً للحرب التقليدية فقط؟ أم يجب أن تنطبق على مثل هذا السلوك؟

صحيح أن الميثاق كتب في 1945 بعد الحرب العالمية الثانية، وكان منع الدول من استخدام القوة هو هدفه الأساسي لكن من الواضح من المصطلحات المستخدمة فيه أن النص لم يكتب بهدف منع

الهجمات الإلكترونية في ذلك الوقت، بل كان المقصود هو الاستخدام التقليدي للقوة بل والتقليدي جدا وهو التقاء جيشين أو أكثر.

مع ذلك فإن الميثاق هو القانون الموجود الذي يمكن تطبيقه على الهجمات الإلكترونية، وحتى يتوافر القانون المتخصص في الحرب السيبرانية فإن الميثاق هو ما يجب أن يطبق عليها. فلا خلاف أنه أقوى وثيقة صاغت القانون الدولي المعاصر تلتزم به جميع دول العالم، والالتزامات الواردة فيه تسمو على ما عداه[1].

ونقطة البداية لتطبيق قاعدة منع استخدام القوة المنصوص عليها في الميثاق على الهجمات الإلكترونية هي تحديد المقصود بالقوة، وهل هي قوة السلاح فقط أم أنه من الممكن أن تتسع لتشمل القوة السيبرانية؟ وبما أن الميثاق – على النحو المشار إليه – لم يعرف القوة الممنوع استخدامها بين الدول في علاقاتها سيتناول هذا المطلب إمكان أن تكون الهجمات السيبرانية مشمولة بقاعدة منع استخدام القوة، وذلك في أربعة فروع: الفرع الأول من هذا المطلب سينظر إلى ذكر القوة في مواقع مختلفة من الميثاق وما إذا جاء معرفا بقوة السلاح، أو مطلقاً بأي نوع من القوة. أما الفرع الثاني فإنه يعالج إمكانية قياس الهجمات السيبرانية بأنواع مختلفة من القوة غير العسكرية، مثل الضغوط السياسية والاقتصادية والنظر إلى كيفية تعامل الميثاق معها، وهل هي مشمولة بقاعدة منع استخدام القوة أم لا؟ في الفرع الثالث سيتم النظر في إمكان الاكتفاء بقاعدة عدم التدخل في تقنين الهجمات السيبرانية بدلا من قاعدة منع استخدام القوة. وأما في الفرع الرابع سيتم قياس الهجمات السيبرانية على أسلحة مشمولة بقاعدة منع استخدام القوة وهي الأسلحة الكيميائية والبيولوجية.

الفرع الأول: مدى عد الهجمات السيبرانية في حكم القوة بالنظر إلى ذكر القوة في المواد المختلفة من الميثاق

تحظر المادة 2(4) – عامة – استخدام القوة إلا في حالة الدفاع عن النفس، أو عندما يأذن بها مجلس الأمن التابع للأمم المتحدة. لمعرفة ماذا يقصد الميثاق بالقوة في المادة 2(4) يمكن النظر إلى ذكر

[1] تنص المادة 103 من ميثاق الأمم المتحدة على أنه: "إذا تعارضت الالتزامات التي يرتبط بها أعضاء "الأمم المتحدة" -وفقاً لأحكام هذا الميثاق- مع أي التزام دولي آخر يرتبطون به فالعبرة بالتزاماتهم المترتبة على هذا الميثاق".
انظر أيضا:
Liivoja, R. (2008). The Scope of the Supremacy Clause of the United Nations Charter. *International and Comparative Law Quarterly*, *57*(3), 583–612. https://doi.org/10.1017/s0020589308000389

مصطلح القوة الوارد في أماكن أخرى من الميثاق؛ لكي يتأكد نطاق القوة المقصودة وهل هي القوة العسكرية وحسب؟ أم أنها مطلقة تشمل جميع أنواع الضغط والإكراه بما في ذلك الهجمات السيبرانية. وقد ذكر لفظ القوة في ست مواضع فقط نذكرها تباعا:

ـ أولاً: جاء ذكر مصطلح القوة في الديباجة، لكنه كان مقرونا بالقوة المسلحة على وجه التحديد كما يأتي:

"وأن نكفل بقبولنا مبادئ معيّنة ورسم الخطط اللازمة لها ألاّ تستخدم القوة المسلحة في غير المصلحة المشتركة"

فالديباجة تقصد القوة التقليدية وهذا ما يؤكده مطلع الديباجة الذي يتحدث عن نبذ الحرب وعدم تكرار ما مرت به البشرية من الحربين العالميتين، مما يرجح أن هدف الميثاق مقتصر على تقييد استخدام قوة السلاح وليس أي نوع آخر من القوة كالقوة السيبرانية.

ـ ثانياً: المادة (4)2 قد ذكرت لفظ القوة مطلقا على النحو الآتي:

"يمتنع أعضاء الهيئة جميعاً في علاقاتهم الدولية عن التهديد باستعمال القوة أو استخدامها"

ـ ثالثا: المادة 41 من الميثاق وهي تتحدث عما يتخذه مجلس الأمن من أعمال في حالات تهديد السلم ووقوع العدوان وجاء مصطلح القوة مقترنا بالقوة المسلحة على نحو ما يأتي:

"لمجلس الأمن أن يقرر ما يجب اتخاذه من التدابير التي لا تتطلب استخدام القوة المسلحة لتنفيذ قراراته، وله أن يطلب إلى أعضاء "الأمم المتحدة" تطبيق هذه التدابير، ويجوز أن يكون من بينها وقف الصلات الاقتصادية والمواصلات .... وقطع العلاقات الدبلوماسية."

تؤكد المادة 41 تحديد القوة بالسلاح، ويزيد من ذلك التأكيد بأنها تضع القوة المسلحة في فقرة منفصلة عن كل التدابير الأخرى التي من الممكن أن يتخذها مجلس الأمن، فكأنما هناك تأكيد ضمني أن السلاح يعد قوة وكل ما عدا مما أسماه الميثاق "تدابير" ضاغطه لا يعد قوة.

ـ رابعا: المادة 44 أيضا في الفصل السابع وتبين ما يتخذه مجلس الأمن من أعمال في حال تهديد السلم والأمن، لكن القوة لم تقترن بالسلاح مباشرة إلا أن السلاح ذكر في موضعين في المادة نفسها كما يأتي:

"إذا قرر مجلس الأمن استخدام القوة، فأنه قبل أن يطلب من عضو غير ممثل فيه تقديم القوات المسلحة وفاءً بالالتزامات المنصوص عليها في المادة 43، ينبغي له أن يدعو هذا العضو إلى أن يشترك إذا شاء في القرارات التي يصدرها فيما يختص باستخدام وحدات من قوات هذا العضو المسلحة"

كما يتبين من النص فإن لفظ القوة – وإن لم يقترن بالسلاح مباشرة – المقصود به هو قوة السلاح لا غير لأن المادة 44 تنظم استخدام مجلس الأمن للقوات المسلحة من غير أعضائه، والنص بعيد كل البعد عن احتواء أنواع أخرى من القوة سوى وحدات من الجيش. مما يؤكد نهج الميثاق بأن ذكر مصطلح القوة عادة ما يقصد به قوة مسلحة.

ـ خامسا: المادة 46 تقع تحت الفصل السابع وهي من أوضح الأمثلة على أن القوة المقصودة في الميثاق هي القوة المسلحة فإنه يقترن فيها لفظ القوة بالسلاح مباشرة كما يأتي:

"الخطط اللازمة لاستخدام القوة المسلحة يضعها مجلس الأمن بمساعدة لجنة أركان الحرب"

ـ سادسا: المادة 51 أيضا تقع تحت الفصل السابع، وهي تتحدث عن الدفاع عن النفس، وسوف يتم تناول المادة 51 بالتفصل في موضع لاحق وحسبنا أن نذكر هنا أن مصطلح القوة أقترن بالسلاح مباشرة على النحو الآتي:

"ليس في هذا الميثاق ما يضعف أو ينتقص الحق الطبيعي للدول، فرادى أو جماعات، في الدفاع عن أنفسهم إذا اعتدت قوة مسلحة على أحد أعضاء الأمم المتحدة"

يتبين إذن، أن الميثاق لم يعرف القوة المقصودة في المادة (4)2 لكنه في خمس مواضع من أصل ستة ذكر فيها لفظ القوة مقصوداً به القوة المسلحة، مما يرجح أن قاعدة منع استخدام القوة المذكورة في

المادة 2(4) تقتصر على القوة المسلحة، أما أنواع القوة الأخرى (كالهجمات السيبرانية) فهي ليست ممنوعة بموجب المادة 2(4) وإن كانت اعتداء على سلامة الأراضي أو الاستقلال السياسي للدول[1].

وخلافاً لما تقدم يمكن أن يقال: إذا كان كل لفظ آخر للقوة في الميثاق قد أقترن بالقوة المسلحة ماعدا المادة 2(4) ذلك؛ لأنها تختلف في نوع القوة، فلا يمكن أن يكون تحديد القوة المسلحة قد سقط سهوا في صياغة ميثاق الأمم المتحدة، بل هو مقصود خصوصاً أن الهدف العام للمادة 2(4) هو تقييد اللجوء إلى القوة، فمن الطبيعي أن يترك لفظ القوة مطلقا لكي يتسع تحريم السلوك العدواني في العلاقات الدولية ويواكب ما يستجد من أدوات تهدد السلم الدولي مثل الهجمات السيبرانية. أما في المواضع الأخرى من الميثاق فهو التزام إيجابي حيث المواد تهدف لتبيان متى وأين تستخدم القوة بشكلها المشروع لذلك من الطبيعي أن تصف بدقة نوع القوة حتى لا يتصاعد بما لا يتناسب مع الموقف. أي من المنطقي التوسع عند تحريم استخدام القوة والتضييق عند الحديث عن السماح باستخدامها.

مع ذلك، بالنظر للنهج الذي عملت به الأمم المتحدة بعد الميثاق يتأكد ان المقصود بقاعدة منع استخدام القوة هو القوة المسلحة، ففي الممارسة الدولية السائدة للدول فقط الحوادث التي تنطوي على استخدام القوة العسكرية تقع تحت حظر استخدام القوة وبالتالي يتأكد أن المقصود انصرف إلى القراءة الضيقة لنص المادة 2(4)[2].

---

[1] للمزيد حول الرأي الذي يرى بالتفسير الضيق لمعنى القوة في الميثاق، انظر:

Dinniss, H. H. (2014). Cyber Warfare and the Laws of War (Cambridge Studies in International and Comparative Law, Series Number 92) (Illustrated ed.). Cambridge: Cambridge University Press, p. 41.

انظر أيضا:

Goldsmith, J. (2013). How Cyber Changes the Laws of War. *European Journal of International Law*, *24*(1), 129–138 [pp. 133-135]. https://doi.org/10.1093/ejil/cht004

[2] Wessendorf, N., Simma, B., Khan, D., Nolte, G., & Paulus, A. (Eds.). (2012). The Charter of the United Nations: A Commentary (Oxford Commentaries on International Law). In *Oxford Commentaries on International Law* (3rd ed., Vol. 1). Oxford, United Kingdom: OUP Oxford. https://doi.org/10.1093/law/9780199639762.001.0001

انظر: التعليق على المادة 2(4)، الفقرة 19

الفرع الثاني: قياس الهجمات السيبرانية على القوة الاقتصادية والسياسية

للرد على نوع القوة المقصود في المادة 2(4) وإمكان أن يستوعب الهجمات الإلكترونية، يمكن مضاهاة القوة السيبرانية بأنواع أخرى من القوة غير المسلحة الموجودة في ذلك الوقت وتحليل موقف المادة 2(4) منه. فالقوة الاقتصادية والقوة السياسية من الوسائل التي كانت الدول تستخدمها في العام 1945. تلك الوسائل ليست قوة تقليدية عسكرية لكنها تشترك معها في معنى الإكراه والقسر. فكيف تعامل القانون الدولي معها حتى يمكن الاستفادة منه في الهجمات السيبرانية.

المقصود بالقوة الاقتصادية إجراء دولي قسري يقتضي وقف الاتصال والتجارة وما إلى ذلك مع دولة انتهكت القانون الدولي، وهذا ما يستخدم كعقوبةً أو إجراءً تأديبياً لإحداث تغيير إيجابي[1] أما القوة السياسية فتتمثل في قطع العلاقات الدبلوماسية واستخدام الخطاب المعادي وحملات دعائية للتشويه ضد دولة ما[2].

وقد نص ميثاق الأمم المتحدة فقد نص على قطع الصلات الاقتصادية والدبلوماسية وأسماها بالتدابير التي يمكن أن يتخذها مجلس الأمن قبل اللجوء إلى القوة، فهي مشروعة في ظل الفصل السابع لمجلس الأمن أما الاستخدام الفردي من قبل الدول فلم ينص عليه الميثاق.

كان هناك نقاش في الأعمال التحضيرية للميثاق حول إضافة هذه النوع من الضغوطات بوصفه نوعاً من القوة الممنوع استخدامها بين الدول في المادة 2(4) فقد كانت بعض الدول ترغب في اضافت الضغوطات الاقتصادية بوصفها نوعاً من القوة، مثل المقترح الذي قدمه ممثل البرازيل[3] لكن لم تتم الموافقة عليه، ورفضه غير مسبب.[4] وهناك من الفقه ما يسوغ سبب عدم تأييده؛ ذلك أنه إذا امتد حكم المادة 2(4) ليشمل أشكالًا أخرى من القوة، فستترك الدول بلا وسائل الضغط على الدول الأخرى التي

---

[1] طاع، زهيرة. (2019). العقوبات الاقتصادية كأداة سياسية في العلاقات الدولية "العراق نموذجا ". مجلة المفكر للدراسات القانونية والسياسية، 2(2)، 148–164 [ص150-151]. استرجع من https://www.asjp.cerist.dz/en/article/123345

[2] وكذلك هناك نوع آخر من القوة الذي كان ممارسا بين الدول في مرحلة ما بعد الميثاق وهو القوة الثقافية. للمزيد انظر:
Curtin, P. A., & Gaither, K. T. (2007). *International Public Relations: Negotiating Culture, Identity, and Power* (1st ed.), p. 235ff. SAGE Publications. https://doi.org/10.4135/9781452224817

[3] لمثال أوضح عن التوسع في منع القوة يشمل أيضًا الإكراه الاقتصادي انظر المادة 19 من ميثاق منظمة الدول الأمريكية 1967:
The Use of Nonviolent Coercion: A Study in Legality under Article 2(4) of the Charter of the United Nations. (1974). *University of Pennsylvania Law Review*, *122*(4), 983–1011 [p. 994]. Retrieved from https://scholarship.law.upenn.edu/penn_law_review/vol122/iss4/13

[4] المرجع السابق

تنتهك القانون الدولي وستكون هذه النتيجة غير مقبولة بالنظر إلى الحالة الراهنة للقانون الدولي، لأنه لا يضمن الامتثال للقانون بشكل فعال من خلال الهيئات الدولية[1]. الخلاصة أن إرادة الدول اجتمعت على عدم التوسيع في نطاق القوة الممنوعة ولا يعني ذلك أن الضغوط الاقتصادية والسياسية خيار مشروع دون قيود بين الدول، فالتطبيقات العملية في ظل الأمم المتحدة عالجت الضغوط الاقتصادية والسياسية من زوايا قانونية مختلفة كأن تدخل في مبدأ عدم التدخل أو الاخلال باتفاقيات دولية[2].

هذا الاستنتاج أكده إعلان العلاقات الودية الذي تبنته الجمعية العامة في 24 أكتوبر 1970 الذي يحتوي على تفسير لمبادئ الميثاق الأساسية[3]. وفي تفسير المبدأ الذي يوجب على الدول الامتناع عن التهديد، أو استخدام القوة في علاقاتها الدولية نجد أن الإعلان يتناول فقط القوة العسكرية. ثم في موضع أخر ينص الإعلان على مبدأ عدم التدخل في الأمور الواقعة ضمن الولاية القضائية المحلية لدولة أخرى وفي سياق هذا المبدأ ينص الإعلان على ما يلي:

"لا يجوز لأي دولة استخدام أو تشجيع استخدام التدابير الاقتصادية أو السياسية أو أي نوع آخر من التدابير لإكراه دولة أخرى".

من خلال هذا النص يمكن تأكيد أن نطاق المادة 2(4) هو القوة العسكرية، وأن أنواع القوة الأخرى تدخل تحت مبدئ عدم التدخل أو مبادئ أخرى في القانون الدولي[4]. أيضاً يتكرر الأمر في اعلان الجمعية العامة عام 1987 بشأن فعالية مبدأ الامتناع عن التهديد باستخدام القوة أو استعمالها في العلاقات الدولية، فكان الإعلان امتداداً لمنهج المادة 2(4) فقد ربط القوة بالسلاح وأما وسائل الإكراه والضغوط الاقتصادية السياسية فقد الحقها بمبدأ عدم التدخل.[5]

---

[1] المرجع السابق – Wessendorf, N., et al. – التعليق على المادة 2(4) – الفقرة 18

[2] داوود، محمود. (نوفمبر، 1993). مبدأ حظر استخدام القوة في العلاقات الدولية: دراسة مقارنة بين الشريعة الإسلامية والقانون الدولي العام (رسالة ماجستير)، ص248. القاهرة، مصر: جامعة الأزهر.
انظر أيضا: المرجع السابق – التعليق على المادة 2(4)، الفقرة 19

[3] قرار الجمعية العامة رقم 2625، *اعلان مبادئ القانون الدولي المتعلقة بالعلاقات الودية والتعاون بين الدول وفقا لميثاق الأمم المتحدة*، A/RES/2625(XXV) (24 أكتوبر 1970). استرجع من https://www.undocs.org/A/RES/2625(XXV)

[4] المرجع السابق – Wessendorf, N., et al. – التعليق على المادة 2(4) – الفقرة 19

[5] قرار الجمعية العامة رقم 42/22، *إعلان زيادة فعالية مبدأ الامتناع عن التهديد باستعمال القوة أو استعمالها في العلاقات الدولية*، A/RES/42/22 (17 مارس 1988). استرجع من https://legal.un.org/avl/ha/ga_42-22/ga_42-22.html
انظر أيضا:

عندما بدأ النقاش حول الحرب الإلكترونية وتكييف الهجمات السيبرانية على المادة 2(4) ليشمل الهجمات السيبرانية بدأ الكُتاب بقياس القوة الاقتصادية والسياسية على الهجمات السيبرانية فرأوا أن القوة الاقتصادية والسياسية تشترك مع القوة العسكرية في عنصر الإكراه أو القسر لحمل الدولة على فعل معين لكنها لم تضاف للمادة 2(4) لأنها ذات طبيعة غير حركية، فربطوا بين ما يعد قوة وما هو حركي "Kinetic"، ذلك لأن الحركة أظهر سمات العمليات العسكرية التي عادة ما تكون حركية ديناميكية غير ثابتة.[1] فالإكراه الدبلوماسي والاقتصادي لا يعد قوة وفقا للمادة 2(4) لأنه ليس عملا حركيا، مثل العمليات العسكرية. ثم إذا ما قيست التكنلوجيا متمثلة في الهجمات السيبرانية والضغط الاقتصادي والسياسي نجدهما يتشابهان في أن كليهما غير حركي، لذلك وبرغم توافر عنصر الإكراه في العمليات السيبرانية إلا أنها لا تدخل في قاعدة منع استخدام القوة لانتفاء صفة الحركة[2].

يتضح هنا أن فريقا من الفقهاء حرص على إخراج الهجمات السيبرانية من نطاق المادة 2(4)؛ وذلك لأنه يرى أن الضرر الذي يأتي من تقنين الهجمات السيبرانية في المادة 2(4) أكبر بكثير من الفائدة المتمثلة في ضبط الهجمات الإلكترونية[3]. فخرق المادة 2(4) هو المحرك لصلاحيات مجلس الأمن تحت الفصل السابع، ومثل هذا المستوى من التحرك الدولي لمجلس الأمن يجب أن يرتبط بالأمور الأكثر جدية مثل الهجوم المسلح من دولة على دولة، أما إذا عُدَّت الهجمات الإلكترونية داخله في مفهوم استخدام القوة في المادة 2(4)، ففيه استنزاف لآلية مجلس الأمن في الفصل السابع[4].

كذلك هناك خطورة التصعيد، فخرق المادة 2(4) هو المحرك لحق استخدام الدفاع الشرعي، فالميثاق يمنع استخدام القوة بين الدول إلا إذا كان رداً على دولة بدأت باستخدام القوة. فإذا عُدَّت الهجمات السيبرانية استخداما للقوة، فهذا سيعطي الدولة التي تم الهجوم عليها الحق في أن ترد بالقوة أيضا وقد تختار ألا ترد بالقوة نفسها أي بالهجمات الإلكترونية، بل قد ترد بالقوة العسكرية التقليدية، مما يفتح

Green, J.A. (Ed.). (2016). *Cyber Warfare: A multidisciplinary analysis: Routledge Studies in Conflict, Security and Technology* (1st ed.), pp. 102-104. Routledge.

[1] عويس، شيماء. (2018). القوة في العالقات الدولية: دراسة تأصيلية. المعهد المصري للدراسات، ص5.

[2] Buchan, R. (2012). Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions? *Journal of Conflict and Security Law*, *17*(2), 212–227 [p. 217]. https://doi.org/10.1093/jcsl/krs014

[3] Waxman, M. C. (2011b). Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4). *The Yale Journal of International Law*, *36*, 421–459 [pp. 426-430]. Retrieved from https://openyls.law.yale.edu/handle/20.500.13051/6629

[4] من أظهر المدافعين عن هذا الرأي هي الكاتبة Mary Ellen O'Connell فإنها تحذر من السماح أن يكون الفضاء الإلكتروني مجالا للحرب.

انظر: المرجع السابق – O'Connell, M. E. – ص198-203

انظر أيضا: المرجع السابق – Green, J. A. – The International Court of Justice – ص115

المجال لتصعيد غاية في الخطورة، خصوصا إذا ما وضعنا في عين الاعتبار الطبيعة المجهولة للهجمات الإلكترونية، فحتى اليوم لا يمكن معرفة المتسبب فيها بشكل قطعي، وإن عرفت الدولة المصدر التي خرجت منها تلك الهجمات فهذا لا يعني بالضرورة أن تكون الدولة المصدر هي التي بدأت الهجوم[1]. فاعتبار الهجمات السيبرانية منطبقة على المادة 2(4) يضع المجتمع الدولي أمام خطر التصعيد، وخطر إدخال جهات غير مسؤولة عن الاعتداء.

وأخيرا فإن المحافظة على سلامة المادة 2(4) يستدعي ألا تُربط بمفهوم جديد ومختلف فيه مثل الهجمات السيبرانية. فالمادة 2(4) – كما أشرنا إليها – حجر الأساس الذي يقوم عليه القانون الدولي المعاصر، وتم التوصل إليها بعد معاناة البشرية في الحروب منذ بدء التاريخ وحتى العام 1945. لذلك تجب المحافظة على وضوحها وقطعيتها، وذلك بحفظها لأبشع وأخطر الجرائم وهو العدوان العسكري المسلح ولا يستثني من استخدام القوة المسلحة إلا تحرك مجلس الأمن تحت الفصل السابع، والدفاع المشروع عن النفس. خصوصا أن الغالبية العظمى من الفقه تتفق أن قاعدة منع استخدام القوة في المادة 2(4) تعد قاعدة دولية آمرة[2].

ويمكن الرد على تلك الآراء التي تدعو إلى عدم عدِّ الهجمات الإلكترونية قوة تحت المادة 2(4) بأن هذه الأسباب أغلبها يعتمد في حجيتها على التحجيم من خطورة الهجمات الإلكترونية، لكن ماذا لو كانت من الخطورة بحيث تحتاج إلى أن تعالج بنص له قوة مثل المادة 2(4). فلو أن الهجوم على إيران أدى إلى انصهار المفاعل النووي، فإن ذلك سيقتل آلاف الأشخاص في المناطق المأهولة بالقرب منه، أو لو أن الهجوم على إستونيا مثلا لم يسبب شللا في المواصلات فقط، بل تم تغيير أنظمة التوجيه الخاصة بمراقبة الحركة الجوية؛ مما أدى إلى إسقاط عدد من الطائرات وخسائر في الأرواح. فإذا قلنا إن المادة 2(4) يجب أن تحفظ للمواقف الأكثر جدية، مثل أن توجه دولة سلاحها ضد دولة أخرى فعندئذ لا يمكن أن نستثني الهجمات الإلكترونية من ذلك؛ لأن بعضها له الآثار نفسها التي تسببها القوة العسكرية، وأحياناً تكون أكثر تدميرا. وإن لم يحدث سيناريو مشابه بعد، إلا أن الهجوم السيبراني الذي وقع على محطة الطاقة النووية في إيران يبين أن توجه الهجمات الإلكترونية ذاهب بهذا الاتجاه. وعليه لا بد من تأكيد من ضرورة إدخال الهجمات السيبرانية في نطاق المادة 2(4).

---

[1] المرجع السابق – ص116

[2] المرجع السابق – The International Court of Justice – Green, J. A. – ص98-99

الفرع الثالث: معالجة الهجمات الإلكترونية في ظل قاعدة عدم التدخل في الشؤون الداخلية للدول الأخرى.

يرى Russell Buchan أن قاعدة منع استخدام القوة قد أخذت أكبر من حجمها في النطاق السيبراني؛ لأنه خلافا لهجوم Stuxnet فإن الهجمات على إستونيا وجورجيا بل وأغلب الهجمات التي حدثت والتي تحدث لا تدخل في نطاق المادة 2(4). لذلك يجب ان يتحول التركيز على مبدأ عدم التدخل[1].

فإذا كان مبدأ منع استخدام القوة محددا حصرا بالقوة المسلحة فيمكن الاتجاه إلى مبدأ أكثر اتساعاً في منع كل وسائل الضغط والإكراه وهو مبدأ عدم التدخل[2]. وهذا المبدأ موجود في أكثر من موضع، فهو موجود جزئيا في المادة 2(7) من الميثاق، التي تنص على منع الأمم المتحدة من التدخل في الأمور التي تعد من صميم السلطان الداخلي للدول، ماعدا إذا كان مجلس الأمن يمارس صلاحياته في حفظ السلم والأمن. أما الصورة الأوسع لمبدأ عدم التدخل – وفيها تقوم الدول منفردة باستخدام الضغط، أو الإكراه سياسيا، أو اقتصاديا، أو ثقافيا في دولة أخرى – فإن جذورها موجودة في القانون الدولي العرفي،[3]وقد نصت علية قرارات الجمعية العامة للأمم المتحدة في إعلان العلاقات الودية 1970، صحيح أنه لم يصدر بوصفه قانونا لأنه من الجمعية العامة فإنه يمثل رأي غالبية دول العالم، وقد تم استخدامه والرجوع إليه مرارا حتى بات قاعدة قانونية عرفية فأكدت محكمة العدل الدولية أن هذا المبدأ هو مبدأ عرفي عام[4].

يعد مبدأ عدم التدخل أشمل وأكثر اتساعا من المادة 2(4) في تقييد سلوك الدول، فهو يشمل منع الإكراه الاقتصادي والسياسي، وقد عرَّفته الجمعية العامة في قرار العلاقات الودية 1970 بالآتي:

"لا يحق لأي دولة أو مجموعة من الدول التدخل، مباشرة أو غير مباشرة، لأي سبب كان، في الشؤون الداخلية أو الخارجية لأية دولة أخرى. وبالتالي، فإن التدخل المسلح وجميع أشكال التدخل أو محاولات

---

[1] المرجع السابق – Buchan, R.

[2] سندل، مصطفى. (2017). مبدأ عدم التدخل في الشؤون الداخلية للدول بين النصوص والمتغيرات الدولية. مجلة القانون والعلوم السياسية، 3(1)، 211–232 [ص213]. استرجع من https://www.asjp.cerist.dz/en/article/78875

[3] Yifeng, C. (2014). Chapter 13: The customary nature of the principle of non-intervention: a methodological note. In *Renmin Chinese Law Review* (Vol. 2, pp. 319–340). https://doi.org/10.4337/9781783473793.00018

[4] Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America). Merits, Judgment. I.C.J. Reports 1986, p. 14 [para. 202, p. 106]

التهديد الأخرى ضد شخصية الدولة، أو ضد عناصرها السياسية والاقتصادية والثقافية، تنتهك القانون الدولي"[1].

ثم عرفته محكمة العدل الدولية 1996 في قضية نيكاراغوا ليس بذكر أمثلة التدخل في الشئون الداخلية فحسب، بل وضعت معيارا لكل تصرف يمكن أن يعد تدخلا غير مشروع وذلك على النحو الآتي:

"التدخل المحظور هو ذلك الذي له تأثير على واحد من الأمور – التي وفقًا لمبدأ السيادة – يسمح للدول أن تقرر فيها بحرية منها – اختيار النظام السياسي والاقتصادي والاجتماعي والثقافي، وصياغة السياسة الخارجية. فالتدخل يعد غير مشروع عندما تستخدم أساليب الإكراه فيما يتعلق بمثل هذه الخيارات، والتي يجب أن تظل حرة".[2]

يتبين من التعريفات السابقة أن الأمثلة المذكورة للتدخل غير المشروع – وهي السياسي، والاقتصادي، والثقافي، والتدخل في السياسة الخارجية – ذكرت على سبيل المثال لا الحصر، وأن معيار التدخل غير المشروع هو كل إكراه يسلب حرية القرارات السيادية للدولة. من هنا يمكن عد الهجمات الإلكترونية من أمثلة التدخل غير المشروع؛ لأنها يمكن أن تتخذ لإكراه الدولة على الأمور التي تعد من حقوقها السيادية. هذا وسيتم تطبيق قاعدة عدم التدخل على الهجمات السيبرانية لاحقا في هذا المبحث، ومن المهم هنا المقارنة بين ما يمكن أن يقدمه هذا المبدأ مقارنة بقاعدة منع استخدام القوة.

لا بد من تأكيد اتساع مبدأ عدم التدخل مقارنة بالمادة 2(4)، لأنها تمنع التدخل بأي وسيلة مسلحة كانت أو غير مسلحة. لذلك تعد جميع استخدامات القوة التي تنتهك المادة 2(4) "تدخلات" محظورة (إذا كانت تهدف إلى إكراه الدولة في قرارات سيادية) بالإضافة إلى ذلك تشمل قاعدة عدم التدخل حالات الضغوط الاقتصادية أو السياسية التي لا تتسع لها قاعدة منع استخدام القوة[3].

---

[1] United Nations, General Assembly, *Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations*, 24 October 1970, A/RES/2625(XXV). Available at: https://www.un.org/ruleoflaw/files/3dda1f104.pdf

[2] Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America). Merits, Judgment. I.C.J. Reports 1986, p. 14 [para. 205, p. 107]

[3] Haslam, E. (2000). Information Warfare: Technological Changes and International Law. *Journal of Conflict and Security Law*, *5*(2), 157–175 [p. 163]. https://doi.org/10.1093/jcsl/5.2.157

مع ذلك فإن مبدأ عدم التدخل غير قادر على التصدي للهجمات الإلكترونية لوحده دون مبدأ عدم استخدام القوة؛ لأنه في جوهره مرتبط بالإكراه. ولكي يعد التدخل غير مشروع يجب فيه وجود عنصر الإكراه بنية تغيير الإرادة السيادية. وعليه الهجمات غير المتصلة بالإكراه ستخرج من نطاق عدم المشروعية، مثال ذلك الهجمات السيبرانية التجسسية التي قامت بها الصين ضد الولايات المتحدة وكانت تهدف للتفوق الاقتصادي والعسكري، مثل تلك الهجمات التجسسية أو الاستغلال السيبراني – وهي أغلب نوع متكرر بين الدول[1]– لا يمكن تطبيق مبدأ عدم التدخل عليها؛ لعدم ارتباطها بالإكراه، وتغيير الإرادة السيادية، لذلك فمبدأ عدم التدخل غير قادر لوحده على التصدي لجميع أنواع الهجمات.

هذا وقاعدة عدم التدخل هي قاعدة عرفية، وقاعدة منع استخدام القوة منصوص عليها في ميثاق الأمم المتحدة وإنه وإن لم توجد هرمية في مصادر قواعد القانون الدولي، فالعرف ونصوص الاتفاقيات تتساوى في الإلزام[2]، لكن الأمر المختلف في قاعدة منع استخدام القوة هو أن هناك نوعا من الإجماع على أنها قاعدة دولية آمرة Jus Cogen على عكس قاعدة عدم التدخل التي لا تعد قاعدة دولية آمرة[3].

إن القاعدة الدولية الآمرة لها قوة خاصة فوفقا لاتفاقية فيينا لا يمكن للدول الاتفاق على مخالفة قاعدة آمرة وأي معاهدة تخالف قاعدة دولية آمرة تعد ملغاة. كذلك إذا ظهرت قاعدة دولية آمرة لاحقة لاتفاقية تحتوي على مخالفة لتلك القاعدة فإن القاعدة اللاحقة تلغي الاتفاقية السابقة[4]. وإن كان يصعب من

---

[1] Wallace, D. A., McCarthy, A. H., & Visger, M. (2019). Peeling Back the Onion of Cyber Espionage after Tallinn 2.0. *Maryland Law Review*, 78(2), 205–246 [p. 205-209]. Retrieved from https://digitalcommons.law.umaryland.edu/mlr/vol78/iss2/2/

[2] للمزيد حول موضوع التدرج في قواعد القانون الدولي، انظر:
علام، وائل. (2012). تدرج قواعد القانون الدولي العام. مجلة الحقوق - جامعة البحرين، (1)، 9–59. استرجع من https://journal.uob.edu.bh/handle/123456789/3288

[3] المرجع السابق – The International Court of Justice – Green, J. A. – ص110
انظر أيضا:
Aloupi, N. (2015). The Right to Non-intervention and Non-interference. *Cambridge Journal of International and Comparative Law*, *4*(3), 566–587 [p. 566]. https://doi.org/10.7574/cjicl.04.03.566

[4] الأمم المتحدة، اتفاقية فيينا للعلاقات الدبلوماسية (23 مايو 1969)
المادة 53: "المعاهدات المتعارضة مع قاعدة آمرة من القواعد العامة للقانون الدولي (النظام العام الدولي) - تكون المعاهدة باطلة إذا كانت وقت عقدها تتعارض مع قاعدة آمرة من القواعد العامة للقانون الدولي ..."
المادة 64: "ظهور قاعدة آمرة جديدة من القواعد العامة للقانون الدولي (النظام العام الدولي) - إذا ظهرت قاعدة آمرة جديدة من القواعد العامة للقانون الدولي فان أية معاهدة نافذة تتعارض معها تصبح باطلة وتنقضي"
المادة 70: آثار انقضاء المعاهدة - 1- ما لم تنص المعاهدة أو يتفق الأطراف على خلاف ذلك فان انقضاء المعاهدة وفقاً لأحكام هذه الاتفاقية: (أ) يحل الأطراف من أي التزام بالاستمرار في تنفيذ المعاهدة. (ب) لا يؤثر على أي حق أو التزام أو مركز قانوني للأطراف نشأ نتيجة تنفيذ المعاهدة قبل انقضائها. 2- إذا نقضت دولة معاهدة جماعية أو انسحبت منها تنطبق الفقرة (1) على العلاقات بين هذه الدولة والدول الأخرى الأطراف في المعاهدة من تاريخ نفاذ ذلك النقض أو الانسحاب."

الناحية العملية أن تجتمع إرادة الدول ضد قاعدة دولية آمرة في اتفاقية دولية لكن مجرد النص على هذه الضمانات حسنٌ.

إن الأهم في موضوع القواعد الآمرة يكمن في مسؤولية الدولة، فهناك مجموعة من الظروف المنصوص عليها في المواد المتعلقة بمسؤولية الدولة[1] على سبيل الحصر وهي تبيح أن تسوِّغ انتهاكها للقانون الدولي ومتلافية أي مسؤولية دولية عن الأفعال غير المشروعة دوليا، وتسمى بالظروف النافية لعدم المشروعية مثل ظرف الضرورة[2]، لكن القاعدة الآمرة لا يمكن للدول الاحتجاج بأي من الظروف النافية لعدم المشروعية لمخالفتها[3].

كذلك من الآثار التي تترتب على إدخال الهجمات الإلكترونية تحت تنظيم قاعدة آمرة أن مخالفة القاعدة الآمرة – في قانون مسؤولية الدولة وفي حالة الإخلال الخطير بالقواعد القطعية – ينشئ التزامات معينة على كل دول العالم منصوص عليها في المادة 41 من المواد المتعلقة بمسؤولية الدولة، وهي التزام التعاون لأنهاء الإخلال بالقواعد القطعية، والالتزام بعدم الاعتراف بشرعية الوضع الذي أنشأه الإخلال بالقواعد القطعية، وعدم تقديم أي عون وأي مساعدة للإبقاء على ذلك الوضع[4].

بالنظر لطبيعة الهجمات الإلكترونية لكونها عابرة للحدود وتتفاوت قدرة الدول في التصدي لها وتحتاج إلى التعاون، وتحمل المسؤولية الجماعية في التصدي لها، لذلك فإن الخواص التي تتميز بها القاعدة الآمرة مهمة في تنظيم الهجمات الإلكترونية؛ بسبب ما توفره من حث على التعاون الدولي وتوحيد الموقف الجماعي، لذلك لا بد من تكييف الهجمات الإلكترونية مع قاعدة آمرة وهذا ما لا ينطبق على قاعدة منع التدخل.

وفضلا عما تقدم به معالجة القانون الدولي للهجمات الإلكترونية يجب أن تكون متناسبة مع قدراتها التدميرية، فالرد المشروع على خرق قاعدة عدم التدخل يكون بالتدابير المضادة، بينما الرد على قاعدة منع استخدم القوة هو الدفاع عن النفس، وقد يكون من المناسب اتخاذ تدابير مضادة لهجمات إلكترونية تجسسية، أو التدخل في الانتخابات، لكن إذا كانت ذات طابع تدميري وقد أحدثت ضررا ماديا فلن تكفي التدابير المضادة لصده وإيقافه، بمعنى أنه قد تكون هناك حاجة حقيقة للدفاع الشرعي عن النفس،

---

[1] A/CN.4/SER.A/2001/Add.1 (Part 2)

[2] المرجع السابق – التعليق على الفصل الخامس "الظروف النافية لعدم المشروعية" – الفقرة (3) – ص91

[3] المرجع السابق – التعليق على المادة 26 – الفقرة (4) – ص110

[4] المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دولياً – المادة 41 – ص11

وهذا لا يكون ممكنا إذا عدت الهجمات السيبرانية تدخلا غير مشروع[1]. لذلك مرة أخرى يجب تأكيد أنه لا يمكن الاستغناء عن قاعدة عدم استخدام القوة في تكييف الهجمات الإلكترونية؛ فالاكتفاء بقاعدة عدم التدخل سيكون قاصرا، وغير كاف لمواجهة قدراتها التدميرية حيث لا يسمح بالدفاع عن النفس كذلك لن يشمل أنواع الهجمات الإلكترونية التي لا تنطوي على إكراه مثل الهجمات التجسسية، لذلك المادة 2(4) يجب أن تشمل الهجمات الإلكترونية.

الفرع الرابع: قياس الهجمات السيبرانية على الأسلحة الكيميائية والبيولوجية

إذا كانت قاعدة منع استخدام القوة تتناول قوة السلاح فلابد من عد الهجمات السيبرانية سلاحاً. والسبيل إلى ذلك هو قياس الهجمات السيبرانية على أنواع من الأسلحة تشابهها في الخصائص. فالهجمات الإلكترونية يجب ألا تقاس على العقوبات الاقتصادية والسياسية، بل تقاس كما في النهج العسكري بقدراتها فمثلا السلاح البيولوجي أو الكيميائي[2] سلاحان بلا شك ولسنوات عديدة كانا يعدان قوة، وفي استخدامهم خرقا للمادة 2(4) لأثرهما المدمر. ولذلك فالأصح والأدق أن يتغير قياس الهجمات الإلكترونية على التدابير الاقتصادية والاجتماعية إلى قياسها على الأسلحة البيولوجية والكيميائية.

ولقد سبقت الإشارة إلى أن السلاح البيولوجي والكيميائي يقعان في نطاق قاعدة منع استخدام القوة، فهل يمكن عد الهجمات الإلكترونية سلاحا خصوصا أنها تشترك مع النوعين الأولين في خاصية عدم الحركة، حيث لا إطلاق نار، ولا تفجير، ولا قوات عسكرية تعبر الحدود فالعملية عبارة عن إطلاق مادة، وهذا غير حركي لكن لنتائجهما المدمرة دخلا في نطاق قاعدة منع استخدام القوة في المادة 2(4). إن إطلاق وصف السلاح على الهجمات الإلكترونية يعني الأخذ بمعيار الأثر لا معيار الحركة أو الأداة؛ لتحديد القوة، فالأثر المدمر هو بالتأكيد استخدام للقوة ويدخل في نطاق 2(4) وإن لم تكن الأداة المستخدمة حركية.

فلا يهم وزن السلاح ثقيل أو خفيف، ولا مادته صلبة أو سائلة، أو غازية، ولا يهم إن كان مرئيا أو غير مرئي، ولا يهم إن كان في العالم الحقيقي أو الافتراضي؛ ذلك لأن الأخذ بمعيار الأثر يبعد الحديث عن ماهية الهجمات الإلكترونية إلى الحديث عن عواقبها المدمرة. في ذلك يؤكد دليل (تالين) "أن مجرد حقيقة استخدام نظام كومبيوتر بدلا من منصة أسلحة تقليدية في أثناء عملية ما ليس له تأثير على

[1] المرجع السابق – Wessendorf, N., et al. – التعليق على المادة 2(4) – الفقرة 22
[2] المرجع السابق – Buchan, R. – ص217

تقرير ما إذا كانت العملية ترقى إلى استخدام القوة. في النطاق السيبراني ليست الأداة المستخدمة هي المحدد –. إذا ما تم تجاوز عتبة استخدام القوة – ولكن عواقب العملية والظروف المحيطة بها".[1]

إن مما يؤكد أن الهجمات السيبرانية تعد سلاح العصر هو تأكيد ذلك في السياسات الدفاعية لمعظم دول العالم[2]. بريطانيا على سبيل المثال في استراتيجية الأمن الوطني نصت على أن "الأنشطة في الفضاء السيبراني هي أسلحة عسكرية قد تستخدم من قبل الدول أو الأفراد"[3] وباقي دول العالم غالبا ما تفرد فصلا في استراتيجياتها الأمنية للعمليات السيبرانية[4].

ومن أهم الأدلة على صحة التوجه تعد الهجمات الإلكترونية سلاحا، رأي محكمة العدل الدولية في فتواها بشأن مشروعية التهديد بالأسلحة النووية أو استخدامها فقد ذهبت إلى:

"أن المادة 2(4) والمادة 42 من الميثاق لم يشترطا نوعا محددا من الأسلحة وينطبقان على أي استخدام للقوة بغض النظر عن ماهية الأسلحة المستخدمة"[5].

فهذا نص صريح يمكن اعتماده لتوجه المحكمة – إلى حسبان استخدام السلاح النووي استخداما للقوة وإن لم يكن سلاحا معتادا كالأسلحة التقليدية، بما يؤكد أن المعيار في عدِّ السلاح قوة تدخل في نطاق المادة 2(4) هو الأثر الذي يحدثه. هذا النص لمحكمة العدل الدولية هو نقطة الاتفاق في تصنيف دخول الهجمات الإلكترونية في نطاق المادة 2(4).

المطلب الثالث

التمييز بين ما يدخل في نطاق المادة 2(4) وغيره من الهجمات الإلكترونية

---

[1] Tallinn Manual 2.0, para. 1, p. 328

[2] للاطلاع على المزيد حول مواقف الدول تجاه الأمن السيبراني، والمجمعة من قبل مركز الامتياز المعني بالدفاع الحاسوبي التعاوني التابع لمنظمة حلف شمال الأطلسي انظر:

NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). (n.d.-b). Cyber security strategies. Retrieved from https://ccdcoe.org/library/strategy-and-governance/

[3] المرجع السابق – Roscini, M. – Cyber Operations and the Use of Force – ص51

[4] المرجع السابق

[5] وأصل نص الفتوى هو:

"These provisions do not refer to specific weapons. They apply to any use of force, regardless of the weapons employed." – *Nuclear Weapons* advisory opinion, para. 39, p. 224

في المطلب السابق تم التوصل إلى نتيجة مفادها أن الهجمات السيبرانية يمكن أن تعد قوة، وبالتالي تكون محرمة بموجب قاعدة منع استخدام القوة (4)2. بيد أن التسلسل المنطقي يفرض تساؤلاً مهماً وهو متى تعد الهجمة الإلكترونية في حكم استخدام القوة. أو أي نوع من أنواع الهجمات الإلكترونية التي تم تعرُّف على صورها في الفصل الأول يعد استخداما للقوة؟

إن السبب الذي يستوجب التفرقة بين ما يدخل في نطاق قاعدة منع استخدام القوة وغيرها هو لمعرفة الرد القانوني المتاح على الهجمة السيبرانية. فالرد على هجوم سيبراني يشكل خرقاً لقاعدة منع استخدام القوة يمكن ان يكون بالدفاع الشرعي عن النفس إذا وصل إلى عتبة الهجوم المسلح كما سيتم تفصيله في المبحث الثاني من هذا الفصل. أما الرد على هجوم سيبراني لا يشكل استخداما للقوة فإنه يكون بالتدابير القانونية، أو التدابير المضادة، أو تدابير حالة الضرورة وهذه الحالات الثلاث سيتم تناولها في الفصل الثالث من هذا البحث.

ينقسم هذا المطلب إلى فرعين، الفرع الأول منها يعالج الهجمات الإلكترونية الداخلة في نطاق قاعدة منع استخدام القوة وأما الفرع الثاني فإنه يعالج الهجمات التي لا تدخل في نطاق قاعدة منع استخدام القوة.

الفرع الأول: الهجمات الإلكترونية الداخلة في نطاق قاعدة منع استخدام القوة

يمكن حصر الحالات التي تعد فيها العملية السيبرانية داخلة في نطاق المادة (4)2 في أربع حالات وهي: الهجمات الإلكترونية التي تضاهي آثارها استخدام القوة، ثم الهجمات التعطيلية ذات النطاق الواسع والضرر الجسيم، ثم الهجمات السيبرانية الصادرة من فاعل غير حكومي برعاية دولة، وأخيرا حالة التهديد باستخدام القوة السيبرانية.

أولا: الهجمات الإلكترونية التي تضاهي آثارها استخدام القوة

في دليل (تالين) أسقط الخبراء المادة 2(4) على ظاهرة الهجمات الإلكترونية كالآتي:

"تعد الهجمات الإلكترونية استخداما للقوة عندما يكون حجمها وتأثيرها قابلا للمقارنة بالعمليات غير السيبرانية التي تصل إلى نفس مستوى استخدام القوة".

هذه القاعدة تحيل الهجمة السيبرانية محل النظر إلى الهجمات التقليدية التي لا خلاف في أنها استخدام للقوة؛ ليتم قياس حجمها ونطاقها وأضرارها ثم تقارن بحجم نطاق وأضرار الهجمة السيبرانية وإذا ما كان هناك تماثل في النتائج فإن الهجوم الإلكتروني يعتبر استخداما للقوة[1].

نص المادة 2(4) لا يحدد أي معيار للجسامة لحسبان الفعل استخداما للقوة كذلك وليس في الأعمال التحضيرية للميثاق ما يوضح درجة الجسامة، فإذا ما تم الأخذ بالتفسير الواسع يُعدُّ أي نوع من السلوك الذي يشكل ضغطاً على سيادة الدولة هو استخدام غير مشروع للقوة، بغض النظر عن حجمه، أو مدته، أو أهدافه[2].

لكن لا يمكن الأخذ بهذا التفسير الواسع لسببين: أولهما: أنه يؤدي إلى نتائج غير منطقية مثل عد الهجمة التي تتسبب في تخريب جهاز حاسوب واحد استخدام للقوة، وهذا ما يجب الحذر منه؛ لأن عد

---

[1] وتجدر الإشارة إلى أنه حتى في تقرير استخدام القوة في العمليات السيبرانية هناك: "نهج قائم على الأدوات" و"نهج القائم على النتائج" بموجب النموذج الأول الذي وضعه برأوني في 2012، يتم إجراء تقييم إذا كان الضرر الناجم عن هجوم إلكتروني يمكن أن يتحقق في السابق فقط من خلال هجوم حركي تقليدي. على سبيل المثال، باستخدام هذا النموذج، فإن الهجوم السيبراني الذي يتم إجراؤه بغرض إغلاق شبكة كهرباء سيعتبر هجومًا مسلحًا. لأنه قبل تطوير القدرات الإلكترونية، كان تدمير شبكة الطاقة يتطلب عادةً قصف محطة طاقة أو استخدام القوة الحركية لتحقيق هذه النتيجة. بالإضافة إلى ذلك، فإن الهجوم الإلكتروني هو استخدام للقوة إذا سعى المهاجم إلى التسبب في تدمير مادي مباشر أو إصابة أو وفاة. بهذا يزيل هذا النهج الحاجة إلى فحص الأداة . اما "النهج القائم على النتائج" الذي وضعه Schmitt في 1999 وهو الذي اخذ به دليل (تالين) غالبًا لا يتم إجراء أي محاولة لتقييم ما إذا كان الضرر الناتج عن هجوم إلكتروني يمكن تحقيقه في السابق من خلال الاستخدام الحركي للقوة فقط. هنا نأخذ في الاعتبار التأثير الكلي الإجمالي لضرر الهجوم الإلكتروني على الدولة الضحية.

انظر: المرجع السابق – Brownlie, I. – ص362

انظر أيضا:

Schmitt, M. N. (1999). Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework. *Columbia Journal of Transnational Law*, *37*, 887–937. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1603800

هذه المقارنة موجودة في:

Madubuike-Ekwe, J. N. (2021). Cyberattack and the Use of Force in International Law. *Beijing Law Review*, *12*(02), 631–649. https://doi.org/10.4236/blr.2021.122034

[2] المرجع السابق – Cyber Operations and the Use of Force – Roscini, M. – ص45

الفعل استخدام للقوة، قد يعطي الدولة الحق في الدفاع عن النفس بأي نوع من القوة وقد تكون هذه القوة سلاحا تقليدياً. ومثل هذه النتيجة تتناقض مع اتفاقية فيينا للمعاهدات التي تشترط ألا يؤدي تفسير المعاهدة إلى نتائج غير منطقية وغير مقبولة[1]. السبب الثاني وكما تم التطرق اليه أعلاه، في الأعمال التحضيرية للميثاق رفضت الدول عدِّ الضغوط السياسية والاقتصادية والدبلوماسية في حكم القوة، لذلك هناك عدم تساهل لدى المجتمع الدولي لتوصيف أي سلوك بالقوة.

هذا فضلا عن أن محكمة العدل الدولية لم تضع معيار لما يعد قوة لكنها – كما سيتم التطرق اليه لاحقا – في الدفاع عن النفس وضعت معيارا للهجوم المسلح: "الحجم والاثر" وقالت: إن الهجوم المسلح هو أشد صور استخدام القوة جسامة[2]، بمعنى أن كل هجوم مسلح هو استخدام للقوة لكن ليس كل استخدام للقوة هو هجوم مسلح. ومع ذلك لم تضع معيارا لما يعتبر استخداما للقوة. لكن في حكمها في قضية اختصاص مصائد الأسماك، 1998 اسبانيا ضد كندا حيث ادعت اسبانيا ان ما قامت به كندا من تدابير قسرية يعتبر خرقا للمادة 2(4) نصت المحكمة في حكمها على:

"أن ما تسمح به التشريعات الكندية من استخدام للقوة يدخل في نطاق تدابير الحفظ والإدارة" لذلك اعدت المحكمة "أفعالا– مثل الصعود على سطح السفن، والتفتيش، والاعتقال، واستخدام الحد الأدنى من القوة – تفسيرا معقولا لمفهوم تدابير الحفظ والإدارة".

وإن كانت محكمة العدل لم تحدد معيارا لاستخدام للقوة فإنه ليس لديها توجه في التساهل أو التوسع في اعتبار أي عنف هو استخداما للقوة تحت المادة 2(4) والدليل على ذلك أن المحكمة كانت قد نظرت في ست قضايا تم الادعاء فيها باستخدام القوة وتنوعت أحكامها بين قبول هذه الادعاءات أو رفضها بحسب ظروف كل قضية[3].

وقد اقترح دليل (تالين) ثمانية معايير تساعد الدول على قياس الهجمة السيبرانية؛ لتقرير ما إذا كانت خرقاً لقاعدة منع استخدام القوة أم لا[4]. أول هذه المعايير وأهما وأكثرها قطعية الجسامة، ويعنى بها

---

[1] تنص المادة 32 من اتفاقية فيينا لقانون المعاهدات (1969) على أنه: "يمكن اللجوء إلى وسائل تكميلية في التفسير، بما في ذلك الأعمال التحضيرية للمعاهدة وملابسات عقدها، وذلك لتأكيد المعنى الناتج عن تطبيق المادة 31، أو لتحديد معنى النص حين يكون من شأن التفسير وفقاً لتلك المادة: (أ) أن يترك المعنى غامضاً أو غير واضح؛ أو (ب) أن يؤدي إلى نتيجة غير منطقية أو غير مقبولة"

[2] *Nicaragua* judgement, para. 191, p. 110

[3] المرجع السابق – O'Connell, M. E. – ص201

[4] بالإضافة إلى تعريف هذه المعايير أورد دليل (تالين) مجموعة من الأسئلة لكل معيار لقياس تحقق حدوثه من عدمه.

الأذى المادي على الممتلكات والأرواح مع استبعاد الآثار التعطيلية للهجمات[1]. ثانيا، فورية الأثر، بحيث تنعدم القدرة على التسوية السلمية[2]. ثالثاً، عنصر المباشرة، ويقصد بها قوة العلاقة السببية بين بداية الهجمات الإلكترونية ونتائجها، فكلما قلَّت العوامل الأخرى المؤثرة في النتيجة كان من السهل إثبات استخدام القوة[3]. رابعاً، درجة الغزو، بمعنى إلى أي مدى استقصد الغزو مؤسسات الدولة؟ (دون المؤسسات الخاصة) أو بناها التحتية أو مرافقها[4]. خامساً، قابلية النتائج للقياس، فكلما كانت عواقب الهجمة قابلة للقياس والتحديد سيكون أسهل على الدولة تقييمها لتقرير ما إذا ما وصلت لمستوى استخدام القوة أم لا[5]. سادساً، الطابع العسكري، الذي إذا ما ثبت سيكون من السهل جدا عد الهجوم الإلكتروني قوة مسلحة. ويتم إثبات الطابع العسكري بإثبات أن الهجمة تم توجيهها من جهة عسكرية كالجيش، أو تم توجيهها إلى هدف عسكري مثل منشئة عسكرية[6]. سابعاً: مدى تورط الدولة في العملية السيبرانية، كأن تصدر من إحدى وكالات الدولة أو قواتها المسلحة، فكلما كانت الصلة أوضح وأوثق بين الدولة والعمليات السيبرانية، زاد احتمال كونها مستخدمة القوة[7]. أخيراً، عنصر عدم الشرعية، فمن الأسهل أن يكون هدف الهجمة الإلكترونية غير مشروع بشكل لا خلاف فيه كتدمير مرفق حيوي، أما هجمات التجسس أو الضغوط النفسية أو الاجتماعية فإنه من الصعوبة عدها خرقا لمبدأ عدم استخدام القوة؛ كونها غير محرمة في القانون الدولي[8]. وكلما توفر عدد أكبر من هذه العوامل، وكلما كانت أوضح كانت فرضية وجود مخالفة لقاعدة منع استخدام القوة؛ أكثر صلابة؛ لأنه بالفعل كل من هذه المعايير فيه ارتباط بجزء من خصائص استخدام القوة؛ لذلك يتوقع أن يزداد الاعتماد عليها في المستقبل؛ لتقرير تطبيق المادة 2(4) على الهجمة السيبرانية من عدمه.

انظر:

Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, I.C.J. Reports 2004, p. 136 [para. 155, p. 199]

انظر:

Questions relating to the Obligation to Prosecute or Extradite (Belgium v. Senegal), Judgment, I.C.J. Reports 2012, p. 422 [para. 68, p. 449]

[1] Barcelona Traction, Light and Power Company, Limited, Preliminary Objections, Judgements, I.C.J Reports 1970, p. 3 [para. 33, p. 33]

[2] المرجع السابق

[3] المرجع السابق

[4] *Barcelona Traction* judgement, paras. 33-34, p. 33

[5] المرجع السابق

[6] *Wall* advisory opinion, para. 155, p. 199

[7] المرجع السابق

[8] المرجع السابق

واقعيا، الهجوم المسلح الحركي الذي يتبعه دمار يطال البنى التحتية، أو الحق وفيات، أو إصابات، يمكن بسهولة الإشارة إليه أنه استخدام للقوة، فإذا أحدث الهجوم الإلكتروني دمارا مشابها على الممتلكات والأرواح فإنه يعد استخداماً للقوة بلا شك. وبعبارة أخرى كلما كانت آثار الهجوم الإلكتروني ظاهرة على ارض الواقع كان إثبات أنه استخدام قوة أسهل، وأكثر إقناعا بين الدول وهذا أمر يتفق عليه الفقه[1].

بيد أن الإشكال يكون في الاستخدام الأبسط للقوة. فهناك حد أدنى من استخدام القوة في العلاقات الدولية، قد يفضي إلى انتهاك قواعد معينة في القانون الدولي، لكن لا يمكن عده انتهاكاً للمادة 2(4). من الأمثلة على ذلك عمليات الاختطاف، واعتراض وتحييد دخول الطائرات في المجال الجوي دون، اذن والمطاردة الشرطية الدولية[2]. لذلك في حالات استخدام القوة في الهجمات السيبرانية كما في استخدام القوة في العلاقات الدولية عامة، فإن الدولة التي وقع عليها الهجوم ستلجأ – دائما – لأقصى قاعدة قانونية تعطيها أوسع مساحة للرد، ولتجريم الطرف المهاجم، وعندئذ فإن تقرير أن تلك الهجمة الإلكترونية هي استخدام للقوة يعتمد على معطيات كل موقف على حدة.

ثانيا: الهجمات التعطيلية التي ذات النطاق الواسع والضرر الجسيم

هناك النوع الآخر من آثار الهجمات الإلكترونية تتلبسه صعوبة في الاتفاق على كونه خرقا للمادة 2(4). ولقد تم تعريف الهجمات التعطيلية في الفصل الأول أنها التي يؤدي فيها الهجوم السيبراني إلى ضرر، لكنه يظل حبيس العالم الإلكتروني، فلا يسبب تخريبا ماديا ملموسا على أرض الواقع، وإنما يسبب ضررا رقميا يعطل مصالح الدولة. فلا دمار على الممتلكات ولا خسائر أو إصابات في الأرواح، بل تلفٌ في المعلومات، أو تعطيل المواقع، أو الشبكات مما يترتب عليه تعطيل أو إزعاج في عمل المرافق.

---

[1] Schmitt, M. N. (2011). Cyber Operations and the Jus Ad Bellum Revisited. *Villanova Law Review*, *56*, 569–606 [p. 573]. Retrieved from https://digitalcommons.law.villanova.edu/vlr/vol56/iss3/10

انظر أيضا: المرجع السابق – Schmitt, M. N. – Computer Network Attack – ص17

انظر أيضا:

Joyner, C. C., & Lotrionte, C. (2001). Information Warfare as International Coercion: Elements of a Legal Framework. *European Journal of International Law*, *12*(5), 825–865 [p. 850]. https://doi.org/10.1093/ejil/12.5.825

انظر أيضا: المرجع السابق – Dinniss, H. H. – ص74

[2] المرجع السابق – Roscini, M. – Cyber Operations and the Use of Force – ص54

دليل (تالين) لا يشجع على حسبان هجمات الازعاج والتعطيل استخداما للقوة[1]، لذلك هناك قصور في تكييف الهجمات التعطيلية؛ بسبب عدم اتفاق الخبراء عليها. مايكل شميت رئيس فرق الخبراء الدوليين الذين وضعوا دليل (تالين) يؤكد أن اتلاف أو تدمير المعلومات غير كاف ليصل إلى مستوى استخدام القوة، ويرى أن القول بغير ذلك له عواقب خطيرة!! لأن فيه تصنيف للغالبية العظمى من العمليات الإلكترونية على أنها هجمات مسلحة.[2] لذلك يصر على أن الهجوم الإلكتروني الذي يتلف بيانات في الحاسوب يجب أن يخرج أثره إلى العالم المادي، مثل التسبب في ارتفاع درجة حرارة المولد واشتعال النار، أو جعل القطار أو مترو الأنفاق لا يمكن السيطرة عليه.[3]

هناك من فقهاء القانون من يرى أنه من المبالغة القول: إن الهجمات الإلكترونية ذات الأثر غير المادي لا يمكن أن يعد استخداما للقوة. إن معظم الحديث عن قدرات الهجمات الإلكترونية في المستقبل يتناول هجمات تعطيلية تشل الحياة العامة، ومعظم الهجمات الإلكترونية التي حدثت بين الدول حتى اللحظة هي هجمات حبيسة العالم الافتراضي في أثرها، قليلة تلك الهجمات التي حركة مادة تحريكا فيزيائيا على ارض الواقع. كانت قليلة وكان سببها اعتماد المجتمعات الحديثة على أنظمة الكمبيوتر والشبكات، وإن التقنيات الإلكترونية قد مكنت الدول من إنتاج نتائج مماثلة لتلك الخاصة – بالأسلحة الحركية، ولكن دونما ضرر مادي[4]. وأما الهجوم السيبراني الذي يدوم أثره أياما ويؤدي إلى إغلاق الشبكة الوطنية، وبالتالي ترك ملايين الأشخاص بدون كهرباء، وتعطيل نظام النقل، ومنع الاتصالات الحكومية، - فمن المرجح أن يتم التعامل معه على أنه استخدام للقوة[5]، ففي هذه الحالات يمكن لآثار التعطيل أن تكون مساوية للدمار الذي تسببه القوة المسلحة التقليدية. فمثل هذا الوضع يتجاوز مجرد الإزعاج ويعطل بشدة بالغة أداء البنية التحتية الحيوية بحيث يمكن أن يندرج ضمن نطاق المادة 2 (4).

---

[1] Tallinn Manual 2.0, commentary to rule 69, para. 9(a), p. 334
Barcelona Traction judgement, paras. 33, p. 33

[2] Schmitt, M. N. (2010). Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts. In *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy* (pp. 151–178) [p. 164]. Washington, DC: National Academies Press.

[3] المرجع السابق

[4] المرجع السابق – Cyber Operations and the Use of Force – Roscini, M. – ص55

[5] المرجع السابق

ماركو روسيني (MARCO ROSCINI) من المؤيدين لتصنيف بعض الهجمات الإلكترونية التعطيلية في عداد استخدام القوة. ويعلل ذلك بأن التوجه الجديد في الحروب هو الابتعاد عن التدمير واقتصار هدف العملية العسكرية على التعطيل والشل؛ لمراعاة إعادة الإعمار السريع بعد الصراع ويعطي بعض الأمثلة على هذا التوجه منها قواعد الاشتباك التي وزعت على القوات الأمريكية في العراق ونصت على أنه "يجب أن تهدف الهجمات على البنية التحتية للعدو، وخطوط الاتصال، والأهداف الاقتصادية إلى تعطيلها وتجنب تدميرها كلما أمكن ذلك"[1]. ويضع شرطين لعدِّ الهجوم الإلكتروني غير المصاحب لأضرار مادية استخداما للقوة، وهو أن يقع الهجوم الإلكتروني على "مرفق حساس للدولة"، وأن تكون آثاره مساوية لهجوم مسلح، حتى لو لم يتسبب في أي هجوم أو إصابة بشرية أو أضرار مادية فورية.

وتجدر الإشارة إلى أن الجمعية العامة في ٢٣ / كانون الأول ديسمبر ٢٠٠٣ أصدرت قرارا بعنوان: "إرساء ثقافة عالمية لأمن الفضاء الحاسوبي وحماية الهياكل الأساسية الحيوية للمعلومات"[2] يوضح ماهية المرفق الحساس. وكان فحوى القرار حماية البنية التحتية للمعلومات الحيوية من الهجمات، فقد دعا القرار إلى عدد من الإجراءات كالتعاون والتنسيق الدولي، وتقاسم المعلومات المتعلقة بالانكشاف والتهديد والحوادث، ووضع قوانين موضوعية وإجرائية تمكن الدول من كشف الهجمات. ومن المهم في هذا القرار أنه أورد أمثلة على ماهية الهياكل الأساسية للمعلومات الحيوية وعبر عنها بأنها "المستخدمة في توليد وتوزيع الطاقة والنقل الجوي والبحري والبنوك والتمويل والتجارة الإلكترونية وإمدادات المياه وتوزيع الغذاء والصحة العامة"[3].

يتضمن هذا القرار أمرين: أولهما: تأكيد لأهمية بعض الهياكل المعلوماتية المتعلقة بالمرافق الحيوية، وأنها بحاجة لحماية خاصة؛ لأن المساس بها خطر على حياة الشعوب. وثانيهما أنه يمكن اعتماد المرافق المذكورة فيه معيارا للمرفق الحساس أو الحيوي، وقد أورد القرار ذلك على سبيل المثال؛ مما

---

[1] المرجع السابق – ص61
للمزيد عن قواعد الاشتباك، انظر:
Watch, H. R., Docherty, B. L., & Garlasco, M. E. (2003). *Off Target*, p. 138. Retrieved from https://www.hrw.org/reports/2003/usa1203/usa1203.pdf

[2] قرار الجمعية العامة 199/58، *إرساء ثقافة عالمية لأمن الفضاء الحاسوبي وحماية الهياكل الأساسية الحيوية للمعلومات*، A/RES/58/199 (23 ديسمبر 2003). استرجع من https://undocs.org/A/RES/58/199

[3] تنص ديباجة القرار السابق على: "وإذ تلاحظ ازدياد الصلات في ما بين الهياكل الأساسية الحيوية لمعظم البلدان – كتلك المستخدمة في جملة أمور منها توليد الطاقة ونقلها وتوزيعها، والنقل الجوي والبحري، والخدمات المصرفية والمالية، والتجارة الإلكترونية، والتزويد بالمياه، وتوزيع الأغذية والصحة العامة – والهياكل الأساسية الحيوية للمعلومات التي تربط بين عملياتها وتؤثر فيها بشكل متزايد"

يعطي الفرصة لكل دولة أن تضيف ما تراه مرفقا حيويا[1]، لكن إن لم تحدد الدولة مرافقها الحساسة فالمرافق المذكورة في هذا القرار تكون غاية في الأهمية وهي أساسية جدا لاستمرار حياة عامة خالية من أي رفاهية وتصلح معيارا لتطبيق المادة 2(4) في حال تم تعطيلها بهجوم إلكتروني.

أما بخصوص متطلب أن تكون آثار الهجوم السيبراني التعطيلي مساوية لهجوم مسلح فيرى روسيني ذلك ممكنا. فمثلا إذا تم تفجير البورصة أو المؤسسات المالية الأخرى حركيًا وتعطلت الأسواق نتيجة لذلك، فهذا بالتأكيد يعد استخدامًا للقوة المسلحة، وليس إكراها اقتصاديا، على الرغم من أنه من المحتمل أن تفوق العواقب الاقتصادية للعملية الأضرار المادية التي لحقت بالمباني. وعليه، لماذا لا يطبق نفس الاستنتاج عندما يتم إغلاق البورصة لمدة طويلة (بسبب هجوم إلكتروني) بدلاً من قصفها؟ ففي هذا السيناريو يشترك الهجوم الإلكتروني مع الهجوم الحركي في الأثر فإنه من المنطقي القول: إن الهجوم الإلكتروني التعطيلي يمكن أن يدخل في نطاق المادة 2(4)[2]. أما إذا لم يكن الاضطراب الناجم شديدًا فيكون الهجوم الإلكتروني أقل عرضة لعده استخدامًا للقوة، وكذلك الأمر إذا كان الهجوم الإلكتروني غير متعلق بمرفق حساس للدولة كأن يقع هجوم إلكتروني على جامعة ويتسبب في تعطيلها لأيام أو مجمع تجاري ونحوه مما لا يمكن عده هجوما إلكترونيا يستخدم القوة.

وفي تقرير صادر عن المجلس القومي للبحوث في واشنطن، نوقشت الهجمات الإلكترونية ضد البورصات التي تحدث بشكل متكررة ومستمرة، مما يعطل التداول لمدة طويلة من الزمن، يعني أياما وأسابيع فهذا من المرجح عده استخداما للقوة، لكنه على الجانب الآخر لم يشجع على عده هجوما مسلحا يحرك الحق في الدفاع الشرعي عن النفس[3] وذلك في محاولة لاحتواء التصعيد المحتمل. وقد ذهب مايكل شميت إلى أن المجلس القومي للبحوث أساء التقدير؛ لأن الحقيقة أن الدول إذا أعطيت فرصة لتكون ضحية استخدام قوة لن تفوت خيار اللجوء للدفاع عن النفس، وستحاول الدفع تجاه تكييف الهجمة السيبرانية أنها استخداما للقوة يصل إلى عتبة الهجوم المسلح؛ لتحريك حقها في الدفاع الشرعي. فلا يمكن تغيير ما اسماه شميت "قواعد اللعبة" بمعنى ان نعد الهجوم السيبراني استخداما للقوة، لكنه

[1] تنص ديباجة القرار السابق على "وإذ تدرك أن كل بلد سيحدد بنفسه الهياكل الأساسية الحيوية للمعلومات الخاصة به"

[2] المرجع السابق – Cyber Operations and the Use of Force – Roscini, M. – ص62

[3] المرجع السابق – Technology, Law, and Ethics – National Research Council – ص254

لا يمكن أن يصل إلى مستوى الهجوم المسلح؛ لأن أصحاب السيادة بالتأكيد سيحاولون الاستفادة القصوى من الموقف لحماية مصالحهم الوطنية[1].

ويبدو أن الرأي الأخير أكثر تماشياً مع روح الميثاق الذي يهدف إلى تقليص استخدام الدول للقوة إلى أقصى نقطة ممكنة، فإذا كان الأمر كما حذر منه شميت بمعنى أن تكييف الهجمات التعطيلية أنها استخدام للقوة وأن ذلك يفتح المجال لعدها هجوما مسلحاً، مما يفتح المجال للرد عليها بالدفاع عن النفس، وهو غالبا ما ستحاول الدولة الضحية لمثل تلك الهجمات القيام به، ولذلك فقد يكون من الأفضل قصر قاعدة استخدام القوة على الهجمات السيبرانية التي تضاهي آثارها التدميرية استخدام القوة وليس آثارها الاقتصادية فحسب.

ثالثا: الهجمات الصادرة من فاعل غير حكومي برعاية دولة

بداية لا بد من الإشارة إلى أن موضوع الجماعات الفاعلة غير الحكومية سيتم تفصيله في الدفاع عن النفس، لكن لا بد من الإشارة هنا إلى أن دعم دولة ما للهجمات السيبرانية التي ينفذها فاعل غير حكومي كالجماعات المسلحة، أو الشركات الخاصة، أو حتى الأفراد تعد استخداما للقوة من قبل تلك الدولة الراعية، إذا انطبقت – على هجومها – معايير استخدام القوة في الهجوم السيبراني.

فالحديث في هذا القسم يسلط الضوء على قضية من يقوم بالهجمات التي تعد قوة؟ وليس ماهي الهجمات التي تعبر قوة؟ فالسؤال الأخير تمت الإجابة عليه في القسم أعلاه، وهي: الهجمات السيبرانية المشابهة لآثار الهجوم التقليدي التدميرية، لكن ذلك النقاش كان على اعتبار ان تلك الهجمات صدرت من دولة. في هذه الحالة يتم التأكيد أن نفس الهجمات إذا صدرت من فاعل غير حكومي برعاية دولة تعد استخداما للقوة من قبل الدولة الراعية.

ويحسن هنا الوقوف على حكم محكمة العدل الدولية في قضية نيكاراجوا الذي ينص على أن:

[1] المرجع السابق – Proceedings of a Workshop – National Research Council – ص177

"الفعل الذي يرقى إلى حد استخدام القوة لا يقتصر على الاستخدام المباشر للأسلحة من قبل دولة ضد دولة أخرى، ولكن أيضًا أي تسليح وتدريب للجماعات المسلحة لتقوم؛ بالاعتداء على دولة أخرى يعد انتهاكًا للمادة 2 (4)، حتى وإن لم يكن هجومًا مسلحًا"[1].

وهذه الحالة ذات صلة مباشرة بالهجمات السيبرانية، وهو مثال تطبيقي واضح، فعندما تنخرط الدولة في تدريب جماعة مسلحة على العمليات السيبرانية، وتوفر لها المعدات المطلوبة من برامج وفيروسات ضارة، وأجهزة كومبيوتر، وشبكات انترنت، ويكون ذلك بهدف القيام بهجمات إلكترونية ترقى إلى استخدام القوة على دولة أخرى، فإن الدولة الأولى تعد مسؤولة عن الهجمات الإلكترونية تحت بند المادة 2(4) من ميثاق الأمم المتحدة.

رابعا: التهديد باستخدام القوة السيبرانية

من الناحية الواقعية تهدد الدول باستخدام القوة باستمرار، فقبول المجتمع الدولي أو تسامحه مع التهديد أكثر من الاستخدام الفعلي للقوة، لكن من الناحية النظرية كلاهما (التهديد والاستخدام) يدخلان في مبدأ المنع[2] وهو أمر ثوري جاءت به المادة 2(4)، المشكلة أن هناك غموضا بخصوص مكونات التهديد باستخدام القوة.

ليس ثمة تعريف متفق عليه للتهديد باستخدام القوة إلا أنه من أكثر التعريفات استخداماً هو تعريف إيان برونلي الذي عرف التهديد باستخدام القوة أنه " وعيد صريح أو ضمني صادر من دولة معينة باللجوء إلى القوة في حالة عدم القبول بتنفيذ مطالبات معينة لتلك الدولة"[3]. هذا التعريف يعنى في جوهر بعنصر القسر دون عناصر أخرى مطلوبة لتحقق التهديد باستخدام القوة بموجب المادة 2(4)، مثل تلك العناصر يوفرها تعريف أوليفر كورتن الذي عرف التهديد باستخدام القوة كالآتي "وعيد مستقبلي

[1] *Nicaragua* judgement, para. 228, p. 118
[2] Weller, M., Rylatt, J. W., & Solomou, A. (Eds.). (2015). *The Oxford Handbook of the Use of Force in International Law*, p. 115. Oxford, United Kingdom: Oxford University Press.
[3] Roscini, M. (2007). Threats of Armed Force and Contemporary International Law. *Netherlands International Law Review*, *54*(02), 229–277 [p. 234]. https://doi.org/10.1017/s0165070x0700229x

صريح أو ضمني باستخدام غير مشروع للقوة ضد دولة أو أكثر بحيث يعتمد تحقيق تنفيذ التهديد على إرادة الطرف الذي قام به"[1].

يتبين مما سبق أنه لكي يكون التهديد غير مشروع يجب أن يكون موضوع التهديد – أي الفعل الذي يتم التهديد به – هو استخدام غير مشروع للقوة. فلا يعد تهديد الدولة التي تتوعد باستخدام أشد القوة دفاعا عن نفسها حال وقوع الهجوم عليها، أو عندما يهدد مجلس الأمن باستخدام صلاحياته تحت الفصل السابع لحفظ السلم والأمن. فإذا كان غير مشروع، يستوي أن يكون ضمنياً كما في التلميحات الدبلوماسية حين يصرح المتحدث باسم الدولة بأن لديهم قوة الكترونية، ولن يترددوا في استخدامها، أو صريحاً كأن يكون التهديد شفهيًا أو مكتوبًا بشكل يعرب صراحة عن استعداد الدولة للجوء إلى القوة. كذلك يجب أن يصل التهديد إلى علم الدولة المستهدفة، وذلك ليتحقق عنصر القسر الذي هو جوهر التهديد[2]. وأخيرا يجب أن يكون التهديد واقعياً أو ضمن قدرات الدولة التي تصدره؛ وذلك ليؤخذ بجدية ويؤتي أثرة، وهذا معنى أن يعتمد تنفيذ التهديد على إرادة الطرف الذي قام به.

دليل (تالين) يسقط التهديد باستخدام القوة على الهجمات الإلكترونية على النحو التالي:

"العملية السيبرانية، أو التهديد بالعملية السيبرانية يعد تهديدا غير مشروع عندما يكون العمل المهدد به في حال تنفيذه استخداما غير مشروع بالقوة"[3].

في هذا التعريف هناك فرضان: أولهما: التهديد السيبراني باستخدام القوة، والثاني التهديد باستخدام القوة السيبرانية. الأول هو تهديد باستخدام القوة التقليدية يتم الإبلاغ عنه من خلال الفضاء الإلكتروني. فالعملية السيبرانية هي مجرد أداة لإيصال التهديد باستخدام القوة المسلحة. مثال ذلك أن يكون ناطق باسم حكومة دولة (أ) مهددا الدولة (ب) باستخدام رادع للقوة خلال مؤتمر صحفي، فيصل التهديد إلى الدولة (ب) عبر وسائل الإعلام، وهي وسيلة سيبرانية. أما في الفرض الثاني فإن موضوع التهديد هو استخدام القوة السيبرانية كأن تصرح الدولة (أ) بأنها ستستخدم منظومتها الهجومية السيبرانية المطورة

---

[1] Corten, O. (2021). Chapter 2. What Do 'Use of Force' and 'Threat of Force' Mean? In *The Law Against War: The Prohibition on the Use of Force in Contemporary International Law (French Studies in International Law)* (pp. 61–136) [p. 94]. Oxford, United Kingdom: Hart Publishing. https://doi.org/10.5040/9781509949021.ch-002

[2] المرجع السابق – Cyber Operations in International Law – M.N. Schmitt – ص153

[3] Tallinn Manual 2.0, rule 70, p. 338

لشن هجوم يشل كل مفاصل الدولة (ب)[1]. في كلتا الحالتين إذا توفرت في التهديد العناصر المذكورة أعلاه سيكون تهديداً غير مشروع باستخدام القوة تحت بند المادة 2(4).

ولم يعط التهديد بالقوة اهتماما كافياً من البحث كما في الاستخدام الفعلي للقوة، إلا عندما يتعلق الموضوع بالدفاع عن النفس الاستباقي؛ فإنه يكون للتهديد باستخدام القوة أثر مهم في إضفاء الشرعية على الهجوم الاستباقي دفاعاً عن النفس[2]. والسبب في ذلك أنهم يرون أنه من المبالغة فصل التهديد باستخدام القوة عن الاستخدام الفعلي للقوة؛ لأن التهديدات التي تم تنفيذها فقط هي التي يتم إدانتها[3]. فضلا عن أن التهديد بالقوة يمنع أحيانا استخدام القوة، فعندما يمارس التهديد بشكل معقول وبعناية، من أجل الحفاظ على السلام والأمن ضمن معايير أهداف الأمم المتحدة أو للحفاظ على الحق المشروع للدولة، فإنه قانوني.[4] يمكن تأييد هذا الاتجاه فعليا، فمن ناحية يبقى التهديد باستخدامك القوة غير مشروع بنص الميثاق، إضافة إلى أن مجلس الأمن والجمعية العامة أدانا التهديد بالقوة مرارا في عدة قرارات.[5] لكن في الرأي الاستشاري الصادر عن محكمة العدل الدولية بشأن الأسلحة النووية اقرت المحكمة بوجود تهديد مشروع باستخدام القوة، فقد رأت المحكمة:

---

[1] Tallinn Manual 2.0, commentary to rule 70, para. 2, p. 338

[2] للمزيد عن علاقة القوة بالدفاع الاستباقي عن النفس، انظر:

Green, J. A., & Grimal, F. (2011). The Threat of Force as an Action in Self-Defense Under International Law. *Vanderbilt Journal of Transnational Law*, *44*(2), 285–329. Retrieved from https://scholarship.law.vanderbilt.edu/vjtl/vol44/iss2/2

[3] Sadurska, R. (1988). Threats of Force. *The American Journal of International Law*, *82*(2), 239–268. https://doi.org/10.2307/2203188

[4] المرجع السابق – ص245

[5] اتخذ مجلس الأمن العديد من القرارات التي تدين التهديد باستخدام القوة أو تطالب الدول بالامتناع عن مثل هذه التهديدات، كما هو الحال في القرارات التالية، دون الإشارة صراحةً إلى حظر التهديد باستخدام القوة

UN Security Council, Security Council resolution 186 (1964) [The Cyprus Question], 4 March 1964, S/5575 (1964), available at: http://unscr.com/en/resolutions/186

UN Security Council, Security Council resolution 187 (1964) [The Cyprus Question], 13 March 1964, S/5603 (1964), available at: http://unscr.com/en/resolutions/187

Security Council resolution 326 (1973) [Provocation by Southern Rhodesia], 2 February 1973, S/RES/326 (1973), available at: http://unscr.com/en/resolutions/326

Security Council resolution 411 (1977) [Mozambique-Southern Rhodesia], 30 June 1977, S/RES/411 (1977), available at: http://unscr.com/en/resolutions/411

Security Council resolution 487 (1981) [Iraq-Israel], 19 June 1981, S/RES/487 (1981), available at: http://unscr.com/en/resolutions/487

Security Council resolution 573 (1985) [Israel-Tunisia], 4 October 1985, S/RES/573 (1985), available at: http://unscr.com/en/resolutions/573

"إن مفهومي "التهديد" و "استخدام" القوة بموجب الفقرة 4 من المادة 2 من الميثاق قائمين معًا، بمعنى أنه إذا كان استخدام القوة بحد ذاته في حالة معينة غير قانوني –لأي سبب من الأسباب– فإن التهديد باستخدام هذه القوة سيكون بالمثل غير قانوني. وباختصار، لكي يكون قانونياً، فإن إعلان الدولة لاستخدام القوة يجب أن يكون متوافقا مع الميثاق"[1].

في النطاق السيبراني، للتهديد بالهجمات السيبرانية درجة عالية من الأهمية، فهناك توجه يرى أن كل الهجمات الإلكترونية التي حدثت حتى اليوم لا تصل لأن تكون استخداماً للقوة وإن كانت ستدخل في نطاق المادة 2(4) فهو بوصفها تهديدا.

فرانسوا ديليرو يرى في كتاب الهجمات الإلكترونية والقانون الدولي أن الهجمات الإلكترونية على جورجيا فرضية مقنعة لعدها تهديدا بحسبان أنها **سبقت** النزاع المسلح بين روسيا وجورجيا وهي (هجمات سيبرانية تعطيلية DDoS[2]) واستمرت تلك الهجمات خلال الحرب، لكن إذا ما تم التركيز على تكييف الهجمات **السابقة** للحرب، يمكن أن تعد تمهيدا للحرب، أو تهديدا ضمنيا باستخدام القوة.

أما في إستونيا، فيرى ديليرو أن هناك حالة تدعو إلى القول: إن العمليات الإلكترونية يمكن أن تكون تهديدًا باستخدام القوة[3]. فالبلد يعتمد بشكل كبير على الانترنت في البنية الأساسية، فإذا ما أخذنا في الحسبان النتائج التي أدت إلى الشلل الجزئي للدولة، والحد من قدرتها الدولة على الرد في حالة العمل العسكري، مع الأخذ في الحسبان أنه حدثت خلال مرحلة العلاقات المتصدعة بين الدولة المستهدفة والدولة المدعى عليها، يمكن أن تكون تلك العمليات السيبرانية تدابير تمهيدية محتملة لاستخدام القوة. بناء على هذا، يمكن عدها انتهاك حظر التهديد بالقوة المنصوص عليه في المادة 2، الفقرة 4 من ميثاق الأمم المتحدة.

أما Stuxnet الذي أحدث أضرارًا مادية بأجهزة الطرد المركزي في محطة الطاقة النووية في إيران فإن ديليرو يرى أن طريقة عمله تؤكد أن الهدف من وراء العملية هو التهديد وليس التدمير البسيط الذي حدث. فكان من الممكن تعديل بعض البيانات، وربما حذف البرنامج قيد التشغيل المنشأة النووية

---

[1] *Nuclear Weapons* advisory opinion, para. 47, p. 246

[2] للمزيد عن شل خدمات آلة أو شبكة وجعلها غير متاحه عن طريق إغراقها بطلبات من الأنظمة المخترق، انظر:
Delerue, F. (2020). *Cyber Operations and International Law*, p. 321. Cambridge, United Kingdom: Cambridge University Press. https://doi.org/10.1017/9781108780605

[3] المرجع السابق – ص321-322

أو تنفيذ أي أعمال أخرى غير مدمرة، ولكن بدلاً من ذلك تم تدمير أجهزة الطرد المركزي؛ لغرض إشعار صاحب المنشأة النووية، وبالتالي الدولة بقدرة المهاجم على الدخول في النظام المعني. فهو تهديد باستخدام القوة ليظهر الجاني استعداده وقدرته[1].

يجدر الانتباه انه لا إستونيا ولا جورجيا[2] ولا حتى إيران صرحت أن تلك العمليات السيبرانية استخدام للقوة أو تهديد باستخدامها. هذا التحليل يمثل وجهة نظر الكاتب ديليرو ، ويمكن الاتفاق معه في الهجمات السيبرانية على جورجيا التي سبقت الاستخدام الفعلي للقوة، لأنها كانت هجمات تعطيلية تهدف للاستفزاز والضغط على الدولة أكثر منها إحداث ضرر، مما ينطبق عليه الوعيد باستخدام القوة؛ مما يجعله تهديدا سيبرانيا باستخدام القوة. أما في إستونيا وإيران ذواتي الضرر الواسع النطاق أو المماثل آثار الهجوم التقليدي فيصعب الاتفاق مع تكييف الهجمات بأنها تهديد باستخدام القوة. فالتهديد يجب ألا يتجاوز كونه وعيدا أما إذا بدأ الضرر الحقيقي الذي المؤثر على الدولة فالهجوم السيبراني هنا يتجاوز التهديد باستخدام القوة، فإن لم يصل إلى الاستخدام الفعلي للقوة يمكن يتم تكييفه وفق مبدأ احترام للسيادة أو تدخل في الشأن الداخلي أو غيرها. لذلك يبدو ان هدف الكاتب هو عرض امكانية تطبيق تكييف الهجمات بالتهديد.[3]

الفرع الثاني: الهجمات الإلكترونية التي لا تدخل في نطاق المادة (4)2

من الصعب حصر الحالات التي تكون فيها الهجمات الإلكترونية غير داخلة في نطاق المادة (4)2؛ لأنها تمثل الغالبية العظمى من الهجمات. لكن إذا كانت القاعدة العامة هي أن الهجمات الإلكترونية التي تماثل نتائجها استخدام القوة تخضع لقاعدة منع استخدم القوة، فإنه يمكن القول: إن كل الهجمات الإلكترونية ذات الأضرار الخفيفة والمتوسطة التي لا تضاهي آثار استخدم القوة التقليدية لن تخضع في تكييفها إلى المادة (4)2 من ميثاق الأمم المتحدة.

هذا الأمر ينطبق على معظم الهجمات الإلكترونية فمعظم الهجمات التي حدثت إن لم يكن جميعها لم تصل إلى عتبة استخدام القوة. حتى الآن الهجوم السيبراني الوحيد الذي يمكن القول: إن هناك احتمالا

---

[1] المرجع السابق – Delerue, F. – ص323-324

[2] المرجع السابق – IIFFMCG Report

[3] وذلك بدليل ان الكاتب في آخر الكتاب اعتبر هجوم ستكسنت (Stuxnet) استخدام للقوة مع احتمال اعتباره هجوم مسلح. للمزيد، انظر صفحة 500 من المرجع السابق.

حقيقياً لعده استخداما غير مشروع للقوة هو هجوم Stuxnet الذي وقع على إيران في 2010[1]. ذلك لأن هناك أثرا حركيا تدميريا غير قليل، فالهجوم تسبب في انفجارات أودت ب 1000 جهاز طرد مركزي. أما لو كان الهجوم السيبراني تسبب في حدوث انفجار في جهاز حاسوب واحد مثلا فقد يختلف الأمر.

كذلك الأمر في حالة الهجمات الإلكترونية التعطيلية DDOS التي تسبب شللا في الجهاز أو في الموقع أو الشبكة، فإنها لكي تعد استخداما للقوة فلا بد من تحديد معياري المرفق الحيوي والجسامة التي تعادل في نتائجها استخدام القوة التقليدية، فتسبب الهجمات "كما الحرب" شللا في قطاعات مهمة تؤثر على حياة كل المواطنين. وإن كان مثال إستونيا الأقرب لمثل هذه الحالة لكن لا إستونيا ولا أي دولة أو منظمة دولية أو هيئة تابعة لمنظمة دولية صرحت بأن الذي تعرضت له إستونيا في 2007 يعد استخداما للقوة، وإن كان هناك بعض الآراء ترى أنه مؤهل جيد لاستخدام القوة غير المشروعة؛ لما ينطبق عليه من شل المرافق الحساسة على نطاق واسع، لكنها غير كافية لتغليب هذا التوجه[2].

كذلك الهجمات التخريبية ذات الأثر الرقمي وهي التي تهدف إلى تدمير المواقع الإلكترونية وقواعد المعلومات الخاصة بالدولة من الصعب أن تصل في نتائجها إلى مرحلة استخدام القوة. في عام 2012 تعرضت شركة أرامكو السعودية لهجوم إلكتروني لفايروس أطلق عليه أسم "شمعون" ، وقد دمر البيانات

[1] Richardson, J. (2011). Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield. *UIC John Marshall Journal of Information Technology & Privacy Law*, *29*(1), 1–28. Retrieved from https://repository.law.uic.edu/jitpl/vol29/iss1/1/
Foltz, A. C. (2012). Stuxnet, Schmitt Analysis, and the Cyber Use-of-Force Debate. *Joint Force Quarterly (JFQ)*, *67*, 40–48 [p. 44]. Retrieved from https://apps.dtic.mil/sti/citations/ADA618715
Hollis, D. B. (2011, January 25). Could Deploying Stuxnet be a War Crime? Retrieved from http://opiniojuris.org/2011/01/25/could-deploying-stuxnet-be-a-war-crime/

[2] Maliha, N. (2020). *Cyber Warfare: Challenges in The Application of International Humanitarian Law To Virtual Conflict*. Retrieved from https://www.researchgate.net/publication/343979992_Cyber_Warfare_Challenges_In_The_Application_Of_International_Humanitarian_Law_To_Virtual_Conflict

الموجودة على أجهزة الشركة البالغ عددها 30,000 جهاز[1] ومع ذلك لم يتم تحسب تلك الهجمة الإلكترونية هجوما مسلحا[2] ولا حتى استخداما للقوة[3].

خلاصة القول: إن الهجمات الإلكترونية التي لا تصل آثارها إلى العناصر المكونة للمادة 2(4) من استخدام للقوة أو تهديد باستخدام القوة أو هجوم مسلح فأنها لن تدخل في نطاق المادة 2(4). بالطبع هذا لا يعني أن الهجمات التي لا تدخل في نطاق المادة 2(4) مشروعة لكنها تكيف تحت قواعد قانونية أخرى. ومثلما يكون حصر أنواع الهجمات الإلكترونية التي لا تدخل في نطاق قاعدة منع استخدام القوة صعبا، فكذلك في الصعوبة حصر القواعد القانونية التي تكيفها، لكن من أهم ما يتم استخدامه لتكييف الهجمات الإلكترونية هو قاعدة التدخل غير المشروع في الشئون الداخلية للدولة، ومبدأ السيادة الإقليمية ومبدأ بذل العناية.

أولا: مبدأ عدم التدخل

تم الحديث عن قاعدة عدم التدخل وأنها برغم اتساعها لا تغني عن ضرورة تكييف الهجمات السيبرانية وفقا لقاعدة منع استخدام القوة. ولقد سبق تعريف القاعدة فلذلك سيتم الاكتفاء هنا بالاختبار أو الشروط الواجب توافرها لكي تحسب العملية الإلكترونية تدخلاً محظورًا، وهي ثلاثة شروط[4]:

أولها: يجب أن يؤثر الفعل السيبراني على تلك القضايا التي يحق للدول أن تقرر فيها بحرية بموجب سيادتها، وهذا نطاق واسع يشمل الشؤون الداخلية والخارجية. ومن أمثلة النوع الأول، اختيار النظام

---

[1] للمزيد عن حادثة الهجمات السيبرانية على أرامكو في 2012، انظر:
Christopher, B., & Tikk-Ringas, E. (working paper). Hack or Attack? Shamoon and the Evolution of Cyber Conflict. James A. Baker III Institute for Public Policy of Rice University.

[2] Schmitt, M. N. (2010b). Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts. In *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy* (pp. 151–178) [p. 164]. Washington, DC: National Academies Press. https://doi.org/10.17226/12997

[3] المرجع السابق – Roscini, M. – Cyber Operations and the Use of Force – ص55

[4] تقسيم الشروط الثلاثة موجود في:
Prohibition of intervention. (2022). In International Cyber Law in Practice: Interactive Toolkit. Retrieved from https://cyberlaw.ccdcoe.org/wiki/Prohibition_of_intervention#cite_ref-5

السياسي والاقتصادي والاجتماعي والثقافي أو إجراء انتخابات وطنية. ومن أمثلة النوع الثاني، رسم السياسة الخارجية للدولة، والاعتراف بالدول، وعضوية المنظمات الدولية[1].

والثاني: يجب أن يهدف الفعل إلى الإكراه، وبمعنى آخر يشترط وجود نية الإكراه[2]. ولا يوجد تعريف مقبول لمصطلح "الإكراه" في القانون الدولي[3]. في هذا الصدد، ظهر نهجان رئيسان في السياق السيبراني:

وبحسب النهج الأول، ينطوي الفعل على الإكراه إذا كان مصمماً خصيصاً لإجبار الدولة الضحية على تغيير سلوكها فيما يتعلق بمسألة ضمن مجالها السيادي. وبموجب هذا النهج، فإن مفتاح خرق مبدأ عدم التدخل يكمن في أن "الفعل القسري يجب أن يكون ذا قدرة على إجبار الدولة المستهدفة على الانخراط في عمل ما كانت لتتخذه، أو حملها على الامتناع عن القيام بعمل كانت ستتخذه "[4].

وفي إطار النهج الثاني يكون المقصود بالإكراه: أن يحرم فعل ما الدولة المستهدفة فعليًا من قدرتها على التحكم في الأمور الواقعة ضمن نطاق سيادتها. ويختلف هذا النهج عن الأول؛ لأنه يكتفي بمجرد حرمان الدولة المستهدفة بفعل الإكراه من السيطرة على مسألة سيادية، حتى لو لم يحدث تحرك فعلي من الدولة لتغيير سلوكها جبراً[5].

ولكن في النهجين كليهما، فإن مجرد التأثير على الدولة المستهدفة عن طريق الإقناع، أو الدعاية، أو التسبب في إزعاج دون أي هدف معين لا يكفي للتوصيف بأنه إكراه.

---

[1] المبدأ الخاص بواجب عدم التدخل في الشؤون التي تكون من صميم الولاية القومية لدولة ما وفقا للميثاق: "ولا يجوز لأي دولة استخدام التدابير الاقتصادية أو السياسية أو أي نوع آخر من التدابير، أو تشجيع استخدامها، لإكراه دولة أخرى على النزول عن ممارسة حقوقها السياسية والحصول منها على اية مزايا."
قرار الجمعية العامة 25/2525، *اعلان مبادئ القانون الدولي المتعلقة بالعلاقات الودية والتعاون بين الدول وفقا لميثاق الأمم المتحدة*، A/RES/2625(XXV) (24 أكتوبر 1970). استرجع من https://www.undocs.org/A/RES/2625(XXV)
انظر أيضا: قرار الجمعية العامة 52/119، احترام *مبدأي السيادة الوطنية وعدم التدخل في الشؤون الداخلية للدول في عملياتها الانتخابية*، A/RES/52/119 (12 ديسمبر 1997). استرجع من https://www.un.org/ar/ga/52/res/res52119.htm

[2] Tallinn Manual 2.0, commentary to rule 66, para. 27, p. 321

[3] Moynihan, H. (2020). The vital role of international law in the framework for responsible state behaviour in cyberspace. *Journal of Cyber Policy*, *6*(3), 394–410 [p. 403]. https://doi.org/10.1080/23738871.2020.1832550
Tallinn Manual 2.0, commentary to rule 66, para. 18, p. 317

[4] Tallinn Manual 2.0, commentary to rule 66, para. 21, p. 318

[5] كان موقف بعض الخبراء في دليل (تالين) أنه لكي يكون العمل قسريًا، يكفي أن يتسبب الفعل بحرمان الدولة من السيطرة على المسألة المعنية.
للمزيد انظر:

Tallinn Manual 2.0, commentary to rule 66, para. 19, p. 318

ثالثاً: يجب أن تكون هناك علاقة سببية بين الفعل الهادف للإكراه وبين التأثير على الشؤون الداخلية أو الخارجية للدولة المستهدفة [1].

يتبين أن جوهر مبدأ عدم التدخل هو عنصر الإكراه، ولتكييف أي هجمات سيبرانية أنها تدخلٌ غير مشروع يجب البدء في البحث عن وجود إكراه على مسألة من المسائل التي يحق للدولة أن تقرر فيها بمقتضى سيادتها. نجد ذلك ينطبق بوضوح في مثال الهجمات التي حدثت في إستونيا 2007؛ فقد كان نقل التمثال الذي يمثل حقبة مؤلمة من الاحتلال السوفييتي شأنا داخليا مرتبطا باختيار النظام السياسي في البلد، ويحق لإستونيا أن تتخذ فيه قرارها بحرية بموجب سيادتها على إقليمها. وليس من الصعب الاتفاق على أن الهجمات السيبرانية التي حدثت عقب نقل التمثال مباشرة كانت تهدف إلى التأثير على ذلك القرار السيادي الإستوني. وعليه كان يمكن لإستونيا أن تعلن أنها تعرضت لتدخل غير مشروع في شئونها الداخلية وأنها سترد عليه بالتدابير القانونية أو التدابير المضادة.

ويبدو الأمر أكثر صعوبة في الانتخابات الامريكية. فصحيح أن الهجمات الإلكترونية بنوعيها اللذين تم التطرق إليهما في الفصل الأول، كانت تهدف إلى التأثير على أحد الشؤن الداخلية المرتبطة بسيادة الدولة، وهي الانتخابات الرئاسية. لكن حقيقة يصعب إيجاد عنصر الإكراه بكلا المعيارين المذكورين أعلاه. نعم قد تم التلاعب بالعملية الانتخابية بطريقة لم يكن مقررا لها! لكن ذلك تم بنشر معلومات حقيقية لتوعية الجمهور ولا يوجد إكراه في ذلك. وأن كانت بعض تلك المعلومات تم الحصول عليها بعملية قرصنة لشبكة كمبيوتر اللجنة الوطنية الديمقراطية (DNC) –تحديدا البريد الالكتروني للمرشحة الرئاسية هيلاري كلينتون– فإن ذلك بعيد عن الإكراه وإن كان يمكن أن ينطبق عليه خرق مبدأ عدم السيادة كما سيتم معالجته بعد قليل.

أما عمليات التجسس الأمريكي–الصيني فهي بعيدة تماما عن عدها تدخلا في الشأن الداخلي؛ وذلك لخلو هذه العمليات من عنصر الإكراه الذي يجبر الدولة على تغيير سلوكها، أو يحرمها من سيطرتها على مسألة سيادية. وإن انعدم وجود قاعدة في القانون الدولي تحرم التجسس فإن الطريقة التي تتم بها العملية التجسسية يمكن أن تعد خرقا للسيادة.

[1] Tallinn Manual 2.0, commentary to rule 66, para. 24, p. 320

ثانيا: مبدأ السيادة الإقليمية

السيادة هي الاستقلال من الخضوع لأية سلطة أخرى، ولا سيما سلطة دولة أخرى. إنها استقلال خارجي فيما يتعلق بحرية العمل خارج حدودها. وهي استقلال داخلي فيما يتعلق بحرية عمل الدولة داخل حدودها. السيادة تنطوي على سلطة إقليمية بحسبانها تشتمل على حق الدولة في ممارسة السلطة العليا على جميع الأشخاص والأشياء داخل أراضيها[1].

أكد تقرير 2013 لفريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي أن احترام السيادة ينطبق في الفضاء السيبراني. تجدر الإشارة إلى أن هذا التقرير صادقت عليه الجمعية العامة للأمم المتحدة[2] ، وبذلك يمكن القول: إن له قوة عرفية في القانون الدولي. وقد نص في موضوع السيادة على الآتي:

"تنطبق سيادة الدولة والقواعد والمبادئ الدولية المنبثقة عنها على سلوك الدول فيما يتعلق بالأنشطة المتصلة بموضوع تكنولوجيا المعلومات والاتصالات، وعلى ولايتها القضائية بشأن هياكلها الأساسية لتكنولوجيا المعلومات والاتصالات داخل أراضيها"[3].

ويجب التأكيد على أن مبدأ السيادة لا يمكن أن ينطبق إلا في العلاقات بين الدول[4]. وذلك مستمد من النظرة التقليدية أن الالتزام باحترام السيادة هو التزام تتقابل به الدول. وإن كانت المعاهدات الدولية تتوجه نحو ترتيب حقوق والتزامات تجاه الأفراد لكن الامر لا ينطبق على السيادة؛ ذلك أنه لا يمكن لأفعال الأفراد العاديين، أو الشركات، أو الجماعات المسلحة أن تعد انتهاكا لسيادة دولة. لكن من الممكن تصور أن قيام فرد أو جماعة غير حكومية بالدخول غير القانوني لدولة معينة ينتهك سيادتها إذا نسب عمل الفرد أو الجماعة إلى دولة معينة أي كان يمثل دولة معينة، أما إذا لم ينسب إلى دولة معينة فدخول الفرد بطريقة غير مشروعة لا يمكن أن يعد انتهاكاً للسيادة، لكنه مجرد مخالفة للقانون

---

[1] Jennings, R., & Watts, A. (2008). *Oppenheim's International Law: Volume 1 Peace* (9th ed.), p. 382. Oxford University Press.

[2] قرار الجمعية العامة 243/68، *التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي*، A/RES/68/243 (9 يناير 2014). استرجع من https://undocs.org/A/RES/68/243

[3] قرار الجمعية العامة 98/68، *تقرير فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي*، A/68/98 (24 يونيو 2013). استرجع من https://undocs.org/A/68/98

[4] Tallinn Manual 2.0, commentary to rule 4, para. 2, p. 17

انظر أيضا: المرجع السابق – Delerue, F. – ص210

الداخلي لتلك الدولة في مواجهة الأشخاص الذين قاموا به[1]، أو أن يمكن يكون انتهاكا لقاعدة بذل العناية في مواجهة الدولة التي صدر الهجوم من إقليمها إذا توافرت شروط قاعدة بذل العناية كما سيتم تفصيلها لاحقا. خلاصة الأمر انتهاك السيادة لا يكون إلا من قبل دولة أو من قبل جماعات من غير الدولة إذا كانت تعمل نيابة عن دولة، أما أفعال الأفراد والجماعات المنفصلة عن الدول فلا يمكن عدها انتهاك للسيادة.

وقبل التفصيل في انطباق قاعدة احترام السيادة في الفضاء السيبراني تجدر الإشارة إلى أن هناك انقساما بين الدول حول إمكانية وجود انتهاك للسيادة دون أن يكون مرتبطا بانتهاكات أخرى. فمن ناحية يرى الرأي الأول أن حظر انتهاك سيادة الدول الأخرى هو قاعدة أساسية جوهرية من قواعد القانون الدولي، وخرقها فعل غير مشروع دوليًا. وقد اعتُمِد هذا الرأي من قبل العديد من الدول منها: النمسا[2]، وجمهورية التشيك[3]، وفنلندا[4]، وفرنسا[5]، وألمانيا[6]، وإيران[7].

---

[1] Tallinn Manual 2.0, commentary to rule 4, para. 21, p. 23

[2] United Nations, Open-ended Working Group (OWEG), *Pre-Draft Report of the OEWG - ICT Comments by Austria* (31 March 2020). Retrieved from https://front.un-arm.org/wp-content/uploads/2020/04/comments-by-austria.pdf

[3] Czech Republic, The National Cyber and Information Security Agency (NÚKIB), *Czech Republic Statement at the 2nd substantive session of the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security of the First Committee of the General Assembly of the United Nations* (11 February 2020). Retrieved from https://www.nukib.cz/download/publications_en/CZ%20Statement%20-%20OEWG%20-%20International%20Law%2011.02.2020.pdf

[4] Finland, Finish Ministry of Foreign Affairs, *International law and cyberspace - Finland's national positions* (19 October 2020). Retrieved from https://um.fi/documents/35732/0/Cyber+and+international+law%3B+Finland%27s+views.pdf/41404cbb-d300-a3b9-92e4-a7d675d5d585?t=1602758856859

[5] United Nations, UN Office for Disarmament Affairs (UNUDO), *International Law Applied to Operations in Cyberspace - paper shared by France with the open-ended working group established by resolution 75/240* (December 2021). Retrieved from https://documents.unoda.org/wp-content/uploads/2021/12/French-position-on-international-law-applied-to-cyberspace.pdf

[6] Federal Republic of Germany, German Federal Foreign Office and the German Federal Ministry of Defence, *On the Application of International Law in Cyberspace* (March 2021). Retrieved from https://www.auswaertiges-amt.de/blob/2446304/2ae17233b62966a4b7f16d50ca3c6802/on-the-application-of-international-law-in-cyberspace-data.pdf

[7] nournews. (2020, August 18). General Staff of Iranian Armed Forces Warns of Tough Reaction to Any Cyber Threat. *nournews*.

أما الرأي الآخر فهو أن السيادة مبدأ من مبادئ القانون الدولي له دور في توجيه العلاقات الدولية، لكنه (في النطاق السيبراني) لا يرقى إلى مستوى قاعدة أساسية قائمة بذاتها[1]. وقد تبنت هذا الرأي الآن من قبل دولة واحدة هي المملكة المتحدة[2]، وصدق عليه المستشار العام بوزارة الدفاع الأمريكية[3]. من خلال هذا النهج، لا يمكن للعمليات الإلكترونية أن تنتهك السيادة كقاعدة مستقله من قواعد القانون الدولي، لأنه لكي يتعرض مبدأ السيادة للخرق – وفقا لهذا الرأي– لابد أن يصل الفعل السيبراني الضار لمستوى التدخل في الشأن الداخلي، أو مستوى استخدام للقوة. أما مجرد خرق السيادة لوحدة فلا يكفي لأخذه على محمل الجد كفعل غير مشروع دوليا.

وردا على ذلك يمكن القول: أولا: يجب تذكر اننا نطبق قواعد القانون الدولي كما هي على الهجمات السيبرانية، وقاعدة السيادة موجودة مستقلةً في القانون الدولي، ودليل ذلك أن محكمة العدل الدولية قد حكمت بها دون اقترانها باستخدام القوة، أو قاعدة عدم التدخل[4]. ثانيا: يبدو أن محاولة فصل الأفعال السيبرانية الضارة عن قاعدة السيادة تهدف لإطلاق يد الدول في القيام بهجمات سيبرانية –أقل مستوى التدخل في الشأن الداخلي– دون أن تنتهك أي قانون، بالأخص أفعال التجسس السيبراني، فإذا لم تكن هناك قاعدة تجرم التجسس لكن من الصعب القيام به دوم خرق سيادة الدولة فإذا لم يكن هناك خرق

---

[1] Corn, G. P., & Taylor, R. (2017). Sovereignty in the Age of Cyber. *AJIL Unbound*, *111*, 207–212. https://doi.org/10.1017/aju.2017.57

[2] القى المدعي العام السابق للمملكة المتحدة Jeremy Wright خطابا بعنوان (القانون السيبراني والقانون الدولي في القرن الحادي والعشرين) في 23 مايو 2018، وأكد في كلمته أن:"سعى البعض للدفاع عن وجود قاعدة خاصة بالفضاء السيبراني لـ "انتهاك السيادة الإقليمية" فيما يتعلق بالتدخل في شبكات الكمبيوتر لدولة أخرى دون موافقتها. السيادة هي بالطبع قاعدة أساسية في النظام بين الدول. لكنني لست مقتنعًا بأنه يمكننا حاليًا الاستخلاص من المبدأ العام قاعدة محددة للنطاق السيبراني بحيث تكون منفصلة عن قاعدة عدم التدخل في الشؤون الداخلية. لذلك فإن موقف حكومة المملكة المتحدة هو أنه لا توجد قاعدة كهذه في القانون الدولي في الوقت الحالي."

Wright, J. (23 May 2018) *Cyber and International Law in the 21st Century* [Speech]. GOV.UK. Retrieved from https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century

[3] Hon. Ney, P.C. Jr. (2 March 2020) *DOD General Counsel Remarks at U.S. Cyber Command Legal Conference* [Speech]. US Department of Defense. Retrieved from https://www.defense.gov/News/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/

[4] Certain Activities Carried Out by Nicaragua in the Border Area (Costa Rica v. Nicaragua) and Construction of a Road in Costa Rica along the San Juan River (Nicaragua v. Costa Rica), Judgment, I.C.J. Reports 2015, p. 665 [para. 93, p. 703]

لا يقترن انتهاك السيادة الإقليمية دائمًا باستخدام القوة. في قضية (كوستاريكا ضد نيكاراغوا) وجدت المحكمة بعض الأنشطة التي قامت بها نيكاراغوا في المنطقة الحدودية منذ عام 2010 وهي حفر ثلاثة قنابل وإنشاء وجود عسكري في أجزاء من تلك المنطقة تمثل خرقا لسيادة كوستاريكا الإقليمية، وذلك دون الحاجة للنظر إلى ادعاء منفصل بالاستخدام غير المشروع للقوة.

للسيادة بشكل مستقل ستكون الدول حرة في القيام به بمعزل عن المسؤولية والمحاسبة والرد عليها بالتدابير المضادة. ولذلك أخذ دليل (تالين) بالرأي الأول القائل بوجود قاعدة السيادة مستقلةً.

وبعد فإذا كانت الدراسة بصدد البحث عن الأفعال السيبرانية التي تكون انتهاكا للسيادة، وجب تعريف انتهاك السيادة، وهو يحدث عندما تمارس دولة سلطتها في إقليم دولة أخرى دون موافقتها في أمور يكون للدولة الإقليمية حق حصري في ممارستها باستقلال؛ لأنها تعد أعمالا حكومية[1]. تطبيقا لانتهاك السيادة بالهجمات السيبرانية يجب التفريق بين نوعين من الهجمات الإلكترونية. **الأولى** هي التي تحتاج إلى احداث اختراق في النظام المستهدف؛ لتتمكن من العمل، **والثانية** هي التي لا تحتاج لمثل ذلك الاختراق لتتفعل.

والمثال الجيد لتوضيح هذا الرأي هو حادثة تجسس المخابرات الألمانية التي انكشفت عام 2008. ففي العام 2006 قامت المخابرات الخارجية الألمانية بالتجسس على اتصالات وزير التجارة الأفغاني وصحفي في صحيفة Der Spiegel الألمانية. وللقيام بذلك زرعت دائرة الاستخبارات الاتحادية الألمانية برنامج تجسس حصان طروادة في شبكة الكمبيوتر في وزارة التجارة والصناعة في أفغانستان. ومن الواضح أن التجسس على الصحفي الألماني والوزير الأفغاني لم يكن في حد ذاته فعلا غير مشروع دوليًا. فليس هناك قاعدة قانونية تحرم التجسس بين الدول، فهو أمر تقوم به الدول باستمرار، لكن من ناحية أخرى، زرع حصان طروادة في شبكة حكومية أفغانية يشكل انتهاكا واضحا لسيادة أفغانستان[2]. وعلى ضوء هذا المثال، وعلى الرغم من عدم وجود حظر عام للتجسس بموجب القانون الدولي فإنه لا يمكن تصور قيام عملية تجسسية دون انتهاك للسيادة في مرحلة ما، خصوصا إذا ما كانت القاعدة أن الفعل غير المصرح به من قبل دولة على أراضي الدولة المستهدفة ينتهك السيادة الإقليمية للأخيرة.

---

[1] Moynihan, H. (2019, December). *The Application of International Law to State Cyberattacks: Sovereignty and Non-intervention*, p.15. Chatham House. Retrieved from https://www.chathamhouse.org/sites/default/files/publications/research/2019-11-29-Intl-Law-Cyberattacks.pdf

[2] How German Spies Eavesdropped on an Afghan Ministry. (2008, April 28). *Spiegel International*. Retrieved from https://www.spiegel.de/international/germany/bnd-scandal-how-german-spies-eavesdropped-on-an-afghan-ministry-a-550212.html

Bocev, P. (2008, April 28). Le patron de l'espionnage allemand est sur la sellette. *LEFIGARO*. Retrieved from https://www.lefigaro.fr/international/2008/04/29/01003-20080429ARTFIG00010-le-patron-de-l-espionnage-allemand-est-sur-la-sellette.php

أما النوع الآخر من العمليات السيبرانية فهو تلك العمليات التي لا تحتاج إلى اختراق النظام المستهدف من أجل إحداث آثارها. على سبيل المثال، هجمات تعطيل الوصول DDoS تعمل بطريقة إغراق البنية التحتية للمعلومات والاتصالات بالطلبات؛ لجعلها غير متاحة. ففي هذه الحالة كل طلب فردي لا يعد ضاراً أو غير قانوني، لكن الكم الهائل من الطلبات المتزامنة هو الذي يعطل الأداء الطبيعي للنظام المستهدف. إذ لا يوجد اختراق للنظام المستهدف، وبالتالي لا يوجد اختراق للأراضي، ولا انتهاك سيادة الدولة المستهدفة يكون محل تساؤل.

هنا أيضاً يرى François Delerue أن هجمات تعطيل الخدمة تعد انتهاكا للسيادة خصوصا إذا ما وضعنا في الحسبان أن النتيجة هي إبطاء النظام أو جعله غير متوافر والنتيجة بحد ذاتها غير مصرح بها، ويمكن أن تعد انتهاكا للسيادة[1]. لكن يجب تذكر أن السيادة الإقليمية لا تنتهك إلا من قبل دولة، وإثبات أن منشأ هذا النوع من الهجمات متصل بدولة معينة شبة مستحيل حالياً، لأنها عادة ما تأتي من أماكن عديدة من العالم، فالهجمات الإلكترونية على إستونيا 2007 أتت من أكثر من 178 دولة في وقت واحد[2]!! كذلك من الصعوبة اثبات أن دولة ما هي المسؤولة عن هذه الهجمات، لأن هناك سوابق من منظمات المجتمع المدني أو أفرادا يمتلكون الهدف نفسه فيتفقون على إرهاق موقع أو نظام معين بالطلبات حتى يتعطل[3]. لذلك لن يمكن الدفع بانتهاك السيادة الإقليمية إلا إذا أمكن إثبات هجمات DDoS قد تم إجراؤها تحت سيطرة دولة ما، فإن أمكن إثبات مؤكد لتورط جزئي للدولة في عمليات منع الوصول فمن المحتمل أن ترقى الهجمات إلى مستوى انتهاك السيادة الإقليمية للدولة الضحية[4].

ويبدو انه من المنطقي ترجيح التوجه الذي يرى أن الهجمات السيبرانية التي تطلق عن بعد – دون إحداث اختراق في أنظمة الدولة المستهدفة –تصنف خرق لمبدأ السيادة، فيجب تذكر أن خرق السيادة لا يكون إلا من دولة[5] قامت بتلك الهجمات التعطيلية العدائية، وسلوك مثل هذا لا بد أن يجد تكييفا يحفظ حق الدولة الضحية في استخدام الإجراءات المضادة، فالهجمات ذات الأثر الحركي يمكن ان تصنف أنها استخدام للقوة أو تهديد بالقوة فضلا عن أنها خرق للسيادة. بيد أن الهجمات التعطيلية

---

[1] المرجع السابق – Delerue, F. – ص262

[2] Chayes, A. (2015). 10 - Cyber Attacks and Cyber Warfare: Framing the Issues. In *Borderless Wars: Civil Military Disorder and Legal Uncertainty* (pp. 130–143). Cambridge, United Kingdom: Cambridge University Press. https://doi.org/10.1017/CBO9781316271551.011

[3] المرجع السابق – Delerue, F. – ص326

[4] المرجع السابق – Delerue, F. – ص226-228

[5] يُقصد من "الدولة" هنا أن تشمل، أجهزة الدولة، وكلاء الدولة أو الجهات الفاعلة والوكلاء من غير الدول إذا كان من الممكن أن تُنسب أفعالهم إلى الدولة بموجب قواعد الإسناد المنصوص عليها في مواد لجنة القانون الدولي بشأن مسؤولية الدولة.

يصعب تكييفها أنها قوة أو هجوم مسلح أو حتى تدخُّلٌ غير مشروع؛ لأنه في أحيان كثيرة يصعب إثبات عنصر الإكراه، لذلك لابد أن تدخل في مبدأ احترام السيادة، خصوصا أن فيها محاكاه فعلية لمعنى خرق السيادة في النطاق السيبراني، فهي قيام دولة بفعل غير مرغوب فيه في نطاق دولة أخرى ودون إذن منها.

وتجدر الإشارة إلى أن دليل (تالين) أخذ منحى آخر في تحديد متى تنتهك الهجمات السيبرانية السيادة. فهو يقترح أولا النظر في طبيعة الهدف[1]. فإذا استهدفت الهجمات السيبرانية ما يعرف بـ "الوظائف الحكومية المتأصلة" Inherent Governmental Functions وهي تلك الوظائف التي تقوم بها الحكومة حصراً مثل تنظيم الانتخابات، والضرائب، فإن أي مس بتلك الأهداف هو انتهاك للسيادة، حتى لو لم تحقق الهجمات أي ضرر بغض النظر عن نوع الهجمات وطبيعتها[2].

اما إذا كانت الهجمات تستهدف غير تلك الوظائف الحكومية المتأصلة فقد جعل دليل (تالين) من آثار الهجمات ركيزة لتحديد صحة انتهاك السيادة. فقسم الخبراء درجة الانتهاك ثلاثة مستويات (الضرر المادي)، (فقدان الوظيفة)، (التعدي على السلامة الإقليمية). وقد اتفق الخبراء أن النوعان: الأول والثاني يعدان انتهاكا للسيادة، بينما النوع الأخير مختلف فيه بين الخبراء[3].

وتطبيقا لذلك فإن الهجمات التي تحدث جرحا أو إصابة أو تدميرا فلا خلاف على أنها تنتهك سيادة الدولة الضحية. كذلك من المتفق عليه بينهم أن التخريب أو التعطيل الوظيفي الدائم أي أن الشيء (كالخادم في الحاسوب، أو وحدات التخزين، أو الحواسيب، أو أجزاء منها) لن يعمل باستمرار ففي هذه الحالة نكون أمام انتهاك لمبدأ السيادة. مثلا، رفع حرارة خوادم الإنترنت (Servers) بما يسبب ضررا دائما[4]. أما الهجمات التي تسبب نتائج دون فقدان الوظيفة الدائم كأن تكون النتيجة أقل من التخريب أو مثل أن النظام أصبح يعمل ببطيء أو أصبح غير متوفر بشكل مؤقت أو كانت النتيجة مسح بعض المعلومات، فلم يتفق الخبراء على اعد هذه الأفعال انتهاكا للسيادة، وتركوا المجال بانتظار رأي الدول. لذلك فالهجمات السيبرانية التي تستهدف البنية التحتية وتسبب بطأً في عمها لا تعد –وفقا لديل (تالين)– انتهاكا للسيادة[5].

---

[1] Tallinn Manual 2.0, commentary to rule 4, para. 10, p. 20
[2] Tallinn Manual 2.0, commentary to rule 4, para. 15, pp. 21-22
[3] Tallinn Manual 2.0, commentary to rule 4, para. 11, p. 20
[4] Tallinn Manual 2.0, commentary to rule 4, para. 13, pp. 20-21
[5] Tallinn Manual 2.0, commentary to rule 4, para. 14, p. 21

منهج François Delerue للسيادة في الفضاء السيبراني اعتمد على طريقة عمل الهجمة السيبرانية وأما دليل (تالين) فقد اعتمد على طبيعة الهدف في المرحلة الأولى، وطبيعة الضرر الذي تسببه الهجمة السيبرانية في مرحلة لاحقة. النهجين يعطيان نتائج مختلفة في الواقع العملي. فخلافا لدليل (تالين)، يؤدي تطبيق François Delerue مجرد وجود الفايروس في النظام إلى عده خرقا للسيادة بغض النظر عن الأضرار أحدثت أم لم تحدث؟ وبغض النظر عن هدف العملية السيبرانية أكان يهدف إلى تقويض أعمال الحكومة أم لا؟ وهذا يعني أنه أكثر اتساعا في عد الهجمات السيبرانية خرقا لقاعدة احترام السيادة.

ولترجيح أحد الرأيين يمكن القول: إن تنظير François Delerue أكثر محاكاة لفكرة السيادة. ففي الوضع العادي يحدث انتهاك للسيادة عندما تعبر دولة ما فعليًا إلى الإقليم أو المجال الجوي الوطني لدولة أخرى دون موافقتها. وبالتالي، فلماذا يكون مختلفا في الفضاء السيبراني؟ ولماذا انتهاك السيادة قبل تغلغل الدولة في البنية التحتية لتكنولوجيا المعلومات والاتصالات في دولة أخرى يعتمد على عتبة الضرر؟ في قانون مسؤولية الدولة – كما سيتم معالجته في الفصل الثالث – ليس الضرر عنصرا مكونا للفعل الغير مشروع، وتكفي مخالفة القاعدة القانونية ونسبتها إلى دولة، فلماذا يشترط دليل (تالين) الضرر في خرق السيادة في النوع الثاني من الهجمات[1]. على كل المنهجين كلاهما مطروحان بانتظار تطبيق الدول، وإن ما يتم الأخذ به في الواقع العملي بين الدول هو الذي سيتحول إلى قاعدة قانونية.

ثالثا: مبدأ بذل العناية اللازمة Due Diligence

مبدأ بذل العناية في القانون الدولي غير منصوص عليه في ميثاق الأمم المتحدة، لكن له قوة عرفية[2] وهو أحد المبادئ المشتقة من مبدأ السيادة، فإذا كان مبدأ السيادة ينطبق على عدد من الحقوق للدولة ذات السيادة مثل الحق في عدم التدخل في الشأن الداخلي، فهو أيضا ينطبق على بعض الالتزامات

[1] المرجع السابق – Delerue, F. – ص218

[2] Flemme, M. (2004). *Due Diligence in International Law* (Master Thesis). Faculty of Law - Lund University, p. 12. Retrieved from https://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=1557482&file
Samuel, K. L. H. (2018). The Legal Character of Due Diligence: Standards, Obligations, or Both? *Central Asian Yearbook of International Law*. https://doi.org/10.2139/ssrn.3264764

الدولية مثل مبدأ بذل العناية الذي تلزم الدول بموجبه الدولة ذات السيادة بحماية حقوق الدول الأخرى داخل إقليمها[1].

تطرقت محكمة العدل الدولية في قضية قناة كورفو لمبدأ العناية اللازمة وعرفته بأنه:

"التزام كل دولة بعدم السماح –عن علم– باستخدام أراضيها لأعمال تتعارض مع حقوق الدول الأخرى"[2].

وفي نطاق الهجمات الإلكترونية أكد تقرير فريق الخبراء الحكوميين للأمم المتحدة لعام 2015[3] مبدأ بذل العناية بالنص على أنه:

"ينبغي للدول ألا تسمح، عن علم، باستخدام إقليمها لارتكاب أفعال غير مشروعة دوليا باستخدام تكنولوجيا المعلومات والاتصالات"[4].

إن لمبدأ بذل العناية في مجال الهجمات الإلكترونية أهمية كبيرة، فهو يتصدى لحالة الهجمات المرتكبة من الجماعات الفاعلة من غير الدول. فإذا كانت الدول في الفضاء السيبراني غالبا ما تتنكر بالجماعات الفاعلة للتنصل من مسؤوليتها، فإن قاعدة بذل – العناية إذا انطبقت عناصرها – تجعل الدولة مسؤولة عن الأعمال الضارة التي تخرج من إقليمها، بغض النظر عمن قام بها: دولة أو أشخاص عاديون. ولذلك أهمية كبيرة. فمن ناحية تكون الدولة التي قصرت في واجب بذل العناية هي المسؤولة عن تعويض الدولة المتضررة من الهجمات السيبرانية التي أطلقت عليها من إقليم الدولة المسؤولة، وإن كان من أطلقها جماعات مسلحة، أو شركات، أو حتى افراد عاديون. ومن ناحية أخرى فأنه إذا تحققت

---

[1] تجدر الإشارة إلى أن مبدأ بذل العناية يجد جذوره في القانون الدولي البيئي فهو يرتبط بمنع الضرر البيئي العابر للحدود، وتمت الاستفادة منه في مجال قانون اللجوء إلى الحرب وخصوصا في التقنين السيبراني. وللمزيد عن أصل قاعدة بذل العناية في قضايا الضرر البيئي العابر للحدود انظر:

Foster, C. E. (2021). Global Regulatory Standards in Environmental and Health Disputes: Regulatory Coherence, Due Regard, and Due Diligence, pp. 27-30. Oxford, United Kingdom: Oxford University Press.

[2] "Every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States" - Corfu Channel case, Judgment of April 9th, 1949: I.C.J. Reports 1949, p. 4 [p. 22]

[3] الأمم المتحدة، الجمعية العامة، *فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي. مذكرة من الأمين العام*، A/70/174 (22 يوليو 2015). استرجع من https://undocs.org/A/70/174

تجدر الإشارة إلى ان تقرير فريق الخبراء الحكوميين لعام 2015 أيضا (كما تقرير عام 2013) تم تبني مخرجاته بقرار من الجمعية العامة للأمم المتحدة. انظر:

قرار الجمعية العامة 70/237، *التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي*، A/RES/70/237 (30 ديسمبر 2015). استرجع من https://undocs.org/A/RES/70/237

[4] A/70/174 – المرجع السابق – الفقرة 13(ج)، ص11

عناصر واجب بذل العناية يحق للدولة الضحية الرد على الدولة التي قصرت في بذل العناية. فالدولة الضحية تستطيع الرد بالتدابير المضادة على الدولة التي تخرج الهجمات من إقليمها إذا ثبت أنها مقصرة في بذل العناية؛ لوقف أفعال الجماعات غير الحكومية. وسيأتي التفصيل في شروط التدابير المضادة في الفصل الثالث.

يقصد ببذل العناية في الفضاء السيبراني وجوب أن تتخذ الدولة التدابير **الممكنة وفقاً لاستطاعتها** المعقولة لوقف الهجمات السيبرانية الضارة الصادرة من إقليمها. ولكي يقوم هذا الواجب على الدولة هناك خمسة عناصر يجب توافرها. إذا تخلف أحدها يسقط التزام الدولة منشأ الهجمات ببذل العناية وبالتالي يسقط حق الدولة الضحية بالرد. ونعرض العناصر الخمسة تباعاً على النحو الآتي:

أولاً: السيطرة على الإقليم[1]

المطلوب هنا هو السيطرة الفعلية على أرض الواقع وليس الولاية الإدارية أو التبعية القضائية. فاذا كان مبدأ بذل العناية مرتبطا بالسيادة الإقليمية فلا خلاف على التزام الدولة ببذل العناية داخل أراضيها، فتلزم الدولة بعدم استخدام أي جزء من أرضها بما يحويه من بنية تحتية سيبرانية مركزاً للفعل الضار بحقوق الدول الأخرى. هنا يمكن أن يطرح سؤال حول مدى إمكانية أن تلتزم الدولة ببذل العناية الواجبة في إقليم غير إقليمها الوطني.

محرك الالتزام ببذل العناية هو السيطرة. فالذي يسيطر هو المسؤول أمام القانون عن بذل العناية في مكان سيطرته. فإذا كانت الدولة تسيطر على إقليم غير إقليمها فهي المسؤولة عن بذل العناية في ذلك الإقليم. ويمكن تصور ذلك في حالتين: الأولى إذا كانت الدولة تسيطر على قاعدة أو مركز أو بنية تحتية سيبرانية في دولة أخرى فأنها تكون مسؤولة عما يصدر منها[2]. مثال ذلك القواعد العسكرية المملوكة للولايات المتحدة خارج حدودها، فالولايات المتحدة هي المسؤولة ألا يصدر من هذه القواعد ما يضر بدول أخرى.

[1] Tallinn Manual 2.0, commentary to rule 6, p. 30
[2] Tallinn Manual 2.0, commentary to rule 6, para. 10, p. 33

في الحالة الثانية تكون الدولة ملزمة ببذل العناية اللازمة في إقليم غير إقليمها إذا كانت هي التي تسيطر على ذلك الإقليم[1]، هنا الحديث عن حالة الاحتلال الذي تعرفة اتفاقية لاهاي "تعتبر أرض الدولة محتلة حين تكون تحت السلطة الفعلية لجيش العدو. ولا يشمل الاحتلال سوى الأراضي التي يمكن أن تمارس فيها هذه السلطة "[2] ويتبين من التعريف أن الاحتلال قد يكون كليا مثلما كانت احتلال الولايات المتحدة للعراق فقد كان الانتشار العسكري كبيراً للولايات المتحدة على الأراضي العراقية، وقد يكون جزئيا مثل حالة الدول التي تسيطر على إقليم معين من الدولة ففي الحالة الأخيرة تكون الدولة مسؤولة ببذل العناية في الجزء الذي يقع تحت سيطرتها فقط.

ثانياً: وجود العلم الحقيقي أو المفترض بالهجمات

يجب أن تعلم الدولة أن ما يخرج من أراضيها أو عبر أراضيها من هجمات إلكترونية يؤثر على حق الدول الأخرى، ويسبب ضررا، فإذا تناهى إلى علم الدولة أن نشاطا صادرا من إقليمها يؤثر على حق دولة أخرى فعليها التدخل فورا وقد تعلم الدولة ذلك بنفسها عن طريق رصد الهجمات الإلكترونية عبر وكالة الأمن السيبراني لديها، أو –وهو الاحتمال الاغلب– أن تقدم لها الدولة المستهدفة تقريرا يثبت استخدام إقليم الدولة الأولى لإطلاق هجمات إلكترونية ضارة. وهذا ما يعرف بالعلم الحقيقي[3].

وإذا تعذر العلم الحقيقي وجب النظر في إمكانية العلم الافتراضي. فإذا ادعت أنها لا تعلم بخروج الهجمات الإلكترونية الضارة بحق الدولة الضحية من إقليمها فيجب النظر إلى الظروف التي حدثت فيها الهجمات السيبرانية، وما إذا كانت دولة أخرى في نفس الظروف ووفق المسار الطبيعي للأحداث كان يمكن، أو كان يتوجب عليها أن تعلم، فهنا نكون أمام العلم المفترض[4].

---

[1] Tallinn Manual 2.0, commentary to rule 6, para. 9, pp. 32-33

[2] تنص المادة 42 من اتفاقية لاهاي الخاصة باحترام قوانين وأعراف الحرب: "تعتبر أرض الدولة محتلة حين تكون تحت السلطة الفعلية لجيش العدو ولا يشمل الاحتلال سوى الأراضي التي يمكن أن تمارس فيها هذه السلطة بعد قيامها."
المؤتمر الدولي (لاهاي)، *اتفاقية لاهاي الرابعة الخاصة باحترام قوانين وأعراف الحرب البرية ومرفقها اللائحة المتعلقة بقوانين وأعراف الحرب البرية* (18 أكتوبر 1907). استرجع من https://www.icrc.org/ar/doc/resources/documents/misc/62tc8a.ht

[3] Tallinn Manual 2.0, commentary to rule 6, para. 37, p. 40

[4] Tallinn Manual 2.0, commentary to rule 6, paras. 38-42, pp. 40-42

ثالثاً: وجود هجوم سيبراني قائم

يؤكد مايكل شميت أن الالتزام ببذل عناية لا يمكن قيامه إلا بصدد هجوم إلكتروني حال وقائم فبذل العناية التزام ينشأ بنشأة الهجوم السيبراني وينتهي بانتهائه[1]، ذلك لأن بذل العناية في نطاق الهجمات السيبرانية هو التزام علاجي يتلخص في التزام الدولة بإيقاف الهجوم الذي انطلق من إقليمها أو عبره، ويضر بحقوق الدول الأخرى. والالتزام بإيقاف الهجوم يتطلب وجود هجوم سيبراني قائم[2].

وهذا يحتم توافر ثلاثة أطراف لقيام قاعدة العناية اللازمة، وهي أولا، الدولة المستهدفة، ثانيا، دولة المنشأ أو الدولة التي يستخدم إقليمها لإطلاق الهجمات الإلكترونية وهي الدولة الملزمة ببذل العناية، وثالثا، طرف ثالث لا يمثل دولة المنشأ، لكنه يستخدم إقليمها أو إقليم يقع تحت سيطرتها. هذا الطرف الثالث يمكن أن تكون دولة ثالثة تستخدم إقليم دولة أخرى بهدف التضليل، وقد يكون جماعات مسلحة على إقليم دولة المنشأ، أو شركات خاصة، أو حتى أفراد عاديين[3]. وأيا كان الطرف فإن الدولة التي تخرج منها الهجمات –الضارة بحقوق الدول الأخرى– ملزمة بإيقافها بموجب مبدأ بذل العناية.

تجدر الإشارة إلى أن بذل العناية المتفق عليه هو بذل العناية اللاحقة أو العلاجية؛ مما يقضي بواجب الدولة بإيقاف (إيقاف هجوم حال) الهجمات الإلكترونية الصادرة من إقليمها. أما الالتزام الوقائي (منع الهجوم من أن يقع ابتداء)، وإن كان طموحا جيدا ان يتحول واجب بذل العناية إلى الجانب الوقائي، لكن حاليا لا يوجد التزام قانوني يلزم الدول بمعرفة كل ما يحدث من أعمال غير مشروعة على أراضيها[4]، فدليل (تالين) يرى أنه لا يوجد –حاليا– ما يكفي من الممارسة الدولية والتوافق الدولي للالتزام بالبعد الوقائي، حيث يؤكد الخبراء أنه لا يمكن إلزام الدول بأمر هم غير ملتزمين به وفقا للنظام الحالي[5].

---

[1] Schmitt, M. N. (2015). In Defense of Due Diligence in Cyberspace. *The Yale Law Journal*, *125* (Forum 68), 68–81 [pp. 75-76]. Retrieved from https://www.yalelawjournal.org/forum/in-defense-of-due-diligence-in-cyberspace

[2] المرجع السابق

[3] Tallinn Manual 2.0, commentary to rule 6, para. 7, p. 32

[4] Crawford, J. (2013). State Responsibility: The General Part, p. 226. Cambridge, United Kingdom: Cambridge University Press.

[5] Tallinn Manual 2.0, commentary to rule 6, para. 5, pp. 31-32

وعادة ما يستدل على واجب العناية العلاجي من حكم محكمة العدل الدولية في قضية قناة كورفو فقد جاء في حكمها أنه:

"لا يمكن الاستنتاج من مجرد حقيقة السيطرة التي تمارسها دولة ما على أراضيها ومياهها أنها كانت تعلم بالضرورة، أو كان من المفترض أن تعلم، بأي فعل غير قانوني يُرتكب فيها"[1].

ويبدو هذا التوجه منطقيا؛ لأنه من الصعوبة إلزام الدولة بمراقبة جميع الحركات التي تمر عبرها أو تصدر منها أو العابرة لها. حتى وإن كان من الممكن مراقبة كل مرور على حركة الإنترنت، فإن تحديد تلك الهجمات الضارة التي تهدد حقوق الدول الأخرى يتطلب الكثير من العمل لمعالجة البيانات الخاضعة للمراقبة، وإن كانت ذات صلة بواجب بذل العناية. كذلك هناك بعد آخر وهو تهديد الحريات وحقوق الإنسان، –وخصوصا الحق في الخصوصية– جعل الالتزام ببذل عناية التزام وقائي فيه إطلاق ليد السلطات في مسألة التجسس على حياة كل الأشخاص على إقليمها؛ للتأكد من عدم وجود نية للقيام بهجمات إلكترونية غير مشروعة.

لكن هناك توجه يقوم ضد دليل (تالين)، يرى أن بذل العناية يتكون من مرحلتين: أولهما: هي اليقظة، والثانية هي بذل العناية؛ لإيقاف الفعل الإلكتروني الضار الصادر من إقليم الدولة. يقصد باليقظة مراقبة الأنشطة الإلكترونية في المنطقة لمنع الاستخدام الضار للإنترنت بالبنية التحتية الموجودة داخل حدود الدولة[2]. والسؤال الذي يرتبط بواجب اليقظة –إن وجد– هو هل يجب أن تتحرك الدولة وتبذل العناية بناء على المعلومات المسبقة التي تملكها؟ لأن هذا يدخل في الجانب الوقائي الذي هو في رأي دليل (تالين) لا توجد ممارسة كافية لدعمه. فإذا تم الأخذ بواجب اليقظة ثم واجب العمل ببذل العناية

---

[1] *Corfu Channel* judgement, p. 18

[2] المرجع السابق – Schmitt, M. N. – In Defense of Due Diligence in Cyberspace – ص75-76
انظر أيضا:
Sun, Y. (2022). The Future of Due Diligence in Cyberspace. *New York University Journal of International Law and Politics, 54*(2), 753–764 [p. 752]. Retrieved from https://www.nyujilp.org/wp-content/uploads/2022/05/nyi_54-2-449-460_Sun.pdf
Dias, T., & Coco, A. (2022). Cyber due diligence in international law. Oxford Institute for Ethics, Law and Armed Conflict, p. 147. Retrieved from https://www.elac.ox.ac.uk/wp-content/uploads/2022/03/finalreport-bsg-elac-cyberduediligenceininternationallawpdf.pdf
Geiss, R., & Lahmann, H. (2013). Freedom and Security in Cyberspace: Shifting the Focus away from Military Responses towards Non-Forcible Countermeasures and Collective Threat-Prevention. In *Peacetime Regime for State Activities in Cyberspace* (pp. 621–657) [pp. 654-655]. Tallinn, Estonia: NATO CCD COE Publications.

بناء على اليقظة يسقط شرط "وجود هجوم سيبراني حال"، ويصبح التحرك ببذل العناية ضد هجوم سيبراني وشيك أو محتمل.

ويبدو أن الرأي القائل باقتصار قاعدة بذل العناية على المهمة العلاجية هو الأقرب إلى القبول. بالتأكيد من الجيد القول: إن على الدول واجب رقابة الاستخدام الضار للأنترنت، وواجب التحرك لمنع العمليات الضارة بحقوق الدول الأخرى إذا تناهت لعلمها، لكن هذه الأقوال حديثة نسبيا لذلك يمكن أن تعد من قبيل السلوك المسؤول، لكن لا يمكن القول: إنها واجب قانوني ملزم وتحاسب عليه الدول التي لا تقوم به؛ لأن جانب الإلزام لم ينضج بعد.

بالرغم من أن مؤيدي هذا الرأي يشيرون إلى حكم محكمة العدل الدولية في قضية تطبيق اتفاقية منع جريمة الإبادة الجماعية والمعاقبة عليها فقد ذهبت المحكمة إلى:

" أن التزام الدولة بالتصرف يظهر عندما تعلم الدولة، أو يجب أن تعلم بها بشكل طبيعي الخطر الشديد للإبادة الجماعية"[1]

لكن يرُّد (تالين) أنه في –هذا الصدد– يجب التمييز بين قواعد القانون الدولي العامة والقواعد غير العامة التي تهدف لمنع حدوث فعل معين. بناء عليه حكم المحكمة كان خاصاً بواجب منع الإبادة الجماعية الذي تكون الوقاية فيه ركنا اساسيا. لكن لا يوجد مثل هذا الالتزام الأساسي المتميز فيما يتعلق بالعمليات السيبرانية الضارة بشكل خاص. لذلك، تطبق القاعدة العامة لمبدأ بذل للعناية وهي علاجية[2]. برغم ذلك، فالاعتراض قائم على واجب اليقظة وليس التحرك ضد الهجوم السيبراني المحتمل إذا تناهى إلى علم الدولة. فمايكل شميت لا ينفي إمكان قيام واجب بذل العناية ضد هجوم سيبراني غير قائم لكنه وشيك بمعنى بدأ تنفيذه لكن نتائجه لم تظهر أو تكتمل بعد. فيكون واجباً على الدولة

---

[1] Art. 1: "The Contracting Parties confirm that genocide, whether committed in time of peace or in time of war, is a crime under international law which they undertake to prevent and to punish." UN General Assembly, *Convention on the Prevention and Punishment of the Crime of Genocide*, 9 December 1948, United Nations, Treaty Series, vol. 78, p. 277, available at: https://www.refworld.org/docid/3ae6b3ac0.html [accessed 17 September 2022]

انظر أيضا:

Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), Judgment, I.C.J. Reports 2007, p. 43 [para. 431, pp. 221-222]

[2] Tallinn Manual 2.0, commentary to rule 6, para. 6, p. 32

أن تبذل العناية متى ما علمت بهذا الهجوم السيبراني المحتمل، كأن توقفه الدولة في مرحلة التخطيط أو بداية التنفيذ[1].

كذلك يجب الانتباه إلى ما يعنيه واجب اليقظة. فلن تستطيع الدولة بذل العناية الوقائي إلا بمراقبة كل استخدامات الأنترنت على إقليمها! الضارة والمشروعة، وربما وجبت زيادة صلاحيات أجهزة المخابرات والتجسس والعناصر الأمنية، وهذا يستتبع خرق للحق في الخصوصية، وفيه تقييد خطير للحريات. وإلى أن توجد طرق تستطيع بها الدولة رصد النشاط السيبراني الضار – دون أن يكون في ذلك تأثير على الحقوق والحريات– فإنه من الصعب تطبيق الشق الوقائي لمبدأ بذل العناية.

رابعاً: أن تؤثر الهجمات على حق مقرر بمقتضى القانون الدولي للدولة الأخرى

لكي يتحرك واجب الدولة في بذل العناية لا بد أن تؤثر الهجمات السيبرانية على حق تملكه الدولة بموجب القانون الدولي، كالحق في عدم التدخل في الشأن الداخلي، أو الحق في عدم العدوان، أو عدم استخدام القوة أو في عدم انتهاك مبدأ السيادة. وقد وضع دليل (تالين) هذا الشرط بهدف التفريق بين ما يعد حقا يعتبر حق وفقا للقانون، وما هو مصلحة وطنية[2]. فمثلا من مصلحة الدولة ألا يتم التجسس على معلومات مواطنيها أو بياناتها الحكومية، لكن ليس هناك قاعدة قانونية تحمي هذه المصلحة! لذلك يسقط واجب بذل العناية، فليس واجباً على الدولة التحرك إلا إذا علمت أن الهجمات الصادرة من إقليمها تمس حقوق أحد الدول. يجد هذا الشرط تأكيده من خلال تعريف قضية قناة كورفو لمبدأ بذل العناية اللازمة الذي ينص على "التزام كل دولة بعدم السماح عن علم باستخدام أراضيها لأعمال تتعارض مع **حقوق الدول الأخرى**"[3].

[1] The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) [natoccdcoe]. (2018, June 20). *Due Diligence in Cyberspace - CyCon 2018* [Video file] 14:00. Retrieved from https://youtu.be/YOIuiNfaZU8?t=840

[2] Tallinn Manual 2.0, commentary to rule 6, para. 2, p. 31; para. 15, p. 34

[3] *Corfu Channel* judgment, p. 22

خامساً: أن تكون لتلك الهجمات آثار وعواقب جادة Serious Adverse Consequences

كذلك هناك معيار مهم لقيام واجب التدخل ببذل العناية من قبل الدولة، وهو أن تكون الهجمات الإلكترونية على قدر من الخطورة والجدية[1]، فلا ينفذ الواجب بمجرد إزعاج إلكتروني مثل التشويش والحرمان الطفيف المؤقت من الخدمة. بل، يجب أن يرتفع الضرر إلى المستوى الذي يصبح مصدر قلق مشروع في العلاقات بين الدول. ويستوي في ذلك أن يكون الأذى على منشآت أو ممتلكات حكومية أو خاصة، طالما أن الهجمات تمس حقا بمقتضى القانون الدولي. إن اشتراط الآثار الجادة للهجمات منطقي. فبذل العناية فيه تحريك لأجهزة الدولة، فلا بد من التمييز بين الهجمات التي تجعل الدولة مسائلة عن واجبها ببذل العناية وملايين الهجمات والعمليات السيبرانية التي تحدث على مدار الساعة من قبل الأفراد.

هذا المعيار الذي يجد جذوره في التشريعات البيئية التي تهتم بمسألة الأذى العابر للحدود. مثلا في قضية Semelter 1941 بين الولايات المتحدة وكندا رأت هيئة التحكيم[2]:

"لا يحق لأية دولة استخدام أراضيها أو السماح باستخدامها بطريقة تؤدي إلى احداث ضرر بسبب الابخرة في إقليم آخر أو الممتلكات أو الأشخاص الموجودين فيه عندما تكون الحالة ذات عواقب على قدر من الخطورة والجدية".[3]

---

[1] Tallinn Manual 2.0, commentary to rule 6, para. 38, p. 40

[2] ترايل سملتر (Trail Smelter) وهي شركة كندية مقرها في كندا تسببت أنشطتها المتمثلة في معالجة الرصاص والزنك بتلويث الغابات عبر الحدود الأمريكية الكندية، واتلاف المحاصيل، حتى وصلت الأدخنة إلى واشنطن، وتسببت في ازعاج السكان. وقد سعت الولايات المتحدة من خلال اللجوء للتحكيم الحصول على تعويضات من كندا بسبب التلوث الصادر من اقليمها. انظر:
Trail Smelter Case (United States v. Canada) (1938 and 1941) 3 R.I.A.A. 1905. Retrieved from https://legal.un.org/riaa/cases/vol_III/1905-1982.pdf
Jensen, E. T., & Watts, S. (2021). Cyber Due Diligence. *Oklahoma Law Review*, *73*(4), 645–710 [p. 665]. Retrieved from https://digitalcommons.law.ou.edu/cgi/viewcontent.cgi?article=2215&context=olr

[3] *Trail Smelter* case, p. 1965

المطلوب من الدولة التي تصدر الهجمات من إقليمها إذا توافرت شروط بذل العناية:

إذا كانت الدولة تملك السيطرة على الإقليم الذي تنطلق منه الهجمات السيبرانية الضارة تجاه الدولة الضحية، وكانت تعلم بتلك الهجمات، كأن تشعرها الدولة الضحية أو أن ينتشر خبر الهجمات في الإعلام، أو كان يفترض أن تعلم مقارنة باي دولة في الظروف نفسها وكانت الهجمات واسعة النطاق وذات آثار جادة، تؤثر على حقوق الدولة الضحية –بموجب القانون الدولي، وكانت الدولة تستطيع القيام بتدابير تحد من تلك الهجمات الضارة– يصبح من الواجب على الدولة التي تصدر الهجمات من إقليمها **أن تتخذ كل التدابير الممكنة لديها لوقف تلك الهجمات السيبرانية الضارة**[1]. فلا تحاسب الدولة إلا على إمكاناتها، وما تستطيع القيام به.

المبحث الثاني

الدفاع عن النفس ضد الهجمات السيبرانية

بعد أن نص ميثاق الأمم المتحدة على قاعدة منع استخدام القوة بالطريقة التي تم تفصيلها سابقا، حدد الميثاق حالتين فقط يمكن بمقتضاهما مخالفة هذه القاعدة، أو بالأحرى استثنائين من قاعدة استخدام القوة حيث يمكن للدول أن تستخدم قوة السلاح ضد دولة أخرى، وهما: حالة الدفاع عن النفس بمقتضى المادة 51، وحالة استخدام مجلس الأمن لصلاحياته؛ لحفظ السلم والأمن الدولي، بموجب الفصل السابع من الميثاق وتسمى الأمن الجماعي.

فيما يخص مجلس الأمن ومهمته في مواجهة هذه الظاهرة فإنه موضوع سيتم التطرق إليه في المبحث الثالث من هذا الفصل. لكن نكتفي بالإشارة هنا إلى إن مجلس الأمن يملك كل الأدوات التشريعية التي تسمح له بممارسة عمل فعال في تنظيم السلام في الفضاء السيبراني. ومع ذلك فهذا أمر غير متوقع نتيجة لحالة الشلل التي يعيشها المجلس واتساع الهوة بين المعسكر الشرقي والغربي يوما بعد يوم. فضلا عن أنه يبدو أن موضوع الهجمات السيبرانية لم يدخل ضمن أولويات مجلس الأمن بعد، فحتى

[1] Tallinn Manual 2.0, commentary to rule 6, para. 43, p. 42; commentary to rule 7, para. 2, p. 43; commentary to rule 7, para. 18, p. 47

الآن لم يصدر قرار بخصوص الهجمات السيبرانية[1] برغم الدعوات المتكررة من قبل الأمين العام لإيلاء الظاهرة الاهتمام اللازم.

أما الدفاع عن النفس ضد الهجمات السيبرانية فهو محل تفصيل هذا المبحث، وهو المعتاد في تدرج منظومة استخدام القوة في العلاقات الدولية، فبعد مناقشة قاعدة منع استخدام القوة يتبعها عادة الدفاع عن النفس بوصفه أوضح استثناء من تلك القاعدة. فالدفاع عن النفس كحق قديم قدم الدولة، أقر به الميثاق وبأصالته. لذلك عندما تستخدم الدول القوة، فأنها لا تجادل في قاعدة منع استخدام القوة. لكنها تجادل في حق الدفاع عن النفس فنجدها تحاول التوسع في الدفاع عن النفس؛ لإدخال بعد التصرفات تحت شرعية الدفاع عن النفس. لذلك ظهر الدفاع عن النفس التراكمي والدفاع عن النفس الاستباقي والدفاع عن النفس ضد الجماعات الفاعلة من غير الدول.

المطلب الأول يعالج دراسة قاعدة الدفاع عن النفس في وضعها التقليدي، ولا نعني بالتقليدي هنا الهجوم بالسلاح التقليدي، بل نعني الهجوم السيبراني المكتمل الأركان من دولة على دولة أخرى، وفي المقابل العناصر الواجب توافرها لقيام حق الدفاع عن النفس في هذه الحالة. ثم في المطلب الثاني ستقف الدراسة على حالات التوسع في الدفاع عن النفس، ومدى شرعيتها وانطباقها على خصوصية الهجمات السيبرانية.

المطلب الأول

الدفاع عن النفس ضد الهجمات السيبرانية في صورته التقليدية

الدفاع الشرعي عن النفس كما هو مطبق اليوم وفقا للقانون الدولي ينطلق من ثلاثة عناصر أو ثلاثة شروط تجعله حقا مشروعا. والعناصر الثلاثة هي مزيج من قواعد عرفية وقواعد جاء بها الميثاق. فالعرف جاء بشرطي الضرورة والتناسب، والميثاق جاء بشرط الهجوم المسلح. يناقش هذا المطلب القاعدتين العرفيتين وقاعدة الهجوم المسلح مع محاولة تطبيقها على الهجمات السيبرانية.

[1] تجد الإشارة إلى أن المجلس عقد جلسة نقاشية عامة لظاهرة الهجمات السيبرانية دون أن تتلوها خطوات عملية للتصدي لهذه المشكلة، الجلسة النقاشية موجودة على الرابط التالي:
Security Council [United Nations - UN Web TV]. (2021, June 29). Cyber security - Security Council, VTC Open debate [Video file]. Retrieved from https://media.un.org/en/asset/k1e/k1egd92tkq

من الضروري الانتباه إلى أنه –في دراسة هذا المطلب– هناك أمر لا بد أن يتم حاضرا وهو أن الحديث مقتصر على الدفاع عن النفس ضد هجوم سيبراني فقط. فالدفاع عن النفس ضد هجوم مسلح تقليدي –وإن كان ذلك الدفاع بوسيلة سيبرانية– ليس موضوع جدل في القانون الدولي، خصوصا إذا اكتملت عناصر الهجوم المسلح فللدولة أن تختار الأداة المناسبة للرد من الأدوات المطروحة كالطائرات الحربية، أو الهجمات السيبرانية، طالما كان ذلك متماشيا مع متطلبات الضرورة والتناسب. لكن الجدل هو الرد بالدفاع عن النفس ضد الهجوم السيبراني، سواء أكان الرد بوسيلة سيبرانية مشابهة؟ أم كان الرد بالسلاح التقليدي، وفي هذا الأخير تشتد مخاوف التصعيد والحروب. لذلك كل الحديث في المبحث القادم يعنى بالدفاع عن النفس ضد هجوم مسلح سيبراني.

الفرع الأول: شروط الدفاع عن النفس في القانون الدولي العرفي (الضرورة والتناسب)

كما أسلفنا فإن الدفاع عن النفس قديم قدم الدولة. استخدمته الدول قبل ميثاق الأمم المتحدة، لكن هناك حادثة فاصلةً في استخدام الدفاع عن النفس، تفصل بين الاستخدام العشوائي –إن صح التعبير– وبين الاستخدام المضبوط بإطار من المشروعية، وهي حادثة السفينة كارولاين.[1] هذه الحادثة لا بد من ذكرها؛ لأن المبادئ التي جاءت بها (الضرورة والتناسب) لازالت إلى اليوم متطلبات قانونية في الدفاع عن النفس.

حادثة كارولاينا 1837م:

كارولاين هي سفينة بخارية مملوكة ملكية خاصة لمواطنين أمريكان. في العام 1837م كانت أمريكا قد نالت استقلالها، بعكس كندا التي مازالت تحت الاستعمار البريطاني. استخدمت سفينة كارولاين لدعم حركة التحرر الكندية، فكانت تنقل الرجال والذخائر من الولايات المتحدة عبر نهر نياجرا وصولاً إلى كندا. ما تجدر ملاحظته أن ذلك لم يكن تصرفاً صادراً من الحكومة الأمريكية، لكن من مواطنين أمريكيين داعمين للثوار الكنديين. قامت قوات بريطانية خاصة بمهاجمة السفينة عندما كانت راسية في نيويورك. ونتيجة للهجوم فقد بعض من كان على سطح السفينة حياته وأجبر البقية على مغادرتها، ثم أُشعلت النار فيها وأُغرقت في نهر نياجرا. سوغت بريطانيا لهذا الفعل أنه دفاع عن إقليمها في كندا. هذه الحادثة كانت سبباً في بدء مراسلات دبلوماسية بين وزير الخارجية الأمريكي آنذاك (دانييل وبستر)

[1] هذا يعني أن حادثة كارولاين هي أول مساهم تاريخي في تقنين الدفاع عن النفس، فقبلها وجدت فكرة "الحرب العادلة الآتية من الديانة المسيحية" لكنها الأصل العرفي للدفاع عن النفس كما هو في صورته الحالية اليوم.

وممثل بريطانيا في واشنطن (اللورد آشبرتون). تبادل الرجلان مراسلات بخصوص الحادثة لعدة سنوات تلت، تلك المراسلات تُعدُّ غاية في الأهمية؛ لأنها أسست لقواعد فعل الدفاع عن النفس[1].

ومما جاء في رسائل (دانييل وبستر):

- لنكون أمام حالة دفاع عن النفس يجب أن تكون هناك "ضرورة ملحة لممارسة هذا الحق، وألا تترك الظروف المحيطة للطرف المعني فرصة لاختيار الوسيلة التي يراها مناسبة، وألا يكون هناك وقت لإمكانية التشاور وتدبر الأمر".
- " فعل الدفاع يجب ألا يتضمن شيئاً غير معقول أو مفرط. بما أن الفعل، تبرره ضرورة الدفاع عن النفس، يجب أن يكون محدوداً بسبب هذه الضرورة، ويبقى بوضوح في حدودها."[2]

هذا النص أصبح يعرف لاحقا باختبار كارولاين، وقد ظل المرجع والأساس لفعل الدفاع عن النفس لأكثر من مئة عام. يستنتج من قراءة الفقرتين أنه لكي يكون الفعل دفاعاً عن النفس يجب أولاً أن تكون هناك ضرورة للدفاع عن النفس، وثانيا فعل الدفاع يجب ألا يكون غير معقول أو مفرط (أن يكون متناسباً). اتفق الرجلان كلاهما على معياري الضرورة والتناسب؛ ليكون الدفاع عن النفس صحيحاً ومشروعاً، ا لم يتفقا على تحققهما في حادثة كارولاين، فالممثل البريطاني قال بتوافر المعيارين والوزير وبستر أصر على عدم توافرهما[3].

يصعب القول: إن حادثة واحدة أسست قاعدة دولية عرفية بمفردها، إلا أن المبدئين الذين جاءت بهما حادثة كارولاين (الضرورة والتناسب) لاقت قبولاً واستخداماً متكرراً بين الدول (ببطء لكن ثابت)[4]. فهي

---

[1] Nichols, T. M. (2008). *Eve of Destruction: The Coming Age of Preventive War*, p. 2. University of Pennsylvania Press.

[2] يتكرر النص في كثير من الأوراق التي تعالج الدفاع عن النفس مثلا:

Stevens, K. R. (1989). *Border Diplomacy: The Caroline and McLeod Affairs in Anglo-American-Canadian Relations, 1837-1842* (1st ed.). University Alabama Press.

Rogoff, M. A., & Collins, E. Jr. (1990). The Caroline Incident and the Development of International Law. *Brooklyn Journal of International Law*, *16*, 493.

Sofaer, A. D. (2003). On the Necessity of Pre- emption. *European Journal of International Law*, *14*(2), 209–226. Retrieved from http://ejil.org/pdfs/14/2/411.pdf

[3] Ruys, T., Corten, O., & Hofer, A. (Eds.). (2018). *The Use of Force in International Law: A Case-Based Approach*, pp. 5-10. Oxford, United Kingdom: Oxford University Press. https://doi.org/10.1093/law/9780198784357.001.0001

[4] تجدر الإشارة إلى أن محكمة العدل الدولية أقرت شرطي الضرورة والتناسب بوصفهما شروطا للدفاع عن النفس، في حكم نيكاراغوا وأعادت تأكيدهما عليهما في قضية المنصات النفطية وفي فتوى الأسلحة النووية

Nicaragua judgment, para. 176, p. 94; para. 194, p. 103

Oil Platforms judgment, paras. 43, p. 183; paras. 73–74, pp. 196-197; para.76, p. 198

لم تصنع قانوناً بمفردها، لكنها الجذور والأصل لقاعدتين عرفيتين مهمتين. ففي ذلك الوقت لم يكن هناك مبدأ عدم استخدام القوة، وعذر الدول بالدفاع عن النفس كان مقبولاً وإن لم يكن متناسباً. لكن من بعد حادثة كارولاين فإن الدفاع عن النفس لا يمكن أن يكون مشروعا إلا بتحقق معياري الضرورة والتناسب[1]، اللذين يختلفان هنا في القانون الدولي عنهما في القانون الجنائي، وسنوضح كلاً منهما على حدة ثم نطبقه على الهجمات الإلكترونية في القانون الدولي.

القسم الأول: الضرورة في الدفاع عن النفس ضد هجمات سيبرانية[2]

عندما القول: إن فعل الدفاع يجب أن يكون ضرورياً فإن ذلك لا يعني أن تكون الدولة في حالة تهديد وجودي[3]، أي إما أن تدافع عن نفسها أو أنها لن تكون موجودة. بل يكفي ألا يكون هناك خيار آخر سوى الدفاع عن النفس [4]. ليس لأن الدولة لن تكون موجودة بعد ذلك إذا لم تدافع عن نفسها، ولكن الهجوم حاصل عليها الآن أو قادم إليها مباشرة فلا تملك خيارا سوى صده بالقوة دفاعاً عن نفسك، – بمعنى آخر– لأن اللجوء إلى القوة هو الخيار الأخير الذي لا يوجد سواه لوقف الهجوم المسلح[5]. إنه من المهم فهم المقصود بالخيار الأخير، أو آخر الحلول بوصفه معيارا للضرورة. وهذا يعني أنه قد تم استنفاد جميع الطرق السلمية ولم يبق طريق غير اللجوء إلى القوة دفاعاً عن النفس. أي أنه على الدولة أن تثبت أنها قامت بالتفاوض، أو حاولت التفاوض مع الدولة الغازية، أو قامت بإجراءات كقطع العلاقات الدبلوماسية والاقتصادية، أو تكون حاولت أخذ المسألة إلى مجلس الأمن. وبعبارة أخرى على الدولة أن تثبت أنها قامت بكل الإجراءات السلمية الممكنة ولم تنفع في وقف الهجوم عليها لذلك فاستخدام القوة هو خيارها الأخير[6].

وهناك بديل آخر لإثبات عنصر الضرورة، وهو عندما تكون الدولة في ظرف قهري بحيث لا يمكن أن تتوقع منها الدول الأخرى أن تبدأ بالتفاوض في مثل ذلك الموقف، لذلك فإن مقتضيات المنطق تتطلب

Nuclear Weapons advisory opinion, para. 41, p. 245

[1] O'Brien, J. (2001). International Law (1st ed.), p. 682. Abingdon, United Kingdom: Routledge.
[2] Gardam, J. (2009). *Necessity, Proportionality and the Use of Force by States*. Cambridge, United Kingdom: Cambridge University Press. https://doi.org/10.1017/CBO9780511494178
[3] المرجع السابق
[4] المرجع السابق – ص150
[5] المرجع السابق – The International Court of Justice – Green, J. A. – ص76
[6] المرجع السابق – ص80-85

الاستنتاج أنه الحل الأخير دون أن تقوم الدولة بسلك كل الطرق السلمية المتاحة لتسوية النزاع[1]. كل ما على الدولة إثباته هنا أنه من غير المنطقي أن يتوقع منها أن تقبل بالتفاوض، أو تتخذ إجراءات مثل العقوبات الاقتصادية، لأن الموقف لا يسمح إلا باستخدام القوة وفقا لمقتضيات العقل والمنطق.

ففي الواقع لا يلوم المجتمع الدولي دولة دافعت عن نفسها بعد قيام قوات مسلحة بعبور حدودها والتوغل في عمق أراضيها، بحجة أنها لم تحاول التفاوض، فلا أحد يتوقع التفاوض في مثل هذه الظروف، ويصبح الدفاع عن النفس باستخدام القوة هو التصرف الوحيد المنطقي لرد العدوان. لكن إذا كانت غارة بسيطة نسبيا عندها يمكن القول: أنه متوقع من الدولة أن تحاول فتح قناة للمحادثة والتفاهم قبل أن تسارع بالرد بالقوة. فآخر حل أو آخر خيار لا يعني أنها مسألة وجود أي لحماية وجود الدولة بل يعني حماية مصالحها الأمنية، المشكلة هنا أن هذا المعيار يترك المجال للدول لتقدر حالة الضرورة تقديراً شخصياً[2].

الضرورة في الهجمات السيبرانية:

ننتقل بالحديث إلى الهجمات السيبراية وعنصر الضرورة في الدفاع عن النفس ضد الهجمات السيبرانية. ففي نطاق العمليات السيبرانية لا يختلف النقاش عن القاعدة العامة للضرورة فيجب أن تثبت الدولة التي تعرضت لهجوم سيبراني مسلح ان قرار الدفاع عن النفس كان ضروريا لصد الهجوم الإلكتروني بمعنى أن الدفاع هو الاستجابة الوحيدة الممكنة لوقف الهجوم السيبراني المسلح[3]. ليس في بداية العملية الدفاعية فحسب بل يجب أن يكون عنصر الضرورة حاضرا في كل عملية في الهجوم الدفاعي، فكل خطوة يجب أن تكون مرتبطة بإحباط الهجوم الإلكتروني الذي تتعرض له الدولة.

ولا يشترط أن يكون الرد على العملية السيبرانية سيبرانياً بالمثل فيمكن أن يكون ماديا طالما أنه ضروري لصد الهجوم. مثلا الهجمة الدفاعية يمكن أن تكون استهدافا ماديا للبنية التحتية المستخدمة في العمليات السيبرانية، مثل خوادم الإنترنت، أو البنى التحتية المستخدمة لربط أجهزة الكومبيوتر ونقل البرامج والوسائط مثل الأسلاك والمحولات، أو ضرب النظام الكهربائي الذي يشغل العملية السيبرانية – وكذلك

[1] المرجع السابق – ص85-86
[2] المرجع السابق
[3] المرجع السابق
Dinstein, Y. (2012). *War, Aggression and Self-Defence,* p. 232. Cambridge, United Kingdom: Cambridge University Press.

البنية التحتية التي تنطلق منها العمليات السيبرانية كأجهزة الحاسوب والمبنى الذي يحتويها.[1] كل ذلك دفاع عن النفس موجه نحو وقف الهجمات الإلكترونية.

وكما أن الضرورة دفاعا عن النفس في سياقها العام تعني آخر الحلول كذلك فإن مفتاح تحليل الضرورة في السياق السيبراني هو وجود أو عدم وجود مسارات عمل بديلة لا تصل لمستوى استخدام العنف[2]. تلك التدابير السلمية التي تحتم على الدولة التي تتعرض إلى هجوم أن تقوم بها مثل محاولة التواصل مع الدولة التي قامت بالهجوم، والتفاوض، من الممكن أن يكون الهجوم الإلكتروني على دفعات تظهر آثارها في مراحل قد يصعب تطبيق تلك المعايير في بعض سيناريوهات الهجمات الإلكترونية، خصوصا إذا كانت الهجمة قصيرة ومباغته؛ لذلك فإن هناك تدابير سلمية أخرى أكثر تناسبا.

ومن امثلة التدابير السلمية المتوقع البدء بها في سيناريو الهجوم الإلكتروني أن تكون الدولة المستهدفة قادرة على اتخاذ ما يعرف باستخدام الدفاعات السيبرانية السلبية قبل الدفاع السيبراني النشط.[3] ومثالها بأن تضبط الميزات الأمنية لنظامها الخاص بحيث تمنع المتسللين من الوصول وذلك بتصحيح الثغرات الأمنية التي تستغلها العملية الإلكترونية الهجومية، أو أن تقوم بفصل الإنترنت مؤقتا ونحو ذلك من الإجراءات السلبية غير الهجومية، وبالتالي فإن الدفاع عن النفس من شأنه أن يصبح غير ضروري.

كذلك وإن كان استخدام القوة التقليدية –دفاعا عن النفس ضد هجمات إلكترونية– ضروريا لصدها، فإنه يجب على الدولة المستهدفة أولاً أن تنظر في إمكانية اتخاذ إجراءات سيبرانية مضادة ضد الدولة المهاجمة قبل التفكير في تدابير الدفاع عن النفس. ومن أمثلة ذلك أن يكون لديها إمكانية مثل إيقاف تشغيل الكمبيوتر الذي تستخدمه الدولة المهاجمة؛ لارتكاب العملية الإلكترونية[4] فهو الخيار المفضل على استخدام القوة في الدفاع عن النفس ضد الجاني البشري[5]. وبمعنى آخر أينما وجد إمكان الإجراء السيبراني المضاد وجب أن تنتفي الضرورة للدفاع عن النفس باستخدام السلاح[6].

---

[1] المرجع السابق – Delerue, F. – ص323-324

[2] Tallinn Manual 2.0, commentary to rule 72, para. 3, p. 349

[3] المرجع السابق

[4] المرجع السابق – Delerue, F. – ص323-324

[5] المرجع السابق

[6] Dinstein, Y. (2002). Computer Network Attacks and Self-Defense. *International Law Studies, 76*(1), 99–119 [p. 109]. Retrieved from https://digital-commons.usnwc.edu/ils/vol76/iss1/20/

المرجع السابق – Dinniss, H. H. – ص102-103

مثل هذا التدرج يمكن أن يعد استكمالا لمطلب استنفاد الخيارات غير القسرية في النطاق السيبراني قبل اتخاذ القرار باستخدام القوة دفاعا عن النفس. وبالتالي يمكن القول: إن الضرورة تتحقق فقط إذا كانت جميع الخيارات غير القسرية المذكورة قد استنفدت، وإن استخدام القوة التقليدية للدفاع عن النفس هو الملاذ الأخير، والطريقة الفعالة الوحيدة لصد الهجوم المسلح. وهذا أمر بدأت الدول تلتزم به في استراتيجيات الدفاع السيبراني والوطني. وعلى سبيل المثال يمكن الاستشهاد بالولايات المتحدة في آخر تصريح لها عن سياستها في الضرورة:

"قبل اللجوء إلى التدابير القسرية للدفاع عن النفس ضد هجوم مسلح فعلي، أو وشيك في الفضاء السيبراني أو من خلاله، ينبغي للدول أن تنظر فيما إذا كانت الدفاعات الإلكترونية السلبية أو الدفاعات النشطة التي تقل عن عتبة استخدام القوة ستكون كافية لتحييد الهجوم المسلح أو التهديد الوشيك به"[1]

كذلك مما يرتبط بالضرورة التحقق من أن الهجوم السيبراني ليس حادثًا[2]، وإلا فإن الرد بالدفاع عن النفس سيكون غير ضروري. وهذا الأمر يمكن التحقق منه جزئيا عن طريق طبيعة الهجمات الإلكترونية ودقة استهدافها لجهة حيوية في الدولة، وهل الخطأ وارد أصلا في هذا النطاق أم غير وارد، لكن الجزء الأهم في ذلك هو التحقق من كون الهجوم دولياً أم لا، فإن لم يكن دولياً –أي لم تقف خلفه دولة– يختلف الرد من الدفاع عن النفس إلى التعاون واعتماد تدابير إنفاذ القانون ضد الجهات الفاعلة غير الحكومية مع الدولة التي نشأت منها الهجمات الإلكترونية[3]. لكن ذلك يحتاج إلى حد أدنى من تحديد هوية منفذ الهجوم، وهذا أمر يصعب التحقق منه؛ لأن طبيعة الإنترنت تجعل من الممكن انتحال مصدر الهجوم، لكن المطلوب هو اتخاذ كل الوسائل المتاحة للوصول لبناء استنتاج معقول دال على مصدر الهجوم، وهذا أمر سيتم التطرق له في الفصل الثالث بشيء من التفصيل.

أخيرا فإن الضرورة في نطاق الهجمات الإلكترونية يختلف تقديرها من دولة لأخرى فالدولة ذات الأنظمة السيبرانية الدفاعية القوية وذات الاستراتيجيات السيبرانية الهجومية الواضحة قد لا يكون ضروريا لها أن ترد بالدفاع عن النفس بالطرق التقليدية بقدر الدولة ذات الإمكانات السيبرانية اليسيرة. كذلك في تقدير عنصر الضرورة يجب الأخذ بالظروف المصاحبة لكل دولة، مثلا إذا تعرضت الدولة (أ) لهجمات

---

[1] United Nations, General Assembly, *Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States*, A/76/136 (13 July 2021), p. 137. Available from https://undocs.org/en/A/76/136

[2] المرجع السابق – Delerue, F. – ص89

[3] المرجع السابق

إلكترونية على أحد منشآت البنية التحتية فشرعت في الرد على الدولة (ب) بهجمات إلكترونية مضادة قبل أن تعلم أن الدولة (ب) قررت إنهاء الهجمات. فإنه من الناحية الواقعية انتفت الضرورة في الإجراءات السيبرانية التي قامت بها الدولة (أ) لكن تصرفها ليس له صلة مباشرة بمسألة ما إذا كانت قد تصرفت بشكل قانوني دفاعًا عن النفس. فتقييم الضرورة يتم بناء على الوقت الذي اتخذت فيه الدولة (أ) الإجراء، والظروف التي ألجأتها إلى إجرائها ذلك، فإذا تبين أن تقديرها لضرورة الرد كان بناء على معطيات معقولة فهذا لا ينال من عنصر الضرورة الذي يجعل الدفاع عن النفس مشروعا[1].

القسم الثاني: التناسب في الدفاع عن النفس ضد الهجمات السيبرانية

التناسب هو مطلب دائم في ردود أفعال الدول، وهو مقترن بالمعقولية. والبعد عن المبالغة بالرد، هو الذي يفصل بين الدفاع عن النفس بشكل مشروع وبين الاعتداء غير المشروع، وهو معيار مهم لعدم الوقوع في التصعيد؛ بأن يسمح للدول أن تدافع عن سيادتها واستقلالها دون تدمير الدول الأخرى. والتناسب عامة يعني أن يكون شيء متناسباً مع شيء آخر، أي هو توازن بين شيئين. فإذا طبقنا ذلك على نطاق الدفاع عن النفس فأنه يعني أن فعل الدفاع عن النفس يجب أن يكون متناسبا مع الهجوم.

وفي تفصيل ذلك هناك مذهبان[2] أولهما: ينادي بالتماثل، وهو الفهم التقليدي للتناسب حيث يرى أن الدفاع عن النفس يعني التماثل مع القوة المستخدمة في العدوان. فإن هاجمت قوات قليلة العدد فإنه لا يمكن الرد إلا بالعدد نفسه ليتحقق التناسب[3]. المشكلة هنا أن التماثل في الرد قد لا يكون كافياً للدفاع عن الدولة ودحر الهجوم عليها، أو قد ينجح في صد الهجوم مؤقتا، لكنه يترك المجال للغزاة لإعادة تنظيم الصفوف وإعادة الهجوم.

لذلك أغلب فقهاء القانون والقضاء الدولي يذهب إلى المذهب الثاني الذي يرى أن التناسب لا يعني بالضرورة التماثل مع الهجوم بل يقاس التناسب بشيء آخر وهو التناسب مع "هدف إيقاف الهجوم"[4].

---

[1] Tallinn Manual 2.0, commentary to rule 72, para. 6, p. 350

[2] المرجع السابق – The International Court of Justice – Green, J. A. – ص88

[3] المرجع السابق – Gazzini, T. – ص148

[4] Higgins, R. (1995). *Problems and Process: International Law and How We Use It* (Reprint ed.). Oxford, United Kingdom: Clarendon Press. https://doi.org/10.1093/law/9780198764106.001.0001;

المرجع السابق – O'Connell, D. P. – ص64

المرجع السابق – Gazzini, T. – ص46

أي أنه طالما أن الدولة لا تستخدم القوة بشكل يتعدى الهدف الدفاعي وهو هنا وقف الهجوم إذن فالفعل مشروع. "وبالتالي مزيد من القوة قد يكون ضروريا لوقف الهجوم، أو قد تكون القوة المطلوبة أقل من تلك التي استخدمت في الاعتداء. كذلك بإمكان الدولة أن تغير على دولة أخرى لعدد من المرات في صورة دفاعية بشكل دوريا ولمدة محددة من الزمن، وإن كان ذلك ردا على هجوم مسلح واحد، طالما أن ذلك يحقق الهدف الدفاعي بشكل معقول. إن في ربط التناسب في الدفاع عن النفس مع **هدف وقف الهجوم المسلح** حماية من استخدام عذر الدفاع عن النفس لأغراض انتقامية، فلا يحق للدولة بحجة الدفاع عن النفس السعي إلى إحداث المقدار نفسه من الأضرار المادية والبشرية التي حدثت على إقليمها، لأن كل ما يجب أن يهدف إليه فعل الدفاع هو إيقاف الهجوم المسلح وإلا سقطت الشرعية عن فعل الدفاع.

في العام 1979م كان هناك توتر عسكري على الحدود بين أوغندا وتنزانيا. اعتدت أوغندا بالقوة المسلحة على تنزانيا، وردت تنزانيا بالقوة، وكان الرد متناسبا في البداية. لكن بعد ذلك أخذت القوات التانزانية بالتضخم والتوغل في الدولة؛ مما أسفر في النهاية عن تغيير النظام الحاكم في أوغندا وبذلك أصبح استخدام القوة غير متناسب[1]. فبالرغم من أن استخدام القوة كان مشروعا في البداية، لأن هدفه كان تأمين الحدود، وضمان عدم حصول هجمات أخرى تالية إلا أنه لم يعد مشروعا؛ لأنه فقد عنصر التناسب مع هدف الدفاع. فلكي تدافع تنزانيا عن نفسها لم تكن بحاجة لتغيير النظام.

مرة أخرى المشكلة هنا (في شرط التناسب مع الهدف) تكمن في ترك المجال للتقدير الشخصي للدول، أكثر بكثير من شرط التكافؤ مع حجم القوة المستخدمة. فهنا يكون المجال متاحاً للدول لاستخدام أي مقدار من القوة طالما أنها تعتقد أنه يدحر العدوان ويحقق الأمن. لكن تجدر الملاحظة أن معياري التناسب بالتماثل مع القوة المستخدمة في العدوان أو التناسب مع هدف وقف الهجوم ليسا منفصلين

Wedgwood, R. (1992). Proportionality and Necessity in American National Security Decision Making. *Proceedings of the ASIL (American Society of International Law) Annual Meeting*, *86*, 58–67 [p. 59]. https://doi.org/10.1017/s0272503700094295;

رأي القاضية هيغينز المذيل لفتوى الأسلحة النووية: "مصطلح التناسب في الدفاع عن النفس يحد الاستجابة إلى المقدار الصحيح للرد على الهجوم المسلح. إن مصطلح التناسب يشير إلى ما هو الرد المتناسب لصد الهجوم، وليس ما هو متماثل بين صيغة الهجوم وصيغة الرد عليه"

Nuclear Weapons advisory opinion, Dissenting Opinion of Judge Higgins, para. 5, p. 583

[1] Mugabe, F. (2021, January 9). How bar fight sparked the 1979 Uganda - Tanzania war. *Monitor - Uganda Edition*. Retrieved from https://www.monitor.co.ug

عن بعضها عن بعض تماماً. فغالباً الفعل غير المتناسب بشكل كبير في معيار التكافؤ مع القوة المستخدمة لن يكون متناسباً مع الهدف الدفاعي[1].

التناسب في الهجمات السيبرانية:

اذا كان التناسب مع هدف الدفاع هو المنطلق لمناقشة التناسب الدفاع عن النفس ضد هجوم تقليدي، فإن التناسب في الهجمات السيبرانية –كما في القاعدة العامة– لا يعني التماثل أو المعاملة بالمثل، لذلك ليست هناك حاجه لاستخدام الوسيلة السيبرانية نفسها للرد عليها. فيمكن استخدام الوسيلة السيبرانية دفاعا عن النفس ضد هذه الهجمات مثل الرد بتعطيل الخوادم (السيرفرات) المستخدمة في الهجوم، لكن إذا لم تتوافر القدرات السيبرانية الهجومية الكافية أو كانت التحصينات السيبرانية للدولة المعتدية قوية فيمكن اتخاذ خيار الهجوم الحركي دفاعا عن النفس ردًا على هجوم إلكتروني[2].

ومما يدخل في مفهوم التناسب (التناسب الزماني)[3]، وهو المدة المعقولة بين الهجوم المسلح والرد دفاعا عن النفس، إن المدة المعقولة مما يتسق فيها توجيه الدفاع عن النفس مع هدف ايقاف الهجوم المسلح ويمنع الأعمال الانتقامية. لا يوجد مدة محددة لما يعد معقولا فعبارة المدة المعقولة مرنة غير محددة، والأمر يختلف من دولة إلى أخرى. مثلا بعد أحداث الحادي عشر من سبتمبر احتاجت الولايات المتحدة إلى مدة شهر من التحضيرات قبل اتخاذ إجراء الدفاع عن النفس وقد عد ذلك مقبولا[4]. بينما قضت محكمة العدل الدولية في حكم نيكاراجوا على سبيل المثال، أن التدابير التي اتخذتها الولايات المتحدة ليست ضرورية؛ لأنها تدخلت بعد أشهر من نهاية الهجوم المسلح المزعوم[5]. التناسب الزماني ذو أهمية كبيرة في الهجمات السيبرانية، لما تتصف به من صعوبة في التعقب، فالعملية السيبرانية قد تستغرق دقائق لإحداث أضرار جسيمة، لكن قد تستغرق التحقيقات في معرفة مصدر الهجمات السيبرانية

---

[1] Kretzmer, D. (2013). The Inherent Right to Self-Defence and Proportionality in Jus Ad Bellum. *European Journal of International Law*, *24*(1), 235–282 [p. 235]. https://doi.org/10.1093/ejil/chs087

[2] المرجع السابق – Delerue, F. – ص89

[3] للمزيد عن التناسب الزماني، انظر:

O'Meara, C. (2018, July). *Necessity and Proportionality and the Right of Self-Defence in International Law* (PhD Thesis). Faculty of Laws, University College London, p. 158-160. Retrieved from https://discovery.ucl.ac.uk/id/eprint/10057299/1/PhD%20Thesis%20-%20FINAL%20VERSION%20.pdf

[4] المرجع السابق – Delerue, F. – ص477

[5] المرجع السابق

أشهرا، فإذا ظهرت الدولة المسؤولة بعد عدة أشهر من التحقيقات، فهل يحق لها الرد بالدفاع الشرعي عن النفس[1]؟

بالنظرة الأولى التقليدية للإجابة عن ذلك يكون الرد بالدفاع عن النفس غير مشروع؛ لأن الضرورة انتفت! ذلك أن المدة الزمنية تسمح باتخاذ العديد من الإجراءات الأخرى، غير استخدام القوة دفاعا عن النفس، كالتفاوض مع الدولة المعتدية، وتقديم إخطار مجلس الأمن بالموقف، أو اتخاذ تدابير مضادة ضد الدولة المعتدية؛ حتى تقوم بالتعويض عن الأضرار التي نجمت من الهجوم السيبراني. وسينتفي التناسب؛ لأنه يكون مقيدا بوقف الهجوم وانقضاء المدة المعقولة للرد. وبمزيد من التحليل يمكن تصور أن الهجوم السيبراني توقف، لكن لم ينتَهِ بعد، وأن الذي تم جزء من سلسة هجمات مستمرة، فإذا استطاعت الدولة تقديم أدلة قوية ومقنعة على ذلك، فإنه يمكن أن تستخدم عذر الدفاع عن النفس، لكن ليس عن الجزء الذي حدث من الهجوم السيبراني، بل باستخدام الدفاع عن النفس ضد تهديد بهجوم سيبراني متوقع، وهو ما يعرف بالدفاع الاستباقي، وهو ما يناقش في المطلب الثاني من هذا المبحث.

هذا تجدر الإشارة إلى أنه وإن كانت المدة المعقولة للدفاع عن النفس غير معروفة وتختلف بحسب كل موقف، فإن المادة 51 من الميثاق قد حددت أحد محركات التناسب الزماني لانتهاء الحق في الدفاع عن النفس، وهو تحرك مجلس الأمن وفق تدابير نظام الأمن الجماعي، وبالتالي يجب أن يتوقف الدفاع عن النفس بمجرد اتخاذ مجلس الأمن "التدابير اللازمة لحفظ السلم والأمن الدولي ".[2]

ويشمل مفهوم التناسب أن يكون استخدام القوة الدفاعية موجهاً ضد المكان الذي يصدر منه الخطر (التناسب المكاني)، فالتناسب يفرض أيضًا قيودًا جغرافية على الدفاع عن النفس، مما يعني أن القوة الدفاعية "يجب أن توجه إلى منطقة التهديد حصرا.[3] وقد أيدت محكمة العدل الدولية في قضية الأنشطة المسلحة في إقليم الكونغو فكرة التناسب في النطاق الجغرافي في استخدام الدفاع عن النفس فجاء في الحكم:

---

[1] المرجع السابق

[2] المرجع السابق – Roscini, M. – Cyber Operations and the Use of Force – ص89

[3] المرجع السابق – O'Meara, C. – ص161

"لاحظت المحكمة أن استيلاء أوغندا على المطارات والمدن على بعد مئات الكيلومترات من حدودها لا يبدو متناسبا مع سلسلة الهجمات التي حدثت عبر الحدود والتي زعمت أوغندا ترقى إلى تحريك الحق في استخدام القوة في للدفاع عن النفس"[1].

وبالرغم أن المحكمة أظهرت أن امتداد الحق في الدفاع عن النفس عبر مئات الكيلومترات عن الهجمات الحدودية ليس متناسبا فإنها لم تبين ما هو النطاق الجغرافي الذي يعد مناسبا.

وربما هذا الغموض في مقياس التناسب المكاني هو الذي جعل هناك فراغا فقهيا للتصدي له، فلم يقترح دليل (تالين) تفصيلا للتناسب المكاني في نطاق الهجمات السيبرانية. لكن هذا الأمر غاية في الأهمية خصوصا إذا اختارت الدولة الرد بنفس الوسيلة وهي الهجمات السيبرانية. فاستخدام السلاح التقليدي يمكن أن يحصر نطاقه بوضوح، ثم قياس تناسبه من عدمه، لكن الطبيعة غير المرئية للهجمات السيبرانية قد تشجع على المبالغة في الانتشار الجغرافي؛ مما يضرب عنصر التناسب ويؤدي لنزع الشرعية عن الدفاع عن النفس.

وبهذا يتبين أن ثمة مأخذا مشتركا على نوعي التناسب: الزماني والمكاني، هذا المأخذ هو سعة الزمان والمكان فيهما كليهما! وكما تقرر ضبط التناسب الزماني بالمعقولية وبقاء عنصر الضرورة، فإنه لابد من ضبط التناسب المكاني في الهجمات السيبرانية وفقا للقاعدة العامة للتناسب وهو التناسب مع هدف صد الهجوم بنجاح. فالدفاع عن النفس ضد هجمات سيبرانية قد لا يستلزم شل جميع المرافق الحيوية في الدولة المعتدية، أو انتقاء أهداف متفرقة للهجمات السيبرانية المضادة لتسبيب أكبر قدر من الخسائر المادية كتعطيل سوق البورصة. في كل موقع جغرافي تمارس فيه عمليات الدفاع المشروع عن النفس لابد أن يكون هناك ارتباط بصد الهجمات السيبرانية العدوانية فإن لم يوجد ذلك الرابط في أي موقع، كان الدفاع عن النفس غير مشروع في ذلك الموقع على الأقل.

يحدث في الواقع العملي أن الدول تدفع بضرورة استخدام القوة دفاعا عن النفس حتى لو كان الهجوم السيبراني عليها يسيرا فتزعم أن –الهجوم وإن كان يسيرا– الرد عليه ضروري؛ لأنه يهدد الأمن الوطني واستخدام القوة هو آخر الحلول المتبقية، كأن يستهدف الهجوم السيبراني محطة الكهرباء الرئيسة في بلد صغير يعتمد عليها.

[1] *Armed Activities* judgment, para. 147, p. 223

يمكن القول إن شرطي الضرورة والتناسب ذوا طابع شخصي، خصوصا في البداية عندما تقرر الدولة أن تدافع عن نفسها، ثم تقرر ما هو ضروري وما هو متناسب، فليس هناك معيار دقيق يحكم نظرة الدولة الشخصية. ولكن بعد ذلك، قبول المجتمع الدولي لمشروعية الدفاع عن النفس، وقبول فقهاء القانون الدولي، واقتناع محكمة العدل الدولية وربما حتى قبول مجلس الأمن من عدمه، يضفي على الحالة شيئاً من الموضوعية، لذلك في موقف الدفاع عن النفس يتعين أن تحاول الدولة اختيار ما يمكن تسويغه بسهوله لاحقا. وهنا تجدر الإشارة إلى أنه وإن كان يمكن –من الناحية النظرية وفقا للضرورة والتناسب– استخدام حق الدفاع عن النفس ضد الهجمات الإلكترونية عبر الوسائل المادية، لكن الرد السيبراني على هجوم مسلح إلكتروني أكثر قبولا من الناحية السياسية من التحرك العسكري.

الفرع الثاني: شروط الدفاع عن النفس في ميثاق الأمم المتحدة (الهجوم المسلح)

ميثاق الأمم المتحدة ليس أول وثيقة دولية تتناول الدفاع عن النفس. فقد سبقته إلى ذلك عدة محاولات لتأصيل حق الدفاع عن النفس، أهمها ميثاق عصبة الأمم. بالرغم من أن هذا لم يشر مباشرة إلى حق الدول في الدفاع عن نفسها فإن ذلك يستشف ضمنا من بعض نصوصه [1]. لكن ميثاق الأمم المتحدة وبالأخص المادة 51 منه هو المؤسس الحقيقي لمشروعية الدفاع عن النفس في المفهوم المعاصر.

تنص المادة 51 منه على أنه:

"ليس في هذا الميثاق ما يضعف أو ينتقص الحق الطبيعي للدول، فرادى أو جماعات، في الدفاع عن أنفسهم إذا اعتدت قوة مسلحة على أحد أعضاء الأمم المتحدة وذلك إلى أن يتخذ مجلس الأمن التدابير اللازمة لحفظ السلم والأمن الدولي، والتدابير التي اتخذها الأعضاء استعمالاً لحق الدفاع عن النفس تبلغ إلى المجلس فورا، ولا تؤثر تلك التدابير بأي حال فيما للمجلس – بمقتضى سلطته ومسؤولياته المستمرة من أحكام هذا الميثاق – من الحق في أن يتخذ في أي وقت ما يرى ضرورة لاتخاذه من الأعمال لحفظ السلم والأمن الدولي أو إعادته إلى نصابه."

يتضح من قراءة النص عدة أمور:

---

[1] للمزيد عن التطور التاريخي لحق الدفاع عن النفس انظر:
منية، العمري .(2010–2011) .*الدفاع الشرعي في القانون الدولي العام* (أطروحة ماجستير). كلية الحقوق والعلوم السياسية - جامعة الإخوة منتوري .استرجع من https://bu.umc.edu.dz/theses/droit/AELA3806.pdf

- يتوجد عذر الدفاع عن النفس أينما يوجد اعتداء مسلح، أي هناك اشتراط زمني لا يمكن ممارسة حق الدفاع عن النفس إلا ضد هجوم مسلح حال وواقع. يتبين ذلك من خلال عبارة "إذا اعتدت قوة مسلحة" أي أن الاعتداء حدث بالفعل لا أنه سيحدث في المستقبل.
- كل إجراء تتخذه الدولة باسم الدفاع عن النفس يجب أن تبلغ به مجلس الأمن فوراً.
- يبقى استخدام القوة باسم الدفاع عن النفس مشروعاً حتى يبدأ مجلس الأمن باتخاذ إجراءاته بشأن الوضع. العلاقة بين الدفاع الشرعي ومجلس الأمن تنطلق من فكرة مركزية استخدام القوة، فالأصل أن لا أحد لديه الحق في استخدام القوة سوى مجلس الأمن بحكم أن مهمة حفظ السلم والأمن الدوليين تقع على عاتقه، وإباحة الدفاع عن النفس وجد لسد تلك الفجوة بين الهجوم الحاصل على الدولة وبين تحرك المجلس لحفظ السلم والأمن.
- لم يرد ذكر الضرورة والتناسب.

قد يفهم من ذلك أن المادة 51 تنسخ هاتين القاعدتين العرفيتين خصوصا وأن في القانون الدولي لا يوجد أي هرمية بين القانون المكتوب والعرف كما في القوانين الوطنية، لكن القاعدة الجديدة تسمو على القاعدة القديمة بغض النظر عن طبيعتها عرفية كانت أو مكتوبة [1].

لكن المادة 51 تبدأ بالنص على أنه: **لا شيء يضعف أو ينتقص** الحق الطبيعي– وفي بعض الترجمات الحق **الموروث** (The Inherent Right)– للدول في الدفاع عن النفس. أي أن المادة 51 لم تأت لتغير الدفاع عن النفس بل تحفظ الدفاع عن النفس كما كان موجودا قبلها. لذلك فعل الدفاع عن النفس محكوم أولا بشرطي الضرورة والتناسب (وإن لم يردا في النص) وثانياً بالمادة 51. هذه الفكرة تبنتها محكمة العدل الدولية في قضية نيكاراجوا 1986[2].

وكررت الفكرة في قضية المنصات النفطية؛ فقد نصت في حكمها على أنه:

"من أجل إثبات أن ممارسة حق الدفاع عن النفس حق الدفاع عن النفس مسوغة قانونياً، فإن على الولايات المتحدة أن تُظهر أن الهجمات قد شُنت عليها من قبل إيران، وأن تلك الهجمات توصف بأنها

[1] Voyiakis, E., & Goldsmith, J. L. (1999). A Theory of Customary International Law. University of Chicago Law Review, 63. https://doi.org/10.2139/ssrn.895462

[2] *Nicaragua* judgement, para. 174, p. 94

Nuclear Weapons advisory opinion, para. 39, p. 244

"هجمات مسلحة" بالمعنى المقصود في المادة 51 من ميثاق الأمم المتحدة، وعلى النحو المفهوم في القانون العرفي بشأن استخدام القوة"[1]

أما في فتوى الأسلحة النووية، فقد أعلنت المحكمة قطعيا:

"أن إخضاع ممارسة حق الدفاع عن النفس لشرطي الضرورة والتناسب ملزم بموجب قاعدة قانونية عرفية"[2]

إذن لفهم الدفاع عن النفس يجب فهم كل من القواعد العرفية والمادة 51. ففعل الدفاع يجب أن يكون ضروريا ومتناسبا، لكنه أيضا يجب أن يكون في سياق الرد على هجوم مسلح ويجب أن يبلغ به مجلس الأمن، ويظل فعل الدفاع مشروعا حتى يتخذ مجلس الأمن ما يراه مناسبا من إجراءات.

يتضح أنه بالإضافة للضرورة والتناسب هناك حاجة لشرط ثالث جاءت به المادة 51 من الميثاق ليقوم حق الدفاع عن النفس وهو الهجوم المسلح. وتحديد ماهية الهجوم المسلح تحتاج إلى بعض التفصيل. لذلك سيتم في الفرع الأول من المطلب الآتي توضيح المقصود بالهجوم المسلح كما جاء في الميثاق، ثم في الفرع الثاني سيتم النظر في إمكانية اعتبار الهجمات السيبرانية هجوما مسلحا.

القسم الأول: مدى عدِّ الهجوم السيبراني في حكم الهجوم المسلح

في محاولة تطبيق معايير الهجوم المسلح على الهجمات السيبرانية ينبغي تذكر أن الهجمة السيبرانية لكي تعد هجوما مسلحاً يؤهل للرد بالدفاع عن النفس يجب أن يكون استعمال للقوة أولاً. وقد تمت مناقشة معايير الهجمات الإلكترونية التي تعد قوة تدخل في نطاق المادة (4)2 وهي:1- الهجمات التي في حجمها وأثرها تضاهي اثارها استخدام القوة 2- الهجمات التعطيلية ذات النطاق الواسع والضرر الجسيم 3- الهجمات السيبرانية الصادرة من فاعل غير حكومي برعاية دولة 4- التهديد باستخدام القوة السيبرانية.

قضية التهديد باستخدام القوة لن تكون موضع نقاش في الهجوم المسلح؛ ذلك لأنه لا يوجد هجوم مسلح، بل هو وعد باللجوء إلى القوة في حالة عدم الامتثال، لكن من ناحية أخرى هناك الدفاع عن

[1] *Oil Platforms* judgement, para. 51, p. 186
[2] *Nuclear Weapons* advisory opinion, para. 41, p. 245

النفس ضد التهديد باستخدام القوة والذي يعرف أيضا "بالدفاع الاستباقي عن النفس" وهو ليس نوعا تقليديا من الدفاع عن النفس بل هو من الأنواع التوسعية في الدفاع عن النفس لذلك سيتم معالجته في المطلب الثاني من هذا المبحث الثاني. أما حالة الهجمات السيبرانية الصادرة من فاعل غير حكومي فإنها تعنى بمن قام بالهجمات السيبرانية بينما المطلوب هنا هو فحص الهجمات السيبرانية نفسها، ومتى تعبر عتبة الهجوم المسلح. لذلك سيقتصر هذا القسم على النوعين الأولين من الهجمات الذين تمت مناقشتهم في قاعدة استخدام القوة وهما:

1- الهجمات التي تضاهي في آثارها استخدام القوة التقليدية، والمقصود هو الهجمات التي تنجح في إحداث ضرر مادي على الأرواح والممتلكات.

2 -الهجمات التعطيلية ذات الضرر الجسيم، وهي تلك الهجمات التي تظل حبيسة العالم الافتراضي فلا تحرك ساكنا، لكنها عبر طبيعتها التعطيلية تسبب أضرارا جسيمة قد ترقى إلى استخدام القوة، في حال استهدافها مرفقا حيويا يمس حياة الشعب.

السؤال الذي يطرح في مقام الدفاع عن النفس هو أي من صور استخدام القوة السيبرانية المذكورة أعلاه يرقى لأن يصبح هجوما مسلحا؟

أ) الهجمات السيبرانية ذات الأثر الحركي المضاهي لآثار الهجوم المسلح:

إن تحديد الهجمات السيبرانية التي تصل لعتبة الهجوم المسلح أمر معقد، ومتغير بسبب عدم وجود معيار موضوعي واضح، يقاس به تحقق الجسامة من عدمه. فاذا تم أخذ بمعياري محكمة العدل الدولية للهجوم المسلح وهو "الحجم والأثر" -وهذا جاء في دليل (تالين) الذي أكد أن الهجوم السيبراني يعد هجوما مسلحا إذا كان في حجمه وأثره يضاهي حجم وأثر الهجوم المسلح التقليدي- فإن المشكلة في الأخذ بالمعيارين أن المحكمة لم تبين ما هو الحجم والأثر المطلوبان ولم تعط اختبارا معينا لقياس الحجم والجسامة[1]. وشأن هذا المعيار في الهجوم السيبراني المسلح شأنه في الهجوم التقليدي المسلح، فليس من قياس تحقق معيار كهذا؛ لأن تحقق الحجم والأثر الجسيمين يختلفان فهجوم إلكتروني قد يعد

[1] مع العلم أن دليل (تالين) وضع استخدام القوة والهجوم المسلح في قاعدة واحدة وجعل الفرق بينهم في الجسامة.

كبيرا وجسيما في دوله صغيرة، وهو نفسه قد لا يكون له أثر مهم في دولة أكبر. والحقيقة أن الأمر متروك للدول أن تجادل فيما تراه جسيماً[1].

بيد أن محكمة العدل الدولية في –فتوى الأسلحة النووية– بينت أن المادة 2(4) من ميثاق الأمم المتحدة تنطبق على أي استخدام للقوة، بغض النظر عن السلاح المستخدم، فالاحتمالية مفتوحة من الناحية النظرية للهجمات السيبرانية أن تصل إلى مستوى الهجوم المسلح وإن لم يحدث أن دفعت دولة بتعرضها لهجوم مسلح سيبراني حتى هذه اللحظة[2]، لكن هذه الاحتمالية قائمة لذلك لا بد أن تواجه تشريعيا.

في الكتابات الفقهية –خلال العشر سنوات الأخيرة التي تعالج مسألة استخدام القوة في الفضاء السيبراني– اتفاق على أن الهجوم السيبراني الذي يصل إلى مستوى الهجوم المسلح وبالتالي ينضج حق الدفاع عن النفس متصور في الهجمات التي تحرك ساكناً في العالم المادي فكلما كانت الآثار قد تسببت بتدمير أكبر أو تخريب أشد أو إصابة أبلغ على أرض الواقع _وليس في العالم السيبراني حصرا_ كانت أكثر إقناعا بمستوى الهجوم المسلح. فعندئذ تكون الآثار الملموسة للهجمات السيبرانية أسهل حصراً، وأقيس أثراً بالهجمات المسلحة التقليدية[3].

من الأمثلة على ذلك، الهجمات التي تستهدف فقدان التحكم بالكمبيوتر المتحكم بأنظمة دعم الحياة في المستشفيات؛ مما يسبب خسائر بشرية؛ ومثلها الهجمات التي تستهدف فقدان السيطرة على أجهزة الكمبيوتر المتصلة بالسدود المائية ومحطات المياة؛ مما يؤدي إلى حدوث فيضانات في المناطق المأهولة؛ مما ينتج عنها تخريب الممتلكات، وتعريض حياة الناس للخطر، ومثل ذلك الهجمات

---

[1] للمزيد، انظر في تحليل Green لمعنى أكثر أنواع استخدامات القوة جسامة في قراءة أحكام محكمة العدل الدولية لينتهي بأن المحكمة قبلت فقط الأهداف العسكرية غير الإقليمية على أنها قادرة على تشكيل هجمات مسلحة.
انظر: المرجع السابق – The International Court of Justice – Green, J. A. – ص41-33

[2] Tallinn Manual, commentary to 'Law of International Responsibility', para. 13, p. 83
المرجع السابق – O'Connell, M. E. – ص190-191 وص199
المرجع السابق – Cyber Operations and the Use of Force – Roscini, M. – ص104

[3] المرجع السابق – Cyber Operations and the Use of Force – Roscini, M. – ص70
المرجع السابق – O'Connell, M. E. – ص190-191 وص199
Tallinn Manual 2.0, commentary to rule 71, paras. 6-7, p. 341
Tsagourias, N. (2012). Cyber attacks, self-defence and the problem of attribution. *Journal of Conflict and Security Law*, *17*(2), 229–244 [p. 230-233]. https://doi.org/10.1093/jcsl/krs019
المرجع السابق – Buchan, R. – ص227
المرجع السابق – Delerue, F. – ص332

المصممة للتسبب بحوادث مميتة متعمدة هندسيًا على سبيل المثال، من خلال المعلومات الخاطئة التي يتم إدخالها إلى أجهزة الكمبيوتر المتصلة بالطائرات، ومن هذه الامثلة إدخال بيانات خاطئة بشكل متعمد قاصدة التحريض على انهيار مفاعل نووي؛ مما يؤدي إلى إطلاق مواد مشعة، يمكن أن ينتج عنها عدد لا يحصى من الضحايا وخاصة إذا كانت المناطق المجاورة مكتظة بالسكان، كل تلك الأمثلة –التي تبدأ سيبرانياً وتنتهي على أرض الواقع بالدمار والتخريب أو الوفاه والإصابة– يسهل الاتفاق على عدها هجوماً مسلحاً[1].

تأكيدا على قلة الخلاف في عد الهجمات السيبرانية –ذات الآثار التدميرية– هجوما مسلحاً فأنه يمكن القول إن: جميع الدول التي أعلنت عن سياساتها الدفاعية ضد الهجمات الإلكترونية، أقرت بإمكانية بلوغ الهجمات السيبرانية حد الهجوم المسلح حتى في أكثر الدول تشددا مثل البرازيل، التي ترى أن الدفاع عن النفس –بوصفه استثناء للمبدأ العام بشأن حظر استخدام القوة– يجب تفسيره بشكل مقيد رافضةً فكرة الدفاع الاستباقي عن النفس أو فكرة أن يكون الدفاع عن النفس ضد الجماعات المسلحة المستقلة، لكنها ترى بالحق في استخدام القوة دفاعا عن النفس ضد الهجمات السيبرانية التي تصل إلى مستوى الهجوم المسلح[2].

ب) الهجمات السيبرانية المسلحة ذات الأثر غير الحركي:

إذا كان الأمر واضحا بالنسبة للهجمات السيبرانية المسلحة ذات النطاق والآثار التدميرية المشابهة للهجمات المسلحة التقليدية، فإنه يتسم بالغموض في حالة الهجمات التي لا تخلف تدميرا مادياً لكنها تقتصر (تعطيل أو تبديل[3]) البيانات الرقمية مما قد ينجم عنه تعطيل استخدام الجهاز أو الخدمة أو المنشأة بالطريقة التي خصصت لأجلها فضلا عن الخسائر الاقتصادية. إن أهم المراجع في تقنين

---

[1] المرجع السابق – Computer Network Attacks and Self-Defense – Dinstein, Y – المرجع السابق – ص105

[2] A/76/136

[3] الحقيقة هناك صورة ثالثة لعمل الهجمات ذات الأثر غير الحركي وهي سرقة المعلومات لكن الرأي الغالب منهم هذا البحث يرى بان سرقة المعلومات لا يمكن أن تشكل هجوما مسلحا بالنظر إلى أنه لا يؤدي إلى خسائر بشرية ولا حتى اقتصادية بشكل مباشر. انظر:

المرجع السابق – Cyber Operations and the Use of Force – Roscini, M. – ص71

Tallinn Manual 2.0, commentary to rule 71, para. 8, p. 341

لكن لا يخلو الأمر من بعض الأصوات التي تجادل بأن سرقة المعلومات الحيوية للأمن القومي والمعلومات العسكرية الحساسة يمكن أن تؤدي إلى عواقب وخيمة وبالتالي من المحتمل أن يتم تصنيفها على أنها هجوم مسلح. انظر.

Joyner, C. C. (2001). Information Warfare as International Coercion: Elements of a Legal Framework. *European Journal of International Law*, *12*(5), 825–865 [p. 855]. https://doi.org/10.1093/ejil/12.5.825

الهجمات السيبرانية –كدليل (تالين)–[1] تتردد في الجزم بإمكانية وجود هجوم مسلح من خلال هجمات سيبرانية تعطيلية لا تحرك ساكنا على أرض الواقع تاركةً ذلك للمستقبل، ولتطبيقات الدول في عد الهجمات التعطيلية هجمات مسلحة من عدمه[2].

بيد أنه الناحية النظرية –على الأقل– من الممكن تطبيق معيار محكمة العدل الدولية للهجوم المسلح على الهجمات التعطيلية. فإذا كان الهجوم المسلح –وفقا لمحكمة العدل الدولية– هو أكثر صور استخدام القوة جسامة، ولا يطلق على العملية أنها هجوم مسلح إلا بسبب حجمها وآثارها غير العادية، فإنه يمكن القول: إن العمليات التعطيلية التي تصل في حجمها (نطاقه) وأثرها (أضراره) إلى ما يقارب حجم وآثار الهجمات المسلحة التقليدية تعد هجوما مسلحا.

وإذا ما كانت الهجمات التعطيلية ذات نطاق واسع–وتمكنت من إحداث شلل في عدد من المرافق والخدمات التي تقدمها الدولة، واستمرت لمدة ليست بالقصيرة كأن تستمر عدة أيام، وكانت أضرارها وخصوصا الاقتصادية منها جسيمة كأن تقدر بالمليارات كما هي خسائر الهجوم المسلح التقليدي- أمكن وفقا لمعيار الحجم والأثر عد الهجوم السيبراني في حكم الهجوم المسلح الذي يحرك الحق بالدفاع الشرعي عن النفس. مثلا، هجوم إلكتروني يؤدي إلى إغلاق المؤسسات الوطنية المالية لفترة طويلة،

---

[1] المرجع السابق – Delerue, F. – ص333

Tallinn Manual 2.0, commentary to rule 71, para. 12

[2] من الضروري التذكير باختلاف معيار الهجوم المسلح في قانون اللجوء إلى الحرب عنه في قانون النزاع المسلح. ففي حين يتم توخي الحذر في التوسعة من نطاق الهجوم المسلح في قانون اللجوء إلى الحرب لما يترتب علية استخدام الدفاع الشرعي عن النفس وبالتالي خطر التصعيد، فإنه في قانون النزاع المسلح يتم التوسيع من نطاق الهجوم السيبراني المسلح حيث تنطبق عليه قواعد قانون النزاع المسلح من قاعدة التمييز بين المدنيين والعسكريين وحماية الأغراض بما في ذلك البيانات الرقمية. لذلك فاللجنة الدولية للصليب الأحمر تدفع نحو التوسع في مفهوم الهجوم المسلح ف النطاق السيبراني، يتبين ذلك من تقرير القانون الدولي الإنساني والعمليات السيبرانية خلال النزاعات المسلحة (ورقة موقف اللجنة الدولية للصليب الأحمر) الذي نص على الآتي:

"وإذا فسر مفهوم الهجوم على أنه يشير فقط إلى العمليات التي تسبب الوفاة أو الإصابة أو الضرر المادي، فإن أي عملية سيبرانية تهدف إلى تعطيل شبكة مدنية (مثل الكهرباء أو الخدمات المصرفية أو الاتصالات)، أو من المتوقع أن تتسبب في حدوث هذا التأثير بصورة عرضية، قد لا تكون مشمولة بقواعد القانون الدولي الإنساني الأساسية، التي تحمي السكان المدنيين والاعيان المدنية. وسيكون من الصعب التوفيق ما بين مثل هذا الفهم التقييدي المفرط لفكرة الهجوم وبين هدف قواعد القانون الدولي الإنساني"

انظر:

المنظمة الدولية للصليب الأحمر (نوفمبر 2019) القانون الدولي الإنساني والعمليات السيبرانية خلال النزاعات المسلحة، ص7-8. استرجع من https://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts

مشلاً اقتصاد الدولة متسببا في انهيار العملة الوطنية، مما يعد هجوما إلكترونيا واسع النطلق، فمن المحتمل إلى حد كبير ان يصل إلى "هجوم مسلح" يحرك حق الدفاع عن النفس[1].

ليست الأضرار المالية فقط هي التي يُحتمل أن ترقى إلى مستوى استخدام القوة، بل أيضًا إذا اقتصر الأمر على مجرد التعطيل، كما في حالة الهجمات الإلكترونية التي تعطل خدمات الدولة والسير الطبيعي لمرافقها، كأن تُعيق بشدة البنى التحتية الحيوية في الدولة، ولا يعني ذلك تدميرها المادي، ولكن عدم توفرها بمعنى عدم القدرة على تحقيق الغرض التي تم إعدادها من أجله، يمكن أن يجعل الهجوم عليها هجومًا مسلحًا وان لم يرتبط ذلك بخسائر مالية جسيمة؛ لأن عدم توافر المرفق أو الخدمة يمكن أن يعد احد آثار الهجوم المسلح التقليدي التي يمكن أخذها بالحسبان عند المقارنة مع الهجوم المسلح السيبراني[2].

يمكن المجادلة أن الاستعداد للمستقبل يحتم التوسيع في الاعتراف بقدرات الهجمات السيبرانية، فلا يحصر معنى الهجوم المسلح في الهجمات السيبرانية ذات الأثر الحركي أو التدميري وحسب. فالدمار والتفجير والإصابات الجسدية هي أحد آثار الهجوم المسلح، لكن على الجانب الآخر هناك الآثار الاقتصادية. فالشلل الذي تحدثه الهجمات التعطيلية يمكن أن تكون خسائره الاقتصادية تضاهي آثار الحروب. وهناك جانب آخر وهو فقدان الشعور بالأمن الذي تحدثه حالة الشلل في الخدمات المقدمة فتنتقل الدولة إلى وضع طارئ مغاير للحياة الطبيعية.

وأما الزعم بأنه إذا كان فتح باب الدفاع عن النفس أمام الهجمات السيبرانية التعطيلية مدعاة للقلق؛ بسبب احتمالية التصعيد الذي قد يؤدي إلى حدوث نزاعات عسكرية عرضية وغير ضرورية، فإنه يمكن الرد بأن الشروط المطروحة تعتبر ضمانة معقولة في عدم الإفراط في استخدام حق الدفاع عن النفس ضد أي هجوم إلكتروني. فالهجوم المسلح السيبراني ذو الأثر التعطيلي يجب أن يتعدى مرحلة عتبة استخدام القوة أولاً؛ مما يتطلب أن يكون الهجوم التعطيلي واسع النطاق على مرفق حساس، ثم التحقق من أن (الحجم) و(الأثر) جسيمان يفوقان نطاق وآثار الاستخدام العادي للقوة إلى درجة يمكن مضاهاتها بحجم وأثر هجوم مسلح تقليدي. فعلى سبيل المثال إذا استهدفت هجمة سيبرانية أنظمة مراقبة الحركة

---

[1] المرجع السابق – Roscini, M. – Cyber Operations and the Use of Force – ص74

[2] المرجع السابق – Tsagourias, N. – ص231

Melzer, N. (2011). *Cyberwarfare and International Law*. United Nations Institute for Disarmament Research, p. 14. Retrieved from https://unidir.org/sites/default/files/publication/pdfs//cyberwarfare-and-international-law-382.pdf

الجوية للدولة جنباً إلى الأنظمة المصرفية، والمرافق العامة للدولة، فإنه يمكن جدا تفهم وجهة النظر القائلة: إن هذا الهجوم هو هجوم مسلح. وذلك لتشابه آثاره مع الهجوم المسلح التقليدي من الناحية المالية، وانعدام السير الطبيعي للأمور بسبب عدم توافر الخدمات الخاصة بتلك المرافق.

ولما كانت تلك الاحتمالية قائمة من الناحية النظرية بدأت الدول تصرح في استراتيجياتها في الدفاع السيبراني[1] بأنها ستعد الهجمات السيبرانية –وإن كانت آثارها غير حركية– في حكم الهجوم المسلح. وكانت الولايات المتحدة من الدول السباقة في التوسع في استخدام الدفاع عن النفس عامة والأمر نفسة في السياق السيبراني فقد نص تقرير وزارة الدفاع بخصوص سياسة الفضاء السيبراني صراحة على أن الهجمات السيبرانية التي تستهدف الاقتصاد الأمريكي هجوم مسلح:

"الولايات المتحدة تحتفظ لنفسها بالحق في استخدام "جميع الوسائل الضرورية" ضد "الأعمال العدائية" بما في ذلك الهجمات الإلكترونية الكبيرة ليس فقط ضد حكومة الولايات المتحدة أو الجيش ولكن أيضًا ضد الاقتصاد الأمريكي"[2].

بالإضافة إلى الولايات المتحدة فإن إعلان هيئة الأركان العامة للقوات المسلحة لجمهورية إيران الإسلامية بشأن القانون الدولي المطبق على الفضاء السيبراني من أوضح الأمثلة التي أخذت بنظرية المرفق الحساس لعد الهجمات التعطيلية هجمات مسلحة:

فقد جاءت المادة الرابعة منه بعنوان "استخدام القوة والهجوم الإلكتروني من وجهة نظر القوات المسلحة لجمهورية إيران الإسلامية " ونصت على الآتي:

تعتقد القوات المسلحة لجمهورية إيران الإسلامية أن تلك العمليات الإلكترونية التي تؤدي إلى:

1. أضرار مادية بالممتلكات و/أو الأشخاص على نطاق واسع وخطير و/أو من المحتمل منطقيا أن تؤدي إلى مثل هذه الآثار تشكل استخداما للقوة. إذا كانت مثل هذه العمليات تؤثر على البنى

[1] المرجع السابق – Cyber security strategies – CCDCOE

[2] Department of Defense Cyberspace, USA. (2011, November). *A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934* (Policy Report), p. 4. Retrieved from https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-059.pdf

التحتية الوطنية الحيوية، بما في ذلك البنى التحتية الدفاعية – سواء أكانت مملوكة للقطاع العام أم الخاص – فأنها تنتهك مبدأ عدم استخدام القوة.

2. تعتقد القوات المسلحة لجمهورية إيران الإسلامية أيضًا أن حقها في الدفاع عن النفس سيكون محفوظًا إذا وصلت خطورة العملية الإلكترونية ضد البنية التحتية الحيوية للدولة إلى عتبة الهجوم المسلح التقليدي[1].

ومثال ثالث على ذلك: الحكومة الهولندية في تقرير 2011 "للحرب السيبرانية" فقد نص التقرير على أنه:

"يجب حسبان الهجوم السيبراني المنظم على وظائف الدولة الأساسية بمنزلة "هجوم مسلح" بالمعنى المقصود في المادة 51 من ميثاق الأمم المتحدة إذا تسبب في –أو وجد احتمال– إحداث اضطراب خطير في عمل الدولة، أو عواقب وخيمة، أو طويلة الأمد على استقرار الدولة، حتى لو لم يكن هناك ضررًا مادياً على الممتلكات أو الأشخاص. في مثل هذه الحالات، يجب أن يكون هناك اضطراب في الدولة و / أو المجتمع، أو محاولة متواصلة لذلك، وليس مجرد إعاقة أو تأخير الأداء الطبيعي للمهام"[2].

كذلك صرحت جمهورية سنغافورة في مناقشة في الجمعية العامة للأمم المتحدة حول سلوك الدولة في الفضاء السيبراني في السياق الدولي بما يتماشى مع هذا التوجه ونص هذا التصريح على ما يأتي:

"من وجهة نظر سنغافورة، من الممكن، في ظروف محدودة معينة، أن يرقى النشاط السيبراني الضار إلى مستوى هجوم مسلح، حتى لو لم يتسبب بالضرورة في الوفاة، أو الإصابة، أو الضرر المادي، أو

---

[1] Declaration of General Staff of the Armed Forces of the Islamic Republic of Iran Regarding International Law Applicable to the Cyberspace. (2020, August 17). *Young Journalists Club (YJC)*. Retrieved from https://www.yjc.news/en/news/47482/declaration-of-general-staff-of-the-armed-forces-of-the-islamic-republic-of-iran-regarding-international-law-applicable-to-the-cyberspace

[2] Advisory Council on International Affairs (AIV) & Advisory Committee on Public International Law (CAVV). (2011, December). *Cyber Warfare* (No 77, AIV / No 22, CAVV), p. 21. Retrieved from https://cyberwar.nl/d/20120426_cavv-advies-nr-22-digitale-oorlogsvoering-en.pdf

كذلك نجد موقف نيوزيلاندا مشابها لموقف هولندا، انظر التقرير الصادر من وزارة الخارجية النيوزيلاندية (2021) بخصوص انطباق القانون الدولي في الفضاء السيبراني:

Ministry of Foreign Affairs and Trade. (2020, December). *The Application of International Law to State Activity in Cyberspace*, para. 7, pp. 1-2. New Zealand. Retrieved from https://dpmc.govt.nz/sites/default/files/2020-12/The%20Application%20of%20International%20Law%20to%20State%20Activity%20in%20Cyberspace.pdf

التدمير. قد يكون أحد الأمثلة على ذلك هو عملية إلكترونية مستهدفة تتسبب في انقطاع مستمر وطويل الأجل للبنية التحتية الحيوية في سنغافورة".[1]

وحينما أعلنت فرنسا أيضا عن "القانون الدولي المطبق على العمليات في الفضاء الإلكتروني2021 " جاء في فقرة الهجمات السيبرانية المصنفة كهجمات مسلحة:

"يمكن تصنيف الهجوم الإلكتروني على أنه هجوم مسلح إذا تسبب في خسائر كبيرة في الأرواح أو أضرار مادية أو اقتصادية كبيرة. سيكون هذا هو الحال بالنسبة لعملية في الفضاء السيبراني تتسبب في فشل البنية التحتية الحساسة مع عواقب وخيمة من شأنها أن تشل بالكامل".[2]

فهذه ستة نماذج (وهي الولايات المتحدة، وإيران، وهولندا، وسنغافورة، ونيوزيلاندا، وفرنسا) كلها تجمع أن الأضرار الاقتصادية والمالية كما الخسائر البشرية أو التدميرية يمكن أن تؤهل تدخل الهجوم السيبراني في حكم الهجوم المسلح. لكن يجب التنويه أن دولا أخرى فضلت التحفظ على ذلك، وصرحت بحصر اعتبار الهجمات الإلكترونية هجمات مسلحة إذا أحدثت أضرار على الممتلكات والأرواح كبريطانيا عام 2018[3]. لكن يمكن القول: إن أغلب السياسات الدفاعية السيبرانية للدول المؤثرة تعترف بإمكانية بلوغ الهجمات السيبرانية التعطيلية مرحلة الهجوم المسلح، وترى وجود الحق في الدفاع عن النفس، أما متى وكيف تبلغ الهجمات السيبرانية تلك المرحلة فهو أمر غالبا مسكوت؛ عنه لأن الدول تفضل ألا تستبق المستقبل، وتدرس كل هجوم سيبراني بظروفه المحيطة، ثم تقرر في ماهيته ومدى الحاجة للرد عليه دون أن تلزم نفسها بسياسة معينة قبل حدوث الأمر. ففي دول مثل سويسرا وإستونيا وغيرها المسألة هي مسألة انتظار.

ويبدو أن جميع الآراء والنظريات فيما يعد هجوماً مسلحاً من عدمه مازالت في مرحلة الانتظار بما في ذلك دليل (تالين) الذي انقسم الخبراء فيه بخصوص مثال الهجمات السيبرانية التي تضرب سوق

---

[1] A/76/136

[2] UN Office for Disarmament Affairs. (2021, December). *International Law Applied to Operations in Cyberspace (Paper shared by France with the Open-ended working group established by resolution 75/240)*. Retrieved from https://documents.unoda.org/wp-content/uploads/2021/12/French-position-on-international-law-applied-to-cyberspace.pdf

[3] ولكن يجب الإشارة إلى ان المملكة المتحدة قد أصدرت سياستها السيبرانية الجديدة في العام 2021 والتي تركت فيها تقييم المعنى الهجوم المسلح لظروف كل هجوم على حده. للمزيد انظر:
المرجع السابق – Wright, J.

الأوراق المالية وتؤدي إلى خسائر بالمليارات! فرأى بعض الخبراء أن مجرد الخسائر المالية لا يمكن أن يؤدي إلى ضرر إلى درجة تصنيف العملية الإلكترونية على أنها هجوم مسلح. وأكد آخرون على أن الآثار الكارثية لمثل هذا الانهيار قد تكون كافية لوصف العملية أنها هجوم مسلح[1] وبقي الأمر معلقا بسبب هذا الخلاف بين الرأيين، والأمر متروك للدول أي نهج ستختار تطبيقه في المستقبل؟

في رأي الباحثة من الأفضل عدم التشجيع على عد الهجمات السيبرانية التعطيلية ذات الأضرار الاقتصادية في حكم الهجوم المسلح، إلا إذا سبب هذا الهجوم المسلح خسائر في الأرواح، أو تدمير واسع النطاق في الممتلكات. إن قبول الهجمات التعطيلية كهجمات مسلحة تعتمد على مقارنة الآثار الاقتصادية للهجوم المسلح بالآثار الاقتصادية للهجوم السيبراني، وهي في الحقيقة مقارنة غير صحيحة لأنها تهتم بالأضرار الفرعية للهجوم المسلح بدلا من تلك الرئيسة المرتبطة بجوهرة. فأول ما يحسب في الهجمات المسلحة وفي الحروب هو الضحايا والدمار. الخسائر الاقتصادية لا تقارن ببشاعة الدماء والموت والركام والأشلاء والقصف، لمثل ذلك وضع الدفاع عن النفس "للاستخدام الجسيم للقوة" فكيف تتم المساواة بين الخسائر الاقتصادية والهجوم المسلح. الهجمات السيبرانية التعطيلية قد تسبب حالة من الرعب والشلل في البلاد (وذلك في أقصى الهجمات السيبرانية نجاحا وتعقيدا) لكن إذا ما بقيت الأرواح سالمة والبنى التحتية غير مدمرة فذلك لا يضاهي "الاستخدام الجسيم للقوة".[2] القول بغير ذلك فيه خروج عن قصد الميثاق وعن النطاق الذي وضعته محكمة العدل الدولية للهجوم المسلح.

كذلك ينبغي الانتباه إلى أن الخسائر الاقتصادية موجودة في نطاقات مختلفة في العلاقات الدولية، ولا تكون مرتبطة بالدفاع عن النفس. مثلا، العقوبات تسبب خسائر اقتصادية جسيمة تؤثر على حياة السكان ورفاة البلد ونموه، لكن هل تمت إباحة الدفاع عن النفس ضد العقوبات الاقتصادية، حتى لو كانت تلك التي تصدر من دولة ضد أخرى بصفة فردية خارج نطاق الأمم المتحدة. لماذا يقبل مواجهة الهجمات السيبرانية التعطيلية التي تسبب خسائر اقتصادية دفاعا عن النفس مع أنها تشابه العقوبات الاقتصادية في آثارها؟ قد يجادل البعض أن العقوبات يمكن ان تتم بشكل قانوني في إطار التدابير المضادة المشروعة، والهجوم السيبراني التعطيلي غير مشروع ويأتي في إطار الفعل العدواني، مع أن

[1] Tallinn Manual 2.0, commentary to rule 71, para. 12, p. 342

[2] في سبيل ذلك نقترح عقد مقارنة بين عواقب الهجمات السيبرانية على إستونيا 2007 التي استمرت ثلاثة أسابيع والهجوم الإسرائيلي على غزة عام 2008 الذي استمر ثلاثة أسابيع أيضا.

العقوبات أحيانا تتعدى الضغط أو الإكراه الذي كانت تقصده وتصل إلى تهديد حياة الناس كأن تتسبب بمجاعة كما حدث في العراق[1].

أخيرا فالهجوم السيبراني التعطيلي له علاج يكفيه، وهو التدابير المضادة، والتعويض عن الخسائر بموجب قواعد مسؤولية الدولة. فالطبيعة التعطيلية غير التدميرية تسمح بالتدابير المضادة، أو بالتدابير القانونية، أو بأخذ الموضوع إلى مجلس الأمن أو أي من أجهزة الأمم المتحدة، كذلك تسمح بالتعاون الدولي السريع وتبادل الخبرات للسيطرة على الهجوم السيبراني، وتسمح بالتفاوض مع الدولة منشأ الهجمات. كل ذلك ينفي حالة الضرورة المطلوبة في الدفاع عن النفس التي لا تترك مجالاً لمسارات العمل البديلة.

أما بخصوص وجود ما يكفي من الضمانات لتأمين عدم اللجوء غير الضروري للدفاع عن النفس فنذكر قول مايكل شميت الذي يؤكد أن الدول التي تتعرض لهذا النوع من الهجمات ستجادل بتعرضها لهجوم مسلح يستحق الرد بالدفاع عن النفس[2] ففي النهاية الأمر هناك مجال للجدال يحركه المصالح الوطنية. والدول ستتصرف وفقاً لتكييفها الذي تراه. فالصحيح أن يغلق المجال بوضوح وتكييف الدفاع عن النفس ضد العمليات السيبرانية التي لا تسبب إصابة أو تدمير خارج إطار الشرعية.

أما إذا لم تظهر آثار الهجوم السيبراني على الأرواح والممتلكات **لكن هناك احتمالية حقيقة** بأنه لو ترك فأنه سيتسبب في إصابة أو موت أو تدمير، فقد يكون ذلك مؤهلا لاعتبار الهجوم السيبراني في حكم الهجوم المسلح، وبالتالي مشروعية الدفاع عن النفس، كأن يستهدف أجهزة المستشفيات أو يستهدف وحدات التحكم في مواد قابلة للاشتعال أو الانفجار، هنا يمكن عد الهجوم التعطيلي في حكم الهجوم المسلح. وهذا يدخل فيما يعرف بالدفاع الاعتراضي عن النفس حيث بدأ الهجوم المسلح، لكن لم تكتمل نتائجه بعد وهذا سيعالج في المبحث الثاني من هذا الفصل في مطلب الدفاع عن النفس ضد تهديد بهجوم سيبراني مسلح.

هذه حالة يصعب تقديرها، لأنها تتطلب توقع دقيق لآثار العملية السيبرانية التعطيلية. فوفقًا لدليل (تالين) حين أجاب عن سؤال ماهي آثار العملية السيبرانية التي يمكن الأخذ بها لتقرير وجود هجوم

---

[1] Provost, R. (1992). Starvation as a Weapon: Legal Implications of the United Nations Food Blockade Against Iraq and Kuwait. *Columbia Journal of Transnational Law*, *30*, 577–639. Retrieved from https://ssrn.com/abstract=1332012

[2] المرجع السابق – Proceedings of a Workshop – National Research Council – ص177

مسلح من عدمه نص على أن: "جميع **النتائج المتوقعة بشكل معقول** للعملية السيبرانية مؤهلة"[1]. على سبيل المثال، حالة عملية إلكترونية تستهدف محطة تنقية المياه –بغض النظر عن خسائر الدولة الاقتصادية– وهي حالة تسبب توقع المرض والموت الناجمين عن الشرب الملوث للمياه، وهذه أحد الآثار التي تتشابه مع آثار الهجوم المسلح التقليدي وبالتالي فالدفاع عن النفس ممكن[2]. ومثل ذلك أن يبدأ الهجوم السيبراني بالتلاعب في نظام مصنع كيماويات مما قد ينتج عنه إطلاق مواد سامة تودي بحياة السكان القريبين منه، فكذلك هنا يمكن اللجوء إلى الدفاع عن النفس لوقف تلك العمليات السيبرانية باعتبار أن آثارها المتوقعة بشكل معقول متشابهة مع الهجوم المسلح. مرة أخرى هذه الحالة ليس من السهل تقديرها، لكن عامة يمكن القول إن وجود علاقة سببية مباشرة بين احتمال الموت أو التدمير وبين الهجوم السيبراني التعطيلي، وإذا كان الهجوم قد تمت نسبته إلى دولة وكان استخدام القوة هو الملاذ الأخير وكان نجاح العملية الدفاعية مرجحاً لتحقيق هدف الدفاع، وكانت العملية الدفاعية متناسبة مع هدف الدفاع به فإن كل ذلك يرجح من شرعية الدفاع عن النفس[3].

المطلب الثاني

الأنواع التوسعية في الدفاع عن النفس وانطباقها على الهجوم السيبراني

ظهرت بعد ميثاق الأمم المتحدة أنواع جديدة توسع من تطبيق حق الدفاع الشرعي عن النفس. فحينما ترغب الدول في استخدام القوة فأنها لا تجادل في قاعدة منع استخدام القوة ولا في اصدار استثناء جديد عليها، بل تستخدم تلك الاستثناءات الراسخة في الميثاق. مثلا استخدام القوة للتدخل لأسباب إنسانية يواجه برفض قانوني قوي في مشروعيته؛ لأنه غير موجود في الميثاق[4]. لكن الاستناد على الدفاع عن النفس وفق الميثاق –إن لم يكن أقل جدلا– فهو أكثر قابلية للنقاش. لذلك أدخلت الدول –تحت مظلة المادة 51 من الميثاق– الدفاع عن النفس الجماعي، والدفاع عن النفس الاستباقي، والدفاع عن النفس

---

[1] Tallinn Manual 2.0, commentary to rule 71, para. 13, p. 343

[2] Tallinn Manual 2.0, commentary to rule 71, para. 13, p. 343

[3] O'Connell, M. E., & Arimatsu, L. (2012, May). *Cyber Security and International Law*, p. 6. Presented at the International Law: Meeting Summary, London, United Kingdom: Chatham House. Retrieved from https://www.chathamhouse.org/sites/default/files/public/Research/International%20Law/290512summary.pdf

[4] المرجع السابق – Dinstein, Y. – War, Aggression and Self-Defence – المرجع السابق – ص244

انظر أيضا:

Orford, A. (2009). Reading Humanitarian Intervention: Human Rights and the Use of Force in International Law. Cambridge, United Kingdom: Cambridge University Press.

ضد الجماعات المسلحة من غير الدول، والدفاع عن النفس ضد هجوم مسلح بشكل تراكمي، وغيرها من الأمثلة منها ما يعد مشروعا بنص الميثاق، ومنها ما لا يزال مثارا للجدل في قانونيته، لكن بالتأكيد هناك توجه في سلوك الدول يدفع نحو التوسيع للنظرة الكلاسيكية في الدفاع عن النفس، وهذا له أثر مباشر على الهجمات السيبرانية لأنه لا يعالج بقانون خاص بها، لذلك فإن التوسيع في الدفاع عن النفس ضد الهجوم التقليدي يتبعه توسيع في الدفاع عن النفس إذا كان الهجوم إلكتروني. يناقش هذا الفرع بعض الأنواع التوسعية في استخدام القوة ومدى انطباقها على الطبيعة السيبرانية.

الفرع الأول: الدفاع عن النفس ضد هجوم مسلح تراكمي

في قضية نيكاراجوا 1986م عرَّفت محكمة العدل الدولية الهجوم المسلح بأنه:

"أكثر الصور جسامة لاستخدام القوة "[1]

أي أن الهجوم المسلح يعني استخدام قوة بليغة وجسيمة، وليس مجرد استخدام محدود أو خفيف للقوة. فاستخدام القوة أكثر شمولا من الهجوم المسلح، وإن كان الأخير أحد أنواع استخدام القوة[2]. وفي قضية المنصات النفطية 2003م أكدت محكمة العدل الفكرة نفسها بنصها:

" ليس كل استخدام للقوة يرقى إلى أن يكون هجوما مسلحا، لكن كل هجوم مسلح هو استخدام للقوة."[3]

الفكرة التي تؤكدها محكمة العدل الدولية هي أنه ليس كل استخدام للقوة ضد الدولة يبيح المسارعة والرد علية بالقوة، بل يجب أن تتعرض إلى قوة جسيمة. فاشتراط أن يكون الاعتداء جسيما هو الضامن لتحقق معيار الضرورة؛ لأن الدفاع عن النفس لن يكون ضروريا إلا إذا كان الاعتداء على قدر من الجسامة[4].

---

[1] *Nicaragua* judgement, para. 191, p. 101

[2] المرجع السابق – The International Court of Justice – Green, J. A. – ص31-36

[3] *Oil Platforms* judgement, para. 51, p. 186

[4] في العام 1981م وقع هجوم صغير على جمهورية سيشل من قبل مجموعة مسلحة من المرتزقة. الراجح أنهم كانوا مرسلين من دولة جنوب افريقيا، وبالرغم من أنهم كانوا بضع عشرات (43 شخص) أدين الفعل من قبل المجتمع الدولي بأنه اعتداء مسلح. والسبب في ذلك هو أن سيشل جزيرة صغيرة وهذا الهجوم اليسير كان كفيلاً بتدمير مطارها الوحيد والتسبب بفوضى عارمة في البلاد. فمثل هذا الهجوم يعد جسيماً إذا وقع على دولة صغيرة مثل سيشل لكن إذا وقع على دولة مثل الولايات المتحدة لن يعد اعتداء مسلحا؛ لأنه لن يتصف بالجسامة.

السبب وراء اشتراط كون الاعتداء جسيماً –وليس أي استخدام للقوة التي يشرع بسببها حق الدفاع عن النفس– هو الخوف من التصعيد العسكري بسبب حادثة يسيرة[1]. كأن يبدأ الأمر بإطلاق نار خفيف عبر الحدود، فترد الدولة دفاعاً عن النفس، ثم تقوم الدولة المعتدية بالرد على فعل الدفاع، ويتطور الأمر إلى حرب. لذلك فإن الميثاق الصادر مباشرة بعد أعقاب الحرب العالمية الثانية يحاول الحد من استخدام القوة المسلحة بأكبر قدر ممكن بأن يشترط الهجوم المسلح أي الاستخدام الجسيم للقوة، وليس أي استخدام للقوة.

وثم بعد التفريق بين استخدام القوة والهجوم المسلح اتخذت المحكمة معياراً للتفرقة بين استخدام القوة والهجوم المسلحة في فضية نيكاراجوا كما يتبين من النص الآتي:

"الدفاع عن النفس –فرديًا كان أو جماعيًا– لا يمارس إلا ردًا على هجوم مسلح. يجب أن يُفهم من هذا على أنه ليس أي عمل يتم على الحدود الدولية من قبل قوات مسلحة نظامية يدخل في مفهوم الهجوم المسلح، ولكن إذا تم ارسال قوات مسلحة من قبل دولة إلى إقليم دولة أخرى وكانت هذه العملية، بسبب "**حجمها وآثارها**" كان يمكن تصنيفها على أنها هجوم مسلح".[2]

هنا المحكمة تؤكد ضرورة التمييز بين الاعمال العدائية العادية، والهجوم المسلح مع تأكيد أن الأخير فقط هو الذي يخول حق الدفاع عن النفس، ثم بينت أن العملية العسكرية تأخذ هذه الصفة بسبب حجمها (الكم) وأثرها(الكيف) دون أن تحدد ما هو الكم والكيف المطلوب؟ لكن اذا ما أخذنا في الحسبان نص المحكمة أن " الهجوم المسلح هو أكثر الصور جسامة لاستخدام القوة"، فإنه سيتبين أن حجم العملية يجب أن يكون على نطاق واسع والآثار يجب تتصف بالجسامة. فإذا كان الهجوم شاملا وعلى نطاق واسع وليس مجرد تبادل إطلاق نار على نقطة حدودية، أو استهداف شخص محدد وحسب، بل

U.N. SCOR, 36th Sess., 2314 mtg., U.N. Doc. S/PV.2314 (15 December 1981), available from https://digitallibrary.un.org/record/49211
U.N. SCOR, 37th Sess., 2359 mtg., U.N. Doc. S/PV.2359 (20 May 1982), available from https://undocs.org/en/S/PV.2359
U.N. SCOR, 37th Sess., 2361 mtg., U.N. Doc. S/PV.2361 (21 May 1982), available from https://undocs.org/en/S/PV.2361
U.N. SCOR, 37th Sess., 2365 mtg., U.N. Doc. S/PV.2365 (24 May 1982), available from https://undocs.org/en/S/PV.2365
U.N. SCOR, 37th Sess., 2367 mtg., U.N. Doc. S/PV.2367 (25 May 1982), available from https://undocs.org/en/S/PV.2367

المرجع السابق – The International Court of Justice – Green, J. A. – ص155
[1] المرجع السابق – War, Aggression and Self-Defence – Dinstein, Y. – المرجع السابق – ص244
[2] *Nicaragua* judgement, summary of the Judgment of 27 June 1986, p. 165

تتصف آثاره بالجسامة لتدميرها المادي الكبير في الممتلكات مما خلفة الهجوم، أو الجسامة في اعداد الضحايا، فإن العملية تستوفي شرطي الهجوم المسلح الذي يؤهل للحق الشرعي بالدفاع عن النفس.

الرد على استخدام هجوم مسلح تراكمي:

يحدث في الواقع العملي أن تشكو الدول من وجود فراغ تشريعي بين المادة (4)2 –وهي مبدأ المنع من استخدام القوة (أي قوة وإن لم تكن جسيمة)– والمادة 51 من الميثاق وهي الدفاع الشرعي. فقد تقوم دولة باستخدام القوة ضد دولة أخرى، لكن لأن القوة لم تكن جسيمة فإن خيار الدفاع لن يكون مطروحا أمام الدولة المعتدى عليها. فالفراغ التشريعي يضعنا أمام حالتين غريبتين: أحدهما تكون الدولة عرضة للاعتداء باستخدام القوة ولا تملك القيام بأي رد فعل! والأخرى تكون للدولة الفرصة أن تبادر بالعدوان وكل ما عليها فعله هو الحرص على ألا تستخدم القوة بدرجة جسيم ولن تكون عرضه لأي رد[1].

ردا على ذلك طرحت بعض الدول فكرة الهجوم المسلح عن طريق التجميع أو التراكم وهو ما يطلق عليه "Pin Prick Theory of Armed Attack"[(2)]. ومفادها إذا كان هناك عدد من استخدامات القوة لا ترقى إحداها إلى مستوى الهجوم المسلح –لأنها غير جسيمة بالقدر المطلوب– فإنه بالإمكان جمع كل الاعتداءات البسيطة ثم تقاس جسامتها بالنظر إليها كوحدة واحدة، لتشكل هجوماً مسلحاً يخول الرد بالقوة المسلحة. بعبارة أخرى لا نحتاج لهجوم جسيم واحد، يكفي أن يكون لدينا عدد من الهجمات البسيطة (كإطلاق قذيفة أو صاروخ عبر الحدود) من الفاعل نفسه سواء أكان دولة أم لاعب غير دولي بتكرار على مدد متباعدة لترقى تلك الأفعال في مجموعها إلى هجوم مسلح، ولذلك يصبح من الضروري الرد عليه بشكل متناسب. إن من أكبر المؤيدين لهذا المذهب إسرائيل، ولكن استخدمته بعض الدول كبريطانيا والبرتغال[(3)] في سيناريو الهجمات السيبرانية، تحدث هجمات "الوخز بالإبر" حينما يكون الضرر الفردي لكل حادث منخفضًا. لذلك فذلك النوع من الهجمات غير مناسب لمهاجمة أهداف شديدة التحصين كقطاع الاتصالات أو القطاعات العسكرية، لكن نظرًا لأنها استراتيجية طويلة المدى، قد تتمكن هجمات "الوخز بالإبر" من الوقوف على نقاط محددة وتؤدي إلى نتائج جيدة، لا

[1] Gray, C. (2018). International Law and the Use of Force (Foundations of Public International Law) (4th ed.), p. 155. Oxford, United Kingdom: Oxford University Press.
[2] Noortmann, M., Reinisch, A., & Ryngaert, C. (Eds.). (2017). *Non-State Actors in International Law (Studies in International Law)* (Reprint ed.), p. 86. Oxford, United Kingdom: Hart Publishing.
[3] المرجع السابق

تصل إلى التدمير، لكن التعطيل أو انخفاض مستوى الخدمة. فعن طريق الوخز تدريجيًا بهجمات سيبرانية في آلية معقدة يمكن إيقافها، أو على الأقل جعلها تعمل بكفاءة أقل.[1]

لا يوجد نص مكتوب يعطي هذه الممارسة اعترافا بالشرعية، لكن هناك ممارسات دولية منتظمة للدفاع عن النفس ضد "تراكم من استخدام بسيط للقوة" ولم ينكر المجتمع الدولي على مشروعية.[2] كذلك، محكمة العدل الدولية لم تعترض على الفكرة . في قضية الأنشطة المسلحة في إقليم الكونغو، رفضت المحكمة دفع **تجميع استخدام القوة** بسبب نقص الأدلة ليس بسبب عدم قبول الفكرة فنصت في الحكم على الآتي:

"المحكمة ترى، في الأدلة المعروضة عليها –حتى لو كانت هذه السلسلة من الهجمات المؤسفة يمكن اعتبارها تراكمية في طبيعتها– فأنها تبقى غير منسوبة إلى [جمهورية الكونغو الديمقراطية]."[3]

كذلك في قضية المنصات النفطية بين إيران والولايات المتحدة، فقد استخدمت الولايات المُتحدة القوة ضد السفن البحرية الإيرانية ومنصات النفط، وكان تبريرها بأن جاء هذا "رداً على نمط مُستمر من الهجمات التي تشُنها إيران على السُفن التي ترفع العلم الأمريكي "وخز الإبر" وكان رد المحكمة على هذا الدفع في قضية منصات النفط الإيرانية كما يأتي:

"بالنسبة لسؤال "ما إذا كان ذلك الهجوم، إما في حد ذاته أو بالاشتراك مع "سلسلة الهجمات "التي استشهدت بها الولايات المتحدة يمكن تصنيفها على أنها هجوم مسلح" على الولايات المتحدة يبرر الدفاع عن النفس"[4]

ثم فندت المحكمة سلسلة الهجمات التي قصدتها الولايات المتحدة وانتهت المحكمة بقولها:

---

[1] Lemay, A., Fernandeza, J. M., & Knight, S. (2010). *Pinprick attacks, a lesser included case?* In C. Czosseck & K. Podins (Eds.) (pp. 183–194) [pp. 189-191]. Presented at the Conference on Cyber Conflict, Tallinn, Estonia. Retrieved from https://ccdcoe.org/uploads/2018/10/Lemay-Pinprick-attacks-a-lesser-included-case.pdf

[2] لقراءة ممارسات الدول الداعمة لشرعية الدفاع عن النفس ضد هجوم تراكمي انظر:
Jain, A. G. (2014). Rationalising International Law Rules on Self-Defence: The Pin-Prick Doctrine. *Chicago-Kent Journal of International and Comparative Law*, *14*(2), 23–70 [p. 47-58]. Retrieved from https://scholarship.kentlaw.iit.edu/ckjicl/vol14/iss2/2

[3] *Armed Activities* judgement, para. 146, p. 222

[4] *Oil Platforms* judgement, para. 64, p. 191

"حتى لو أخذت بشكل تراكمي ... لا يبدو للمحكمة أن هذه الحوادث تكوّن هجومًا مسلحًا على الولايات المتحدة[1]".

وخلُصت المحكمة إلى أن موقف الولايات المتحدة ضعيف بهذا الشأن؛ لعدم توافر الأدلة الواقعية، إلا ان المحكمة اعترفت بأن هجوماً واحداً في الهجمات المُتسلسلة يُمكن أن يسوغ استخدام القوة[2].

أنصار مذهب "وخز الإبر "الذين يرون أن قواعد الدفع عن النفس غير كافية من الناحية الموضوعية، وأنها مفرطة في التساهل، ومقيدة –بإفراط– لقدرة الدول على حماية نفسها[3] يستخدمون هذين الحكمين دليلا على اعتراف محكمة العدل بالنظرية وبالتالي شرعيتها[4]، فهي لم ترفض الفكرة لكنها رأت أن الأدلة غير كافية لتطبيقها. بينما يمكن القول بخلاف ذلك فالنتيجة أن المحكمة لم تأخذ بمذهب تكوين هجوم مسلح من سلسلة هجمات أصغر، ولم تصادق صراحة على مشروعية الفكرة، لأنها لم ترغب في تقديم مساهمة جديدة في توسيع معايير استخدام الدفاع عن النفس في القانون الدولي[5].

ليس من السهل التسليم بخطورة هذا الادعاء الذي يعرض منظومة استخدام القوة والتي يستند عليها السلم الدولي للانهيار. فهذا المذهب يصطدم تماما مع الميثاق حيث لا يوجد هجوم مسلح يبرر الدفاع عن النفس. ويصطدم مع القانون العرفي خصوصاً شرط الضرورة –كما جاء في اختبار كارولاين–لأن الاستخدام الايسر للقوة ينفي الضرورة الملحة التي لا تترك مجالا لأي وسيلة أخرى سوى الدفاع عن النفس. دائما يذكر أن هناك فراغا بين الهجوم المسلح والاستخدام الأقل للقوة عندما تكون الدولة عرضة للقوة ولا تستطيع الرد عليها، لكن الحقيقة لا يوجد فراغ بل توجد مسارات عمل بديلة، من الخيارات المطروحة –مع الاستخدام الخفيف للقوة– تستطيع الدول اللجوء للإجراءات المضادة كالعقوبات الاقتصادية والطرق الدبلوماسية، أو حتى اللجوء لإبلاغ لمجلس الأمن. وتصطدم نظرية وخز الإبر بشكل أكبر بالتناسب خصوصا التناسب الزماني، وهو المدة المعقولة بين الهجوم والرد عليه، هنا يكون

---

[1] المرجع السابق

[2] *Oil Platforms* judgement, para. 72, p. 195

[3] Guzman, A. T. (2009). Rethinking International Law as Law. *Proceedings of the 115th ASIL Annual Meeting*, *103*, 155–157. https://doi.org/10.1017/s0272503700033978
Shaw, M. N. (2022). *International Law 6th (sixth) edition* (6th ed.). Cambridge, United Kingdom: Cambridge University Press.

[4] المرجع السابق – Jain, A. G. – ص69

[5] Ochoa-Ruiz, N., & Salamanca-Aguado, E. (2005). Exploring the Limits of International Law relating to the Use of Force in Self-defence. *European Journal of International Law*, *16*(3), 499–524 [p. 523]. https://doi.org/10.1093/ejil/chi128

الأمر غير مرتبط بالمدة المعقولة بل بما تعتقد الدولة الضحية أنه الوقت المناسب لها لاستخدام عذر الدفاع عن النفس.

وقد أقر دليل (تالين) بهذه النظرية في المجال السيبراني. فردا على ما إذا كان يجوز للدولة ممارسة حق للدفاع عن النفس ردًا على سلسلة من الحوادث السيبرانية الفردية بوصفها جميعا هجوما مسلحا. بعبارة أخرى هل يمكن أن تكون هجومًا مسلحًا في مجموعها؟ رأى فريق الخبراء الدولي إمكانيه ذلك إذا تحقق أمرين:

- أن تكون جميع الهجمات قد صدرت من المنشأ نفسه[1].
- أن تكون الحوادث الصغيرة في مجموعها تفي بمتطلبات الحجم والأثر[2].

فإذا كان هناك دليل مقنع على أن هذا هو الحال، نكون أمام أسباب معقولة لمعاملة الحوادث المنفردة على أنها هجوم مسلح مركب.

ومن المستغرب أن هذا الرأي جاء باتفاق الخبراء، برغم أن دليل (تالين) قد بين بصراحة خيار الإجراءات المضادة إذا تعرضت الدولة لاستخدام خفيف للقوة[3]. والأمر كذلك يجد تشجيعا كبيرا من الفقه سواء من ناحية الاستخدام العادي للقوة[4] أم استخدام القوة في النطاق السيبراني[5] مسوغين ذلك بعدم كفاية الإجراءات المضادة في تحقيق الردع، فإلى متى تستمر الدولة في حالة عدم الاستقرار خصوصا إذا لم تنجح الإجراءات المضادة، لذلك فالرد بالدفاع عن النفس على مستوى هجوم مسلح، يمكن أن يحقق الردع الذي يعيد الأمور إلى نصابها. مع ذلك فإن تحقيق الردع مستقلا من كل دولة ليس هو التوجه الذي يقوم عليه القانون الدولي المعاصر. وإن كان لا بد من ان يشرع دليل (تالين) مثل هذه الممارسة فإنه من الأجدى أن يضع شرطا باستنفاد الإجراءات المضادة، والتأكد من عدم كفايتها قبل استخدام

---

[1] Tallinn Manual 2.0, commentary to rule 71, para. 11, p. 342

[2] المرجع السابق

[3] Tallinn Manual 2.0, commentary to rule 22, para. 12, pp. 125-126

[4] المرجع السابق – Dinniss, H. H. – ص93-95

المرجع السابق – Cyber Operations and the Use of Force – Roscini, M. – ص108-110

المرجع السابق – Delerue, F. – ص334-335

[5] المرجع السابق – Green, J. A. – The International Court of Justice – ص42

المرجع السابق – Dinstein, Y. – War, Aggression and Self-Defence. – المرجع السابق – ص206-207

Nolte, G., & Randelzhofer, A. (2012). Ch.VII Action with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression, Article 51. In *The Charter of the United Nations: A Commentary, Volume II (3rd Edition)* (3rd ed., p. 1409). Oxford, United Kingdom: Oxford University Press.

الدفاع عن النفس خصوصا أن الطبيعة التراكمية تنفي الضرورة التي تستوجب الرد الفوري باستخدام القوة.

كذلك هناك مشكلة أخرى أن دليل (تالين) اشترط أن تكون الهجمات من المنشأ نفسه، لكنه لم يشترط أن تكون من الطبيعة نفسها، فهل يعني ذلك أنه من الممكن الدمج بين الاستخدام العادي للقوة –مثل تلك المناوشات العسكرية على الحدود– مع بعض الهجمات السيبرانية التي تعطل بعض الخدمات الحكومية مثلا لتكوين هجوم مسلح يهيئ للرد بالدفاع عن النفس. إذا ما تم التسليم بقبول ذلك النوع الهجين وعده هجوما مسلحا تراكميا ففي ذلك توسيع خطير للهجوم المسلح، وهو ينافي توجه محكمة العدل الدولية في تضييق الهجوم المسلح الذي يهيئ للدفاع عن النفس.

الفرع الثاني: الدفاع عن النفس الجماعي ضد الهجمات السيبرانية

المقصود بالدفاع عن النفس الجماعي هو ممارسة الدفاع عن النفس نيابة عن دولة أخرى، مثلاً إذا تعرضت الدولة "أ" للهجوم من قبل الدولة "ب" فتتدخل الدولة "ج" لحماية الدولة "أ". ويمكن أن يحدث ذلك بين دولتين أو أكثر، أو يمكن أن يكون على شكل معاهدة جماعية للدفاع عن النفس إذا تلتزم الدول بالدفاع بعضها عن بعض إذا تعرض أي من أعضائهم لهجوم وأبرز مثال ذلك هو معاهدة حلف الناتو فإن المادة 5 تؤكد أن الهجوم على واحد من الأعضاء هو بمنزلة هجوم ضد جميع الأعضاء[1].

المادة 51 من الميثاق جعلت ذلك ممكناً حيث تبدأ بـ: "ليس في هذا الميثاق ما يضعف أو ينتقص الحق الطبيعي للدول– **فرادى أو جماعات**– في الدفاع عن أنفسهم ..." مما حسم مشروعية هذا النوع من الدفاع عن النفس[2]، طالما أن المعايير المعتادة في الدفاع عن النفس منطبقة، فيجب أن يكون

---

[1] تنص المادة الخامسة من اتفاقية حلف شمال الأطلسي على أنه:
"يتفق الأطراف على أن أي هجوم مسلح ضد واحد أو أكثر منهم في أوروبا أو أمريكا الشمالية يعد هجومًا ضدهم جميعًا، وبالتالي يتفقون على أنه في حالة حدوث مثل هذا الهجوم المسلح، فإن كلا منهم، في إطار ممارسة الدفاع عن النفس الجماعي المعترف به في المادة 51 من ميثاق الأمم المتحدة ، سيساعد الطرف أو الأطراف التي تعرضت للهجوم من خلال اتخاذ الإجراءات التي يراها ضرورية على الفور، فرديا وبالتوافق مع الأطراف الأخرى ، بما في ذلك استخدام الأسلحة المسلحة والقوة، لاستعادة والحفاظ على أمن منطقة شمال الأطلسي. ويجب إبلاغ مجلس الأمن على الفور بأي هجوم مسلح من هذا القبيل وجميع التدابير المتخذة نتيجة له. تنتهي هذه الإجراءات عندما يتخذ مجلس الأمن التدابير اللازمة لاستعادة وصون السلم والأمن الدوليين.
North Atlantic Treaty Organization (Washington), *North Atlantic Treaty*, 9 April 1949, available at: https://www.nato.int/cps/en/natohq/official_texts_17120.htm

[2] بودربالة، صلاح الدين. (2010). استخدام القوة المسلحة في إطار أحكام ميثاق الأمم المتحدة (أطروحة دكتوراه)، ص80-87. جامعة الجزائر. استرجع من
http://193.194.83.98/jspui/bitstream/1635/10291/1/BOUDERBALA_SALAH.pdf

الدفاع الجماعي عن النفس ردا على هجوم مسلح والاستجابة يجب أن تكون ضرورية ومتناسبة. لكن محكمة العدل الدولية نصت في قضية نيكاراغوا على أن هناك معيارين إضافيين للدفاع الجماعي عن النفس وهما:

أولاً أن تعلن الدولة الضحية أنها تعرضت لهجوم مسلح[1]

وثانياً عليها أن تطلب مساعدة الدولة الحامية. لذلك لا يكفي أن تكون الدولة غير قادرة على حماية نفسها، بل عليها أن تطلب المساعدة صراحة[2].

الأساس المنطقي وراء طلب هذه الخطوة الإضافية هو الحماية من سوء الاستخدام حتى لا تتمكن الدول القوية من استخدامها للعدوان ضد الدول الأصغر. لم توضح محكمة العدل الدولية ما إذا كان طلب المساعدة يجب أن يكون موجهًا نحو دولة معينة أم لا، ولكن حتى الآن طلب المساعدة يتم تقديمه لدولة معينة أما الطلب إلى مجهول فإنه لم يتم اختباره بعد. كذلك في الواقع فإن الأمر يتعلق أكثر بجزء الطلب أما الإعلان فهو موجود ضمنيا في طلب المساعدة[3].

هذا الموضوع ينطبق تماما في السياق السيبراني فليس هناك اختلاف عن اشتراطات القاعدة العامة في الدفاع الجماعي التقليدي. فإنه يمكن أن تمارس دولة الدفاع الجماعي عن النفس نيابة عن دولة أخرى إذا تعرضت لهجوم سيبراني مسلح على أن يكون فعل الدفاع ضروريا ومتناسبا[4]، ويجب أن تفعل ذلك في نطاق طلب وموافقة الطرف الآخر.[5] هذا بالإضافة إلى أن الموافقة يجب أن تكون سابقة

---

[1] انظر حكم قضية نيكاراجوا فقرة 195 فقد نص الحكم على أنه: "لا توجد قاعدة في القانون الدولي العرفي تسمح لدولة أخرى بممارسة حق الدفاع الجماعي عن النفس على أساس تقييمها الخاص للموقف. عندما يتم التذرع بالدفاع الجماعي عن النفس، فمن المتوقع أن الدولة التي يستخدم هذا الحق لصالحها تكون قد أعلنت أنها الضحية لهجوم مسلح"

Nicaragua judgement, para. 195, p. 103

[2] حكم قضية نيكاراجوا فقرة 195 حيث نصت المحكمة على ما يأتي: "وجدت المحكمة أنه في القانون الدولي العرفي -سواء أكان من النوع العام أم من ذلك النوع الخاص بنظام البلدان الأمريكية- لا توجد قاعدة تسمح بممارسة الدفاع الجماعي عن النفس في حالة عدم وجود طلب من قبل الدولة التي تعد نفسها ضحية لهجوم مسلح. المحكمة تستنتج أن طلبا صادرا من الدولة التي تدعي انها ضحية هجمات هو مطلب إضافي يضاف إلى مطلب أن تعلن الدولة أنها تعرضت لهجوم مسلح"

Nicaragua judgement, para. 195, p. 103

[3] المرجع السابق – The International Court of Justice – Green, J. A. – ص52-53

[4] Tallinn Manual 2.0, commentary to rule 74, para. 5, p. 355

[5] Tallinn Manual 2.0, commentary to rule 74, para. 3, p. 355

على قيام سلوك الدفاع من الدولة الثالثة، أما الموافقة اللاحقة فتجعل من سلوك الدفاع القادم من طرف ثالث استخداما غير مشروع للقوة، فإنها يمكن أن تخفف من مسؤولية الدولة المرتكبة[1].

ومن الأمثلة التي توضح هذا الموقف حينما كانت جورجيا ضحية للعديد من العمليات السيبرانية خلال النزاع المسلح الروسي الجورجي في عام 2008. واستفادت الحكومة الجورجية من التعاون الدولي في مكافحة هذه العمليات السيبرانية. في مثل هذه الظروف أعطت الحكومة الجورجية الموافقة على الدول الأجنبية للعمل على الخوادم الموجودة داخل أراضيها. هذه العمليات السيبرانية لو لم تكن بموافقة جورجيا كانت انتهاكًا للسيادة الجورجية[2].

في حالة الاتفاق على الأمن الجماعي في معاهدة كمعاهدة كحالة المادة 5 من معاهدة حلف شمال الأطلسي، قد يطرح تساؤل هنا عن اشتراط المساعدة الذي جاءت به محكمة العدل الدولية إذا كان بين الدول اتفاق على الدفاع، أو أن طلب المساعدة كان يسقط، وتستطيع الدول الأطراف مساعدة الدولة الضحية مباشرة دون طلب منها. المادة 5 من معاهدة الناتو لا تشترط طلب الدولة التي تتعرض لهجوم للمساعدة، وتكتفي بتعهد الدول بالدفاع إذا وقع هجوم مسلح على أحد الدول الأعضاء. لكن السؤال من الذي يقرر وقوع هجوم مسلح من عدمه؟ الأرجح أن الدولة الضحية التي يقع على إقليمها الهجوم هي التي تقرره وتعلنه وتطلب المساعدة، فلو أنكرت الدولة الضحية بشكل قاطع وقوع هجوم مسلح على إقليمها، من الأجدر بالتصديق الدولة التي وقع على إقليمها استخدام القوة أو الدولة التي تدعي المساعدة؟ صحيح أن اشتراط محكمة العدل الدولية جاء في الوضع العام حيث لا يوجد اتفاق ومعاهدة الناتو هي معاهدة خاصة، والخاص يقيد العام كقاعدة عامة. لكن لا يمكن أن يترك تقدير الحاجة إلى استخدام القوة لغير الدولة التي تتعرض للهجوم، وذلك لأسباب عسكرية أولاً، فقد يؤدي غياب التنسيق مع الدولة التي ستقوم بالمساعدة على إجهاض الجهود الدفاعية للدولة الضحية وهذا أمر متصور جدا في النطاق السيبراني؛ فإن التداخل في عمليات التنسيب التقني (محاولة معرفة الفاعل) قد يؤذي الأدلة. من ناحية أخرى قد تكون الدولة قادرة على الدفاع عن نفسها كأن تكون متطورة جدا في القطاع العسكري أو السيبراني، هنا المساعدة المفروضة دون طلب قد تُتَهَم بالتدخل غير المشروع أو بالاعتداء على السيادة، فضلا عن اتهامها بالاستخدام غير المشروع للقوة. لذلك الأرجح أن المادة 5 من اتفاقية الناتو لا يسلب حق الدولة الضحية في تقرير الحاجة إلى المساعدة لكنها تسلب حق الدول الأطراف في اختيار عدم المساعدة إذا طلبتها الدولة الضحية. وتجدر الإشارة

[1] المرجع السابق – Delerue, F. – ص345
[2] المرجع السابق – ص346

أن الاستخدام الوحيد للمادة 5 من اتفاقية الناتو كان بسبب هجمات 11/9 وقد طلبت الولايات المتحدة المساعدة من حلفائها في الناتو وبناء عليه تم تفعيلها[1].

مع ذلك هناك من يرى أن الدفاع عن النفس حق وليس واجبا. فالحديث هنا عن دفاع جماعي عن النفس وليس دفاعاً بالنيابة. بمعنى أن الطرف الثالث لم يتحرك دفاعا عن النفس لمساعدة الدولة التي وقع عليها الهجوم فقط، بل هو يدافع عن نفسه (جزئياً على الأقل) وعن مصالحة في المنطقة. مما يجعل الدولة التي وقع الهجوم على إقليمها مجبرة على قبول المساعدة خصوصاً في حالة وجود اتفاق بتنظيم الدفاع عن النفس فهو ملزم للدول بتقديم المساعدة وبقبولها[2].

قد يجدر التوقف هنا عند تجربة الناتو الذي لم يكتف بالتأكيدات المتكررة على امتداد الالتزام في المادة 5 من معاهدة الحلف إلى الفضاء حال تعرض أحد الأطراف لهجوم سيبراني مسلح.[3] بل أنشأ عددا من المراكز لمهمة رصد النشاط السيبراني الضار والتصدي لها نذكر منها[4]:

1-وحدة الاستجابة لحوادث الكومبيوتر (NCIRC) The NATO Computer Incident Response Capability التابعة لحلف الناتو ومقرها بلجيكا، وهي تحمي شبكات الناتو الخاصة من خلال دعم الدفاع الإلكتروني على مدار الساعة. خبراؤها يتعاملون مع الحوادث ويقدمونها للناتو بتحليل محدث للتحديات الإلكترونية التي يتم مواجهتها.

---

[1] North Atlantic Treaty Organization (NATO). (2022a, June 11). Collective defence - Article 5. Retrieved from https://www.nato.int/cps/en/natohq/topics_110496.htm

[2] المرجع السابق – Dinstein, Y. – War, Aggression and Self-Defence. – المرجع السابق – ص294-296

[3] North Atlantic Treaty Organization (NATO). (2016, July 9). *Warsaw Summit Communiqué: Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8–9 July 2016* [Press release], para. 6. Retrieved from https://www.nato.int/cps/en/natohq/official_texts_133169.htm

North Atlantic Treaty Organization (NATO). (2019, November 4). *London Declaration: Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in London 3–4 December 2019* [Press release], para. 31. Retrieved from https://www.nato.int/cps/en/natohq/official_texts_171584.htm

North Atlantic Treaty Organization (NATO). (2021, June 14). *Brussels Summit: Communiqué Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels 14 June 2021* [Press release]. Retrieved from https://www.nato.int/cps/en/natohq/news_185000.htm

[4] المرجع السابق – North Atlantic Treaty Organization (NATO) – NATO Cyber Defence

2–مركز عمليات الفضاء السيبراني Cyberspace Operations Centre يدعم المركز القادة العسكريين بالوعي بالموقف لإبلاغ التحالف. ويقوم المركز أيضًا بتنسيق عمليات الناتو في الفضاء السيبراني، مما يضمن حرية التصرف في هذا المجال وجعل العمليات أكثر مرونة في مواجهة التهديدات الإلكترونية.

3–مركز التميز للدفاع السيبراني التعاوني[1] هو مركز بحث وتدريب معتمد من الناتو للتعامل مع تعليم وأبحاث الدفاع السيبراني من النواحي القانونية والعملية والتكنلوجية. يقدم المركز خبرة قيمة في مجال الدفاع، وتنظيم التدريبات السيبرانية التي يشارك فيها جميع الحلفاء.

الفرع الثالث: الدفاع عن النفس ضد تهديد باستخدام القوة

يتبين بوضوح من قراءة نص المادة 51 أن الحق في الدفاع عن النفس يبدأ بعد وقوع الهجوم المسلح لا قبله. فحالما يبدأ الهجوم المسلح يحق للدولة الضحية الدفاع عن نفسها دون خلاف على شرعية ذلك. لكن الملاحظ أن الدول في أحيان كثيرة تستخدم عذر الدفاع عن النفس قبل وقوع الهجوم المسلح.

وقد حاول فقهاء القانون في زمن ما بعد الميثاق التمسك بعدم مشروعية الدفاع الاستباقي. فإن أصحابها يتمسكون بالتفسير الضيق للنص قائلين: إنه لا يمكن أن يكون الدفاع الاستباقي مشروعاً، لأنه يتخيل الهجوم المسلح قبل أن يحصل، والميثاق يشترط حصوله فعلا قبل الرد عليه. ويضيف الفقيه Philip Jessup بما أن المادة 2(4) من الميثاق تمنع استخدام القوة، وتمنع التهديد بالقوة، فإن التهديد يعطي فرصة للدولة اللجوء لمجلس الأمن، لكنه لا يسوّغ الاستخدام الوقائي للقوة من قبل الدولة التي "تظن" أنها مهددة". لهذا يؤكد الفريق التقليدي أنه إذا شعرت الدولة أنها مهددة بهجوم وشيك، فإن ما عليها فعله هو الالتزام بالميثاق أن تضع المسألة أمام مجلس الأمن، وتكون في حالة تأهب عسكري لرد العدوان قبل وقوعه[2].

الحقيقة أن هذا الرأي لم يصمد كثيرا بعد ميثاق الأمم المتحدة؛ لأن الدول لم تلتزم به. فأصبح لا قيمة له، وبدأ الكتاب يحاولون اعتماد التفسير المرن الذي يسمح بالفعل الاستباقي –إن لم يكن لمجاملة الدول وإعطائها الضوء الأخضر في استخدام القوة– فلتقنين خروجها عن الميثاق بضوابط أخرى كما

[1] NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). (n.d.-a). About us. Retrieved from https://ccdcoe.org/about-us/

[2] Jessup, P. C. (1948). *Modern Law of Nations - An Introduction*, p. 166. New York, United States: Macmillan Publishers.

فعل التوجه المعاصر الذي اشترط ان يكون التهديد وشيكاً. واشترط ان طبيعة خاصة في عنصر الضرورة في الدفاع الاستباقي عن النفس وهي أن يكون التحرك للدفاع قبل الهجوم ضروريا، لأنه لو تم الانتظار حتى بدء الهجوم، فأنه من المتوقع بشكل معقول أن تصبح الدولة غير قادرة على الدفاع عن نفسها بشكل فعال أو سيكون فات الأوان على الدفاع عن النفس[1].

في موضوع الدفاع عن النفس ضد تهديد باستخدام القوة هناك مشكلة في توحيد المصطلح فقد يشار إليه بفعل الدفاع التوقعي (Anticipatory)، أو الوقائي (Preventative)، أو الاستباقي (Preemptive)، أو الاعتراضي (Interceptive) فبعض الكتاب يستخدمونها بوصفها لكن بعضهم يعد كل كلمة لها مدلول خاص. صحيح أنها جميعا تشير إلى مفهوم الاستجابة بالدفاع عن النفس ردًا على تهديد صادر ضد الدولة بدلًا من هجوم حقيقي، لكن بعض الكتاب يعطون هذه المصطلحات معانٍ مختلفة فكأن كل واحدة منها تمثل درجة من درجات اقتراب أو ابتعاد التهديد بالهجوم المسلح، لذلك كلمة (Imminent) وتعني "وشيك" هي كلمة أساسية مرتبطة بشرعية الدفاع عن النفس الاستباقي.

في سياق معالجة الدفاع الاستباقي ردا على تهديد سيبراني سيتم التركيز على النوعين الرئيسين من الدفاع الاستباقي، سيتم الحديث عن مشروعية الدفاع عن النفس استباقياً ضد هجوم سيبراني وشيك، والدفاع عن النفس استباقيا ضد هجوم سيبراني غير وشيك الحدوث.

أولا: الدفاع عن النفس ردا على تهديد وشيك

يمكن القول: إن الدفاع عن النفس الاستباقي ضد تهديد وشيك ينقسم إلى قسمين: أولهما: الدفاع عن النفس الاعتراضي، وهو الذي يكون ضد هجوم مسلح بدأ بالفعل لكنه لم يكتمل ولم ينتج آثاره بعد[2]. والدفاع عن النفس الاستباقي، وهو الدفاع عن النفس ضد هجوم لم يبدأ بعد ولم تتخذ الخطوة الأولى فيه، لكن المؤشرات تشير إلى أنه قريب الحدوث.

<u>الدفاع عن النفس الاعتراضي:</u>

[1] Tallinn Manual 2.0, commentary to rule 73, para. 3, p. 351

[2] المرجع السابق – War, Aggression and Self-Defence. – Dinstein, Y. – المرجع السابق – ص203

مثاله أن يتم إطلاق الصواريخ من دولة ويتم اعتراضها قبل أن تصل بالفعل إلى إقليم الدولة الأخرى. أو تحرك قوات الدولة (أ) بريا لاجتياح الدولة (ب) لكن يتم منعهم بالقوة من عبور الحدود. يرى بعض الفقهاء أنه هو التحرك المرئي الواضح للجيوش أو الطائرات أو القوات البحرية.[1] هذا النوع من الدفاع عن النفس وإن لم يتم النص عليه في ميثاق الأمم المتحدة، لا يثير الكثير من الجدل في مشروعيته، لأن الهجوم بدأ بالفعل، وإن لم تصل نتائجه بعد. فحتى أكثر الآراء تشددا –في منع الدفاع عن النفس ضد تهديد سواء أكان ضد تهديد وشيك أم غير وشيك– لا تعترض على الدفاع عن النفس ضد الهجوم الذي بدأ إطلاقه بالفعل[2]. لأنها لا تعده دفاعا استباقياً وإن لم تكتمل نتيجته بعد.

إنه من الصعوبة بمكان في الهجمات السيبرانية تطبيق مبدأ الدفاع عن النفس الاعتراضي، وذلك لسرعة الهجمات السيبرانية التي تستغرق جزءًا من الثانية للانتقال من بلد المنشأ إلى البلد المستهدف، لذلك حاليا في النظام التكنلوجي الحالي يصعب تطبيق فكرة الدفع الاعتراضي[3]. لكن الدفاع عن النفس الاعتراضي متصور في الحالات التي يتم فيها زرع البرامج الضارة "Malicious Malware" في النظام المستهدف، ويتم اكتشاف وجودها قبل أن تبدأ تلك البرامج بتحقيق أهدافها.

وأشهر مثال يمكن تطبيقه في هذه الحالة هو هجوم Stuxnet الذي أصاب المنشاة الإيرانية، فبعض المراجع ترجح أن الفايروس دخل الدولة، وبقي فيها لأكثر من سنة[4] قبل أن تظهر آثاره على نظام محطة نطنز. فلو أن الفايروس كان قد اكتشف قبل أن يحقق نتائجه النهائية هل كان بإمكان إيران استخدام الدفاع عن النفس بشكل استباقي. أولا يجب تأكيد ضرورة وجود العناصر المحركة للدفاع عن النفس وأولها الهجوم المسلح. هذا يتطلب من الدولة المستهدفة أولاً تحديد إمكان تسبب العملية الإلكترونية في ضرر وبعبارة أدق يجب أن تثبت الدولة أن العملية المرتقبة التي سيتم الدفاع عن النفس ضدها هي في نطاقها وآثارها المتوقعة يمكن أن تكون هجوما مسلحاً.

---

[1] Badr, G. (1980). The Exculpatory Effect of Self-Defense in State Responsibility. Georgia Journal of Comparative and International Law, 10(1), 1–28 [p. 25]. Retrieved from https://digitalcommons.law.uga.edu/gjicl/vol10/iss1/2/

[2] المرجع السابق – Dinstein, Y. – War, Aggression and Self-Defence. – المرجع السابق – ص203

[3] المرجع السابق – Delerue, F.– ص323-324

[4] Finkle, J. (2013, February 26). Researchers say Stuxnet was deployed against Iran in 2007. *Reuters*. Retrieved from https://www.reuters.com/article/us-cyberwar-stuxnet-idUSBRE91P0PP20130226

ثم يشترط الفقه القانوني شرطا آخر يخص الدفاع عن النفس الاعتراضي ضد هجوم سيبراني وشيك، وهو أن **يدخل الهجوم المسلح السيبراني الجزء الأخير من العملية السيبرانية حيث تبدأ نتائج العملية في الظهور**[1]. فإذا كنا بصدد حالة زرع البرامج الضارة في النظام المستهدف فإنه يجب أن يكون الفايروس الضار قد بدأ في استهداف النظام، لا أن يكون في حالة خمول[2]. لأن مجرد بقاء الفايروس خاملا في النظام لا يصل إلى عتبة الهجوم المسلح، وبالتالي لا يمكن اعتراضه بالدفاع عن النفس، وإن كان بالإمكان ان يعد خرقاً لسيادة الدولة، ويؤهل للإجراءات المضادة لكن ليس الدفاع عن النفس. لذلك يتوجب على الدولة إثبات أن النشاط الضار قد بدأ، حتى لو لم ينتج التأثير الكامل للهجوم المسلح.

لذلك بالعودة إلى فايروس Stuxnet بإمكان إيران الرد بالدفاع عن النفس بشكل اعتراضي لو تم اكتشاف الفايروس في النظام، وقبل أن يبدأ بتخريب أجهزة الطرد المركزي، إذا استطاعت اثبات أن الضرر المرتقب من هذا الفايروس يمكن أن يصل إلى مرحلة الهجوم المسلح، وهذا ليس بالأمر السهل، فالمتوقع أن تنكر الدول –وهنا نعني "إسرائيل"– أن الهدف من الفيروس هو الهجوم على المنشاة، وتقول: إنها كانت تقتصر على جمع معلومات عن قدرات إيران النووية[3]. لذلك يأتي الشرط الثاني وهو أن تثبت إيران ان الفيروس بدأ بمحاولة التخريب في المنشأة النووية. الحقيقة هذه الإثباتات تمثل عقبات صعبة في ظل الطبيعة السيبرانية غير المرئية مقارنة بالهجوم الحقيقي. لكن ما يجب تأكيده أن الدفاع عن النفس الاعتراضي مشروع من الناحية النظرية.

الدفاع عن النفس الاستباقي:

وهو الرد بالدفاع عن النفس ضد تهديد وشيك أو قريب الحدوث لكنه **لم يبدأ بعد**، كأن يكون في مرحلة الأعمال التحضيرية. هذا النوع من الدفاع عن النفس لم يتم الاتفاق على مشروعيته بعد[4]. مع ذلك

---

[1] المرجع السابق – Delerue, F –. ص471

المرجع السابق – Roscini, M. – Cyber Operations and the Use of Force – ص79

[2] المرجع السابق – Delerue, F –. ص470

[3] المرجع السابق – Roscini, M. – Cyber Operations and the Use of Force – ص71

[4] انظر البيان الختامي لقمة عدم الانحياز 2006 في هافان تعهد رؤساء دول حركة عدم الانحياز في إعلان هافانا إلى معارضة وإدانة ... اعتماد عقيدة الهجوم الاستباقي (pre-emptive)

Final Document - Disarmament and International Security. (2006, September), 1–68. [para. 22.5, p.11] Presented at the 14th Summit Conference of Heads of State or Government of the Non-Aligned Movement, Havana, Cuba. Retrieved from http://cns.miis.edu/nam/documents/Official_Document/14NAMSummit-Havana-Compiled.pdf

فهو يستخدم بشكل متكرر من قبل الدول[1]. المشكلة هي في تحديد ماهية التهديد الوشيك الذي يمكن الرد عليه بالدفاع عن النفس؟ حقيقة ليس هناك معيار دقيق يفصل بين ما هو وشيك وما هو غير وشيك، وإلى أن يتحدد ذلك بمعاهدة أو عرف دولي هناك عدة تفسيرات للتهديد الوشيك.

محكمة العدل الدولية في قضية نيكاراجوا وعلى غير عادتها صرحت بأنها لن تنظر في مشروعية الدفاع عن النفس ضد تهديد وشيك لتخرج هذا الأمر من نطاق حكمها[2]. لكن أيد هذه الفكرة "الفريق الرفيع المستوى للأمم المتحدة المعني بالتهديدات، والتحديات، والتغيير" الذي تقبَّل فكرة الدفاع الاستباقي في عام 2004 واشترط أن يكون التهديد وشيكاً يمكن إثبات قرب حدوثه، ليس مجرد احتمالية حدوثة في وقت ما في المستقبل:

"مع ذلك، فإن الدولة المهددة، وفقًا للقانون الدولي الراسخ، يمكنها القيام بعمل عسكري طالما التهديد بالهجوم وشيك، ولا توجد وسيلة أخرى لحرفه عن مساره، والإجراء المتخذ متناسب. تنشأ المشكلة عندما يكون التهديد المعني ليس وشيكًا ولكن لا يزال يُدعى أنه حقيقي"[3]

إذن السؤال المرتبط بشرعية هذا النوع من الدفاع عن النفس هو ما هو التهديد الوشيك؟ إدارة الرئيس الأمريكي باراك أوباما أعطت تعريفا دقيقا لمعنى تهديد وشيك (Imminent Threat). فقالت: إن التهديد الوشيك هو الذي سيحدث في ستين يوماً[4]. لكن هذا الرأي لا يصح الأخذ به؛ لأن تلك المدة وضعت لشأن داخلي مختلف تمامًا عن الهجوم المسلح في القانون الدولي. لكن يمكن القول إن المعيار المطلوب لقياس ما يعد وشيكا أو فوريا يجب أن يكون بتلك الدقة. فإذا كانت مدة الستين يوما قد تختلف في نطاق الدفاع عن النفس ضد التهديدات الوشيكة في النطاق الدولي فيجب أن يتم قياس المدة المعقولة عسكريا وسياسيا وقانونيا ليتبلور الوقت المعقول لما يعد هجوما وشيكاً.

لا بد من الإشارة إلى الاختبار الذي وضعه Daniel Bethlehem لقياس ما يعد وشيكاً والذي عد عنصر الفورية واحدًا من خمسة عناصر أخرى. فيرى Bethlehem أن للدولة الحق في الدفاع عن

---

[1] المرجع السابق – The International Court of Justice – Green, J. A. – ص97

[2] *Nicaragua* judgement, para. 35, p. 27

[3] United Nations, General Assembly, *UN High Level Panel on Threats, Challenges and Change in 2004*, A/59/565 (2 December 2004), para. 188, p. 54. available from https://undocs.org/A/59/565

[4] Garcia, M. J., & Elsea, J. K. (2014, September). *U.S. Military Action Against the Islamic State: Answers to Frequently Asked Legal Questions*, p. 16. Library of Congress - Congressional Research Service. Retrieved from https://digital.library.unt.edu/ark:/67531/metadc461904/

نفسها ضد هجوم مسلح وشيك إذا توفرت العناصر التالية: (أ) طبيعة وفورية التهديد، أي مدى كونه وشيكا (ب) مدى احتمالية وقوع هجوم، أي إمكانية التحقق منه وإثباته موضوعيًا (ج) مدى ما إذا كان الهجوم المتوقع جزءًا من نمط منسق من النشاط المسلح المستمر(د) النطاق المحتمل للهجوم والإصابة أو الخسارة أو الضرر المحتمل أن ينجم عنه في حالة عدم وجود إجراءات تتصدى له (هـ) واحتمالية وجود فرص لاتخاذ إجراءات أخرى فعالة للدفاع عن النفس والتي من المتوقع أن تسبب إصابات جانبية أقل خطورة أو خسارة أو ضرر.[1]

يجب الانتباه إلى أن اختبار Bethlehem كان للدفاع عن النفس الاستباقي ضد هجوم مسلح وشيك من فاعل غير حكومي. لذلك نجد في النقطة (ج) عد الهجوم المحتمل نمطًا منسقًآ من نشاط مسلح مستمر، يؤدي إلى استنتاج مفيد وموضوعي أن أولئك الذين يهددون أو يرتكبون مثل هذه الهجمات يعملون عملًا جماعيًا. هذه النقطة يمكن أن تستثنى من اختبار Bethlehem في الدفاع عن النفس ضد هجمات مسلحة وشيكة ودولية والاكتفاء ببقية المعايير الأربعة؛ لأنها لاتتعارض مع الطبيعة الدولية للهجوم المسلح.

تجدر الإشارة أن المدعي العام للمملكة المتحدة Jeremy Wright في خطابه الذي يوضح بعض وجهات نظر حكومة المملكة المتحدة بشأن قانون الدفاع عن النفس. ركز على معايير تقييم اقتراب هجوم مسلح التي وضعها Bethlehem وعدها "تلخيصًا مفيدًا للقانون الحديث في هذا المجال"[2].

في النطاق السيبراني أقر دليل (تالين) الحق في الدفاع عن النفس ضد تهديد سيبراني وشيك فتنص القاعدة 73 منه على انه:

"ينشأ الحق في استخدام القوة في الدفاع عن النفس أمام هجوم إلكتروني حال أو وشيك".

أجمع الخبراء في دليل (تالين) أنه لا تحتاج الدولة إلى الانتظار مكتوفة الأيدي في أثناء استعداد العدو للهجوم، وبدلاً من ذلك، يمكن للدولة أن تدافع عن نفسها بمجرد أن يصبح الهجوم المسلح "وشيكًا". واستخدم دليل (تالين) الحجة نفسها المستخدمة من قبل الفقهاء في الدفاع الاستباقي التقليدي لتبيان

---

[1] Bethlehem, D. (2012). Self-Defense Against an Imminent or Actual Armed Attack by Nonstate Actors. *American Journal of International Law*, *106*(4), 770–777 [para. 8, p. 6]. https://doi.org/10.5305/amerjintelaw.106.4.0769

[2] المرجع السابق – Cyber and International Law – Wright, J. (11 January 2017) *The Modern Law of Self-DefenceI* [Speech]. EJIL: Talk! Retrieved from https://www.ejiltalk.org/the-modern-law-of-self-defence/

مشروعية الدفاع الاستباقي عن هجوم سيبراني. فقال: إنه وإن كانت المادة 51 من الميثاق تشترط حصول الهجوم المسلح بالفعل لقيام مشروعية الرد علية بالدفاع عن النفس فإن الدفاع الاستباقي لا يتعارض مع القواعد العرفية التي أقرتها حادثة كارولاين التي تنص على أن الدفاع عن النفس يوجد حيثما وجدت "ضرورة ملحة لممارسة هذا الحق وألا تترك الظروف المحيطة للطرف المعني فرصة لاختيار الوسيلة التي يراها مناسبة، وألا يكون هناك وقت لإمكانية التشاور وتدبر الأمر". وبما أن المادة 51 تبدأ بالقول "لا شيء في هذا الميثاق يضعف أو ينتقص الحق الموروث في الدفاع عن النفس"، إذن فهي لا تغير شيئا في الدفاع عن النفس، بل تحفظه كما هو قبل نفاذها، أي كما ورد في العرف الدولي. وكما أسلفنا فالعرف الدولي البادئ من حادثة كارولاين لا يتعارض مع الدفاع الإستباقي[1].

اما عن تحديد ما هو الوشيك في النطاق السيبراني فقد انتقد دليل (تالين) المدرسة التي تربط الفعل الوشيك بالعنصر الزمني واستبدل العنصر الزمني بوصفه معيارًا للوشيك بعنصر آخر أسماه "الفرصة الأخيرة" "Last Feasible Window of Opportunity" وفيه يمكن للدولة أن تتصرف استباقيًا الدفاع عن النفس ضد هجوم مسلح إلكتروني عندما:1- يكون المهاجم ملتزمًا بوضوح بشن الهجوم المسلح .2- الدولة الضحية ستفقد فرصتها للدفاع عن نفسها فقدًا فعالًا ما لم تقم بذلك الفعل[2].

فالعنصر الأول يتطلب إثبات أن الدولة تعتزم القيام بالهجوم السيبراني اعتزامًا قطيعًا لا رجعة فيه. كأن تصرح أنها ستشن هجمات سيبرانية على دولة محددة أو حتى المعلومات الاستخباراتية التي تؤكد نية شن الهجمات، سواء كانت تلك النية في الوقت القريب أو البعيد. وفي العنصر الثاني يجب أن تثبت الدولة الطبيعة الخاصة للضرورة في الدفاع عن النفس الاستباقي بأن تثبت أن تحركها دفاع فعال عن النفس قبل وقوع العملية السيبرانية ضروري لو انتظرت حتى يتم الهجوم فعلا فأنها لن تستطيع الدفاع عن نفسها. ففرصتها الناجحة في الدفاع هي الآن قبل إطلاق الهجوم وإلا فأنها لن تتمكن من إيقافه لاحقا. ويؤكد الخبراء أنهم لا يلغون عنصر الزمن تماماً فيمكن أن يبقي مع معيار "الفرصة الأخيرة" مع ترجيحهم للأخير. ويتبين أن العنصر الأول موجود في اختبار Bethlehem الذي ذكر سابقًا،

[1] Tallinn Manual 2.0, commentary to rule 73, para. 2-3, p. 350-351
Murphy, S. D. (2005). The Doctrine of Preemptive Self-Defense. *Villanova Law Review, 50*(3), 699–748. Retrieved from https://digitalcommons.law.villanova.edu/vlr/vol50/iss3/9/
[2] Tallinn Manual 2.0, commentary to rule 73, para. 4, p. 351

تحديدا المعيار(ب) مدى احتمالية وقوع الهجوم. لكن الإضافة القيمة التي جاء بها اختبار الفرصة الأخيرة هي في العنصر الثاني.

يعطي دليل (تالين) مثالا يبين انطباق مشروعية الدفاع عن النفس الاستباقي وفقا لمعيار "الفرصة الأخيرة" جهاز المخابرات لدولة معينة يتلقى معلومات لا جدال فيها أن دولة أخرى تعد ضدها إطلاق عملية إلكترونية من شأنها تدمير خط أنابيب النفط الأساسي في غضون الأسبوعين المقبلين. تتضمن العملية التلاعب بالمتحكمات الدقيقة "Microcontroller" على طول خط الأنابيب لزيادة الضغط فيه؛ مما يؤدي إلى سلسلة من الانفجارات. بما أن جهاز مخابرات الدولة المستهدفة لا يوجد لديه معلومات عن الثغرة أو نقطة الضعف التي سيتم استغلالها للسيطرة، فلن تستطيع إقامة دفاع إلكتروني فعال على المتحكمات الدقيقة. ومع ذلك فإن جهاز مخابرات الدولة المستهدفة قد وفر معلومات عن مكان ووقت اجتماع أولئك المخططين للعملية. هنا يكون للدولة المستهدفة ما يكفي من الأسباب لاستنتاج أن هجومًا مسلحًا وشيكًا سيحدث، وأن استخدام القوة للدفاع عن نفسها أمر ضروري، والضربات ضد هؤلاء الأفراد سيكون متناسبًا قانونيًا[1].

إنه يجب تأكيد أهمية العنصر الزمني وأولويته، ففي هذا المثال الأخير لو لم تذكر عبارة "في غضون أسبوعين" لاختلف حكم شرعية الدفاع عن النفس، فلو كان الاجتماع التخطيطي المذكور في المثال يخطط لتنفيذ هجوم على أنابيب النفط بعد عقدين من التدريب، وجمع الاستخبارات هل سيكون مشروعا استهدافهم الآن باسم الدفاع عن النفس، أو أن البعد الزمني يسقط عنصر الضرورة حيث لا تترك الظروف المحيطة للطرف المعني فرصة للاختيار ولا يكون هناك وقت للتشاور وتدبر الأمر. ولذلك يجب تأكيد أن عنصر القرب الزمني للحدث لا يسقط ولا يتراجع في أهميته. الفريق الرفيع المستوى للأمم المتحدة حينما أقر إمكانية الدفاع عن النفس كان يعول كثيرا على الطبيعة الزمنية للتهديد الذي يجب أن يكون قريبا في الوقت.

الخلاصة في رأي الباحثة هي أن الدفاع الاستباقي عن النفس ضد هجوم مسلح وشيك ولم يبدأ بعد ليس مشروعا بعد ولا يعد من أسس القانون الدولي، وحتى يتم الاستقرار على معنى مقبول لمعنى "وشيك" سيظل الدفاع عن النفس الاستباقي مثارا لشبهة عدم القانونية. بيد انه يبدو أن الدول تتوجه نحو الأخذ به، لذلك فالأحرص هو التحقق من فورية الهجوم المسلح وفق اختبار Bethlehem بالإضافة

[1] Tallinn Manual 2.0, commentary to rule 73, para. 6, p. 352

إلى شرط أن الدولة الضحية ستفقد فرصتها الفعالة للدفاع عن نفسها ما لم تفعل تلك الأفعال (العنصر الثاني من اختبار النافذة الأخيرة). بهذه الطريقة يمكن على الأقل توفير بعض الضبط للمساحة التقديرية الواسعة للدول في تقرير ما يعتبر هجومًا مسلحًا جسيمًا. هذا مع تأكيد أهمية استمرار الجهود للتحديد الدقيق لما يعد "وشيكاً" من الناحية الزمنية.

ثانيا: الدفاع عن النفس ضد تهديد غير وشيك

تنسب هذه الصورة من الدفاع عن النفس إلى بوش الابن (Bush Doctrine)، وقد ظهرت بعد 2002 ومفادها أن الحق في الدفاع عن النفس يمكن أن يتحقق ضد تهديد وإن كان ذلك التهديد ليس قريبا أو ليس مكتملا بعد، لكنه يمكن ان يتكون في المستقبل[1]. بعبارة أخرى لا توجد أعمال تحضيرية أو استعدادات أو نية صريحة أو ضمنية لتنفيذ هجوم مسلح، لكن وفقا لتقدير دولة معينة يمكن أن ينتج وضع تهديدي في المستقبل إذا ترك الحال على ما هو عليه دون تدخل وأحدث مثال عليه هو ما جاء في خطاب الرئيس بوتين في الساعات الأولى من صباح اليوم الذي أعلن فيه عن تحرك عسكري ضد أوكرانيا؛ فإنه قضى الكثير من الوقت في شرح التهديد الذي يمثله توسع الناتو على روسيا ، ففي رأي الرئيس بوتين هذا التوسع ليس أقل من تهديد مستقبلي لوجود روسيا؛ لذلك استند على المادة 51 من الميثاق للقيام "بعملية عسكرية خاصة" . [2]

---

[1] Anghie, A. (2004). The Bush Administration Preemption Doctrine and the United Nations. *Proceedings of the 115th ASIL Annual Meeting, 98,* 326–331. https://doi.org/10.1017/s0272503700061565

الصائغ، محمد. (2009). أسانيد الولايات المتحدة بشأن الحرب الاستباقية. الرافدين للحقوق - جامعة الموصل كلية الحقوق، 11(40)، 229–282. استرجع من https://alaw.mosuljournals.com/pdf_160567_2a6b05cf1b8832033c63b55f687c42c3.html

[2] مثلا هذه بعض المقتطفات مما جاء في خطاب الرئيس الروسي: "بالنسبة للولايات المتحدة وحلفائها، هذه هي ما يسمى بسياسة احتواء روسيا، وهي مكاسب جيوسياسية واضحة. وبالنسبة لبلدنا، فهذه في النهاية مسألة حياة أو موت، وهي مسألة مستقبلنا التاريخي كشعب. وهذه ليست مبالغة: هذا صحيح. هذا تهديد حقيقي ليس فقط لمصالحنا، ولكن لوجود دولتنا وسيادتها. هذا هو الخط الأحمر الذي حذرنا منه مرارًا لقدر تم تجاوزه هنا ... أكرر، أفعالنا هي دفاع عن النفس ضد التهديدات التي تواجهنا ومن كارثة أكبر مما يحصل الآن.. وأدعو إلى التعاون من أجل طي هذه الصفحة المأساوية في أسرع وقت ممكن والمضي قدمًا معًا ... أنا أومن بذلك؛ في هذا مستقبلنا."

لمشاهدة أو قراءة الخطاب كاملا باللغة الإنجليزية:

Sky News. (2022, February 21). *In full: Russian President addresses the nation* [Video file]. Retrieved from https://www.de.com/watch?v=W57I2mzAr9c&feature=youtu.be

مثال ذلك في النطاق السيبراني أن تبني دولة لنفسها قوة سيبرانية هائلة تتفوق فيها على الدول الأخرى، ولا تكون هذه الدولة على وفاق مع دولة أخرى، هنا يمكن للأخيرة أن تضرب منشآت الأولى وأنظمتها السيبرانية حتى لا تسبب تهديدا لها في المستقبل. يكفي دون تفصيل لعناصر هذا الدفاع عن النفس أن نشير إلى عدم مشروعيته باتفاق غالبية فقهاء القانون، فهنا تنتفي كل عناصر مشروعية الدفاع عن النفس من ضرورة، وتناسب، وهجوم مسلح حال، أو وشيك. وهو موقف دليل (تالين) الذي أكد أن الدفاع عن النفس ضد تهديد سيبراني غير وشيك هو غير مشروع وعلى الدولة أن تلجأ إلى مجلس الأمن[1].

الفرع الرابع: الدفاع عن النفس ضد الهجمات السيبرانية الصادرة من الفاعلين غير الحكوميين Non-State Actor

الصورة التقليدية للدفاع عن النفس هو أن تدافع دولة عن نفسها ضد دولة أخرى، لكن ظهر تحدٍ جديد للعالم، وهو الجماعات المسلحة التي نقلت الصراعات من دولية إلى غير دولية. ثم أدت إلى التطورات العسكرية والتكنولوجية وإتاحتها للجهات الخاصة إلى زيادة القدرة التدميرية للجهات غير الحكومية. إن إدراك مدى الدمار الذي يمكن أن تكون عليه تصرفات هذه المجموعات أدى إلى تزايد الآراء المؤيدة لحق الدفاع عن النفس ضدهم[2] ويبدو أن القانون الدولي يتغير ليصبح أكثر تسامحا مع استخدام القوة ضد الجهات الفاعلة غير الحكومية.

The Print. (2022, February 24). Full text of Vladimir Putin's speech announcing 'special military operation' in Ukraine. Retrieved from https://theprint.in/world/full-text-of-vladimir-putins-speech-announcing-special-military-operation-in-ukraine/845714/

لقراءة قانونية في الخطاب انظر:

Milanovic, M. (2022, February 26). What is Russia's Legal Justification for Using Force against Ukraine? Retrieved from https://www.ejiltalk.org/what-is-russias-legal-justification-for-using-force-against-ukraine/

[1] Tallinn Manual 2.0, commentary to rule 73, para. 10, p. 353

[2] Bussolati, N. (2015). 6 The Rise of Non-State Actors in Cyberwarfare. In *Cyber War: Law and Ethics for Virtual Conflicts* (pp. 102–126) [p. 124-125]. Oxford, United Kingdom: Oxford University Press. https://doi.org/10.1093/acprof:oso/9780198717492.003.0007

انظر أيضا: المرجع السابق – Gray, C. – ص239

Crawford, J. (2012). *Brownlie's Principles of Public International Law* (8th ed.). Oxford, United Kingdom: Oxford University Press. https://doi.org/10.1093/he/9780199699698.001.0001

Trapp, K. N. (2007). Back to Basics: Necessity, Proportionality, and the Right of Self-Defence Against Non-State Terrorist Actors. *International and Comparative Law Quarterly*, *56*(1), 141–156. https://doi.org/10.1093/iclq/lei153

يتضح هذا التوجه بوضوح من قرارات مجلس الأمن التي توالت لتؤكد إمكانية استخدام القوة ضد الجماعات الإرهابية التي تهدد السلم والأمن.

فالقرار رقم (1373) (2001) ينص على "إيواء الإرهابيين كعمل يشكل انتهاكًا للقانون الدولي". الفكرة الأولية لاستخدام القوة المبررة ضد الجهات الفاعلة غير الحكومية هي أنه يمكن اتخاذ هذا الإجراء في الدولة التي قد تتواجد فيها الأخيرة، أي يجب اتخاذ الإجراء في أراضي الدولة التي تؤوي الجماعات المسلحة غير النظامية[1].

والقرار رقم 1368[2] (2001) الذي جاء في اليوم التالي لأحداث 11 أدان الهجمات الإرهابية ويهيب بالمجتمع الدولي أن يكافحها لكن الجزء الأهم هو أنه أكد الحق الطبيعي للدول للدفاع عن نفسها. فكان القرار مصمما ليدعم للولايات المتحدة في الدفاع عن النفس.

والقرار 1540 (2004) مؤداه أن تمتنع جميع الدول عن تقديم أي شكل من أشكال الدعم للأطراف من غير الدول التي تحاول تطوير أسلحة نووية أو كيميائية أو بيولوجية[3]. هذا وقد صدر 2325 (2016) ليؤكد ما جاء في القرار الأول ويحث الدول على الالتزام به.

والقرار رقم 2249 (2015) يتناول داعش ويدعو الدول الأعضاء إلى القيام بكل ما في وسعهم؛ لمضاعفة وتنسيق جهودهم؛ لمنع وقمع الأعمال الإرهابية التي يرتكبها داعش، وجبهة النصرة، وجميع الأفراد الآخرين، والجماعات والمؤسسات والكيانات المرتبطة بتنظيم القاعدة [4]. فبالرغم من أنه لم يذكر الدفاع عن النفس صراحة لكنه كان يبرر موقف مجلس الأمن في استخدام الدفاع عن النفس ضد الجهات غير الحكومية.

---

[8] Greenwood, C. (2003). International Law and the Pre-emptive Use of Force: Afghanistan, Al-Qaida, and Iraq. *San Diego International Law Journal*, *4*(7), 7–38. Retrieved from https://digital.sandiego.edu/ilj/vol4/iss1/3/

[1] قرار مجلس الأمن 1373، S/RES/1373 (28 سبتمبر 2001). استرجع من https://undocs.org/ar/S/RES/1373(2001)

[2] قرار مجلس الأمن 1368، S/RES/1368 (12 سبتمبر 2001). استرجع من https://undocs.org/ar/S/RES/1368(2001)

[3] قرار مجلس الأمن، قرار 1540، S/RES/1540 (28 أبريل 2004). استرجع من https://undocs.org/ar/S/RES/1540(2004)

[4] قرار مجلس الأمن، قرار 2249، S/RES/2249 (20 نوفمبر 2015). استرجع من https://undocs.org/ar/S/RES/2249(2015)

وإن كانت قرارات مجلس الأمن لا تؤسس لقاعدة قانونية من تلقاء نفسها فإنها تبين رغبة الدول في التصدي لظاهرة الجماعات المسلحة باستخدام القوة. والملاحظ أن رغبة بعض الدول[1] –أو بعبارة أدق ممارسة بعض الدول للدفاع عن النفس ضد الجماعات المسلحة[2]– يتصادم مع رأي محكمة العدل الدولية. ففي رأي محكمة العدل الدولية لا يمكن القيام بالدفاع عن النفس إلا ردًا على هجوم من قبل دولة أو مجموعات تتصرف نيابة عن دولة، فمحكمة العدل الدولية تركز على الرد على الدولة المسؤولة عن أعمال الجماعات غير الحكومية. بينما مسألة اتخاذ تدابير قسرية ضد جهات غير حكومية مستقلة لا يُعزى سلوكها بالضرورة إلى دولة معينة هو أمر لم تقر المحكمة بشرعيته. موقف محكمة العدل الدولية يتبدى في فتوى الجدار العازل حيث جاء فيه:

"المادة 51 من الميثاق تعترف بوجود متأصل –حق الدفاع عن النفس– في حالة هجوم مسلح من قبل دولة واحدة ضد دولة أخرى. إلا أن إسرائيل لا تدعي أن الهجمات ضدها تُنسب إلى دولة أجنبية. لأن إسرائيل تمارس سيطرتها على الأراضي الفلسطينية المحتلة... فالتهديد الذي يسوِّغ بناء الجدار ينشأ من الداخل وليس من خارج هذه الأرض. ومن ثم فإن الوضع يختلف عن الوضع المتوخى في قراري المجلس 1368 1373، وبالتالي لم تستطع إسرائيل بأي حال من الأحوال الاحتجاج بهذه القرارات في دعم مطالبتها بممارسة حق الدفاع عن النفس. ولذلك خلصت المحكمة إلى أن المادة 51 من ميثاقها لا صلة له بالموضوع في هذه الحالة."

كذلك من أهم ما يُستَنَد إليه عند تسويغ مشروعية الدفاع عن النفس ضد الفاعلين غير الحكوميين هو أن المادة 51 تدور حول دولة الضحية وليس المهاجم. فهي تشرع حق الدفاع عن النفس ضد أي هجوم مسلح "إذا اعتدت قوة مسلحة" بغض النظر عما إذا كان من ارتكاب دولة أو غير دولة. هنا

---

[1] انظر مواقف الدول في الاجتماع غير الرسمي الذي عقدته المكسيك لأعضاء مجلس الأمن في موضوع "الالتزام بنظام الأمن الجماعي لميثاق الأمم المتحدة: استخدام القوة في القانون الدولي والجهات الفاعلة غير التابعة للدول، والدفاع المشروع عن النفس" الأمم المتحدة، الجمعية العامة ومجلس الأمن، رسالة مؤرخة 8 آذار/مارس موجهة إلى رئيسة مجلس الأمن من الممثل الدائم للمكسيك لدى الأمم المتحدة، A/75/766-S/2021/161 (16 مارس 2021). استرجع من https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/066/44/PDF/N2106644.pdf?OpenElement

انظر أيضا:

Haque, A. A. (2021, March 24). Self-Defense Against Non-State Actors: All Over the Map. Retrieved from https://www.justsecurity.org/75487/self-defense-against-non-state-actors-all-over-the-map/

[2] انظر بعض استخدامات الدول للدفاع عن النفس ضد الفاعلين الغير حكوميين:

Lubell, N. (2010). *Extraterritorial Use of Force Against Non-State Actors (Oxford Monographs in International Law)* (1st ed.), p. 29-30. Oxford, United Kingdom: Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199584840.001.0001

تتبين بوضوح إرادة واضعي النص بعدم استبعاد الحالات التي تم فيها تنفيذ الهجوم المسلح من قبل الجهات الفاعلة من غير الدولة. وهذا الإطلاق المتعمد هو السبب الرئيس الذي يعطي الدولة التي تعرضت لهجوم مسلح الرد بالدفاع عن النفس بغض النظر عن هوية المهاجم[1].

ونجد رأي القاضية هيغينز في قضية الجدار مؤيدًا هذا الاتجاه، وضد توجه المحكمة، فقد رأت أن المادة 51 من الميثاق لا تمنع الدفاع عن النفس ضد الجماعات غير الحكومية، وأن القيود التي يتم فرضها ليست من نص الميثاق، ولكن من رأي المحكمة السابق في قضية نيكاراغوا، وهي تعد حكم نيكاراغوا قراءة معيبة لما جاء في قرار مجلس الأمن 3314[2] والنتيجة هي أن الحق في الدفاع عن النفس في هذه الحالة يجب أن يشرع ضد الجماعات المسلحة.[3]

كذلك حينما كررت المحكمة موقفها[4] في قضية الأنشطة المسلحة (جمهورية الكونغو الديموقراطية ضد أوغندا) كان للقاضي Kooijmans (وهو من هيئة القضاة في هذه القضية) رأي مخالف لنهج

---

[1] Singh, V. (n.d.). The Existence of Right to Self-Defense Against The Non-State Actors. Retrieved from https://www.legalserviceindia.com/legal/article-2992-the-existence-of-right-to-self-defense-against-the-non-state-actors.html

[2] تنص المادة 3 الفقرة (ز) من القرار 3314 على أن: "ارسال عصابات الجماعات المسلحة أو قوات غير نظامية أو مرتزقة من قبل دولة ما أو باسمها تقوم ضد دولة أخرى بأعمال من اعمال القوة المسلحة تكون من الخطورة بحيث تعادل الأعمال المحددة أعلاه. أو اشتراك الدولة بعمل ملموس في ذلك"

General Assembly resolution 3314 (XXIX), Definition of Aggression, 14 December 1974, Article 3(g). Retrieved from http://hrlibrary.umn.edu/instree/GAres3314.html

[3] *Construction of a Wall* advisory opinion, Separate opinion of Judge Higgins, para. 33, p. 215

[4] حيث جاء في حكم المحكمة في قضية في قضية جمهورية الكونغو الديموقراطية ضد أوغندا الآتي: "وتجدر الإشارة كذلك إلى أنه بينما زعمت أوغندا أنها تصرفت دفاعًا عن النفس، فإنها لم تدَّع أبدًا أنها تعرضت إلى هجوم مسلح من قبل القوات المسلحة لجمهورية الكونغو الديمقراطية. إن الهجمات المسلحة التي تمت الإشارة إليها جاءت بالأحرى من تحالف القوى الديمقراطية. ...لا يوجد دليل مرضٍ على تورط حكومة جمهورية الكونغو الديمقراطية في هذه.... ولم تكن ممارسة أوغندا لحق الدفاع عن النفس ضد جمهورية الكونغو الديمقراطية حاضرة. وبناءً على ذلك، لا حاجة للمحكمة للرد على ادعاءات الأطراف فيما يتعلق بنص القانون الدولي المعاصر على حق الدفاع عن النفس -وتحت أي ظروف- ضد الهجمات واسعة النطاق من قبل القوات غير النظامية".

Armed Activities judgement, para. 146-147, pp. 222-223

يتبين أن المحكمة كانت مهتمة في المقام الأول بإمكان أن تنسب الهجمات المسلحة إلى جمهورية الكونغو الديمقراطية ولما كانت الإجابة -التي تم التوصل إليها- سلبية، أسقطت المحكمة إمكانية التحقيق في ادعاء الدفاع عن النفس ضد الجهات الفاعلة غير الحكومية. في الواقع، فإن الجملة النهائية في الاقتباس أعلاه تشير إلى أن المحكمة ترى أنها لم تجب على السؤال. مما عده بعضهم البعض ان هناك تراجعًا طفيفًا عن موقف المحكمة في فتوى الجدار، وأن السؤال لا يزال مفتوحا للنقاش لأنه لو شعرت المحكمة أن القضية قد تم تناولها تناوُلًا مُرضيًا في فتوى الجدار، لكانت ستكرر موقفها المعلن في وقت سابق. مع ذلك يمكن تفسير الأمر بأن المحكمة ترى أنها قد قالت كلمتها في الدفاع عن النفس ضد الجماعات المسلحة فلا داعي لتكرار الأمر. انظر الرأيين:
Lubell, N. – المرجع السابق – ص33

المحكمة فقد ذهب إلى أنه من غير المعقول إنكار حق الدولة التي تعرضت للهجوم في الدفاع عن النفس لمجرد عدم وجود دولة مهاجمة والميثاق لا يتطلب ذلك[1].

موضوع استخدام القوة ضد أفعال الجماعات المسلحة ينقسم إلى قسمين رئيسين. القسم الأول منهما هو الدفاع عن النفس ضد الهجمات الصادرة من جماعات غير حكومية تدعمها دولة. والقسم الثاني الدفاع عن النفس ضد الهجمات الصادرة من جماعات غير حكومية مستقلة ولا ترعاها دولة. سيتم التطرق لكل نوع مع إمكانية انطباقه في مجال الهجمات السيبرانية.

أولا: الرد بالدفاع عن النفس ضد هجمات الجماعات غير الحكومية التي ترعاها دولة

لا خلاف على الحق في الدفاع عن النفس ضد أفعال الجماعات التي تدعمها دولة أخرى؛ وذلك لأن أفعال الجماعات غير الحكومية بمقتضى القانون لن تعد صادرة من تلك الجماعات، بل تعد صادرة من الدولة الراعية نفسها. أكدت محكمة العدل الدولية هذا المبدأ في عدد من القضايا أولها وأهمها في حكم نيكاراغوا، فقد ذكرت المحكمة ما يلي:

"يجب أن يُفهم أن الهجوم المسلح يشمل ليس مجرد عمل من قبل القوات النظامية عبر حدود دولية، ولكن أيضًا "المرسلة بوساطة أو نيابة عن دولة من العصابات، أو الجماعات المسلحة، أو غير النظاميين أو المرتزقة، الذين يقومون بأعمال القوة المسلحة ضد دولة أخرى بهذه الدرجة من الخطورة يصل إلى مستوى –في جملة أمور– هجوم مسلح فعلي"[2]

لكن تكمن الصعوبة في إثبات تلك الصلة بين الجماعات المسلحة والدولة الراعية، وفي ذلك عيَّنت محكمة العدل الدولية في قضية نيكاراجوا معياري **الرقابة الصارمة** و**الرقابة الفعالة**. وبالتالي فإن الدفاع عن النفس ضد جماعات غير حكومية وفقا لمحكمة العدل الدولية يجب أن يمر بمرحلتين: أولاهما: التحقق من متطلبات الدفاع عن النفس من ضرورة وتناسب وهجوم مسلح. المرحلة الثانية نسبة الهجوم المسلح الذي قامت به الجماعة غير الحكومية إلى دولة. ثم يأتي الحق في الدفاع عن النفس ضد تلك الدولة. وقد تمت معالجة عناصر شرعية الدفاع عن النفس سابقا في هذا المبحث لذلك سيتم هنا

[1] *Armed Activities* judgement (merits), separate opinion of Judge Kooijmans, para. 29-30, p. 314
[2] *Nicaragua* judgment, para. 195, p. 103

معالجة نسبة أفعال الجماعات المسلحة إلى الدولة تأهيلا لاستخدام الدفاع الشرعي عن النفس. وبالرغم من أن نسبة الفعل غير المشروع إلى الدولة يدخل في المسؤولية الدولية التي سيتم تناولها في الفصل الثالث فإنه أيضا جزء مهم من الدفاع الشرعي عن النفس ضد الفاعلين غير الحكوميين.

في قضية نيكاراجوا كانت أفعال الجماعات المسلحة من غير الدول محل دراسة في القضية، لكن ليس للدفاع الشرعي عن النفس ضد تلك الأفعال بقدر ما هي دراسة تحديد المسؤول عن أفعال تلك الجماعات. فقد ميزت المحكمة بين فئتين من الأفراد لا يتمتعون بوضع الهيئات القانونية للدولة، ولكنهم مع ذلك يتصرفون نيابة عن تلك الدولة، أولى الفئتين: أولئك الذين يعتمدون كليًا على دولة أجنبية ليس فقط من ناحية التمويل والتجهيز فحسب، بل يكون عملهم وفقًا لـ "تخطيط وتوجيه" أجهزة تلك الدولة (وكانوا UCLAS[1] في هذه القضية) أما الفئة الأخرى: فهم الأشخاص –الذين على الرغم من أن تمويلهم وتجهيزهم من قبل دولة أجنبية– فإنهم احتفظوا مع ذلك بدرجة من الاستقلال عن الدولة (كانوا متمردي نيكاراغوا، أو الكونترا)[2].

إذا انطبقت الحالة الأولى فإنه يتحقق معيار الرقابة الصارمة الذي يهدف إلى إثبات ان الفاعل غير الحكومي هو "بحكم الواقع" أحد أجهزة الدولة فهو يهدف إلى نسبة الفاعل غير الحكومي –وبالتالي كل الأفعال التي قام بها– إلى الدولة الراعية. أما إذا تحققت الحالة الثانية، فنكون أمام معيار الرقابة الفعالة الذي يهدف إلى نسبة السلوك محل النقاش –وليس الفاعل غير الحكومي– إلى الدولة الراعية[3].

في اختبار **الرقابة الصارمة** Strict Control ينسب تصرف الفاعل غير الحكومي إلى الدولة إذا كان هذا الفاعل يتصرف معتمدا اعتمادًا كاملًا في وجوده وتحركاته على الدولة، فهو في نهاية المطاف مجرد أداة بيد الدولة[4]؛ لذلك يفهم على أنه جهاز تابع للدولة حتى وإن لم يكن مؤهلًا لذلك بموجب القانون الداخلي للدولة لأن كل تصرفات هذا الجهاز "بحكم الواقع" تنسب إلى الدولة، حتى لو كان ذلك بمنزلة أفعال متجاوزة لحدود السلطة[5].

---

(1) اختصار لعبارة "أصول لاتينية خاضعة للسيطرة أحادية الجانب" (Unilaterally Controlled Latino Assets) : أشخاص من دول متنوعة من أمريكا اللاتينية يُدفَع لهم، ويتصرفون بناءً على تعليمات مباشرة، من أفراد الجيش أو المخابرات الأمريكية.

[2] Cassese, A. (2007). The Nicaragua and Tadic Tests Revisited in Light of the ICJ Judgment on Genocide in Bosnia. *European Journal of International Law*, *18*(4), 649–668 [p. 652]. https://doi.org/10.1093/ejil/chm034

[3] المرجع السابق – Delerue, F.– ص130-131

[4] *Nicaragua* judgement, paras. 109–110, p. 62; *Genocide* judgment, para. 392, p. 205

[5] المرجع السابق – Delerue, F.– ص129

وإثبات تلك العلاقة في حرص إنكار الدول إياها يتسم بالصعوبة، لذلك لم تستطع المحكمة الاستناد إليه في قضية نيكاراجوا[1]. لكن ما يمكن أن يعد تطبيقا أساسيا لاختبار الرقابة الصارمة هو قضية رهائن طهران، فقد قررت محكمة العدل الدولية أن الحكومة الإيرانية مسئولة عن الاستيلاء على السفارة الأمريكية، واحتجازها أفرادًا من قبل المسلحين؛ لأن الحكومة الإيرانية شجعت على هذه الأفعال ووافقت عليها في بيانات مختلفة[2] .فالأشخاص على الرغم من عدم تمتعهم بالوضع القانوني لأجهزة الدولة، في فعل الواقع تحت هذه السيطرة الصارمة من قبل الدولة، يعد أمرًا واقعًا من قبل الدولة لأن الأشخاص وسلوكهم يُنسب إلى الدولة[3].

اما اختبار **السيطرة الفعالة** Effective Control فيتم اللجوء إليه إذا تعذر إثبات الصلة بمقتضى اختبار الرقابة الصارمة[4] فهو يستخدم عندما لا يعد الفاعلين الدوليين –من غير الدولة بحكم الواقع– من أجهزة الدولة، بل عندما تتمتع تلك الجماعات بشيء من الاستقلال عن الدولة الراعية، لكن هناك صلة بين تلك الجماعات والدولة. وهناك ثلاثة معايير لإثبات تلك الصلة إذا وجد أحدها يغني عن الاثنين الآخرين وهم وجود 1–التعليمات 2– أو التوجيه 3– أو درجة من التحكم (Instructions, Direction or Control)[5] من قبل الدولة على الجماعات المسلحة لعد تلك الجماعات متصرفة نيابة عن الدولة. وفي ذلك قضت محكمة العدل الدولية:

أنه من أجل المشاركة في المسؤولية القانونية للولايات المتحدة:

"يجب من حيث المبدأ إثبات أن تلك الدولة لديها سيطرة فعلية على العمليات العسكرية أو شبه العسكرية [المعنية]"[6].

يتبين –مما سبق– أن المطلوب هو درجة عامة من السيطرة، وليس مجرد اعتماد المجموعة على الدولة، فهذا غير كافٍ، فمن الضروري إثبات وجود رقابة فعالة على كل فعل محدد معني في القضية

---

[1] المرجع السابق – ص118

[2] Tehran hostage *judgement*, para. 74, p. 35

[3] المرجع السابق – Delerue, F.– ص119

[4] Milanovic, M. (2006). State Responsibility for Genocide. *European Journal of International Law*, *17*(3), 553–604 [p. 577]. https://doi.org/10.1093/ejil/chl019

[5] نجد أن إختبار الرقابة الفعالة يحاكي المادة 8 من المواد المتعلقة بمسؤولية الدولة: "يعد فعلا صادرا عن لدولة بمقتضى القانون الدولي تصرف شخص أو مجموعة أشخاص إذا كان الشخص أو مجموعة الأشخاص يتصرفون في الواقع بناء على تعليمات تلك الدولة، أو بتوجيهات منها، أو تحت رقابتها لدى القيام بذلك التصرف."
بينما اختبار الرقابة الصارمة يحاكي المادة 4 من قواعد مسؤولية الدولة

[6] *Nicaragua* judgement, para. 115, p. 64

قيد المناقشة. بمعنى إذا كانت القضية دفاعًا عن النفس ضد الدولة الراعية –وفقا للسيطرة الفعالة بسبب هجمات قامت بها مجموعة مسلحة– فلابد من إثبات وجود تعليمات، أو توجيه أو درجة من السيطرة من الدولة الراعية على تلك المجموعة في أثناء تنفيذها تلك الهجمات موضوع الرد بالدفاع عن النفس.

تجدر الإشارة إلى أن كلا الاختبارين يتعرضان للنقد المستمر من الفقه لصعوبة تحققهما وإثباتهما، نذكر من ذلك قاضي محكمة العدل الدولية جينينغز في قضية نيكاراغوا التي تقرر فيها كلا المعيارين، فإنه كان يرى الأخذ بوجود علاقة بين الدولة والجماعات في المواقف التي تجعل فيها الدولة أراضيها –قصدا وعن طيب خاطر– متاحة للجهات الفاعلة غير الحكومية؛ لتنفيذ الهجوم الفعلي؛ بهدف تسهيل الهجوم، أو يقدم الدعم اللوجستي أو الملاذ الآمن[1]. كذلك القاضي عون الخصاونة قاضي محكمة العدل الدولية في قضية الإبادة الجماعية في البوسنة الذي ذيل الحكم برأي قال فيه:

"المتطلب العالي للسيطرة الفعالة –من قبل الدولة على الجماعات الإرهابية، خصوصًا في الحالات التي يكون فيها هدف مشترك بين الدولة والجماعات الفاعلة من غير الدول– هو أمر يعطي الدول القدرة على القيام بأعمال إجرامية من دون تحمل المسؤولية المباشرة عن هذه الأعمال"[2]

– الدفاع عن النفس ضد الهجمات السيبرانية التي تقوم بها جماعات غير حكومية برعاية دولة:

في النطاق السيبراني يمثل التعامل مع الجهات الفاعلة غير الحكومية في الفضاء السيبراني تحديًا للدول عامةً لكن الخطورة الأكبر هي من تلك الهجمات التي تدعمها الدول؛ وذلك لأن غالبية الهجمات الإلكترونية في العالم يتم إطلاقها من قبل جهات فاعلة غير حكومية –على وجه الخصوص مجرمون يبحثون عن المال– تكون هجمات غير متطورة ولها عواقب مجتمعيه قليلة نسبيا[3]. ولكن الجهات الفاعلة المدعومة حكومياً يكون تهديدها الإلكتروني أكبر، فالدول وحدها قادرة على تقديم الأموال

[1] *Nicaragua* judgement, separate opinion of Judge Sir Robert Jennings, p.543-544
[2] *Bosnia genocide* judgement, dissenting opinion of Vice-President Al-Khasawneh, para. 39, p. 256
[3] Meer, S. (2020, June). *How states could respond to non-state cyber-attackers (Policy Report)*. Netherlands Institute of International Relations Clingendael, p. 1. Retrieved from https://www.clingendael.org/sites/default/files/2020-06/Policy_Brief_Cyber_non-state_June_2020.pdf

اللازمة للاستثمار في الهجمات السيبرانية على نطاق واسع وطويل الأجل؛ لإحداث ضرر فعلي واسع النطاق يلحق بالمجتمعات[1].

الهوية المجهولة للفاعل هي إحدى الميزات التي تغري الدول للجوء إلى الهجمات الإلكترونية؛ ذلك أن طلب العمليات الإلكترونية من الجهات الفاعلة غير الحكومية فيه إخفاء أفضل للهوية، وتحايل أكبر على الإسناد التقني، وبالتالي يمكن رفض الاتهامات بالمسؤولية عن الهجمات بسهولة أكبر. فمما يبعد شبهة المسؤولية عن الهجمات الإلكترونية عن الدولة هو أن توظيف تلك الجماعات يتم من غير ممثلي الدولة، فإذا كان تعقب الهجوم الإلكتروني ممكنًا على الإطلاق، وتم الوصول إلى الجهات الفاعلة غير الحكومية، فإنه بإمكان مسؤولي الدولة الإنكار بمعرفة أي شيء يخص الهجمات السيبرانية؛ مما يجعل الأمر أكثر صعوبة على الدول الضحايا؛ لاتخاذ الإجراءات المضادة. لذلك في السنوات القليلة الماضية تم إيلاء المزيد من الاهتمام لهذا النوع الهجين من الفاعل في الفضاء السيبراني المتمثل: الدول التي تستخدم الجهات الفاعلة غير الحكومية في العمليات السيبرانية ضد الدول الأخرى[2].

إن التمييز بين العمليات السيبرانية التي ترعاها الدولة والجرائم السيبرانية الفردية أمر أشبه بالمستحيل –عمليًا في الوقت الحاضر– في ظل المعيارين المذكورين أعلاه. ففي كثير من الحالات يكون الجاني على علاقة مؤكدة بالدولة، لكن بسبب عدم وجود قطعية في الإسناد التقني يجعل من المستحيل تقريبًا إثبات تلك العلاقة بوضوح. على سبيل المثال شاركت شبكة الأعمال الروسية (RBN) –وهي فاعل غير حكومي– في العمليات السيبرانية التي استهدفت جورجيا قبل التدخل العسكري الروسي في عام 2008[3] وفي أثنائه. لكن العتبة العالية التي حددتها محكمة العدل الدولية في معياري السيطرة الصارمة أو الفعالة مقيدة للغاية خصوصا في الظروف السيبرانية. فكل ما يلزم الدولة المتوارية خلف الاعتداء هو الإنكار بوجود علاقة بينها وبين مرتكبي الهجمات السيبرانية، وهذا ما قامت به روسيا في هجماتها على إستونيا وجورجيا ليصبح عبء إثبات تلك العلاقة على كاهل الدولة الضحية، وهو أمر غاية في الصعوبة[4]. لذلك من غير المتوقع أن يعتمد على الدفاع عن النفس للرد على الهجمات السيبرانية حتى تعتمد معايير تنسيب أكثر مراعاة للطبيعة السيبرانية.

---

[1] المرجع السابق
[2] المرجع السابق
[3] المرجع السابق – Delerue, F. – ص122
[4] المرجع السابق

مع ذلك فقد أقر دليل (تالين) بحق الدفاع الشرعي ضد الأفعال الصادرة من جماعات غير حكومية ترعاها الدولة، لأنه ممكن من الناحية النظرية، فلقد نص هذا الدليل على أنه إذا كانت مجموعة من الأفراد تقوم بعمليات من خلال الانترنت نيابة عن دولة موجهة ضد دولة أخرى، وتصل هذه العمليات إلى مستوى التأثيرات الطلوبة، تعد الدولة الأولى مرتكبةً هجوما مسلحاً. هذا الاستنتاج نفسه ينطبق على العمليات الإلكترونية التي يقوم بها مجموعات أو حتى فرد واحد يعمل نيابة عن الدولة[1].

فيمكن تصور انطباق معيار الرقابة الصارمة في الحالة التي تبدي فيها الدولة اهتماما بالمجموعات السيبرانية التي تعمل في الظل وتستخدمها وهو أمر غير مستبعد نظرا لتزايد اهتمام أجهزة الدولة بتطوير الجيش من ناحية الفضاء الإلكتروني، فهؤلاء يصبحون –بحكم الواقع– أحد أجهزة الدولة. هذا ما يشابه الوضع القانوني لحراس الثورة في جمهورية إيران الإسلامية: فقد كانوا في البداية مجموعة من الأفراد، والتي أصبحت بحكم الواقع وبالتالي بحكم القانون عضوًا في الحكومة الجديدة بعد الثورة[2].

ويمكن انطباق معيار السيطرة الفعالة في الحالات التي تكون فيها الدولة هي المسؤولة عن تحديد استراتيجية تنفيذ الهجمة السيبرانية أو كان للدولة أهمية جوهرية في تنفيذ العملية السيبرانية، أي أن تكون هناك مؤشرات تدل على القدرة على إصدار الأوامر لبدء الهجوم السيبراني وإيقافه[3].

لكن لا يمكن أن يعد تواطئ الدولة مع تلك المجموعات أمرا ينسب أفعال تلك المجموعات إلى الدولة من أمثلة التواطئ في النطاق السيبراني عرض "ملجأ افتراضي" للمجموعة، كأن تسمح الدولة باستخدام الخوادم الموجودة داخل أراضيها أو استخدام نظم المعلومات والاتصالات الخاصة، بها لشن هجمات على دولة أخرى[4]. فمجرد تقديم الدعم اللوجستي أو أن تجعل أرضها ملاذا آمنا لا يصل إلى مستوى السيطرة الفعالة التي تتطلب تعليمات، أو توجيه، أو تحكم. هذه فعلا ثغرة قانونية فدعم المجموعات – إلى حد معين– ينفي صلة الدولة بها وبالتالي مسؤوليتها عن أفعال تلك الجماعات. ويمكن للدول أن تستغل تلك المنطقة التي لا يوجد فيها تجريم، وتقدم الدعم المالي الوفير أو الأجهزة دون أن تتدخل أو تفرض سيطرتها على خطط تلك الجماعات وتكتفي بالهدف المشترك.

---

[1] Tallinn Manual 2.0, commentary to rule 71, paras. 16-17, p. 344

[2] المرجع السابق – Delerue, F. – ص122

[3] Tallinn Manual 2.0, commentary to rule 17, paras. 6-7, pp. 96-97

[4] Bussolati, N. – المرجع السابق – ص124

ولا بد من الإشارة إلى أن هذين الاختبارين غير قادرين على استيعاب المعركة ضد تهديدات الجهات الفاعلة غير الحكومية خصوصاً في المجال السيبراني[1]. فالنظرة الاستشرافية إلى مستقبل التهديدات السيبرانية الناشئة من غير الدول، وبرعاية الدول تتطلب مراعاة الطبيعة السيبرانية في قضايا التنسيب والإثبات عامةً. فإذا كان يصعب الوصول إلى علاقة بين المجموعات المسلحة والدول في المجال في الوضع التقليدي الذي يمكن فيه فحص الأسلحة وتتبع التمويل فيكف بالطبيعة السيبرانية مع الهوية المجهولة وصعوبة التتبع لذلك لابد أن تعطي محكمة العدل الدولية مراعاة واقعية خاصة بالطبيعة السيبرانية بما يمكن تطبيقه بشكل معقول على الهجمات السيبرانية. وسيتم التطرق إلى التنسيب والإثبات لاحقا في الفصل الثالث من هذا البحث.

ثانيا: الدفاع عن النفس ضد الهجمات السيبرانية الصادرة من جماعات غير حكومية مستقلة ولا ترعاها الدولة

من الصعب الحديث عن الدفاع عن النفس ضد أفعال الجماعات غير الحكومية المستقلة في النطاق السيبراني، وذلك –أصلًا– لعدم وجود رأي راجح وواضح في الوضع التقليدي يؤكد شرعية مثل هذا السلوك. هناك عدم توافق –إن جاز التعبير– بين الميثاق والعرف من جهة ومحكمة العدل الدولية من جهة أخرى. ولقد تمت مناقشة أراء محكمة العدل المترددة في تشريع الدفاع عن النفس ضد فاعل غير حكومي مستقل. بينما على العكس من ذلك لا تتضمن المادة 51 من الميثاق أي إشارة إلى الفاعل المحتمل فلم تذكر سوى عنصر الهجوم المسلح، فكأنها تسمح بالدفاع عن النفس ضد أي هجوم مسلح بغض النظر عن منشئه دولة أو جماعة غير دولية[2]. كذلك فإن بعضهم يؤكد أن القانون الدولي العرفي في حادثة كارولاين الشهيرة كانت دفاعًا عن النفس ضد جماعات غير حكومية غير مدعومين من حكومة الولايات المتحدة ولا تعد مسؤولة عن تصرفاتهم، ومع ذلك فإن اختبار الضرورة والتناسب لصحة الدفاع عن النفس لم يتطلب في صيغته أن تدعم تلك الجماعات دولة؛ حتى يمكن ممارسة حق الدفاع عن النفس ضد الدولة[3].

---

[1] المرجع السابق – ص125

[2] Burra, S. (2018). Use of Force as Self Defence against Non-State Actors and TWAIL Considerations: A Critical Analysis of India's State Practice. *Asian Yearbook of International Law, 24*, 106–127 [p. 107]. Retrieved from https://www.jstor.org/stable/10.1163/j.ctv1sr6j7f.9

[3] المرجع السابق – Greenwood, C.

أحداث 11 سبتمبر كان لها أثر قوي في تشجيع توجيه السلوك الدولي، ومعه فقه القانون الدولي نحو تأييد مسألة أن الهجمات المسلحة القابلة للرد عليها بالدفاع عن النفس يمكن أن تنشأ من فاعلين غير حكوميين مستقلين. وذلك عندما ردت الولايات المتحدة عسكريا على أساس حق الدفاع عن النفس ضد تنظيم القاعدة الذي ينطلق منه الهجوم متهمةً نظام طالبان بالتسامح والإيواء. وجاءت قرارات مجلس الأمن الدولي 1368 (2001) و1373 (2001). لتأييد العملية العسكرية الأمريكية والاعتراف بحق الولايات المتحدة في التصرف دفاعًا عن النفس بما يتفق مع المادة 51 من ميثاق الأمم المتحدة[1].

ومما زاد من الاهتمام بهذا التوجه هو ظهور تنظيم الدولة الإسلامية "داعش"، والتحالف الدولي للقضاء عليه، فصحيح أن العمليات التي قام بها التحالف ضد التنظيم في العراق كانت وفق الدفاع الجماعي عن النفس؛ فقد طلبت الحكومية العراقية صراحةً المساعدة في الدفاع عن النفس ضد التنظيم[2]. لكن اختلف الأساس القانوني في عمليات التحالف في سوريا، حيث تم الاهتمام بمذهب "**الدولة غير القادرة أو غير الراغبة**" الذي يرى أنه يمكن للدول أن تستخدم القوة ضد الجماعات الإرهابية وإن كانت منفصلة، ولا ترعاها دولة الإقليم، وذلك إذا ثبت أن دولة الإقليم غير قادرة أو غير راغبة على التصدي لهذه الجماعات.

مذهب أو عقيدة الدولة غير القادرة أو غير الراغبة يبدأ بتذكير الدول بواجبها القانوني في منع استخدام إقليمها أو الإقليم الذي تسيطر عليه أن يكون منطلقاً لإيذاء الدول الأخرى (قاعدة بذل العناية). وعليه فعلى الدولة التي يوجد على أرضها فاعلون غير حكوميين اتخاذ كل الإجراءات المعقولة لقمع الهجمات التي تصدر على إقليمها. ومن أمثلة هذه الإجراءات. ما إذا كانت الدولة تجرم ارتكاب هجمات مسلحة، وما إذا كانت الدولة تجري تحقيقات مفصلة في مثل تلك الهجمات. وما إذا كانت الدولة تعتقل مرتكبي تلك الهجمات أو تحاكمهم أو تسلمهم امتثالًا لقرارات مجلس الأمن إن وجدت. فإن لم تكن تلك الإجراءات كافية في قمع أذى تلك الجماعات فعلى الدولة غير القادرة أن تقبل المساعدة من الدولة الضحية أو أي مساعدة دولية أخرى، فإذا فشلت في قبول المساعدة تتحول إلى دولة غير راغبة، ولأنها

[1] المرجع السابق – ص122

[2] Sendut, J. H. (2022, August 22). The Unwilling and Unable Doctrine and Syria. Retrieved from https://www.culs.org.uk/per-incuriam/the-unwilling-and-unable-doctrine-and-syria

غير راغبة في تنفيذ التزامها ببذل العناية فإنه يصبح مشروعا للدول الضحية استخدام الدفاع عن النفس ضد الجماعات المسلحة على اقليمها بالقدر المتناسب والضروري[1].

وبالرغم من أن هذه الممارسة الدولية آخذة منحى متكررًا فإنها ليست قاعدة قانونية، فيجب تذكر أن محكمة العدل الدولية حكمت في قضيتين بعد 11 سبتمبر، وهما فتوى الجدار وقضية الكونغو ضد أوغندا، وهي لا تزال مترددة في توسيع مفهوم الهجوم المسلح ليشمل أفعال الجهات الفاعلة غير الحكومية التي لا تتصرف بناءً تعليمات أو توجيه أو رقابة دولة معينة. لذلك ليس هناك قاعدة ثابته يقاس عليها الامر في الفضاء السيبراني، فإلى اليوم وفقا لقواعد القانون الدولي الراسخة هذا التصرف غير قانوني. ولا يوجد ما يكفي من الممارسة المتكررة للإقرار بشرعيته.

ومع ذلك فإن دليل (تالين) أقر بوجود حق للدول لممارسة الدفاع عن النفس ضد الجماعات غير الحكومية المستقلة دون التطرق إلى مذهب الدولة غير القادرة أو غير الراغبة، فكأنما أباح النتيجة دون المنهج، فقد نص على أنه:

"خلصت أغلبية أعضاء فريق الخبراء الدولي إلى نتيجة أن ممارسات الدول قد أرست حق الدفاع عن النفس في مواجهة العمليات الإلكترونية على مستوى الهجوم المسلح من قبل جهات فاعلة من غير الدول دون تدخل دولة"[2].

فدليل (تالين) يرى أن هناك ممارسة كافية للقول بشرعية الدفاع عن النفس ضد الجماعات المستقلة غير الحكومية، كأن تشن مجموعة إرهابية أو متمردة عملية إلكترونية مدمرة ضد البنية التحتية الحيوية الموجودة في دولة ما، فتلك العملية تعد في حكم الهجوم المسلح ضد الدولة الأخيرة، وحيثما وجد الهجوم المسلح يوجد حق استخدام القوة للدفاع عن النفس. والمشكلة هي أنه لم يتوصل الخبراء إلى توافق في الآراء بشأن ما إذا كان يجب تطبيق معايير أخرى من أجل تفعيل حق الدفاع عن النفس. فمحكمة العدل الدولية وضعت اختبار السيطرة الصارمة أو الفعالة، والفقه وضع مذهب الدولة غير القادرة أو غير الراغبة في حين أن دليل (تالين) أقر بوجود حق للدفاع عن النفس ضد الجماعات المسلحة المستقلة، ولم يضبطه بمعايير أخرى تراعي عدم انتهاك سيادة الدولة التي تستخدمها تلك

[1] Couzigou, I. (2016). The Right to Self-Defence against Non-State Actors: Criteria of the Unwilling or Unablee Test. *Heidelberg Journal of International Law, 77*, 53–55. Retrieved from https://www.zaoerv.de/77_2017/77_2017_1_a_53_55.pdf

[2] Tallinn Manual 2.0, commentary to rule 71, para. 19, p. 345

الجماعات بوصفها قاعدةً، واكتفى بالقول "من المرجح أن يتضح هذا الأمر من خلال ممارسات الدولة"[1]. قد يكون عدم التطرق إلى مذهب الدولة غير القادرة وغير الراغبة بسبب ضعف قيمته القانونية[2] فالاعتماد على قاعدة بذل العناية خاطئ في هذا المذهب؛ لأن التقصير في بذل العناية لا يحرك الدفاع عن النفس، بل يحرك الإجراءات القانونية أو الاجراءات المضادة أو إجراءات الضرورة. كما أنه يؤدي إلى نتائج لا تتفق مع الميثاق كاستخدام القوة المسلحة ضد إقليم دولة غير مذنبة في أفعال الجماعات المسلحة على إقليمها[3]. مثلا:

في عام 2015، أصبحت الولايات المتحدة أول دولة ترد بقوة عسكرية على الهجمات الإلكترونية، عندما استخدمت غارة بطائرة بدون طيار لقتل "جنيد حسين" في الرقة، وهو مواطن بريطاني كان مسؤولاً عن مجموعات قراصنة داعش[4]. وتجدر الإشارة إلى أن محاولة اغتياله لم تنجح من المرة الأولى ونتج عن المحاولة وفاة 3 مدنيين وإصابة خمسة اشخاص[5].

في 5 مايو 2019، استخدمت إسرائيل القوة العسكرية للرد على هجوم إلكتروني لحركة حماس. فأعلن الجيش الإسرائيلي عبر تويتر "لقد أحبطنا محاولة هجوم إلكتروني لحركة حماس ضد أهداف إسرائيلية. بعد عمليتنا الدفاعية الإلكترونية الناجحة، استهدفنا مبنى يعمل فيه عملاء حماس الإلكترونيون"[6].

---

[1] Tallinn Manual 2.0, commentary to rule 71, para. 21, p. 346

[2] ومذهب الدولة "غير القادرة وغير الراغبة" أثبت فشله عندما أنكرته الحكومة السورية من جانبها، فقد أكدت أن الضربات التي تقودها الولايات المتحدة غير قانونية وأنها قد اتخذت خطوات فعالة لمكافحة الإرهاب على الرغم من التدخل الخارجي الضار، للمزيد انظر:
المرجع السابق – Sendut, J. H.

[3] Corten, O. (2021b). The Law Against War: The Prohibition on the Use of Force in Contemporary International Law. In *Do the Prohibition of the Use of Force and Self-Defence Apply to Non-State Actors?* (pp. 137–203) [p. 196]. Oxford, United Kingdom: Hart Publishing. https://doi.org/10.5040/9781509949021.ch-003

[4] Jayakumar, S. (2020). Cyber Attacks by Terrorists and other Malevolent Actors: Prevention and Preparedness. In *Handbook of Terrorism Prevention and Preparedness* (pp. 898–954) [p. 901]. Hague, Netherlands: ICCT Press. https://doi.org/10.19165/2020.6.01

[5] Ackerman, S., & Ross, A. (2016, January 29). Airstrike targeting British hacker working for Isis killed three civilians instead, US admits. *The Guardian*. Retrieved from https://www.theguardian.com/us-news/2016/jan/29/sis-airstrike-syria-civilians-killed-us-military-junaid-hussain

[6] Israel Defense Forces [@IDF]. (2019, May 5). CLEARED FOR RELEASE: We thwarted an attempted Hamas cyber offensive against Israeli targets. Following our successful cyber defensive operation, we [Tweet]. Retrieved from https://twitter.com/IDF/status/1125066395010699264?s=20&t=XDX57wLgyoX8DghScSYZiw

فإذا كانت عملية الولايات المتحدة لها من قرارات مجلس الأمن التي تمت الإشارة إليها ما يمكن أن يسوغ لها قانوناً، فإن العملية الإسرائيلية تثير العديد من الأسئلة حول الحق في الرد بالقوة على العمليات السيبرانية الصادرة من جماعات مسلحة لا ترعاها الدولة. وسلطت الضوء على أهمية عنصر التناسب للرد على هجمات سيبرانية، والتذكير بأنه إذا كانت الدفاعات الإلكترونية السلبية يمكن أن تحبط الهجوم بشكل فعال فلا يمكن أن تطلق الدولة الضحية ردودًا إلكترونية أو حركية من شأنها أن ترقى إلى مستوى استخدام القوة.

قد يكون البت في إقرار هذا التوسع في الدفاع عن النفس أن المزاج العام لدليل (تالين) جاء مسايرا "لا مقوما أو معدلا لسلوك الدول" (خصوصا الولايات المتحدة والمملكة المتحدة أكبر الدافعين لمذهب الدولة الغير قادرة أو الغير راغبة[1]). وقد وضح مايكل شميت محرر دليل (تالين) ذلك فقال: إن الدليل لم يرغب في ان يكون عبئاً على الدول بإعطائهم التزامات غير موجودة خارج الدليل[2]، لكن ما نرغب في الإشارة إليه هنا أنه يمكن تفهم رفض دليل (تالين) لتوسيع التزامات الدول مثلما رفض جعل الالتزام ببذل العناية التزامًا سابقًا على وقوع الهجمات السيبرانية. لكنه هنا بإقراره للدفاع عن النفس ضد فاعلين غير دوليين مستقلين يعطي حقوقاً لدول غير موجودة خارجه كقانون. هذا أمر فيه تفويت للجوء إلى طرق "اللاعنف". فكلما أقرت هذه الإجراءات من الفقهاء تباعدت المسافة بين الواقع وبين قواعد استخدام القوة كما وضعها الميثاق واتفقت عليها إرادة جميع الدول.

إنه ليس من المستبعد أن تتحول هذه الممارسة إلى قاعدة عرفية، لكن الأمر يحتاج إلى تحقق عناصر القاعدة الدولية العرفية من تكرار الممارسة ثم –وهذا هو العنصر الأهم– "اعتقاد أعضاء الجماعة الدولية أن هذا السلوك المتبع ملزم من الناحية القانونية"[3] أما قبل ذلك فوظيفة الفقه ليس تشريع مخالفات الدول، بل ضبطها. لذلك كان من الأجدى أن يكون دليل (تالين) أكثر تحفظاً في تشريعه في المجال

Gori, B. (2022, February). *From Kinetic to Cyber Attacks and Back: The Israeli Approach to Deterrence In Cyberspace and the Multi-Dimensional Threat of Hamas*. University of Florence (Università degli Studi di Firenze), p. 15. Retrieved from https://www.cssii.unifi.it/upload/sub/Pubblicazioni/2022_Gori_Beatrice.pdf

[1] Brunnée, J., & Toope, S. J. (2017). Self-defence against non-state actors: Are powerful states willing but unable to change international law? *International and Comparative Law Quarterly*, *67*(2), 263–286 [p. 277,282]. https://doi.org/10.1017/s0020589317000458

[2] Tallinn Manual 2.0, introduction, pp. 2-3

[3] انظر بشكل عام:

أحمد، مبخوتة. (2021). التطورات المتلاحقة على العرف الدولي باعتباره مصدرا للقانون الدولي. مجلة الحقوق والعلوم الإنسانية، 14(1)، 71–89. استرجع من https://www.asjp.cerist.dz/en/article/149162

السيبراني، ليس فقط لمسالة صعوبة التنسيب، بل لعدم استقرار الركن المعنوي من القاعدة العرفية تجاه هذا السلوك. وتجدر الإشارة إلى أن القاعدة الجديدة المزعومة (الدفاع عن النفس وفقا لمذهب الدولة غير الراغبة وغير القادرة) مدعومة من قبل خمس دول فقط (الولايات المتحدة الأمريكية، وأستراليا، إسرائيل، وتركيا، والمملكة المتحدة)[1].

المبحث الثالث

استخدام القوة من قبل مجلس الأمن

سبق –في مقدمة البحث– توضيح أن الاهتمام بالمواجهة الدولية للهجمات السيبرانية سيكون من منظور الدولة، وليس من منظور الأجهزة والمنظمات الدولية. مع ذلك فإن استخدام مجلس الأمن للقوة تحت الفصل السابع من الميثاق هو الاستثناء الثاني من قاعدة منع استخدام القوة بعد الدفاع عن النفس. لذلك –وفي سبيل إكمال عناصر قاعدة منع استخدام القوة– سيتم التعريج بإيجاز على إمكان مواجهة مجلس الأمن للهجمات السيبرانية باستخدام القوة.

أولا تجدر الإشارة إلى أنه بغض النظر عن تصنيف العملية السيبرانية أنها هجوم مسلح أو غير مسلح يمكن للدولة الضحية لعملية إلكترونية إحالة الوضع إلى مجلس الأمن بموجب (المادة 35 (1))[2] من ميثاق الأمم المتحدة على أنه "موقف قد يؤدي إلى احتكاك دولي أو قد يثير نزاعا"[3] ويجوز للمجلس أن يوصي بتسوية النزاع بالطرق المناسبة (المادة 36(1)).[4] أما إذا كان المجلس يرى أن الوضع يرقى إلى مستوى تهديد للسلام، وخرق للسلم، أو عمل عدواني، فيمكن ان يمارس سلطاته وفق الفصل السابع من الميثاق.[5]

إذن يمكن من الناحية النظرية للدولة المستهدفة بعمليات سيبرانية أن تسعى وفق ميثاق الأمم المتحدة إلى تفعيل الفصل السابع من صلاحيات مجلس الأمن. بالطبع سيكون القيام بذلك امرا شبه مستحيل

---

[1] المرجع السابق – Brunnée, J., & Toope, S. J. – ص282،277

[2] تنص المادة 35 (1) من ميثاق الأمم المتحدة على الآتي: لكل عضو من "الأمم المتحدة" أن ينبه مجلس الأمن أو الجمعية العامة إلى أي نزاع أو موقف من النوع المشار إليه في المادة الرابعة والثلاثين."

[3] تنص المادة 34 من ميثاق الأمم المتحدة: "لمجلس الأمن أن يفحص أي نزاع أو أي موقف قد يؤدي إلى احتكاك دولي أو قد يثير نزاعا لكي يقرر ما إذا كان استمرار هذا النزاع أو الموقف من شأنه أن يعرض للخطر حفظ السلم والأمن الدولي"

[4] تنص المادة 36 (1) من الميثاق على: "لمجلس الأمن في أية مرحلة من مراحل نزاع من النوع المشار إليه في المادة 33 أو موقف شبيه به أن يوصي بما يراه ملائماً من الإجراءات وطرق التسوية."

[5] المرجع السابق – Roscini, M. Cyber Operations and the Use of Force – ص110

بسبب حق النقض الذي تملكه الدول الخمس دائمة العضوية. لكن حتماً من الناحية القانونية فإن مجلس الأمن يملك من الصلاحيات ما يمكن من ردع هذه الظاهرة، ونجد أن المادة 76 من دليل (تالين) قد أسقطت جوهر الفصل السابع من الميثاق على الهجمات السيبرانية كالآتي:

يجب على مجلس الأمن التابع للأمم المتحدة تحديد أن جهازًا إلكترونيًا يوجه عملية تهديد للسلام، أو خرق للسلام، أو عمل من أعمال العدوان (المادة 39 من الميثاق)، قد يسمح للطرف الآخر باتخاذ تدابير لا تنطوي على استخدام القوة بما في ذلك العمليات السيبرانية التي لا تنطوي على استخدام القوة (المادة 41 من الميثاق). وإذا قرر مجلس الأمن أن هذه الإجراءات غير كافية، فيجوز له اتخاذ قرار بشأن تدابير تنطوي على استخدام القوة بما في ذلك القوة السيبرانية (المادة 42 من الميثاق).

وأما المادة 39 من الميثاق فإنها تخول مجلس الأمن سلطة "تحديد وجود أي تهديد للسلام أو خرق للسلام أو فعل العدوان" بل لم يقرر مجلس الأمن مطلقًا أن أي عملية إلكترونية قد تهدد السلم أو الإخلال بالسلام أو العدوان[1]. يجدر الانتباه إلى أن مجلس الأمن حين يمارس صلاحياته وفق المادة 39 ويحدد حالة تهديد للسلم والأمن فإن ذلك يكون بطريقين إما أن يصف حوادث أو مواقف محددة –وعادة ما يقصد نزاع في إقليم معين أو سلوك دولة بعينها– وإما أن يصف ظاهرة أو فعل عدواني في صورة مجردة على أنه يهدد السلم والأمن الدولي، أي دون الإشارة بخاصة إلى الأفعال التي حدثت أو التي على وشك الحدوث[2] كما وصف المجلس ظاهرتين مهمتين بأنهما تهددان السلام وهما: الإرهاب الدولي[3] وانتشار أسلحة الدمار الشامل[4]. العمليات السيبرانية تصل إلى حد تهديد السلام ، وخرق السلام ، أو فعل عدواني في صورة مجردة، على سبيل المثال، هو في داخل سلطة مجلس الأمن في

---

[1] تجدر الإشارة إلى ان الجمعية العامة للأمم المتحدة تعطي مفهوما واسعا لما يمكن أن يعتبر تهديدا للسلام أو فعلا من أفعال العدوان بحيث يمكن أن يشمل ذلك المفهوم العمليات السيبرانية. قرار الجمعية العامة رقم 3314 لعام 1974 الذي كان يهدف لتعريف العدوان جاء في أحد مكونات تعريف العدوان المادة 3 منه الفقرة ب "استخدام لأي سلاح من قبل دولة ضد إقليم دولة أخرى". من هنا نرى بأن الأفعال التي يمكن أن ترقى للعدوان وبالتالي لجرائم ضد السلام يمكن أن تشمل العمليات السيبرانية باعتبارها سلاحا بغض النظر إن كان فاعلوا العملية الإلكترونية دولًا أو جهات فاعلة غير حكومية وبغض النظر ما إذا كانت العملية توصف على انها استخدام للقوة أو هجوم مسلح أو مجرد استغلال إلكتروني، فكل ذلك ليس عاملاً حاسمًا في تقرير أن تهديدًا للسلام موجود وفقا لهذا التعريف. برغم إمكانية اتساع تعريف الجمعية العامة للعدوان ليشمل الهجمات السيبرانية الا انه غير ملزم لمجلس الأمن. انظر قرار الجمعية العامة:

General Assembly resolution 3314 (XXIX) – Article 3(b)

[2] Tallinn Manual 2.0, commentary to rule 76, p. 357, para. 2

[3] قرار مجلس الأمن 1373، S/RES/1373 (28 سبتمبر 2001). استرجع من https://daccess-ods.un.org/tmp/1032731.53305054.html

[4] قرار مجلس الأمن 1540، S/RES/1540 (28 ابريل 2004). استرجع من https://daccess-ods.un.org/access.nsf/Get?OpenAgent&DS=S/RES/1540(2004)&Lang=A

تحديد تلك العمليات السيبرانية موجهة نحو الأنظمة المصرفية الوطنية أو البنية التحتية الوطنية الحيوية مؤهل على هذا النحو.

وفقا للمادة 41 من الفصل السابق من الميثاق يمكن للمجلس اتخاذ تدابير غير قسرية، أي لا تنطوي على استخدام للقوة، لكن يجدر الانتباه إلى أنه لا يمكن تسميتها بالتدابير المضادة؛ لأن التدابير المضادة إجراءات غير قانونية كأصل، أما التدابير غير القسرية لمجلس الأمن فأنها قانونية بموجب ميثاق الأمم المتحدة. وبالتالي، فإن قرار مجلس الأمن يجيز التدخل السيبراني في دولة ما من خلال إتلاف البنية التحتية السيبرانية الموجودة في تلك الدولة من شأنه أن يجعل النشاط قانونيًا، وليس تدبيرًا مضادًا، حتى لو كان ذلك من شأنه أن ينتهك سيادة الدولة المستهدفة[1].

والحقيقة أن لمجلس الأمن صلاحيات واسعة في اختيار التدابير المناسبة غير القسرية، وتقدم المادة 41 من ميثاق الأمم المتحدة بعض الأمثلة مثل قطع الاتصالات وهو إجراء غير قسري يمكن اتخاذه بموافقة مجلس الأمن للتصدي لتهديد السلام أو خرق السلام أو عمل عدواني. فإذا قرر مجلس الأمن قطع الاتصالات الإلكترونية مع دولة معينة فإن باقي الدول أعضاء الأمم المتحدة ملزمون بذلك القرار، وعليهم تنفيذه محليا بتوجيه مزودي الخدمة المحليين باعتماد تدابير تقييدية على تلك الدولة كأن يوضع اسم المجال في القائمة السوداء[2].

أما إذا رأى المجلس أن التدابير لن تكون فعالة، أو ثبت أنها غير كافية لوقف حالة تهديد السلم والأمن الدولي فللمجلس استخدام القوة "تدابير قسرية" بموجب المادة 42 ردا على التهديد السيبراني للسلم والأمن الدولي. وقد يكون استخدام القوة بالوسيلة السيبرانية نفسها كأن تبدأ التدابير القسرية بغطاء كثيف من العمليات السيبرانية التي تسبب شللا شبة تام في مرافق الدولة التي يصدر منها الخطر السيبراني الذي يهدد السلم والأمن، أو أن يكون بوسيلة حركية تقليدية، كأن يشن هجوما مسلحا تقليديا لقصف مركز القيادة السيبراني الذي تصدر منه العمليات السيبرانية التي تهدد السلم والأمن الدوليين[3].

---

[1] Schmitt, M. N. (2013). “Below the Threshold” Cyber Operations: The Countermeasures Response Option and International Law. *Virginia Journal of International Law, 54(3)*, 698-732 [p.702]. Retrieved from https://centaur.reading.ac.uk/89821/1/SSRN-id2353898.pdf

[2] Tallinn Manual 2.0, commentary to rule 76, p. 358, para. 5

[3] Tallinn Manual 2.0, commentary to rule 76, p. 359, para. 8

في الواقع أن آخر تحديث لنشاط مجلس الأمن بخصوص التهديدات السيبرانية للسلم والأمن كان هناك اجتماع رسمي واحد بهذا الخصوص، ومجموعة اجتماعات غير رسمية[1]. هذا الاجتماع كان في يونيو 2021. واتضح فيه اتفاق الدول الغربية على بعض الأسس أهمها انطباق القانون الدولي على الفضاء السيبراني[2] وأهمية آلية العقوبات لردع ظاهرة الهجمات السيبرانية[3]. وفي المقابل انتقدت روسيا بعض الدول؛ لأنها رأت أنها تفسر القانون الدولي في الفضاء السيبراني انتقائيًا غير صحيح، وهذا من شأنه أن يسوغ الضغط والعقوبات من جانب واحد، والاستخدام المحتمل للقوة" ضد الدول الأعضاء الأخرى. كما اعترضوا على مشاركة مجلس الأمن في هذه المسألة، قائلين إنهم يعارضون أي محاولات من جانب المجلس "لمراجعة ... الاتفاقات المتوازنة التي تم التوصل إليها في منتديات الجمعية العامة للأمم المتحدة"[4].

وعقب المناقشة المفتوحة، عممت إستونيا (وهي التي كانت تترأس المجلس حينها) على أعضاء المجلس مشروع بيان رئاسي بشأن الأمن السيبراني. وقد أقرت مسودة البيان بأن الأنشطة السيبرانية الخبيثة تهديدٌ للسلم والأمن الدوليين، وأن التصدي للتهديدات السيبرانية، بوصفها قضية عابرة للحدود، يتطلب تعاونا متعدد الأطراف[5]. لكن مسودة هذا البيان لا يمكن أن تكون محركًا لصلاحيات المجلس بموجب المادة 39 من الفصل السابع؛ ذلك أنها ليست قرارا، بل مسودة بيان خالية من أي قوة تنفيذية ملزمة للدول الأعضاء. فجميع الدول الأعضاء في الأمم المتحدة ملزمون بتنفيذ قرارات مجلس الأمن (بخلاف التوصيات).

وأما واقعيًا فإن أفضل ما يمكن أن تُنصَح به الدولة الضحية –بخصوص اللجوء لمجلس الأمن– فهو محاولة الحصول على قرار إدانة للهجمات السيبرانية التي تتعرض لها لكونها فعلا غير مشروع. مثل ذلك القرار يمنح الدولة الضحية مركزا قانونياً قوياً؛ لتستطيع بعد ذلك سلك طرق المساعدة الذاتية كالدفاع عن النفس أو الإجراءات المضادة أو غيرها من طرق المساعدة الذاتية، أو حتى لتتمكن من سلك طريق القضاء أو التحكيم الدولي.

---

[1] Security Council Report. (2022, January). *In Hindsight: The Security Council and Cyber Threats, an Update*. Retrieved from https://www.securitycouncilreport.org/monthly-forecast/2022-02/in-hindsight-the-security-council-and-cyber-threats-an-update.php

[2] المرجع السابق

[3] المرجع السابق

[4] المرجع السابق

[5] المرجع السابق

الفصل الثالث

سبل المواجهة الدولية للهجمات السيبرانية

المبحث الأول: المسؤولية الدولية عن الهجمات السيبرانية

المطلب الأول: الركن الأول: أن تؤدي العمليات السيبرانية إلى خرق لالتزام دولي.
المطلب الثاني: الركن الثاني: أن يكون بالإمكان نسبة العمليات السيبرانية غير المشروعة إلى دولة.
المطلب الثالث: بعض الحلول المستقبلية المقترحة للتصدي لمشكلة الإثبات وضعف الأدلة التقنية.
المطلب الرابع: آثار المسؤولية الدولية.

المبحث الثاني الاستجابة الدولية الممكنة رداً على الهجمات السيبرانية (عدا الدفاع عن النفس)

المطلب الأول: مواجهة الهجمات السيبرانية باتخاذ إجراءات المساعدة الذاتية.
المطلب الثاني: المواجهة القضائية للهجمات السيبرانية أمام محكمة العدل الدولية.

الفصل الثالث

سبل المواجهة الدولية للهجمات السيبرانية

يهدف هذا الفصل إلى معالجة العمليات السيبرانية التي لا تصل إلى مستوى الهجوم السيبراني المسلح وبالتالي لا تحرك الحق في الدفاع عن النفس للرد عليها. فهنا الهجمات التي لا تفحص بقاعدة منع استخدام القوة؛ بل بالتزامات القانون الدولي الأخرى، ويؤدي الإخلال بها إلى إقامة المسؤولية الدولية مما يحرك الحق بالرد بالتدابير المضادة، أو التدابير القانونية، أو تدابير الضرورة. لذلك ينقسم هذا الفصل إلى جزئين رئيسين: أولهما يعالج موضوع المسؤولية الدولية عن الفعل السيبراني غير المشروع. والقسم الثاني يعالج كيفية الرد أو التصدي للفعل السيبراني غير المشروع.

بالرغم من أن هذا الفصل يعالج المسؤولية الدولية عن الهجمات السيبرانية في نصفه الأول، والرد على الهجمات السيبرانية في نصفه الثاني فإنه قد يجدر التنبيه على أن هناك خروجا مفيدا عن صلب الموضوع. مثلا في المسؤولية الدولية تشترط قواعد مسؤولية الدولة –لقيام مسؤولية الدولة– وجود فعل غير مشروع، أي مخالف للقانون الدولي أيا كان مصدر هذا القانون معاهدة أم عرف أو غير ذلك. ولذلك سنستثمر الفرصة هنا للوقوف على بعض المشكلات الحديثة على الساحة التي تعاني منها عملية تقنين الهجمات السيبرانية، مثل ظاهرة تجزء القوانين بسبب اختلاف الكيانات التي تقوم بالتقنين. ومشكلة الخلط بين القواعد القانونية الملزمة وغير الملزمة في النطاق السيبراني.

كذلك تشترط قواعد مسؤولية الدولة في صورتها الكلاسيكية تنسيب الفعل غير المشروع إلى دولة، ونسبة الفعل السيبراني غير المشروع –كما سيتبين– من أكبر الصعوبات في موضوع الهجمات السيبرانية، لذلك لا مناص من عرض بعض المقترحات الطموحة من جانب الباحثين مما شأنه أن يخفف صعوبة تنسيب الهجمات السيبرانية وتضفي على نتائج التحقيق ثقة ومصداقية.

يتناول النصف الثاني من هذا الفصل، المواجهة الدولية للهجمات السيبرانية، وإن كان الرد عليها يمكن أن يكون بالدفاع عن النفس وهو أكثر الردود ثقلا وأهمية في المواجهة الدولية للهجمات السيبرانية، بيد أن الدفاع عن النفس لصيق بقاعدة منع استخدام القوة؛ لذلك كان من المنطقي وروده في الفصل السابق الذي عالج الهجمات السيبرانية كقوة خاضعة للقاعدة 2(4) من الميثاق، وتبقى الردود الأخرى غير العنيفة أو التي لا تنطوي على استخدام القوة، وهي التدابير المضادة، والتدابير القانونية، وتدابير

حالة الضرورة في القسم المرتبط بمسؤولية الدولة عن الفعل غير المشروع. لكن من الضروري تذكر أن الاستخدام غير المشروع للقوة لا يخرج عن نطاق المسؤولية الدولية، وبالتالي لا يخرج عن نطاق قواعد مسؤولية الدولة عن الفعل غير المشروع. يترتب على ذلك أن الردود غير العنيفة (التدابير المضادة، والتدابير القانونية وتدابير الضرورة) يمكن اتخاذها ضد الاستخدام غير المشروع للقوة، وذلك في حالة عدم وصول استخدام القوة السيبرانية إلى مرحلة الهجوم السيبراني المسلح.

أخيرا من الفرضيات المهمة التي يعالجها هذا الفصل هو إمكان نظر محكمة العدل الدولية في قضية تخص الهجمات السيبرانية بين الدول. محكمة العدل الدولية هي أصدق اختبار لواقعية القواعد وإلزاميتها ومرونتها، والسؤال هنا: إذا ما وصلت قضية تخص الهجمات السيبرانية أمام محكمة العدل فهل يمكن أن تقبلها المحكمة بالنظر إلى خصائص الهجمات السيبرانية من صعوبة الإثبات ومجهولية الفاعل؟

المبحث الأول

المسؤولية الدولية عن الهجمات السيبرانية

في معرض الحديث عن المواجهة الدولية للهجمات السيبرانية فأنه لا يمكن البدء بمواجهة الهجمات دون الحديث أولا عن مسؤولية الدولة عن تلك الهجمات، ولا يمكن الحديث عن المسؤولية الدولية دون الوقوف على "مجموعة المواد المتعلقة بقواعد مسؤولية الدولة عن الفعل غير المشروع". هذه المواد التي وضعتها لجنة القانون الدولي خلال مدة تقارب النصف قرن وهي تعد –على الأقل في معظم موادها– تقنينا لقانون دولي عرفي[1]. وقد أكدت محكمة العدل الدولية الطابع العرفي لهذه القواعد في عدد من الأحكام[2].

ومن المهم –هنا– ذكر أن دليل (تالين) جعلها أحد الأسس لبناء المسؤولية الدولية في العمليات السيبرانية[3] مالم تؤسس قواعد ملزمة أكثر تخصصا ومراعاة للطبيعة السيبرانية[4]. ومالم يستند الطرفان

[1] Pr. Pierre d'Argent, Université catholique de Louvain [International Law MOOC]. (2017, January 27). *55 The Notion of Responsibility* [Video]. Retrieved from https://youtu.be/9yb2uKgzgok
[2] *Nicaragua* judgement, para. 283, p. 142; para. 292, p. 146
[3] Tallinn Manual 2.0, p. 79
[4] Tallinn Manual 2.0, commentary to Section 1, paras. 6-7, pp. 80-81

إلى معايير أخرى في تقرير المسؤولية الدولية [1]فإن الخبراء في دليل (تالين) يذهبون إلى أنه يمكن الاستناد إلى قواعد مسؤولية الدولة؛ لتقرير أمور مثل المسؤولية –بموجب القانون الدولي– عن العمليات الإلكترونية التي تجريها أجهزتها، أو التي تُنسب إليها، ومتى تتحمل الدولة مسؤولية أفعال الجهات الفاعلة من غير الدول في بعض الأحيان إلى الدول؟

تعد قواعد مسؤولية الدولة قواعد ثانوية؛ لأنها تُفَعَّل بعد أن يتم اختراق التزامات دولية ناشئة عن قواعد قانونية أولية. فالقواعد القانونية الدولية الأولية التي تنتج التزامات أساسية تأتي من مختلف مصادر القانون الدولي كالمعاهدات، والعرف الدولي، ومبادئ القانون الدولي. أما قواعد مسؤولية الدولة فهي قواعد ثانوية عرفية تُفَعَّل بشكل تلقائي عند خرق أي التزام أولي[2]. ولقد صادقت الجمعية العامة للأمم المتحدة على قواعد مسؤولية الدولة وذلك مما يؤكد كونها انعكاسا للعرف الدولي، وكثيرا ما تشير الدول –في علاقاتها بالمحاكم، وعلى رأسها محكمة العدل الدولية في أحكامها– إلى قواعد المسؤولية الدولية عن الفعل غير المشروع.

إن قواعد مسؤولية الدولة عن الفعل غير المشروع جعلت المحرك الوحيد للمسؤولية الدولية هو الفعل غير المشروع دوليا Internationally Wrongful Act فأكد أن محرك مسؤولية الدولة هو الفعل غير المشروع وحده دون حاجة إلى ضرر ينجم عنه. وذلك ينهي الجدل الفقهي الذي يعد الضرر ثالث ركن للمسؤولية الدولية بعد الفعل غير المشروع، ونسبة الفعل إلى دولة وتؤكد أن المسؤولية الدولية تتكون من الأخيرين فقط.

لكن ذلك لا يعني تجاهل الأضرار التي تتم بأفعال لا يحضرها القانون، أو بعبارة أخرى الأضرار التي تتم بأفعال مشروعة وفق القانون الدولي. هذا الأمر متصور في الضرر البيئي العابر للحدود ذلك أن الدولة تمارس حقها في تشغيل المصانع على إقليمها، لكن الانبعاثات التي تصدر منها تضر بدولة أخرى. وإن كان غالبا ما يكون ضررا بيئيا، إلا أنه يمكن أن يكون أي ضرر آخر، ومثل ذلك ضرر نجم عن أنشطة مشروعة داخل حدود البلاد وعبر الحدود لدولة أخرى، كأن تقوم الدولة بتدريبات عسكرية تنتج انطلاق صاروخ خطأ إلى دولة مجاورة صديقة وغير معادية. لذلك وضعت لجنة القانون الدولي مجموعة قواعد أخرى وهي " المسؤولية الدولية عن النتائج الضارة الناجمة عن أفعال لا يحضرها

[1] Tallinn Manual 2.0, commentary to Section 1, paras. 5, pp. 80
[2] Tallinn Manual 2.0, commentary to Section 1, paras. 4, pp. 80

القانون الدولي. (المسؤولية الدولية في حالة الخسارة المترتبة على الضرر العابرة للحدود الناجم عن أنشطة خطرة)"[2][1] لتتصدى لهذه الحالة وهي مكونة من ثماني مبادئ، هدفها الأساسي التعويض السريع المنصف الفعال لضحايا الضرر العابر للحدود.[3] وهذا هو جوهر الخلاف فالمسؤولية الدولية عن أضرار ناتجة عن أفعال مشروعة عبارة عن آلية تعويض. أما المسؤولية الدولية عن الفعل غير المشروع فإنها تستتبع حقوقا للدولة المعنية تتعدى التعويض كالدفاع عن النفس، والإجراءات المضادة، واللجوء إلى مجلس الأمن وغيرها. فلا خلاف إذن على الأنشطة السيبرانية المنبثقة عن فعل مشروع نتج عنه ضرر عابر للحدود. لكن ما يقف عليه هذا البحث هو الهجمات السيبرانية في ظل قانون اللجوء إلى الحرب وهذا يتعدى الضرر الناجم عن هجمات سيبرانية مشروعة إلى الهجمات السيبرانية العدوانية. لذلك ستتم معالجة المسؤولية الدولية عن الهجمات السيبرانية وفق قواعد مسؤولية الدولة عن الفعل غير المشروع دوليا، حين لا يكون الضرر ركنا ولا شرطاً لقيام المسؤولية.

كذلك في تعليق الأمر على الفعل غير المشروع استبعاد لمتطلب "سوء النية" وبالتالي القصد الجنائي في النتيجة المتحققة. فكل ما يهم هو أن يكون الفعل غير مشروع وصادر عن الدولة وكفى، وإن كان خرق القانون قد تم بحسن نية، هذا لا يغير من كون الدولة مسؤولة عن الفعل غير المشروع.

فالمادة 1 من قواعد مسؤولية الدولة تنص على أن:

" أي فعل غير مشروع دولياً تقوم به دولة ما يستتبع مسؤوليتها الدولية".

والفعل غير المشروع هو السلوك الذي يخالف موضوع التزام دولي على النحو الذي يظهر في المادة 2 من قواعد مسؤولية الدولة التي توضح عناصر الفعل غير المشروع دولياً:

"ترتكب الدولة فعلاً غير مشروع دولياً إذا كان التصرف المتمثل في عمل أو إغفال:

---

[1] الأمم المتحدة، لجنة القانون الدولي، *تقرير لجنة القانون الدولي إلى الجمعية العامة للأمم المتحدة عن أعمال دورتها الثالثة والخمسين*، المجلد الثاني الجزء الثاني ((A/CN.4/SER.A/2001/Add.1 (Part 2)
https://legal.un.org/ilc/publications/yearbooks/arabic/ilc_2001_v2_p2.pdf
التعليق على المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دولياً، التعليق على المادة 2(7)، ص. 43-44.

[2] الأمم المتحدة، لجنة القانون الدولي، *تقرير لجنة القانون الدولي إلى الجمعية العامة عن أعمال دورتها الثامنة والخمسين*، المجلد الثاني الجزء الثاني ((A/CN.4/SER.A/2006/Add.1 (Part 2)
https://legal.un.org/ilc/publications/yearbooks/arabic/ilc_2006_v2_p2.pdf

[3] المرجع السابق – المبدأ 3 – ص71

(أ) ينسب إلى الدولة بمقتضى القانون الدولي؛ و

(ب) ويكون خرقاً دولياً على الدولة."

يتبين أن الفعل غير المشروع –الذي يرتب المسؤولية الدولية– يتكون من عنصرين أحدهما: موضوعي وهو واقعة السلوك أو الاغفال التي لا تتطابق مع التزام دولي، ثم العنصر الشخصي، وهو أن هذه الواقعة يمكن نسبتها إلى دولة معينة، ونسبة الفعل هنا مسألة أساسية، فالدول هي كيانات مجردة لا يمكنها التصرف دون العنصر البشري[1]. ولسوف يتم الوقوف على العنصرين المكونين للفعل غير المشروع وإسقاطهما على الطبيعة السيبرانية وذلك في قسمين منفصلين.

المطلب الأول

الركن الأول: أن تؤدي العمليات السيبرانية إلى خرق لالتزام دولي

المطلوب أولا لإثبات قيام المسؤولية الدولية أن يكون التزام دولي قد تم الإخلال به، والمرجع في ذلك هو القانون الدولي وحده فإن المادة 3 من قواعد مسؤولية الدولة تنص على أن: "وصف فعل الدولة بأنه غير مشروع دولياً أمر يحكمه القانون الدولي. ولا يتأثر هذا الوصف بكون الفعل ذاته موصوفاً بأنه مشروع في القانون الداخلي".

قد يكون مصدر هذا الالتزام تعاهدي جاء من المعاهدة الدولية، أو عرفي مصدره القانون الدولي العرفي، أو المبادئ العامة للقانون[2]. وقد تتنوع موضوعاته بتنوع قواعد القانون الدولي، فقد يكون الهجوم السيبراني فيه خرق قاعدة منع استخدام القوة، وهو ما تم تفصيله في الفصل الثاني، أو قد يكون في الهجوم السيبراني اعتداء على قاعدة احترام سيادة الدول، أو عدم التدخل في شأنها الداخلي أو غيرها.

لكن يجب الإشارة إلى أن قواعد القانون الدولي السيبراني بدأت في التكون، ويبدو أنها في نهاية المطاف ستكون مجموعة مستقلة من مجموعات القانون الدولي كالقوانين البيئية، وقوانين حقوق الإنسان، وقانون

[1] Tallinn Manual 2.0, commentary to Section 1, paras. 6-7, pp. 80-81

[2] د. فتحية باية. (2016). الفعل غير المشروع في القانون الدولي العام. الحوار الفكري - جامعة أحمد دراية أدرار، 11(11)، 295–299. استرجع من https://www.asjp.cerist.dz/en/downArticle/179/11/11/14826

اللجوء إلى الحرب وقانون النزاعات المسلحة[1]؛ وذلك بسبب الاهتمام غير العادي الذي حظي به موضوع تقنين الهجمات السيبرانية. هناك العديد من الجهات الحكومية وغير الحكومية على مستوى الدول أو الأفراد تخصصت في التصدي لظاهرة الهجمات السيبرانية. لذلك يمكن القول بخصوص المسؤولية الدولية عن الهجمات السيبرانية إنه –بالإضافة إلى المصادر العامة للقانون الدولي– ينبغي الانتباه إلى تدابير ضبط النفس وتدابير بناء الثقة التي تظهر في معظم مقترحات تقنين الهجمات السيبرانية.

بالرغم من أهمية هذه الجهود فإن تعدد المؤسسات التي تحاول تقنين الهجمات السيبرانية واختلاف تخصصاتها أظهر مشكلتين قد تعيقان بلورة القانون الدولي السيبراني، وبالتالي إمكانية تطبيق المسؤولية الدولية عن الفعل السيبراني غير المشروع. الأولى ظاهرة تجزؤ المعايير المقترحة بين مصادر مختلفة وبالتالي وجهات نظر مختلفة قد تصل إلى حد التعارض، وبالتالي تسبب شللا في التطبيق. والمشكلة الأخرى التمييز ببين ما هو ملزم وما هو غير ملزم في هذه المرحلة المبكرة من تقنين الهجمات السيبرانية. ستتم مناقشة هاتين المشكلتين تباعاً لارتباطهما المباشر بماهية الفعل السيبراني غير المشروع وبالتالي المسؤولية الدولية. ويلي ذلك معالجة نوع خاص من الالتزامات الدولية وهو "الالتزام تجاه المجتمع الدولي ككل" وذلك لتسليط الضوء على الأثر غير العادي الذي يمكن أن يؤديه في ضبط سلوك الدول في الهجمات السيبرانية.

أولا: مشكلة تجزء القوانين أو المعايير الدولية التي تحكم الهجمات السيبرانية

إن محاولة تكييف القانون الدولي على الهجمات السيبرانية استقطبت اهتمام الحكومات والمنظمات الدولية والباحثين من كل أقاليم العالم، فبغض النظر عن دليل (تالين) الذي يعد أكثر محاولة لتكييف الهجمات السيبرانية التي أخذتها الحكومات على محمل الجد، هناك جهود أخرى أقل صدى، بعضها يهدف لتكييف القانون الدولي في الفضاء السيبراني مباشرة، وبعضها يهدف لوضع معايير السلوك الصحيح دون جعل القانون الدولي هو المحور الأساسي. يمكن تقسيم هذه المحاولات التشريعية إلى أربع فئات[2].

[1] Alexander Klimburg (Ed.), New Conditions and Constellations in Cyber, The Hague Centre for Strategic Studies, The Hague 2021, p. 9-13. Retrieved from https://cyberstability.org/wp-content/uploads/2021/12/Cyberstability-Paper-Series.pdf

[2] تقسيم الفئات بهذه الطريقة موجود في:

أولا: فئة الجهود على الصعيد الدولي، كمجموعات الأمم المتحدة مثل فريق الخبراء الحكوميين (GGE) يتكون من 25 خبيرا معنيين بشأن تعزيز السلوك المسؤول للدولة في الفضاء السيبراني في سياق الأمن الدولي[1]. والفريق العامل المفتوح العضوية [2](OEWG) وقد سمي بذلك، لأن عضويته مفتوحة لجميع الدول الأعضاء في الأمم المتحدة، وهو معني بمواصلة عمل فريق عمل الخبراء الحكوميين (GGE) في تطوير قواعد ومعايير ومبادئ السلوك المسؤول للدول، ومناقشة طرق تنفيذها، ودراسة إمكان إقامة حوار مؤسسي منتظم بمشاركة واسعة تحت رعاية الأمم المتحدة. هذا بالإضافة إلى منظمات دولية أخرى سعت إلى القيام بعمليات التكييف الخاصة بها، بما في ذلك منظمة شنغهاي،[3] ومجموعة السبع، ومجموعة العشرين[4].

ثانيا: بعيدا عن نطاق الحكومات هناك لجان الخبراء الخاصة، وهي مجموعات من الخبراء المشهورين من خلفيات متنوعة يدرسون ويقدمون توصيات بشأن المعايير الإلكترونية للدول أو أصحاب المصلحة الآخرين، وهم في ذلك يمثلون أنفسهم، حتى لو كانت لديهم ارتباطات حالية مع دول أو شركات أو مؤسسات أخرى محاولة مبكرة في هذا النوع من العملية (على سبيل المثال، اللجنة العالمية لاستقرار الفضاء السيبراني)[5].

Ruhl, C., Hollis, D., Hoffman, W., & Maurer, T. (2020). *Cyberspace and geopolitics: Assessing global cybersecurity norm processes at a crossroads.* Carnegie Endowment for International Peace. Retrieved June 14, 2022, from https://carnegieendowment.org/2020/02/26/cyberspace-and-geopolitics-assessing-global-cybersecurity-norm-processes-at-crossroads-pub-81110

[1] General Assembly resolution 73/266, *Advancing responsible State behaviour in cyberspace in the context of international security*, A/RES/73/266, available from https://documents-dds-ny.un.org/doc/UNDOC/GEN/N18/465/01/PDF/N1846501.pdf?OpenElement

[2] General Assembly resolution 73/27, *Developments in the field of information and telecommunications in the context of international security*, A/RES/73/27, available from https://documents-dds-ny.un.org/doc/UNDOC/GEN/N18/418/04/PDF/N1841804.pdf?OpenElement

[3] الأمم المتحدة، الجمعية العامة، رسالة مؤرخة 9 كانون الثاني/يناير 2015 موجهة إلى الأمين العام من الممثلين الدائمين للاتحاد الروسي وأوزباكستان والصين وطاجيكستان وقيرغيزستان وكازاخستان لدى الأمم المتحدة، A/69/273. استرجع من https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/014/00/PDF/N1501400.pdf?OpenElement

[4] Paltiel, D. (2022, June 02). *G20 Communiqué Agrees on Language to Not Conduct Cyber Economic Espionage.* Retrieved from https://www.csis.org/blogs/strategic-technologies-blog/g20-communiqu%C3%A9-agrees-language-not-conduct-cyber-economic

[5] About. *Cyberstability* (2022, February 28). Retrieved from https://cyberstability.org/about/

ثالثا: المجموعات الصناعية المتخصصة التي تعنى بالقواعد السيبرانية في مجال الصناعة وهي تضع معايير قانونية تخص الصناعة مقابل الأمن السيبراني. وأظهر مثالين –حتى الآن– على مثل هذه العمليات هما اتفاقية الأمن السيبراني التي أطلقتها[1] Microsoft وميثاق الثقة[2] وهو اتفاق تكنلوجي تقوده شركة سيمنز[3].

رابعا: هنالك مجموعات "أصحاب المصلحة المتعددين" وهم خليط من كل ما سبق بما في ذلك الدول، أو المنظمات الدولية، أو الصناعة، أو المجتمع المدني، أو الأوساط الأكاديمية فيجتمعون جميعا في منتدى واحد؛ لمناقشة، أو تحديد، أو تعزيز المعايير الإلكترونية، وقد يكون ذلك برعاية الأمم المتحدة "كمنتدى حوكمة الإنترنت"[4] الذي يعقد سنويا بهدف تعزيز الحوار حول إدارة الإنترنت، وتبادل أفضل الممارسات والخبرات، وتحديد القضايا الناشئة. ومثل "نداء باريس نداء باريس للثقة والأمن في الفضاء السيبراني"[5] وهو محاولة لبناء الدعم لتسعة معايير لتنظيم سلوك كل من الدول وأصحاب المصلحة الآخرين في الفضاء السيبراني.

كل مولدات القوانين السابقة وغيرها كونت ما يعرف بظاهرة تجزء القواعد السيبرانية في القانون الدولي، فيمكن أن ينتج عن هذه الجهود المختلفة قواعد مختلفة موضوعياً، أو حتى قواعد متضادة في معالجتها للموضوع الواحد؛ مما يسمح للدول بالتسوق بين القواعد واختيار ما يناسب مصلحتها الوطنية.

ردا على خطورة ظاهرة تجزؤ القواعد السيبرانية الدولية ناقشت ورقة "الفضاء الإلكتروني والجغرافيا السياسية: تقييم عمليات معايير الأمن السيبراني العالمية عند مفترق طرق"[6] بأن ظاهرة تجزؤ القوانين السيبرانية ظاهرة صحية. فمن البداهة أن تدرس القواعد السيبرانية من مجموعات متعددة

---

[1] About the Cybersecurity Tech Accord. (2019, October 11). Retrieved from https://cybertechaccord.org/about/

[2] Charter of Trust. (2020, November 2). About. Retrieved from https://www.charteroftrust.com/about/

[3] للمزيد عن اتفاق مايكروسوفت وسمنز
Swiss Federal Department of Foreign Affairs (FDFA), & Eggenschwiler, J. (2018, November). *Geneva Dialogue on Responsible Behaviour in Cyberspace: Private Sector*. Presented at the Geneva Dialogue on Responsible Behaviour in Cyberspace, Geneva, Switzerland. Retrieved from https://genevadialogue.ch/wp-content/uploads/Geneva-Dialogue-Role-of-the-Private-Sector.pdf

[4] الأمم المتحدة (7 ديسمبر 2021) منتدى حوكمة الإنترنت يروج لمستقبل رقمي شامل للجميع. استرجع من https://news.un.org/ar/story/2021/12/1089192

[5] Paris Call for Trust and Security in Cyberspace. (n.d.). Retrieved from https://pariscall.international/en/call

[6] المرجع السابق – Ruhl, C. et al.

تعطي عمقا وفهما أوسع لمعرفة أفضل طريقة يمكن أن تعمل بها تلك القوانين. فتوسيع المشاركة في عملية وضع المعايير يوجد بيئات متعددة في التطبيق حيث الفاعلين وطبيعة النشاط مما قد يعطي نتائج أفضل في الأمن السيبراني، وزيادة الثقة في تلك القواعد. مثلا قد تقبل المجموعات الصناعية تكييفها للقواعد السيبرانية أكثر من القواعد التي تخرج من الخبراء الحكوميين، ذلك لأن القواعد التي تخرج من بيئة أو مجتمع معين قد تكون أكثر واقعية وقبول من غيرها بين أعضائه. كذلك وجود عدد من الخطوط تعمل بالتوازي على التقنين السيبراني يمكن أن يمنع وجود حاجز في منطقة واحدة من إعاقة كل التقدم.

وإن مما يبعث على الاطمئنان أن تلك التجارب لا تعمل بمعزل بعضها عن بعض، بل يستفيد بعضها من بعض، وهو ما أسمته الورقة التلقيح المتبادل[1]. فنرى أن عمليات تقنين أو وضع المعايير استندت صراحة إلى عمليات أخرى، فتم اعتماد معايير من تقارير فريق الخبراء الحكوميين للأمم المتحدة في اللجنة العالمية لاستقرار الفضاء السيبراني، ثم اعتمدت المعايير من قبل كل من فريق الخبراء الحكوميين للأمم المتحدة، واللجنة العالمية في نداء باريس، وهكذا كل فئة تبني معاييرها على قواعد الفئة الأخرى والسبب في ذلك هو أن كل الجهات مرتبطة "بالمتخصصين في المعايير الإلكترونية" فالحكومات والمنظمات غير الحكومية ولمجتمعات الصناعية والمجتمع المدني لديهم خبراء يشاركون في واحد أو أكثر من هذه العمليات في وقت واحد. وتربطهم شبكة اتصال رسمية وغير الرسمية[2].

نتيجة لذلك بدأت تتكرر بعض المعايير حتى أصبح هناك نوع من الاجماع العالمي عليها. وهو ما دعا إلى القول: إن قواعد الهجمات السيبرانية بدأت تتبلور في مجموعة منفصلة من القوانين التي ينبغي الانتباه لها في أثناء تطبيق مسؤولية الدولة عن الفعل غير المشروع. إن من أهم أمثلة المعايير التي تتكرر في المقترحات أن تمتنع الدول عن مهاجمة البنى التحتية الحيوية، وعليها الامتناع عن الإضرار بعمل فرق الاستجابة للطوارئ[3]. كذلك مما يتبنى بشكل متكرر اعتراف الحكومات بضرورة حظر سرقة

---

[1] المرجع السابق – Ruhl, C. et al. – ص2

[2] المرجع السابق – Ruhl, C. et al. – ص14

[3] United Nations, General Assembly, *Note by the Secretary General on Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/70/174 (22 July 2015), p. 2. Retrieved from https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/228/35/PDF/N1522835.pdf?OpenElement

الملكية الفكرية عبر الإنترنت، والحقيقة أن هذا أمر ثوري لأن فيه تقييد للأعمال الاستخباراتية والتجسسية التي لطالما عدتها الدول مناطق حرة لا يقيدها القانون[1].

كذلك مما يتكرر الاعتراف به أن الدفاع الإلكتروني هو تمرين تعاوني يتطلب شراكات عبر الحدود والعمل المشترك ضد تهديدات الأمن السيبراني. فمعظم المقترحات الدفاعية تشجع الدول القومية القادرة على دعم الآخرين ضحايا الهجمات الإلكترونية،[2] لذلك قيمة كبيرة في تحميل الدول مسؤولية التعاون والمساعدة[3].

بيد أن الحاجة مستمرة لإبقاء عمليات وضع المعايير المختلفة تحت السيطرة ومنع التعارض فيما بينها في مرحلة التشريع لضمان الانسجام في مرحلة التنفيذ. ففي حين أن التجزؤ مقبول في ظل الظروف الحالية فإنه يجب التحرك نحو بعض التوحيد في المستقبل، وأهم الأفكار التي طرحت في هذا المجال هو إنشاء قواعد معلومات بيانات عمليات التقنين المختلفة بهدف مد الجسور وبناء العلاقات بين عمليات التقنين السيبرانية؛ وذلك لتكون قاعدة البيانات العالمية توثيقا للاتفاقيات الدولية الثنائية والمتعددة الأطراف التي تتناول موضوع التعاون في الأمن السيبراني والتصدي للهجمات السيبرانية[4].

إن أفضل استجابة حتى الآن –فيما تراه الباحثة– لفكرة قاعدة البيانات السيبرانية العالمية هي قاعدة البيانات التي أنشأها مركز التميز للدفاع الإلكتروني التعاوني التابع لحلف الناتو تحت مسمى "مجموعة أدوات القانون السيبراني" وهي مورد تفاعلي ديناميكي على شبكة الإنترنت للقانونيين الذين يتعاملون مع تقاطع القانون الدولي والعمليات الإلكترونية. يتتبع مواقف الدول بخصوص الهجمات السيبرانية في استراتيجيات الأمن السيبراني الوطنية، أو في تصريحات الدول، أو في مناقشات الدول في اللجان الدولية المعنية كلجان الأمم المتحدة ويعرض تساؤلات جميع الدول في أمور مثل: هل تقبل الدولة انطباق القانون الدولي على الهجمات السيبرانية؟ هل تعتقد الدولة بوجود الهجوم المسلح السيبراني؟ هل

---

[1] Charney, S., et al. (2016). *From Articulation to Implementation: Enabling progress on cybersecurity norms.* Microsoft, pp. 4-5. Retrieved from https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVmc8

[2] المرجع السابق – ص5

[3] المرجع السابق – ص5

[4] المرجع السابق – Ruhl, C. et al. – ص24

ترى الدولة بالحق في الدفاع عن النفس ضد الهجمات السيبرانية التقليدية؟ فضلا عن وجهة نظر كل دولة في كيفية تعقب الهجمات والوصول إلى تحديد الفاعل وغيرها[1].

كذلك تجدر الإشارة إلى أن مجتمع الباحثين المهتمين بالقانون الدولي والفضاء السيبراني يترقب دليل (تالين) 3.0 النسخة الثالثة. وهو مشروع يجري العمل عليه يهدف إلى أن يكون انعكاسًا دقيقًا لما وصل إليه القانون الدولي السيبراني. فبالإضافة إلى تحديث القواعد القانونية الواردة في (تالين) 2.0 سيحتوي على موضوعات جديدة ذات أهمية للدول وهي تنقيح الممارسات الحالية للدول فيما يتعلق بالعمليات السيبرانية، بما في ذلك البيانات الرسمية للدول بشأن القانون الدولي، كما سيتم النظر في أنشطة وبيانات المنتديات الدولية، مثل المناقشات على مستوى الأمم المتحدة بشأن السلوك المسؤول للدولة في الفضاء الإلكتروني، وكذلك المنشورات الأكاديمية ومبادرات أصحاب المصلحة المتعددين بعبارة أخرى يتوقع من النسخة الثالثة من دليل (تالين) أن تكون أداة قوية لتقريب وجهات النظر في تطبيق القانون الدولي على الفضاء السيبراني سواء أفي وجهات النظر الحكومية؟ أم الصناعية أم الاكاديمية أم فيما يتعلق بالجهات الفاعلة في المجتمع المدني[2].

ثانيا: مشكلة التمييز بين القواعد القانونية الدولية الملزمة وغيرها

يتفق المجتمع الدولي على انطباق القانون الدولي الحالي على العمليات السيبرانية، ولكن يبدأ الخلاف –بعد ذلك– على ما يعد قاعدة قانونية ملزمة وما يعد سلوكاً مسؤولا لكنه غير ملزم. ويبدو أن الدول تميل إلى تقبل القواعد غير الملزمة بسهولة أكبر مثل "إجراءات بناء الثقة في الفضاء السيبراني" و"سلوك الدول المسؤول في الفضاء السيبراني" التي صدرت ومازالت تصدر بشكل دوري من لجنتي الأمم المتحدة، لكن تزيد الاعتراضات عند الحديث عما هو ملزم أو ما هو غير ملزم أو مشروع أو غير مشروع. كما في الحديث عن مشروعية الرد على الهجمات السيبرانية بوسائل غير سيبرانية [3].

---

[1] المرجع السابق – International cyber law: interactive toolkit
تم دعم المشروع من قبل المؤسسات الشريكة الست التالية: الوكالة التشيكية الوطنية لأمن المعلومات السيبرانية(NÚKIB) ، واللجنة الدولية للصليب الأحمر (اللجنة الدولية)، ومركز التميز للدفاع السيبراني التعاوني التابع لحلف الناتو (CCDCOE) ، وجامعة إكستر (المملكة المتحدة)، والكلية الحربية البحرية الأمريكية (الولايات المتحدة)، وجامعة ووهان (الصين).

[2] NATO Cooperative Cyber Defence Center (CCDCOE). (2021). CCDCOE to Host the Tallinn Manual 3.0 Process. Retrieved from https://ccdcoe.org/news/2020/ccdcoe-to-host-the-tallinn-manual-3-0-process/

[3] المرجع السابق – Delerue, F. – ص24

وسبب هذه المشكلة أن مجموعتي خبراء الأمم المتحدة (OEWG) (GGE) لم تفصل فيما يعد قاعدة قانونية دولية ملزمة، وما يعد قاعدة استرشادية على الرغم من حقيقة أنه تم تكليف المجموعتين بدراسة ثلاثة مفاهيم في القانون الدولي المطبق على الهجمات السيبرانية هي: قواعد (Rules)، ومعايير (Norms)، ومبادئ (Principles) القانون الدولي المطبقة في الفضاء السيبراني، إلا أنه لم تعرف هذه المصطلحات ولم يوضح الفرق بينها، أو الفصل بينها في أقسام مختلفة. بل جاءت الكلمات الثلاث في نفس العنوان. لا خلاف أن القواعد Rules هي القواعد القانونية الملزمة المكتملة الأركان إلا أن درجة الالزام في المعايير والمبادئ أمر غير واضح ومختلف فيه. لذلك فإن تقارير لجنتي الأمم المتحدة حول تطبيق القانون الدولي على الهجمات السيبرانية أدى إلى الكثير من الالتباس حول ما كان المفاوضون يتفقون عليه بالضبط هل هي قواعد تشمل في إلزاميتها الفضاء السيبراني أو هي معايير السلوك المسؤول.

يرى بعض الناقدين أن ما فعلته الأمم المتحدة من خلال عمل فريق عمل الخبراء الحكوميين والفريق العامل المفتوح العضوية فيه تخفيض لبعض القواعد الراسخة في القانون الدولي إلى توصيات غير ملزمة[1]. مثلا في تقرير فريق الخبراء الحكوميين لعام 2015 –وتحت عنوان معايير وقواعد ومبادئ السلوك المسؤول للدول– ورد التقرير ضرورة العمل المشترك للاتفاق على قواعد **طوعية وغير ملزمة** للسلوك المسؤول للدول؛ لتعزيز الفهم المشترك، وتحقيق مزيد من التقارب والاستقرار في الفضاء السيبراني[2]، ثم في سرد تلك المعايير المقترحة نجد التقرير ينص على هذا المعيار:

"ينبغي للدول ألا تسمح عن علم باستخدام إقليمها لارتكاب أفعال غير مشروعة دوليا باستخدام تكنولوجيا المعلومات والاتصالات"[3]

يتبين أن المعني في هذا المعيار هو مبدأ بذل العناية، هذه القاعدة العرفية الراسخة التي أقرتها محكمة العدل الدولية في قضية قناة كورفو تم التعامل معها على أنها من معايير سلوك مسؤول للدول وغير ملزم! وفي ذلك إهدار لإلزامية القاعدة في النطاق السيبراني. هذا الخطأ قد لا يكفي لتجاوزه أن تقرير فريق الخبراء الحكوميين المضمن فيه، وقبل تعداد معايير وقواعد ومبادئ السلوك المسؤول للدول –

[1] Lotrionte, C. (2022). Bringing the Law In: Unlearned Lessons for Diplomats and Others. The Cyber Defense Review, *7(1)*, 23-31 [p.27]. Retrieved from https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/2882573/bringing-the-law-in-unlearned-lessons-for-diplomats-and-others/

[2] المرجع السابق – A/70/174 – الفقرة 9 – ص7

[3] المرجع السابق – A/70/174 – الفقرة 8 – ص13(ج)

وضح في الفقرة 10 من التقرير– أن هذه المعايير "لا تسعى إلى تقييد أو حظر الإجراءات التي تتفق مع القانون الدولي بطريقة أخرى"، لأن ذلك مازال يتيح للدول التنصل من الالتزام بقواعد مهمة في المجال السيبراني، كما أن فيه تشجيعا لتوجه بعض الدول التي ترى أنه برغم انطباق قواعد القانون الدولي على المجال السيبراني فإنه لا يمكن تطبيقها تلقائيا، بل يجب أن يتم تحديد ما يعد ملزما في هذا المجال، بدراسة متأنية تراعي طبيعته الخاصة[1] في حين أن المطلوب من لجنة الخبراء هو الدفع بتطبيق ميثاق الأمم المتحدة وقواعد القانون الدولي كما هي على الفضاء السيبراني وليس العكس.

ومن الدول التي نبهت لهذه المسألة في أثناء مناقشة عمل الفريق العامل المفتوح العضوية دولة فنلندا التي أكدت أهمية قواعد السلوك المسؤول للدول، لكنها نبهت لخطورة الخلط بين القواعد الموجودة التي ترتب حقوقا والتزامات على الدول وبين القواعد غير الملزمة، وأكدت أنها ستدعم تلك المعايير وتقرير مجموعة العمل المفتوحة لعام 2015 على أنها يقيد بعبارة عامة هي: "أن لا شيء من عمل لجنة OEWG يمكن أن ينتقص من قواعد القانون الدولي"[32].

أخيرا، تعكس القواعد الطوعية غير الملزمة توقعات المجتمع الدولي وتضع معايير فيما يتعلق بالسلوك المقبول وغير المقبول للدول في استخدامها لتكنولوجيا المعلومات والاتصالات مما له أثر مهم في تقليل مخاطر سوء الفهم بين الدول، وبالتالي المساهمة في منع الصراع[4]. لكن لا ينبغي النظر إليها على أنها تحل محل القواعد محل التزامات الدول بموجب القانون الدولي، ولا تغيرها، ولكنها توفر إرشادات إضافية محددة بشأن ما يكون سلوكًا مسؤولًا للدولة في المجال السيبراني[5]. فإذا كانت القواعد غير الملزمة مكملة للقانون الدولي القائم وليست بديلة، فإنه يمكن القول إن الامتثال للعديد من قواعد

---

[1] موقف الاحتلال الإسرائيلي الذي يظهر في تصريح نائب المدعي العام الإسرائيلي بشأن تطبيق القانون الدولي على العمليات السيبرانية موجود في
المرجع السابق – Dias, T. & Coco, A. – ص 17

[2] Statement by Ambassador Janne Taalas at the second session of the open-ended Working Group (OEWG) on developments in the field of information and telecommunications in the context of international security, February 10 and 11. Retrieved from https://ccdcoe.org/uploads/2018/10/Statement-on-International-Law-by-Finnish-Ambassador-Janne-Taalas-at-2nd-session-of-OEWG.pdf

[3] United Nations, General Assembly, *Open-ended working group on developments in the field of information and telecommunications in the context of international security* (Final OWEG report), A/AC.290/2021/CRP.2 (10 March 2021), p. 5, para. 25. Available from https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

[4] المرجع السابق – الفقرة 24 – ص4

[5] المرجع السابق – الفقرة 25 – ص5

السلوك المسؤول للدولة في الفضاء السيبراني ليس متوقعًا فقط على أساس طوعي من الدول، ولكنه مطلوب أيضًا بوصفه مسألة من مسائل القانون الدولي المعمول به، بمعنى أنه لن يمكن الامتثال للقاعدة دون الامتثال لمبادئ السلوك المسؤول والعكس صحيح، يعنى أنه في خرق مبادئ السلوك المسؤول لابد أن يتصل بنوع من الانتهاك لقواعد القانون الدولي[1].

ثالثا: الالتزامات المستحقة للمجتمع الدولي ككل أو Obligation Erga Omnes

تمت مناقشة الركن الأول لقيام مسؤولية الدولة، وهو خرق لالتزام قائم بمقتضى قواعد القانون الدولي. وتم توضيح أن التزامات القانون الدولي بتنوع موضوعاتها والمصادر التي ولدتها، قد تختلف في درجة إلزامها "فالقاعدة" تختلف عن "المعيار" عن "المبدأ العام" إلا أن انتهاك القاعدة غير الملزمة كالمبادئ التوجيهية غالبا ما يمكن أن يتصل بانتهاك القواعد الملزمة والراسخة في القانون الدولي. في هذا الجزء سيتم التفصيل في أحد قواعد القانون الدولي وطريقة انطباقها على الطبيعية السيبرانية وهي قاعدة "الالتزامات المستحقة تجاه المجتمع الدولي ككل" السبب في شدة العناية بهذا الالتزام هنا هو قلة تناوله من مجتمع الباحثين برغم ما قد يوفره هذا الالتزام الدولي من مخرج من حالة العجز التي يعيشها مجلس الأمن! فهنا توفر المبادئ العامة في القانون الدولي طريقا آخر للخروج من الحالات التي تهدد السلم والأمن والمصالح الأساسية للمجتمع الدولي، منها قاعدة Erga Omnes وهو مصطلح لاتيني يعرفه قاموس أوكسفورد بالآتي:

"(في القانون الدولي) هناك نوع من الالتزامات يكون في تحقيقها مصلحة قانونية لجميع الدول، لأن موضوعها ذو أهمية للمجتمع الدولي ككل. ويترتب على ذلك أن خرق مثل هذا الالتزام هو مصدر قلق ليس فقط للدولة الضحية، ولكن أيضا لجميع أعضاء المجتمع الدولي الآخرين. وهكذا، في حالة وجود خرق لهذه الالتزامات، يجب العلم أن لكل دولة مسوغا في الاحتجاج (ربما من خلال القنوات القضائية) بمسؤولية الدولة المذنبة في ارتكاب الفعل غير المشروع دوليًا. وقد اقترح أن يكون مثالاً من التزام تجاه الكافة هو **حق الشعب في تقرير المصير**". [2]

[1] المرجع السابق – Akande, D., Coco, A., & Dias, T.

[2] Martin, E. (2003). *erga omnes* obligation. In Oxford Dictionary of Law (5th edition, p. 179). Oxford, Great Britain: Oxford University Press.

نعرج أولا على تطور مصطلح الالتزام تجاه المجتمع الدولي ككل في القانون الدولي المعاصر، ثم مدى قوته الالزامية، وأخيرا نسقطه في نطاق الهجمات السيبرانية، وما يمكن أن يوفره من قوة رادعة لمواجهة السلوك العدواني السيبراني؟

في الغالب تكون العلاقات القانونية الناشئة عن حدوث فعل غير مشروع دولياً علاقات ثنائية، أي منحصرة في نطاق الدولة المسؤولة والدولة المتضررة، إلا أنه تم الاعتراف وعلى نحو متزايد بأن بعض الأفعال غير المشروعة تستلزم المسؤولية من الدولة المعنية تجاه دولة أخرى أو عدة دول أو حتى تجاه المجتمع الدولي ككل[1]. قد تكمن الفلسفة في هذا النوع من الالتزام أن لكل دولة –بحكم عضويتها في المجتمع الدولي– مصلحة قانونية في حماية بعض الحقوق الأساسية والوفاء ببعض الالتزامات الأساسية[2].

اتخذت محكمة العدل الدولية خطوة مهمة –في تأكيد وجود هذا النوع من الالتزامات– في حكمها في قضية برشلونة تراكشن (معدات الجر) 1964 عندما نصت على ما يلي:

"يجب التمييز أساسا بين التزامات الدولة تجاه المجتمع الدولي ككل، وتلك الناشئة تجاه دولة أخرى في مجال الحماية الدبلوماسية، فالأولى بطبيعتها تكون الشغل الشاغل لجميع الدول. ونظرا لأهمية هذه الحقوق، يمكن الأخذ في الحسبان أن جميع الدول لديها مصلحة قانونية لحماية هذه الالتزامات؛ أنها التزامات تجاه الكافة."[3]

ثم ذكرت المحكمة بعض الأمثلة على ما يعد التزاماً تجاه الكل "تنبع هذه الالتزامات –على سبيل المثال، في القانون الدولي المعاصر– من تحريم أعمال العدوان والإبادة الجماعية وكذلك ...المبادئ والقواعد المتعلقة بالحقوق الأساسية للإنسان، بما في ذلك الحماية من العبودية والتمييز العنصري[4]". وفي قضايا لاحقة، أكدت المحكمة من جديد هذه الفكرة مكررة[5] مما ساعد على تقبل فكرة الالتزامات

[1] التعليق على المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دولياً – التعليق على المادة 1 – الفقرة (4) – ص41

[2] المرجع السابق – التعليق على المادة 1 – الفقرة (4) – ص41

[3] *Barcelona Traction* judgement, paras. 33, p. 32

[4] المرجع السابق – الفقرة 34 – ص32

[5] East Timor (Portugal v. Australia), Judgment, I.C.J. Reports 1995, p. 102, para. 29.
Nuclear Weapons advisory opinion, para. 83, p. 258

تجاه الكافة[1]. تكلل ذلك بأن نصت عليها قواعد مسؤولية الدولة، فإن المادة 48 من قواعد مسؤولية الدولة تنص على:

"1 –يحق لأي دولة خلاف الدولة المتضررة أن تحتج بمسؤولية دولة أخرى وفقاً للفقرة ٢(ب) إذا كان الالتزام الذي خرق واجباً تجاه المجتمع الدولي ككل"

لذلك فإن مصطلح "المسؤولية الدولية" في المادة 1 من قواعد مسؤولية الدولة يغطي العلاقات التي تنشأ بموجب القانون الدولي من الفعل غير المشروع دولياً للدولة، ما إذا كانت هذه العلاقات مقصورة على الدولة المخالفة ودولة متضررة واحدة أو ما إذا كان الضرر يمتد إلى دول أخرى، أو إلى أشخاص آخرين من القانون الدولي خصوصاً أن المادة 54 جاءت بعنوان "التدابير المتخذة من جانب دول خلاف الدولة المتضررة" ونصت على ما يلي:

" لا يخل هذا الفصل بحق أي دولة يجوز لها بموجب المادة 48، أن تحتج بمسؤولية دولة أخرى، في اتخاذ تدابير مشروعة ضد تلك الدولة ضماناً لوقف الخرق وللجبر لصالح الدولة المتضررة أو لصالح المستفيدين من الالتزام الذي خرق".

يترتب على ذلك أن خرق التزام Erga Omnes يولد حقا لجميع الدول –وإن لم تكن قد تضررت– أن تثير ذلك الانتهاك، وتطالب بقيام مسؤولية الدولة المخطئة، وأن تتخذ تدابير لتأمين المصلحة الجماعية. أما ماهية هذه التدابير فهي محل نقاش غير مستقر، ومثير للجدل في القانون الدولي. فالسماح بدول ليست ذات علاقة مباشرة بالانتهاك بالتدخل في الموقف، وفرض الإجراءات المضادة بحجة أن الالتزامات محل الانتهاك هي تجاه المجتمع الدولي ككل فيه منزلق خطير نحو التصعيد والتأزيم ومزيد من التمسك بالسيادة الوطنية؛ مما يهدد النظام ككل. وفي نفس الوقت لن يكون هناك قيمة لوجود هذا النوع من الالتزام تجاه جميع الدول إذا لم يكن ثمة إجراء مضاد لانتهاكها.

وللخروج من هذا المنزلق الخطير قررت لجنة القانون الدولي –في التعليقات المذيلة للنسخة النهائية من المواد الخاصة بمسؤولية الدولة– أن أحقية الدول في اتخاذ تدابير مضادة للإخلال بالقواعد التي

[1] للمزيد عن موقف محكمة العدل الدولية:
Pegna, O. L. (1998). *Counter-claims and Obligations Erga Omnes before the International Court of Justice.* European Journal of International Law, 9(4), 724–736. https://doi.org/10.1093/ejil/9.4.724

تمس المجتمع الدولي ككل، في مرحلة جنينية للغاية، ويفضل الامتناع عن تقنينها في هذه المرحلة[1]. على أن اللجنة قررت أن يترك حسم الأمر بخصوص التدابير المضادة للتطور اللاحق في القانون الدولي[2]، إلا أنها أعطت وصفا آخر أو خيارا آخر للدول للتصدي لانتهاك الالتزامات التي تمس المجتمع الدولي ككل، وهو "الحق في اتخاذ "تدابير قانونية" Lawful Measures بدلا من "تدابير مضادة" Countermeasures. التدابير القانونية هي التي لا تنطوي على مخالفة لالتزام قانوني ويمكن اتخاذها ضد الدولة المسؤولة ضماناً لوقف الإخلال[3]، أما التدابير المضادة فهي إجراءات فيها مخالفة لقواعد القانون الدولي، لكن لأنها تأتي في إطار الرد على فعل غير مشروع فهي تعد مشروعة وصحيحة قانوناً. هذا وسيتم التفصيل في معنى التدابير القانونية والتدابير المضادة في المبحث التالي.

خلاصة الأمر أن هناك نوع من الاجماع على وجود بعض الالتزامات التي في خرقها تهديد لمصلحة المجتمع الدولي ككل Erga Omnes، كالعدوان، والإبادة الجماعية، والعبودية. وهناك إجماع على أن خرق هذه الالتزامات يؤهل أي دولة –حتى وإن لم تتضرر– أن تحتج بمسؤولية الدولة التي تنتهك هذا الالتزام. لكن لا يوجد اتفاق على كيفية الرد على انتهاك من هذا النوع من الالتزامات، أو على الأقل إن كان يمكن الذهاب إلى حد اتخاذ إجراءات مضادة ضد الدولة المخالفة، فالذي يمكن ذكره هو أن الرد الذي يمكن اتخاذه من قبل أي دولة من المجتمع الدولي ضد هذا الخرق هو رد ناعم متمثل في إجراءات قانونية ضد الدولة المسؤولة، لا يصل إلى حد التدابير المضادة، أما جبر الضرر فلا يحق سوى الدولة الضحية التي وقع عليها الضرر أن تطلب به.

وهذا الأمر يمكن تطبيقه تماما في النطاق السيبراني كما أكده دليل (تالين) في المادة 30 منه التي تنص على أنه "يجوز لأي دولة الاحتجاج بمسؤولية الدولة التي قامت بإجراء العمليات الإلكترونية التي تخرق التزامًا تجاه الكافة تجاه المجتمع الدولي ككل"[4]. وأعطى مثالا كأن تحرض دولة بارتكاب إبادة جماعية (أحد الالتزامات التي حددها محكمة العدل الدولية بوصفها التزامات تجاه الكافة Erga Omnes) في دولة أخرى عبر الإنترنت (الوسيلة السيبرانية). هنا يمكن لكل الدول (وإن لم تتأثر بالإبادة الجماعية)، أن تتذرع بمسؤولية الدولة الأولى وتطالب بوقف الفعل غير المشروع دوليًا وإعطاء التأكيدات والضمانات بعدم التكرار.

---

[1] التعليق على المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دولياً، التعليق على المادة 54 – الفقرة (3) – ص178

[2] المرجع السابق، التعليق على المادة 54 – الفقرة (6) و (7) – ص 180-181

[3] المرجع السابق، التعليق على المادة 54 – الفقرة (3) – ص178

[4] Tallinn Manual 2.0, commentary to rule 30, paras. 1-2, p. 152

والملاحظ على دليل (تالين) أنه وسع من وسائل الرد على خرق هذا النوع من الالتزامات إلى السماح بأن تتحرك الدول غير المتضررة باستخدام بعض الإجراءات المضادة ضد الدولة الأولى فجاء فيه ما يأتي:

"ومع ذلك، أقر الخبراء أيضا أنه قد تكون هناك حالات متطرفة قد تستخدم فيها الدولة الوسائل الإلكترونية من أجل الرد على الأعمال السيبرانية التي تهدد تهديدا خطيرا المصالح الأساسية لـ "المجتمع الدولي ككل"[1]

ففي المثال السابق إذا نجحت الدولة الأولى في التحريض على الإبادة الجماعية وبدأ الوضع خطرا جاز لباقي الدول التدخل بالوسيلة السيبرانية نفسها لإنهاء هذا التحريض والسيطرة عليه. كما تم التوضيح في تفعيل لفكرة هذا النوع من الالتزام مخرج قانوني لحفظ السلم والأمن في حالة فشل مجلس الأمن في التحرك للقيام بهذه الوظيفة. خصوصا أن هناك قواعد ضابطة للإجراءات المضادة تضمن تطبيقها في الموقف المطلوب وبالكيفية والكمية المطلوبة مما يكون محل مناقشة في المبحث الثاني من هذا الفصل.

ومن أمثلة تعزيز فهم الالتزام تجاه الكافة Erga Omnes أن تشن دولة هجوما سيبرانيا على دولة أخرى تعد مركزا لسلعة أساسية عالمية كالنفط، فلو شنت دولة هجمات سيبرانية قوية، ومنظمة على شركات انتاج النفط في الخليج العربي؛ مما يؤدي إلى توقف الإنتاج تماما وانقطاعه عن العالم لبضعة أسابيع، فالأمر يكون بصدد خرق لالتزام عدم العدوان الذي عدته محكمة العدل الدولية أحد أنواع الالتزامات تجاه المجتمع الدولي ككل، وبالفعل فأنه يؤثر في مصلحة المجتمع الدولي ككل لأنه يوقف الإنتاج مما يسبب أزمة عالمية، لذلك من المتصور أن تعتمد الدول على مبدأ الالتزام تجاه الكافة Erga Omnes في إثارة مسؤولية الدولة المتسببة في الهجوم، وإن لم تكن من الدول التي وقع عليها الهجوم المباشر، وإن لم يكن اقتصادها أو صناعتها قد تضررت بهذا الفعل بسبب كونها هي الأخرى دولة نفطية أو لديها مخزون يكفيها من النفط، لكن تأثير تلك الهجمات على مصلحة المجتمع الدولي يسمح لجهاز الأمن الوطني في أي دولة بالرد على الدولة المعتدية بالهجمات السيبرانية نفسها. وللحديث عن قاعدة Erga Omnes بقية في قسم التدابير المضادة ضد انتهاك هذا النوع من الالتزام.

المطلب الثاني

[1] Tallinn Manual 2.0, commentary to rule 26, para. 3, p. 136

الركن الثاني: أن تكون نسبة العمليات السيبرانية غير المشروعة للدولة ممكنة

الدول كيانات مطلقة لا يمكنها القيام بفعل إلا من خلال أشخاص فأن يصدر الفعل من الدولة يعني أن ينسب إليها عبر أشخاص يمثلونها. ولكي تتم نسبة فعل –كالهجوم السيبراني– إلى الدولة لابد من إعمال مجالين: المجال القانوني والمجال السيبراني التقني. بعض الدراسات في موضوع المسؤولية الدولية عن الهجمات السيبرانية تستبعد الإسناد التقني باعتبار أن نسبة الفعل إلى الدولة عملية قانونية أو على الأقل يجب أن ينظر إليها القانونيون كذلك[1]. إذا كان ذلك ممكناً في تنسيب الأفعال غير المشروعة الأخرى فإنه غير ممكن في الهجمات السيبرانية غير المشروعة. نعم هي عملية قانونية في نسبة الفعل إلى الدولة إذا كان الفعل غير المشروع خرقا لالتزام تعاهدي في اتفاقيات التجارة بين دولتين، وهي كذلك في عملية قانونية إذا كان الالتزام غير المشروع متمثل بتحرك دبابة من الدولة (أ) إلى داخل حدود الدولة (ب). لكن لنسبة هجمات سيبرانية إلى دولة معينة لا بد أن يأتي إثباتها من بعد آخر هو نفس البعد الذي تتحرك فيه العمليات السيبرانية، وبدون هذا الدليل لن يكون هناك إثبات ومن ثم تنسيب الفعل إلى الدولة قانوناً. ونظرا للطبيعة الخاصة للهجمات السيبرانية التي تتنكر برداء المجهولية في الفضاء السيبراني لابد أن يتكون نسبة الفعل إلى الدولة من شقين الشق التقني والشق القانوني. وسيعرض هذا القسمان تباعاً.

الفرع الأول: نسبة الهجمات السيبرانية للدولة قانوناً

يمكن الاعتماد في البعد القانوني –لنسبة الهجمات السيبرانية غير المشروعة إلى دولة معينة– على قواعد مسؤولية الدولة. وقد تم تفصيل الشق الأول في المسؤولية الدولية، وهو متى تعد الهجمات السيبرانية فعلا غير مشروع. سيتم الآن النظر في الشق الثاني وهو نسبة ذلك الفعل غير المشروع إلى الدولة. المعتمد في تمييز الهجمات السيبرانية من أنها عمل عدواني دولي، أو جريمة فردية، لا يقاس

---

[1] نجد ذلك بشكل خاص في الكتابات العربية حول هذا الموضوع مثلا المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر.
انظر: طلال العيسى، وعدي عيسى. (2019). المسؤوليّة الدّوليّة النّاشئة عن الهجمات السّيبرانيّة في ضوء القانون الدّولي المعاصر. مجلة الزرقاء للبحوث والدراسات الإنسانية، 19(1). استرجع من
https://zujournal.zu.edu.jo/index.php/2017-2/16-3-2024/864-2019-04-29-12-30-47
كذلك المتحدث Jason Healey في مؤتمر CyCon 2019
NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) [natoccdcoe]. (2019, August 12). *Cyber Deterrence and NATO - CyCon 2019* [Video file]. Retrieved from https://www.youtube.com/watch?v=QT7-RJ6PeAw&list=LL&index=7&t=3390s

من جانب الضحية، إذا كانت الضحية حكومة أو شركة في القطاع الخاص. لكن المعتمد لتحريك المسؤولية الدولية هو النظر فيمن يقف خلف الهجمات، أدولة؟ أم ليست دولة؟ وهل للفاعل المتسبب بالهجمات علاقة بدولة معينة؟

كذلك لا تكفي معرفة الدولة التي صدرت الهجمات من إقليمها؛ لتقرير مسؤوليتها الدولية، لذلك نجد أن دليل (تالين) قد أكد هذه الفكرة في القاعدة الثامنة التي تنص على أن "حقيقة أن العملية الإلكترونية قد تم توجيهها عبر البنية التحتية السيبرانية الموجودة في دولة ما ليست دليلاً كافياً لإسناد العملية إلى تلك الدولة"[1]. المطلوب إذن لنسبة العمليات السيبرانية إلى الدولة أن يتحقق إنشاء صلة بين الفاعل والدولة. هنا تأتي مهمة قواعد مسؤولية الدولة التي تحدد متى يعد الفعل غير المشروع (والمقصود هنا الهجمات السيبرانية) صادراً من الدولة؟ ونعرض فيما يأتي هذه الحالات ثم الإشكالية التي قد تعيق الإسناد القانوني للهجمات السيبرانية.

أولا: حالات نسبة الهجمات السيبرانية قانوناً إلى الدولة

أوردت قواعد مسؤولية الدولة ست مجموعات من الأشخاص الذين تنسب أفعالهم للدولة وبالتالي تتحمل الدولة المسؤولية عنهم. نتناولها تباعا مع إعطاء أمثله عنهم في المجال السيبراني.

المجموعة الأولى: العمليات السيبرانية التي تجريها أجهزة الدولة[2]

أي عناصر السلطة الحكومية سواء أكانت تنفيذية؟ أم تشريعية؟ أم قضائية؟ وسواء أكانت تتبع أجهزة الحكومة المركزية؟ أم الحكومات الإقليمية؟ فإنها تنسب إلى الدولة[3]. ذلك أن جهاز الدولة يتكون من أي شخص له ذلك المركز بمقتضى القانون الداخلي للدولة، وبعبارة أخرى إذا كان كيان معين بمقتضى القانون الداخلي يعد أحد أجهزة الدولة، فهو كذلك بمقتضى القانون الدولي أيضا. أما مجرد ملكية الدولة لمكان معين فإنها لا تؤهل كونه أحد أجهزة الدولة.

---

[1] الأمم المتحدة، الجمعية العامة، الدورة السادسة والخمسون، المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دولياً، المؤرخ تشرين الثاني/ نوفمبر 2001، (A/RES/56/83)، المادة 8

[2] المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دولياً – المادة 4 – ص3

[3] المرجع السابق

من المتصور ارتباط العمليات السيبرانية التي تصدر من الدولة بالمؤسسات العسكرية والأمنية فيها كالجيش والمخابرات، لكن أصبحت معظم الدول تمتلك أجهزة وطنية متخصصة لشن الهجمات السيبرانية، ورصدها، والرد عليها بحسب ما تنص عليه سياسات الأمن السيبراني لديها. مثال ذلك القيادة السيبرانية الأمريكية،[1] ووحدة الفضاء الإلكتروني التابعة لرابطة الدفاع الإستوني[2] ووكالة فرنسا الوطنية السيبرانية.[3]هذه الأجهزة التي لها ما يشبهها في معظم دول العالم تعد أفعالها في الفضاء السيبراني صادرة من الدولة. لكن لا يعني ذلك أن يشترط تخصص الجهاز في الشأن السيبراني، فإذا تعرضت وزارة الصناعة في دولة معينة لهجوم سيبراني أدى إلى منع الوصول إلى خدماتها الإلكترونية –وكان ذلك متزامنا مع هجوم إعلامي من نظيرتها في دولة ما، فقررت وزارة الصناعة في الدولة الأولى ربط الهجمات السيبرانية بالحملة الاعلامية والرد عليه بهجوم سيبراني تعطيلي على نظيرتها– فإن سلوك الوزارة يمثل الدولة وإن لم تكن متخصصة في الشأن السيبراني أو العسكري أو الأمني وحسبها أن تكون أحد أجهزة الدولة.

المجموعة الثانية: العمليات السيبرانية التي يقوم بها بعض الأشخاص والكيانات في أثناء ممارستهم بعض اختصاصات الحكومة.[4]

الحديث هنا أن حالة التفويض[5]، لشخص طبيعي أو اعتباري لا يعد أحد أجهزة الدولة، لكنه بمقتضى القانون الداخلي يعطى بعض اختصاصات السلطة الحكومية. هؤلاء الأشخاص أو الكيانات المفوضين إذا انتهكوا التزاما من التزامات الدولة يعد فعلهم هذا غير مشروع دوليا، وينسب إلى الدولة التي فوضتهم. ويشترط أن يصدر التفويض من الدولة، كما يشترط فيه ألا يكون ضمنيا، بل صريحا[6] صدر

---

[1] U.S. Cyber Command. (n.d.). Home USCYBERCOM. Retrieved from https://www.cybercom.mil/

[2] Estonian Defence League. (n.d.). Estonian Defence League's Cyber Unit. Retrieved from https://www.kaitseliit.ee/en/cyber-unit

[3] Agence nationale de la sécurité des systèmes d'information (ANSSI). (n.d.). The National Cybersecurity Agency of France. Retrieved from https://www.ssi.gouv.fr/en/cybersecurity-in-france/the-national-cybersecurity-agency-of-france/

[4] المرجع السابق – A/RES/56/83 – المادة 5 – ص3

[5] الصديقي، سعيد (مارس 29، 2020) القانون الدولي العام 11: مسؤولية الدولة عن أفعالها غير المشروعة دوليا (فيديو) 24:00. استرجع من https://www.youtube.com/watch?v=BG_jl9THDaM&t=1206s

[6] حتوت، فوزي. (1439 هـ). التفويض الاداري في ضوء النصوص القانونية وأحكام القضاء الاداري "دراسة مقارنة". المجلة القضائية الصادرة عن وزارة العدل السعودية، (14)، 58-152 (ص92-93). استرجع من https://adlm.moj.gov.sa/Alqadaeya/attach/955.pdf

بموجب قانون أو قرار إداري، أو عقد، وليست كل صلاحية حكومية تم التفويض فيها يمكن أن تعد فعلا دوليا غير مشروع، فإنه ينبغي أن تكون الصلاحيات من تلك التي تمارسها الدولة بوصفها صاحبة سيادة وسلطان، وهي تختلف عن التصرفات التي تقوم بها الدولة وتقوم فيها مقام الأفراد العاديين.

وأوضح مثال على ذلك هو الشركات العسكرية والأمنية الخاصة التي تتعاقد معها الدول غالبا، لتنفيذ مهام عسكرية خارج الحدود وقد يكون من أهم الأمثلة على ذلك شركة "بلاك ووتر" التي استخدمتها الولايات المتحدة في العراق. فمن خصائص هذه الشركات أنها شركات تجارية تقدم الخدمات بمقابل مادي[1] كذلك من خصائصها أنها مملوكة ملكية خاصة، فهي ملك للأفراد وليس للحكومات والدول[2].

يحتل موضوع مسؤولية الدولة عن الفعل غير المشروع حيزا مهما عند مناقشة هذه المسؤولية. فقد بات معتادا أن تلجأ الدول للقطاع الخاص لطلب الخدمات السيبرانية منه وستتم مناقشة إيجابيات وسلبيات استخدام القطاع الخاص من قبل الدولة في جزء التنسيب، لكن ما يجب تأكيده هو أنه لمجرد أن هجمات سيبرانية هجومية تصدر من القطاع الخاص فهذا لا ينفي مسؤولية الدولة، إذا كانت صلاحيات القطاع الخاص في اجراء تلك الهجمات جاءت من الحكومة، أما أعمال القطاع الخاص التي لا تعد من صلاحيات الحكومة أو التي لم تتم بتفويض منها فإنه لا يمكن نسبتها إلى الدولة. كحالة الدولة التي تتعاقد مع شركة خاصة لإجراءات الدفاع السيبراني عن الشبكات العسكرية التي حددتها الحكومة، ففي أثناء تقديم هذه الخدمات تُنسب أنشطة الشركة إلى الدولة، أما باقي أنشطة الشركة لا تمثل الدولة حتى عندما تقدم الشركة الخدمة نفسها إلى كيانات خاصة، فأنشطتها لا تنسب إلى الدولة. فشروط الإسناد في هذه الحالة هي أن تكون الأعمال المعنية ذات طابع حكومي، وأن يكون الكيان مخولا من قبل الدولة للقيام بها.[3]

المجموعة الثالثة: الهجمات السيبرانية الصادرة من الأجهزة التي توضع تحت تصرف الدولة من قبل دولة أخرى.[4]

[1] طالب، ياسين. (2018). الشركات العسكرية والأمنية الخاصة ودورها كفاعل مؤثر في العلاقات الدولية. Annales de l'université d'Alger، 32(4)، 38-59(ص44). استرجع من https://www.asjp.cerist.dz/en/downArticle/18/32/4/69946

[2] المرجع السابق – ص 45

[3] Tallinn Manual 2.0, commentary to rule 15, para. 11, p. 90

[4] المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دولياً – المادة 6 – ص3

Tallinn Manual 2.0, commentary to rule 16, p. 93

قد توضع أجهزة الدولة –في بعض الأحيان مؤقتا تحت تصرف الدول الأخرى؛ من أجل أداء وظائف حكومية محددة. أوضح مثال على ذلك القواعد العسكرية. ويرى دليل (تالين) في هذه الحالة أن تصرفات الجهاز منسوبة إلى الدولة المستقبلة وحدها عند استيفاء شرطين واقعيين: (1) حصرية السيطرة؛ (2) وأن يتم تنفيذ الأعمال لمصلحة الدولة المستقبلة وبالنيابة عنها.

إن اشتراط السيطرة نتيجة منطقية؛ لأن مناط المسؤولية هو السيطرة، فحيثما كانت الدولة تسيطر كانت مسؤولة عن مخرجات الكيان أو الإقليم أو الجهاز الذي تسيطر عليه. لذلك فالدولة المستقبلة للجهاز الذي وضع تحت تصرفها هي المسؤولة عما يصدر منها ولا يمس بسيطرة الدولة المستقبلة إذا كان الجهاز يتلقى دعماً مادياً أو لوجستياً من الدولة المرسلة[1]، لكن إذا كان الجهاز المرسل يتلقى تعليماته من الدولة المرسلة فذلك يسقط مسؤولية الدولة المستقبلة، كذلك تسقط مسؤولية الدولة المستقبلة إذا كان الجهاز يعمل وفق أوامر كل من الدولة المرسلة والمستقبلة فلكي تكون الدولة المستقبلة مسؤولة يجب أن تكون لها السيطرة الحصرية[2].

أما بخصوص اشتراط أن يكون الجهاز المرسل ينفذ أعمالا لمصلحة الدولة المستقبلة وبالنيابة عنها، فالمقصود هنا هو الطابع الحكومي في الأعمال التي ينفذها الجهاز المرسل كالقيام بعمليات سيبرانية هجومية، أو دفاعية ضد دولة أخرى، أما إذا كان الجهاز المرسل من دولة أخرى مختصا بالأمور التي تقوم بها الدولة وكأنها فرد عادي كأنشطة البيع والشراء والتأجير وقام الجهاز بخرق التزام دولي على الدول أثناء ذلك فذلك لا يقيم مسؤولية الدولة المستقبلة.[3]

كذلك يضيف دليل (تالين) معيارا آخر وهو "المصلحة المباشرة" لتحميل الدولة المستقبلة المسؤولية، يعني أن تكون الهجمات السيبرانية التي يقوم بها الجهاز المرسل تصب في مصلحتها المباشرة. ذلك لأن الدولة المرسلة لابد أن تكون لها مصلحة غير مباشرة في إرسال الجهاز إلى دولة أخرى، ولكي تنتقل المسؤولية الدولية عن أفعال الجهاز المرسل يجب أن تكون الأنشطة التي يقوم بها بكثافة هو تحقيق مصالح وأغراض الدولة المستقبلة[4]. أما إذا كانت المصلحة التي يعمل لها الجهاز مشتركة بين الدولتين فلن تتحمل الدولة المستقبلة المسؤولية، وإن كان دليل (تالين) لم ينص على ذلك، فإن مما

[1] Tallinn Manual 2.0, commentary to rule 16, para. 2, p. 93
[2] Tallinn Manual 2.0, commentary to rule 16, para. 3, p. 93
[3] Tallinn Manual 2.0, commentary to rule 16, paras. 5-6, p. 94
[4] Tallinn Manual 2.0, commentary to rule 16, para. 4, pp. 93-94

يمكن استنتاجه أن المسؤولية في حالة المصلحة المشتركة تتحملها الدولة المرسلة بسبب أن الجهاز المرسل يقوم ببعض أعمال الحكومة، وهي القاعدة التي تمت مناقشتها في المجموعة الثانية.

المجموعة الرابعة: الهجمات السيبرانية المخالفة أو المتجاوزة للصلاحيات المعطاة من قبل الدولة.[1]

سواء أصدرت من الأجهزة الرسمية والأشخاص والكيانات المفوضة؛ لممارسة بعض اختصاصات الحكومة، أم عن الأجهزة التي توضع تحت تصرف الدولة من قبل دولة أخرى. في المجموعات الثلاث التي تمت مناقشتها إذا أخطأ أحد الأشخاص من هذه الفئات وتجاوز الصلاحيات، أو التعليمات، أو الأوامر المعطاة له، وقام بعمليات سيبرانية فيها انتهاك لالتزام دولي، فإن ذلك الخرق ينسب إلى الدولة لا إلى الفرد أو الكيان الذي قامت به الدولة، وسيكون انتهاكا للقانون الدولي تتحمل الدولة مسؤوليته، وتعد الدولة مصدرها؛ حتى لا تتهرب من مسؤوليتها، وتحقيقا للاستقرار في العلاقات الدولية. فالدولة مسؤولة عما يصدر من الجهات التي تمثلها لأنها تعمل تحت إمرتها وعليها واجب الرقابة، والتدريب، والتوجيه وهي تمثل تلك الجهات في أفعالها الخاطئة تماما كما تمثلها في أفعالها الصحيحة التي تتم وفق التعليمات. القول بغير ذلك يسمح بسوء التصرف، وبانتهاكات للقانون –الدولي– لا آخر لها، دون محاسبة الدول وتحميلها المسؤولية بحجة أن الدولة لم توافق على ذلك التصرف.

مناط التمييز بين التصرف المخالف الذي ينسب للفرد، والتصرف المخالف الذي ينسب للحكومة هو أن يكون ذلك الفعل أحد الأعمال الحكومية، أي الأعمال التي تعد من واجب الحكومة القيام بها والحقيقة أن معيار تحديد تلك الأعمال فيه شيء من الغموض. فإما أن ينص القانون على أن هذا العمل من أعمال الحكومة، وهو الوضع المثالي الذي لا يترك مجالا للبس، لكن إن لم يكن هناك مرجع قانوني عن درجة مسائلة الحكومة عن ممارسة هذا الاختصاص فإن لجنة القانون الدولي تقترح –في تعليقها على قواعد مسؤولية الدولة– النظر إلى تاريخ الدولة المعنية في عد هذا العمل من أعمال الحكومة[2] أي دراسة الأوضاع التاريخية والسياسية والثقافية لكل حالة على حدة، لتقرير أهي من الأمور التي يمكن للحكومة أن تفوض فيها؟

---

[1] المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دولياً – المادة 7 – ص3

[2] التعليق على المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دولياً – التعليق على المادة 5 – الفقرة (6) – ص54

إن مما يعد من أعمال الحكومة – في الوضع العادي– جباية الضرائب، وإقامة الانتخابات العامة والحفاظ على الأمن وإنفاذ القانون[1]. أما أعمال الحكومة السيبرانية فقد يكون منها تعزيز حماية الشبكات الوطنية والمرافق الحيوية والمعلومات الحساسة التي تمس أمن الدولة إلكترونياً، واكتشاف الهجمات السيبرانية التي تمس أحد هذه الأهداف، والتصدي للهجمات السيبرانية الخارجية بالدفاع السلبي أو الدفاع عن النفس بالطرق التقليدية، وإجراءات التتبع الرقمي؛ لمعرفة المسؤول عن تلك الهجمات وإقامة مسؤوليته ومطالبته بالتعويض.

المجموعة الخامسة: الهجمات السيبرانية الصادرة من الأفراد حال غياب السلطة الرسمية أو في حال انعدام قدرتها على القيام بمهامها.

الهجمات السيبرانية الصادرة من شخص أو مجموعة أشخاص إذا كانوا في الواقع يمارسون بعض اختصاصات السلطة الحكومية في حال غياب السلطة الرسمية، أو في حال انعدام قدرتها على القيام بمهامها، وفي ظروف تستدعي ممارسة تلك الاختصاصات[2]. ويكون الوضع في مثل هذه الحالات وضع انهيار الدولة، أو شلل مرافقها فيقوم بعض الأشخاص طبيعيون أو اعتباريون بممارسة اختصاصات الدولة أمور تتوقف عليها حياة العامة[3]. يتبين أن نسبة التصرف إلى الدول في هذه الحالة تتطلب ثلاثة أمور؛ أولها: أن يتصل فعلياً بممارسة بعض اختصاصات السلطات الحكومية، والثاني، يجب أن يكون التصرف قد صدر في غياب السلطات الرسمية أو في حالة تعطلها، والثالث، يجب أن تستدعي الظروف القائمة ممارسة اختصاصات السلطة تلك[4].

مثلا قد تتعرض الدولة لهجمات سيبرانية قوية تهدد كل المعلومات الموجودة في حواسيبها المدنية والعسكرية، ولا يوجد أي خيار لتقليل أضرار تلك الهجمات سوى قطع خدمة الانترنت عن الدولة كلها. فتقوم شركة خاصة –تملك شبكة انترنت خاصة تعمل بالاتصال مع الأقمار الصناعة (أي منفصلة عن شبكة الكابلات التي تزود الدولة بالإنترنت) – بمحاولة اكتشاف الثغرات التي مكنتها من الدخول إلى نظام الدولة لتقوية المنظومة الدفاعة الحكومية، والأهم محاولة تتبع مصدر تلك الهجمات، وتجميع

---

[1] Tallinn Manual 2.0, commentary to rule 4, para. 16, p. 22

[2] "التصرفات التي يتم القيام بها في غياب السلطات الرسمية أو في حالة عدم قيامها بمهامها"
انظر: المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دولياً – المادة 9 – ص4
Tallinn Manual 2.0, commentary to rule 15, para. 17, p. 92

[3] المرجع السابق – محاضرة الأستاذ سعيد الصديقي

[4] التعليق على المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دولياً – التعليق على المادة 9 – الفقرة 3 – ص 62

الأدلة بهذا الخصوص. ففي مثل هذه الأعمال –وطالما أن الظرف سيئ لدرجة أن الدولة تعجز عن أداء وظائفها الحكومية– فإن تصرفات الكيان الخاص تنسب إلى الدولة، فإذا كان في أحد الإجراءات التي قام بها خرقا لالتزام واجب تجاه دولة أخرى، فإن هذا الخرق يعد صادرا من الدولة، وتكون مسؤولة عنه دوليا[1].

المجموعة السادسة: الهجمات السيبرانية التي يتم القيام بها بناء على توجيهات الدولة أو تحت رقابتها.[2]

تم الحديث في الفصل السابق عن الدفاع عن النفس ضد الجماعات الفاعلة غير الحكومية والحديث عن المعيارين اللذين وضعتهما محكمة العدل الدولية؛ لربط تلك الجماعات، أو سلوك الجماعات بدولة معينة، ومن ثم تحميلها مسؤولية الأفعال غير المشروعة التي تقوم بها هذه الجماعات والمعياران هما: معيار "الرقابة الصارمة"، ومعيار "الرقابة الفعالة".

ولكي يربط الأمر بقواعد مسؤولية الدولة يمكن القول إن معيار الرقابة الصارمة –وهو الأشد– "إثبات الاعتماد الكلي لهذه الجماعات على الدولة" يحاكي الحالة الأولى من حالات نسبة الفعل إلى الدولة (المجموعة الأولى أعلاه) وهي الحالة التي يصدر فيها الفعل من أحد أجهزة الدولة، فهنا إذا انطبق المعيار عُد الجهاز أحد أجهزة الدولة "بحكم الواقع"، فالجهاز عندئذ يكون تابعا للدولة، وإن لم يكن مؤهلا على هذا النحو بموجب القانون الداخلي، ففي هذا المعيار يعد الفاعل غير الحكومي أداة بيد الدولة، وأفعاله المخالفة للقانون الدولي تنسب للدولة، وتكون مسؤولة عنها قانوناً[3]. أما المعيار الآخر وهو معيار السيطرة الفعالة "الذي يستخدم عندما لا يعتبر الفاعلين الدوليين من غير الدولة بحكم الواقع من أجهزة الدولة بل عندما تتمتع تلك الجماعات بشيء من الاستقلال عن الدولة[4]" فهو تطبيق لهذه المجموعة (المجموعة السادسة) من حالات نسبة الفعل إلى الدولة.

وتنص المادة 8 من قواعد مسؤولية الدولة على أنه:

---

[1] Tallinn Manual 2.0, commentary to rule 15, para. 17, p. 92

[2] المرجع السابق – A/RES/56/83 – المادة 10 – ص5

[3] المرجع السابق – Delerue, F. – ص129

[4] المرجع السابق

"يعد فعلاً صادراً عن الدولة –بمقتضى القانون الدولي– تصرفُ شخص أو مجموعة أشخاص إذا كان الشخص أو مجموعة الأشخاص يتصرفون في الواقع بناء على تعليمات تلك الدولة أو بتوجيهات منها أو تحت رقابتها لدى القيام بذلك التصرف".

نجد في هذه المادة ثلاثة مصطلحات هي: "تعليمات" "توجيه" "رقابة" الدولة على فعل هذه الجماعات ترى لجنة القانون الدولي في تعليقها على المادة 8 المصطلحات الثلاثة تمثل حالتين أولهما حيث تكون الدولة أكثر تورطا حالة التعليمات حيث تصدر الدولة تعليمات يتصرف الأفراد والجماعات بناء عليها في الفعل غير المشروع. والحالة الثانية وهي أكثر عمومية حالة التوجيه والرقابة حيث يتصرف الأفراد بأنفسهم في الفعل غير المشروع لكن هناك توجيه أو رقابة عامة من الدولة[1]. وفي الحالتين تشدد لجنة القانون الدولي على ضرورة الأخذ بمعيار الفعالية أي أن التعليمات والرقابة والتوجيه يجب أن يكون فعالا في إحداث الفعل غير المشروع من عدمه[2]. ومن الواضح أن مبدأ الفعالية أخذته لجنة القانون الدولي من محكمة العدل الدولية في قضية نيكاراجوا التي اتخذت فيها المحكمة اختبار "السيطرة الفعالة".

وأما ما يتعلق بالمقدار المطلوب لتوافر هذه الحالات الثلاث فإن لجنة القانون الدولي ترى أن الوضع يختلف من حالة لأخرى، وأن على الطرف الذي يدعي مسؤولية الدولة عن أفعال الجماعات غير الحكومية أن يقوم بإثبات وجود أحد الشروط الثلاثة "تعليمات" "توجيه" "" رقابة" بين الدولة والجماعة ومدى فاعليتها في ارتكاب الفعل غير المشروع ويكفي إثبات أحدها لا جميعها[3].

ولا يشترط هنا أن يكون الفعل غير المشروع الذي أخل بالتزام دولي عملا من أعمال الحكومة، لأن هذه الحالة تحدث عادة عندما تجند أو تحرض الحكومة أفرادا عاديين على القيام بالفعل غير المشروع مع بقائهم خارج السلك الرسمي للدولة. أما في حالة تجاوز الجماعات أو الأفراد غير الحكوميين تعليمات أو توجيهات الحكومة في القيام بالفعل الضار فإن لجنة القانون الدولي رأت أن الدولة تتحمل مسؤولية هذا التجاوز خصوصا أنها تتحمله في الحالات المشروعة فمن باب أولى أن تتحمله في حالة

[1] التعليق على المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دولياً – التعليق على المادة 8 – الفقرة (1) – ص59
[2] المرجع السابق – التعليق على المادة 8 – الفقرة (1) – ص59
[3] المرجع السابق – التعليق على المادة 8 – الفقرة (7) – ص61

إصدار تعليمات غير مشروعة، خصوصا أنه يفترض أن هناك درجة من الرقابة على أفعال هذه الجماعات[1].

ثانيا: مشكلة نسبة العملية السيبرانية قانوناً إلى الدولة

المشكلة في هذه القواعد التي يوفرها القانون الدولي أن هناك حلقة مفقودة بين الوقائع وتطبيق قواعد نسبة الفعل إلى الدولة. سببها صعوبة إثبات الصلة بين الفاعل والدولة لصعوبة إثبات مصدر الهجمات ابتداءً. الإثبات يبدأ تقنيا؛ لتحديد المكان الذي صدرت منه الهجمة، ثم الجهاز وأخيرا الشخص الذي قام بها، ثم يأتي دور تلك المجموعات في نسبت تصرف الفرد إلى دولة. فإذا كان الأساس والمنطلق وهو هنا الإثبات التقني ضعيفًا، أو لا يوفر اليقين المطلق حيث يمكن تزويره، فإنه من الصعوبة الوصول إلى تلك القواعد التي يجب أن تبنى على فعل واضح صدر من شخص واضح وهذا لا يتوافر في نطاق الهجمات السيبرانية.

أشار دليل (تالين) إلى هذه المسألة دون أن يوفر لها حلا، وقد نص في هذا الشأن على أنه "ينطبق قانون مسؤولية الدولة موضوعيا على الوقائع كما هي موجودة أو غير موجودة... أما أسئلة الأعباء والمعايير وطرق الإثبات فهي عامة مسألة قضائية، أو أنواع أخرى من الإجراءات التي تقررها الهيئة ذات الصلة، لأنه في الواقع أعباء ومعايير وأساليب الإثبات تختلف حسب الأغراض التي تعمل من أجلها هذه الهيئات"[2].

ثالثا: حل مشكلة نسبة العملية السيبرانية قانوناً إلى الدولة

هناك قاعدة قانونية تمتلك من المرونة ما يجعلها تتناسب مع قواعد مسؤولية الدولة ومع الطبيعة السيبرانية، وهي قاعدة بذل العناية. قاعدة بذل العناية تحمِّل الدولة المسؤولية الدولية بموجب قاعدة الفعل السلبي: الإهمال، والالتزام الذي لم تقم به الدولة، لذلك فتقرير الصلة بين الفاعل والدولة غير مطلوب، بل الأهم أن تحديد الفاعل نفسه غير مطلوب، فغير مطلوب معرفة من الذي لم يقم ببذل العناية الواجبة من أجهزة الدولة، هذا شأن داخلي يخص الدولة المسؤولة. يكفي أن الدولة لم تبذل عناية تمنع وقوع هذه الهجمات، ويكفي إثبات أنه تم استخدام إقليم الدولة لإطلاق الهجمات السيبرانية

[1] الأمم المتحدة، لجنة القانون الدولي – التعليق على المادة 8 – الفقرة (8) – ص61-62

[2] Tallinn Manual 2.0, para. 8, p. 81

والدولة كانت تعلم، أو كان يفترض أن تعلم لكنها لم تقم بالمطلوب. هذا يتطابق مع عبارة يكررها الدارسون في موضوع تنسيب الهجمات السيبرانية بمقتضى القانون الدولي وهي "لا يهم من قام بها المهم على من يقع اللوم".[1]

فالمقترح هنا أن تكون نقطة البداية في اثبات المسؤولية الدولية عن الهجمات السيبرانية بتكييف الهجمات بأنها خرق لقاعدة بذل العناية، وليس قاعدة احترام السيادة، أو عدم التدخل في الشأن الداخلي، أو عدم استخدام القوة. لأن المرحلة الثانية وهي تنسيب الفعل إلى الدولة ستكون أقل تطلبا وأكثر تماشيا مع صعوبة الإثبات التقني. خصوصا مع إمكان دفع العلم المفترض. أي أن الدولة مسؤولة عن الهجمات التي صدرت من إقليمها حتى وإن لم تعلم، لأنه كان يفترض بها أن تعلم مقارنة بدولة أخرى في مكانها. هذا يمكن أن ينطبق إذا كانت الهجمات السيبرانية في الهجمات السيبرانية الكبيرة والمنتظمة والمكثفة التي تكون آثارها كفيلة بأن تصيب دولة بالشلل.

قد تكون المشكلة أن دليل (تالين) يرى بأن قاعدة بذل العناية تنقسم إلى قسمين أحدهما: ملزم والآخر لم تقرر الفقه وممارسات الدول على إلزامه بعد. فهو لا يرى بالمهمة الوقائية لقاعدة بذل العناية أي أن تمنع الدول وقوع الهجمات، لكنه التزام يتفعل في أثناء هجوم سيبراني حال، يصدر من الدولة المسؤولة مما قد يحمل الدولة مسؤولية أقل من القواعد الأخرى التي لا ترتبط بحالة انطلاق الهجمات فقط، بل يمكن أن تمتد إلى التحضير والباعث وبالتالي يمكن أن تتحمل الدولة مسؤولية أكبر[2].

مع ذلك حتى ذلك الحين الذي يمكن للتنسيب التقني أن يحدد الشخص المسؤول بسهولة ويقين معقول يمكن الاعتماد على قاعدة بذل العناية في تحميل الدولة المسؤولية الدولية، وبالتالي الرد عليها بالإجراءات المضادة أو رفع الموضوع إلى الإجراءات القضائية. أما الدفاع عن النفس فلن يكون جائزا إلا في حالة خرق قاعدة استخدام القوة وفي حالة وجود هجوم مسلح.

الفرع الثاني

[1] Healey, J. (2012, February). Beyond Attribution: Seeking National Responsibility in Cyberspace. Atlantic Council, p. 1. Retrieved from https://www.files.ethz.ch/isn/142271/022212_ACUS_NatlResponsibilityCyber.pdf

[2] للمزيد عن دور قاعدة بذل العناية في الفضاء السيبراني:
المرجع السابق – Schmitt, M.N. – In Defense of Due Diligence in Cyberspace

نسبة العملية السيبرانية إلى الدولة تقنياً

الإسناد الإلكتروني هو العملية التي يتم من خلالها جمع الأدلة على نشاط إلكتروني ضار وتحليلها، وربطها بطرف المنشأ.[1] أهم صفات الهجمات السيبرانية أنها مجهولة المصدر، وعملية الإثبات في الهجمات السيبرانية تهدف إلى إهدار هذه الصفة؛ وذلك بكشف مصدر الهجمات. التعقب للوصول إلى مصدر الهجمات السيبرانية أولا هي عملية تعقب الجهاز الذي تم استخدامه في الهجمات، ثم معرفه الشخص الذي قام بالهجمات، ثم معرفة الجهة المسؤولة التي يعمل هذا الشخص وفقا لتعليماتها. وقد سبق إيضاح أن التعقب التقني أهم وسيلة لمعرفة مصدر الهجمات السيبرانية، وإن كان التعقب قد تطور في قدراته حتى أصبح ناجحا في تحديد الموقع والجهاز الذي صدرت منه الهجمة فإنه دائما هناك مجال للتزوير والتلاعب. وعليه نعرض في هذا الفرع بعض الأدوات التقنية المطروحة لتعقب الهجمات السيبرانية وما قد تثيره من إشكالات في تحميل الدولة المسؤولية عن الهجمات السيبرانية.

أولا: بعض أدوات الإثبات التقني

1-عنوان التحكم بالوصول للوسائط MAC:

هو عبارة عن عنوان فريد موجود في جميع الأجهزة القابلة للاتصال بالإنترنت مقترن ببطاقة الشبكة NIC. وبطاقة الشبكة عبارة جزء صلب من الجهاز يصل الجهاز بالإنترنت، ولا يمكن الاتصال بالإنترنت بدونه. عنوان MAC يتكون من 12 رقمًا. أما استخدامه فهو داخلي في الشبكة الداخلية الواحدة، أي على مستوى جهاز التوجيه "Router"[2]. فجهاز التوجيه "Router" يستطيع تحويل البيانات والطلبات بين الأجهزة المتصلة به بواسطة الـ MAC حسب الطلب. مثلا داخل المنزل الواحد يتصل بالراوتر أجهزة الحاسوب والهواتف والطابعات وغيرها، وجميع الأجهزة لديها عنوان MAC يميزه الراوتر. فإذا ما صدر أمر من أحد الأجهزة المتصلة بالراوتر إلى آخر كطلب من الهاتف المحمول إلى الطابعة فأنه يستخدم عناوين MAC لإيصال الأمر إلى الجهاز الصحيح. تكمن أهمية هذا الأمر

---

[1] Tannery, C. (2019, April 17). Cyber Attribution: Essential Component of Incident Response or Optional Extra. Retrieved from https://www.exabeam.com/incident-response/cyber-attribution-essential-component-of-incident-response-or-optional-extra/ (بتصرف)

[2] Garg, U, et al. (2012). MAC and Logical addressing (A Review Study). *Journal of Engineering Research and Applications (IJERA), 2*(3), 474-480 [p. 476]. Retrieved from https://www.ijera.com/papers/Vol2_issue3/CB23474480.pdf

في الإثبات أنه يمكن استخدام تقنيات مختلفة لتتبع عناوين MAC المتصلة بشبكة، وتحديد أصحابها ومراقبتهم[1]. تقنية التتبع هذه يتم استخدامها لأغراض التسويق باستهداف الفئة التي قد تكون مهتمة بالمنتج[2]. عنوان ماك MAC لأن هذا العنوان لا يمكن تغييره في الجهاز نفسه، لكن يمكن انتحاله بإجراء بسيط يستطيع أي شخص القيام به[3]. وبالتالي فإن الإسناد التقني الذي يعتمد على عنوان MAC لا يمكن أن يكون كافيا بمفرده للإثبات.

2-عنوان بروتوكول الانترنت IP Address:

يشير عنوان بروتوكول الإنترنتIP إلى عنوان فريد أو ملصق رقمي مخصص لكل جهاز متصل بشبكة كمبيوتر باستخدام بروتوكول الإنترنت (IP) للاتصال. ولأن عنوان الـIP متعلق بالشبكة التي يتصل بها الجهاز فهو يمكن أن يتغير بتغير الشبكة. هذا بعكس عنوان MAC المرتبط بالجهاز وبالتالي لا يتغير بتغير الشبكة. لذلك يمكن تشبيه عنوان IP بمكان الشخص الذي يمكن أن يتغير بتغير موقعه أما عنوان الـ MAC فيمكن تشبيهه باسم الشخص الذي يحمله معه أينما كان ولا يتغير بتغير المكان[4].

وظيفة عناوين IP الرئيسة نقل البيانات بين الأجهزة، لكن ليس على مستوى الشبكات الداخلية، بل على مستوى أجهزة التوجيه والخوادم المختلفة. ومن ثم، يجب أن تحتوي كل حزمة بيانات على عنوان

---

[1] "في مقابلة مع إدوارد سنودن كشف أن وكالة الأمن القومي لديها القدرة لرسم خريطة لحركة كل فرد في المدينة من خلال مراقبة MAC الخاصة بهم العنوان وهو تعريف فريد ينبعث من كل هاتف خلوي وجهاز كمبيوتر وجهاز إلكتروني آخر" المقابلة موجودة في:

Bamford, J. (2020, January 8). Edward Snowden: The Untold Story. *Wired*. Retrieved from https://www.wired.com/2014/08/edward-snowden/

[2] IAB. (2021, January 26). The Mobile Identity Guide for Marketers. Retrieved from https://www.iab.com/insights/themobileidguide/

[3] Yusuf Imam, M. A., & Biswas, P. K. (2019). MAC ADDRESS CLONING TECHNIQUE RESULTS. *International Journal of Engineering Applied Sciences and Technology, 4(1),* 1–5. https://doi.org/10.33564/ijeast.2019.v04i01.001

Cunche, M., & Matte, C. (2016, November). *On Wi-Fi Tracking and the Pitfalls of MAC Address Randomization*. Presented at the Journée Nationale de l'Internet des Objets Nouveaux défis de l'Internet des Objets: Interaction Homme-Machine et Facteurs Humains, Cité de l'Innovation, Nokia Paris-Saclay. Retrieved from https://ido2016.sciencesconf.org/122873/Privacy_v4.pdf

[4] Neso Academy. (2019, November 17). *Basics of MAC Addressing* [Video file]. Retrieved from https://www.youtube.com/watch?v=FkiTOMn-XGw

IP الخاص بالمصدر والوجهة والمعلومات الرئيسة الأخرى؛ ليتم تسليمها بنجاح[1]. لذلك كل عنوان IP فريد عالميا.

من الممكن استخدام عناوين الـIP لتتبع وتحديد مواقع الأجهزة التي تم عن طريقها تنفيذ الهجمات السيبرانية عن طريق العديد من الطرق التابعة للأمن السيبراني. الخطوة الأولى تبدأ بتحديد عنوان الـIP للجهاز أو الأجهزة التي صدرت منها الهجمات ومن الممكن استخدام بعض تطبيقات الأمن السيبراني مثل (IP GEOLOCATION) لتحديد الموقع والبلد والمدينة التي صدرت منها الهجمات بناء على عنوان الـIP[2]. هنا تكمن أهمية علم الأمن السيبراني بحيث يمكن استخدام بعض البروتوكولات المتطورة الخاصة بالأمن السيبراني لتتبع الهجمات ومحاولة إيقافها. علما أنه من الممكن لمنفذي الهجمات السيبرانية انتحال عناوين IP لأشخاص آخرين.

ومع ذلك يمكن التلاعب بعناوين الـIP بسهولة وهذا ما يلجأ إليه المهاجمون لإخفاء هوية المرسل، وتجاوز أنظمة الحماية، كأن يتم تغييره إلى نفس عنوان المستقبل فلا ترفضه أنظمة الحماية. مثلا في الهجمات التي وقعت على إستونيا 2007 أظهر التحقيق أن بعض عناوين IP جاءت من روسيا، لكن العمليات السيبرانية لم تأت من مكان واحد، بل من 178 دولة[3] وهوما يكاد يكون من المستحيل أن يكون المشاركون في هذه الهجمات ضد استونا من هذا العدد الكبير من البلدان، والأرجح أن الجناة استخدموا تقنيات مختلفة لإخفاء هويتهم وموقعهم تعتمد على شبكات الروبوتات – شبكات من أجهزة الكمبيوتر المخترقة المستخدمة بدون إذن مالكها –.

لتعقيد الأمور، قد يحاول المشاركون أيضًا خلق انطباع بأن دولة معينة تقف وراء الهجوم السيبراني. الحديث هنا عن حالة الانتحال، وهي تقنية إلكترونية مستخدمة على نطاق واسع تهدف إلى التظاهر بالهوية. على سبيل المثال، في عام 2013، تم تصعيد هجمات سيبرانية خبيثة على مواقع الحكومة الأوكرانية وانتحلت الهجمات شخصية مركز التميز للدفاع الإلكتروني التعاوني التابع لحلف الناتو (CCD COE) وجعلها تبدو كما لو أن المنظمة هي التي نفذتها. وهذا خلاف الواقع فلم تصدر الهجمات من المركز. ثم قام المهاجمون الحقيقيون بتوجيه عملياتهم ضد موقع المركز (CCD COE)

[1] Cybersecurity Tutorial For Beginners: IP Addressing. (2021, October 15). Retrieved from https://cybercoastal.com/cybersecurity-tutorial-for-beginners-ip-addressing/

[2] K. (2022, April 6). Catch a Hacker: How to Trace an IP Address. Retrieved from https://www.colocationamerica.com/blog/catch-a-hacker-how-to-trace-an-ip-address

[3] المرجع السابق – Delerue, F. – ص68

التابع لحلف الناتو، وضد قوات الدفاع الإستونية، وضد جيوش دول الناتو الأخرى، لكنهم جعلوا الأمر يبدو كما لو كان أوكرانيًا حيث قاموا بانتحال عناوين IP الخاص بالحكومة الأوكرانية[1].

3-الرقم التسلسلي:

إن تتبع الرقم التسلسلي من الوسائل التي يمكن أن تستخدم في تنسيب الهجمات السيبرانية. ذلك أن كل الأجهزة التي تستخدم في الهجمات السيبرانية لها رقم تسلسلي يمكن تتبعه. فأجهزة الحاسوب أو الهواتف ذات رقم تسلسلي، والفرق بين هذا الرقم ورقم الـMAC هو أن مصدر الرقم التسلسلي في "الماك" هو من معهد مهندسي الكهرباء والإلكترونيات (IEEE)[2] أما الرقم التسلسلي Serial Number فهو يُعطى من الجهة المصنعة، وهو ضروري لعمل هذه الأجهزة فلكل رقم تسلسلي برامج معينة يمكن أن يستخدمها[3]. كذلك يكون الرقم التسلسلي مفيدا حين تَعرُّض الجهاز لسرقة. حتى البرامج لها أرقام تسلسلية يمكن تتبعها، ومن ثم الوصول إلى الجهاز الذي يستخدمها وبالتالي الشخص الذي يستخدمه. لكن الحقيقة أن كل هذه الأمور يمكن إخفاؤها، أو تحريفها أو التلاعب بها. فالرقم التسلسلي المحفور على الجهاز يمكن كشطه وتغييره والرقم التسلسلي الموجود في البرامج يمكن التلاعب بشفرته وتغييره.[4]

4-الأختام الزمنية:

هي كل ما يتعلق بالجدول الزمني في الهجمات السيبرانية. متى حدثت؟ متى اكتشفت؟ متى ظهر نوع البرنامج الخبيث! إن تتبع الأختام الزمنية من شأنه أن يربط الهجمات المتعددة بفاعل واحد. ولقد ساعد تتبع الأختام الزمنية على ربط الهجمات التي حصلت في لجنة الحزب الديمقراطي الوطنية قبل الانتخابات الأمريكية 2016 بهجمات مماثلة حصلت لمنظمات دبلوماسية في وقت متقارب مما رجح أن المصدر واحد[5].

---

[1] Tallinn Manual 2.0, commentary to rule 15, para. 15, p. 91

[2] المرجع السابق – Garg, U, et al.

[3] المرجع السابق – Delerue, F. – ص57

[4] المرجع السابق – Delerue, F. – ص58

[5] ديفيس الثاني، جون إس، وآخرون – المرجع السابق – ص12

5-السلاسل النصية:

قراءة السلاسل النصية الموجودة في الهجوم السيبراني أسلوب تعقب مستخدم في بعض الهجمات مثلا في حالة Stuxnet هجوم سيبراني غير مباشر وغير مرتبط بالإنترنت، لذلك فالتنسيب التقني اعتمد على تحليل السلاسل النصية التي وجدت في فايروس Stuxnet[1]. فيها بعض الكلمات والرموز الموجودة في التوراة مما كان سببا في توجيه الاتهام لإسرائيل. كذلك تكمن أهمية السلاسل النصية في ربط الهجمات بعضها ببعض ومعرفة اشتراكها في مصدر واحد مثلا[2]، بعض الأوامر الموجودة في السلاسل النصية في الهجمات التي وقعت على البنك المركزي على بنغلادش عام 2016[3] هي نفسها الموجودة في الهجمات التي وقعت على شركة سوني[4] 2014 مما رجح فرضية أن مصدر الهجمات واحد وهو كوريا الشمالية.

مع ذلك فإن الطريقتين كلتيهما (الأختام الزمنية والسلاسل النصية) غير مضمونين ويمكن التلاعب بها وهو ما سيحرص عليه المهاجمون للتخفي والتضليل.

ثانيا: مشكلة الإثبات التقني في الفضاء السيبراني

لاريب أن التحدي الرئيس –عند تحديد مصدر الهجمات الإلكترونية– يكمن في صعوبة التوصّل إلى نتيجة بشأن المصدر، ونظرا للطبيعة السيبرانية، فإنها ليست بالمهمة السهلة، والسبب في ذلك، القدرة على إخفاء الهوية والقدرة على تغيير الأدلة أو البصمات الرقمية؛ فعندما يقدم الطب الشرعي الرقمي

---

[1] المرجع السابق – ص11

[2] المرجع السابق – ص11-12

[3] عمليات سيبرانية تمكنت من سرقة 81 مليون دولار من مصرف بنغلادش المركزي. للمزيد:
Banka, N. (2021, June 30). Explained: The story of how North Korea hackers stole $81 million from Bangladesh Bank. *The Indian Express*. Retrieved from https://indianexpress.com/article/explained/bangladesh-bank-robbery-north-korea-lazarus-heist-7375441/

[4] هجمات سيبرانية استهدفت شركة سوني للإنتاج السينمائي وأدت إلى توقف كبير عن العمل بالإضافة إلى تسريبات حساسة من ايميلات الموظفين، وأفلام لم تعرض بعد في الصالات السينمائية. وقد هدد المهاجمون بالمزيد من الهجمات في حالة مضي الشركة قدما في خطتها في عرض فيلم كوميدي عن اغتيال رئيس كوريا الشمالية. تم فتح تحقيق حكومي وتوصل لنتيجة مفادها أن كوريا الشمالية تقف خلف الهجمات، لكن الحكومة الامريكية رفضت الكشف عن الأدلة المستخدمة في عملية التنسيب. للمزيد:
Mehrotra, K., & Voreacos, D. (2021, February 18). U.S. Calls North Korean Hackers 'World's Leading Bank Robbers'. *Bloomberg - Middle East Edition*. Retrieved from https://www.bloomberg.com/news/articles/2021-02-17/u-s-charges-3-north-koreans-linked-to-sony-hack-in-new-scheme

دليلا على أن الهجمة قد صدرت من دولة معينة، فهذا لا يعني بالضرورة أن تكون الهجمات قد صدرت من تلك الدولة فعلا فربما يكون شخص أو مجموعة أشخاص على إقليم هذه الدولة يعملون لصالح دولة أخرى، أو يعملون مستقلين لصالح أنفسهم. فالاحتمالات لا حدود لها أمام أي دليل سيبراني وحتى هذه اللحظة من المستحيل الجزم بقطعيته.

فقد تكون نتيجة التعقب غير صحيحة إذا ما تم التلاعب بالأدلة كعنوان الـIP وتغييره بحيث يبدو أنه قد خرج من دولة معينة أو مجموعة دول بينما في الحقيقة يكون قد خرج من دولة أخرى. بل إن بعض الجناة أدخلوا تلميحات مضللة في رمز الفيروس في محاولة لإلقاء اللوم على طرف ثالث! ثم تأتي مشكلة التفسير الخاطئ المحتمل للأدلة المتاحة والذي يوجد خطرًا حقيقيًا على العلاقات الدولية[1]. خصوصا وإننا نشهد استعدادا متزايدا من الدول التي وقعت ضحية للعمليات السيبرانية العدائية لإسنادها إلى دول أخرى[2].

المشكلة الأخرى التي تزيد من صعوبة الإسناد وتعقيده هي مذهب الدول المستمر لرفض الكشف عن التقنيات التي استخدمتها في التحقيق التقني. فنتيجة الإسناد نادرًا ما تكون مصحوبة في الممارسة العملية بالإفراج عن الأدلة الأساسية؛ مما يجعل البيانات العلنية عن تحديد المصدر تقابل بالريبة والتشكيك، والمطالبة بشفافية أكبر بشأن التحقيق والأدلة التي يستند إليها[3]. وإن الرفض عن الإفصاح عن الأدلة فيه شيء من المنطق! لأنه عندما تصبح الأطراف الخبيثة على دراية بتقنيات التنسيب التقني المستخدمة في الاستراتيجيات الدفاعية، فإنها غير ذات جدوى[4]. هذا هو الواقع الحالي على الرغم من الدعم الدولي الواسع النطاق لمبدأ أنه ينبغي للدول –حيثما أمكن– توفير الأساس لذلك الإسناد. وعلى سبيل المثال، فإن مجموعة الخبراء الحكوميين التابعة للأمم المتحدة لعام 2015 والقائمة

[1] Manshu, X. (2022). Beyond Public Cyber Attribution: Reflections and Responses. In *Managing U.S.-China Tensions Over Public Cyber Attribution* (pp. 25–32). Retrieved from https://carnegieendowment.org/files/Perkovich_et_al_Cyber_Attribution_web.pdf

[2] المرجع السابق

[3] Tallinn Manual 2.0, para. 3, p. 83

[4] Pitropakis, N., et al. (2018). An Enhanced Cyber Attack Attribution Framework. In S. Furnell, H. Mouratidis, & G. Pernul (Eds.), *Trust, Privacy and Security in Digital Business* (pp. 213–228). Regensburg, Germany. https://doi.org/10.1007/978-3-319-98385-1_15

على التطورات في مجال المعلومات والاتصالات في سياق الأمن الدولي، والذي أقر تقريره بالإجماع هؤلاء الخبراء أشاروا إلى أن "الاتهامات بتنظيم وتنفيذ أفعال غير مشروعة ضد الدول ينبغي إثباتها[1]."

ومع ذلك لم تتجاوب الدول مع هذه الدعوات، فوصفت مسؤولية الإفراج عن الأدلة الكامنة وراء الإسناد بأنها قاعدة مكملة، وغير ملزمة لسلوك الدولة المسؤولة، وليس بوصفه التزامًا قانونيًا[2]. لذلك، فإن الدول الرئيسة، مثل الولايات المتحدة والمملكة المتحدة، اتخذت موقفًا مفاده أنه لا يوجد واجب قانوني لمرافقة التصريحات العامة للإسناد مع الكشف عن أي دليل تقني.[3] ويُسوَّغ ذلك عند هؤلاء بعدد من الأسباب، لكن أكثر هذه الأسباب شيوعًا هو أن مثل هذه الممارسة يمكن أن تخاطر بالكشف عن الذكاء للمصادر والأساليب والقدرات السيبرانية. وقد يكون ذلك صحيحا لكن لا يمكن تجاهل احتمالية أن عملية الإسناد قد تنطوي على انتهاك لسيادة الدولة التي يشتبه في صدور الهجمات السيبرانية منها؛ مما يضعف الموقف القانوني للدولة الضحية. ومهما كانت الأسباب –فأنه في غياب الأدلة الداعمة– ستظل مصداقية الإسناد العام مفتوحة للطعن.

وتجدر الإشارة إلى أن مشكلة الإسناد حاليا ليست مشكلة القدرة على الوصول إلى الفاعل بقدر ما هي مشكلة عدم الثقة في نتيجة التنسيب وعدم قبول الأدلة أو كفايتها لإدانة الطرف الآخر. فبرغم القدرة على تحريف الأدلة يراهن خبراء الأمن السيبراني على تطور قدرات التعقب إلى حد يمكنها من تجاوز ذلك التحريف[4] والدليل على ذلك أن هناك نجاحات عديدة في إلقاء القبض على الأفراد المرتكبين للجرائم السيبرانية العابرة للحدود حيث لا مسؤولية دولية على الدولة لكنها مسؤولية جنائية على الفرد. على الأقل إن لم يتم القبض عليهم يتم تعرفهم على أنهم مصدر الهجمات السيبرانية، ووضعهم على لائحة المطلوبين للعدالة[5]. ذلك لأنه في نطاق الجريمة الإلكترونية يمكن التحقق من نتيجة التعقب

---

[1] Shany, Y., & Schmitt, M. N. (2020). An International Attribution Mechanism for Hostile Cyber Operations. *International Law Studies*, *96*(1), 196–222 [p. 213-214]. Retrieved from https://digital-commons.usnwc.edu/ils/vol96/iss1/8/

[2] المرجع السابق – ص213

[3] المرجع السابق – ص214

[4] AO Kaspersky Lab. (2021). *The power of threat attribution*, p. 1. Retrieved from https://media.kaspersky.com/en/business-security/enterprise/threat-attribution-engine-whitepaper.pdf

[5] من أمثلة لائحة المطلوبين للعدالة لمكتب التحقيق الفيدرالي جون تشانغ هيوك31 عامًا؛ وكيم إيل 27 عامًا؛ وبارك جين هيوك، 36 عامًا ، تزعم ال FBI أنهم كانوا أعضاء في وحدات المكتب العام للاستطلاع (RGB) ، وهي وكالة استخبارات عسكرية تابعة لجمهورية كوريا الديمقراطية الشعبية (DPRK)، شاركت في عمليات قرصنة إجرامية. منها هجمات سوني الشهيرة.
PARK JIN HYOK. (2021, November 16). [Press release]. Retrieved from https://www.fbi.gov/wanted/cyber/park-jin-hyok

التقني بسهولة أكبر من التحقق منه على الصعيد الدولي. فاستخراج الأمر القضائي بإلقاء القبض على شخص مشتبه به أسهل بكثير من خطاب على صعيد السياسة الخارجية يدين دولة ما لارتكابها هجمات سيبرانية. لذلك يبدو أن مشكلة القدرة على تزييف الأدلة في التتبع السيبراني ليست المشكلة بقدر ما هي مشكلة عدم ثقة في الدليل، وقدرة الطرف المهاجم على النفي.

ثالثا: الحل المتبع من الدول حالياً للتغلب على مشكلة الإسناد التقني

للتغلب على مشكلة الإسناد السيبراني يجب أن تعد نتيجة التعقب التقني أحد محاور الإثبات في الهجمات السيبرانية[1]، يضاف إليها التنسيب القانوني والظروف السياسية المصاحبة، ولذلك لابد من الإجابة عن الأسئلة التالية: هل الدولة في حالة حرب؟ أو عداء مشتعل، أو عداء تاريخي؟ هل إطلاق الهجمات السيبرانية يتناسب مع سلوك الدولة التي يدعى أنها قامت بها؟ وهل في تلك الهجمات السيبرانية ما يناسب مصلحتها الوطنية أو خطابها السياسي تجاه الدولة الضحية؟ فإذا ما تطابق ذلك مع مؤشرات نتيجة التعقب التقني يكون الشك معقولًا، ويمكن للدولة أن تتصرف بناء عليه. فمثلا لم يستغرق اتهام الولايات المتحدة وإسرائيل بالوقوف خلف هجمات Stuxnet الكثير من الوقت، فهما أكثر من له مصلحة في تخريب برنامج إيران النووي[2]. ومثال آخر هجمات شمعون التي وقعت على أرامكو السعودية فقد كان فيها ملف التوتر السعودي الإيراني هو نقطة البداية في التنسيب[3].

وفي أثناء التحقيق في مصدر Stuxnet –وهو البرنامج الضار الذي تم تصميمه لتخريب منشأة تخصيب اليورانيوم الإيرانية– أخذ المحللون في الحسبان حقائق مختلفة، بما في ذلك مقال نشره ضابط استخبارات أمريكي سابق قبل عام واحد من اكتشاف Stuxnet، يحدد مخططًا استراتيجيًا إلكترونيا.

KIM IL. (2021, November 16). [Press release]. Retrieved from https://www.fbi.gov/wanted/cyber/kim-il

JON CHANG HYOK. (2021, November 16). [Press release]. Retrieved from https://www.fbi.gov/wanted/cyber/jon-chang-hyok

[1] Carter, R. A., & Enoizi, J. (2021). Mapping a Path to Cyber Attribution Consensus. The Geneva Association, p. 13. Retrieved from https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf_public/cyber-attribution_web_final.pdf

[2] ديفيس الثاني، جون إس، وآخرون – المرجع السابق – ص13

[3] ديفيس الثاني، جون إس، وآخرون – المرجع السابق – ص13

ضد أجهزة الطرد المركزي، هذا المقال بالإضافة إلى المستوى العالي من التطور في البرنامج أدى إلى استنتاج أن إسرائيل ليست الفاعل الوحيد وأن حكومة الولايات المتحدة متورطة[1].

يقترح Jose Pagliery أحد محللي التهديدات الإلكترونية المخضرمين مجموعة من الخطوات الأساسية لإثبات الإسناد، نرى أنها تمزج بين البعد التقني، والسياسي، والظرفي للهجمات؛ فيرى أنه يجب أولاً، تحديد من هم مهندسو البرامج الضارة المستخدمة في الهجوم، وذلك من خلال تحديد نمط البرمجيات الخبيثة. ثانيًا، يجب الأخذ في الحسبان توقيت الهجوم الذي قد يُظهر السياق الذي وقع فيه. ثالثًا، النظر إلى فئة الضحايا المستهدفين لاكتشاف المستفيدين من الهجوم[2].

وأما البعد الاستخباراتي فإنه يمكن أن يؤدي أثرًا مهما في تعزيز الإثبات في الهجمات الإلكترونية، ومتابعة الشبكات المستخدمة في الهجوم إذا ما استخدم المهاجمون الشبكات ليتواصلوا مع بعضهم ببعض؛ فإنه يمكن تتبع تواصلهم للحصول على أدلة عن المصدر، أو الراعي للهجوم، أو الوصول إلى طرف في الدولة المشتبه في رعايتها للهجمات، ومراقبة عن طريق الاستخبارات حتى تتحصل الدولة على دليل في ضلوع الدولة الراعية. أو الدخول إلى الانترنت المظلم ومراقبة المعلومات والطلبات التي تمت من خلاله وتحليلها[3]. هذا الأمر إذا كانت الدولة تملك جهاز استخباراتياً قوياً، وهو ليس الواقع غالباً. لذلك يمكن العودة إلى تأكيد أهمية التعاون الدولي في هذا المجال، ومسؤولية الدول القادرة في توفير المساعدة للدول غير القادرة. كذلك يمكن اللجوء إلى فكرة الاستعانة بالقطاع الخاص والشركات التي تقوم بأنشطة استخباراتية.

ولابد –على الدوام– من النظر إلى الظروف المصاحبة للهجمات السيبرانية. فذلك –وإن كان لا يبني دليلا قطعيا– فإنه يؤسس دليلا مبنيا على المعقولية، فالشك يكون معقولا إذا ما ترافق مع سيناريوهات جيوسياسية تؤكده[4]. لكن يجب ألا يعتمد على البعد السياسي وحده دون النظر إلى الجانب التقني،

---

[1] Mueller, P., & Yadegari, B. (2012). *The Stuxnet Worm*. University of Arizona. Retrieved from https://www2.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/2012/topic9-final/report.pdf

[2] Pagliery, J. (2014, October 31). It looks like Russia and smells like Russia . . . but is it Russia? *CNN*. Retrieved from https://money.cnn.com/2014/10/31/technology/security/russia-hackers/index.html

[3] ديفيس الثاني، جون إس، وآخرون – المرجع السابق – ص14-16

[4] وفي ذلك صرحت وزيرة الخارجية الاستونية في حديثها عن معقولية الشك، وتنسيب الهجمات التي تعرضت لها إستونيا عام 2007 "اذا كنت تمشي كالدب (كناية عن الدب الروسي) وتتحدث كالدب اذن انت دب"

فالموضوع هنا فيه خطورة على العلاقات الدولية لإمكان استغلال العداءات بين الدول في تنفيذ هجمات سيبرانية وفيه خطورة على سيادة القانون بدلا من المصالح والاعتبارات السياسية فلابد أن يصل التنسيب التقني إلى نتيجة إن لم تكن مطابقة ولا منفتحة عليها فعلى الأقل لا تتعارض مع الاحتمالات السياسية والظرفية والتاريخية والاستخباراتية، لذلك يعرف Clara Assumpção إسناد الهجمات السيبرانية بين الدول بأنه "حكم سياسي يعتمد على المعلومات التقنية والاستراتيجية"[1]. ويشدد على ضرورة تحليل الجانبين التقني والبشري للعملية، مثل أنماط حياة الهجوم، ومستوى الموارد المستثمرة فيه. يساعد هذا التحليل، جنبًا إلى جنب مع دراسة السياق الجيوسياسي والتاريخ والسياسة والمعلومات التي تم جمعها من خلال الاستخبارات، في إلقاء الضوء على التأثير لتبني الهجوم أو دعمة من دولة معادية[2].

هذا يؤكد ضرورة قدرات التنسيب التقني على تخطي برامج التحريف وإخفاء الهوية وصولاً إلى الفاعل الأصلي. فإذا تبين أن كل تلك الاحتمالات متجهة نحو دولة معينة في قيامها بالهجمات السيبرانية أو مسؤوليتها عنها، فإنه يمكن القول: إن هناك شكًا معقولًا[3] يمكن للدولة التحرك به، والرد على الهجمات السيبرانية بناء عليه.

لكن يجب التنويه إلى أنه في العلاقات الدولية، من الحكمة دبلوماسياً وقانونياً الرد على عمل عدواني من قبل دولة أخرى بما يتناسب مع مستوى اليقين بأن الدولة المعتدية تقف فعلًا وراء الفعل، كلما زاد تأكد الأدلة، أمكن أن تكون الاستجابة أكثر شدة، بشرط ألا تتجاوز الاستجابة حدود القانون الدولي المسموح بها من ضرورة وتناسب[4]. ويجب أن تكون ثقة الدولة في دقة إسنادها لعملية إلكترونية معادية هي الدافع على مدى استعدادها لفرض عواقب وخيمة تتزايد على الدولة التي تعد مسؤولة[5].

---

natoccdcoe. (2017, November 7). *Tallinn Manual 2.0 & Gray Zones in International Law - CyCon 2017* [Video file]. Retrieved from https://youtu.be/w38HSUlnX6U

[1] Assumpção, C. (2020, May 11). The Problem of Cyber Attribution Between States. Retrieved from https://www.e-ir.info/2020/05/06/the-problem-of-cyber-attribution-between-states/

[2] المرجع السابق

[3] National Research Council. (2010). *Proceedings of a Workshop on Deterring Cyberattacks*. Washington, DC: The National Academies Press. https://doi.org/10.17226/12997

[4] Kittichaisaree, K. (2017). Public International Law of Cyberspace. In Law, Governance and Technology Series, 32, p. 43. Cham, Switzerland: Springer.

[5] Davis, J. (2022). Tallinn Paper: Developing Applicable Standards of Proof for Peacetime Cyber Attribution. *The 13th Tallinn Paper*, p. 17. Retrieved from https://ccdcoe.org/uploads/2022/03/Jeremy-K.-Davis-Standards_of_Attribution.pdf

تجدر الإشارة إلى أن استخدام الابعاد الاستخباراتي والسياسي والظرفي ليس الحل المطروح في سياق المسؤولية الدولية عن الهجمات السيبرانية فحسب، بل هو ما تأخذ به أدبيات علم الحاسوب والأمن السيبراني لمعرفة الفاعل في حالات أبسط من أن تأخذ بعدا دوليا، كالجرائم الإلكترونية بين الأشخاص في الأنظمة القانونية الداخلية، [1]ذلك لأن اليقين بالدليل التقني غير القابل لإثبات العكس غير مطروح حالياً، ولابد للتوصل لأي نتيجة من الاستعانة بالظروف المحيطة بالهجوم السيبراني مع الدليل التقني.

فإذا كان الأمر بين الشك واليقين وجب أن يطرح السؤال حول مقدار اليقين الذي يتطلبه القانون الدولي في تنسيب الفعل إلى الدولة واكتمال أركان المسؤولية الدولية. الحقيقة اننا لنعرف كم من اليقين يكفي للإثبات في القانون الدولي يجب أن نحدد أولا لماذا الحاجة إلى الإثبات؟ أو لماذا الحاجة إلى إثبات قيام مسؤولية الدولة عن النشاط السيبراني الضار؟ أو كيف تستخدم مسؤولية الدولة بعد إثباتها. تجيب عن ذلك Liis Vihul في ورقتها في المؤتمر الدولي الحادي عشر حول الصراع السيبراني (CyCon 2019) الذي نظمه مركز التميز للدفاع السيبراني التعاوني التابع لحلف الناتو (CCDCOE). فهي ترى أن الحاجة إلى إثبات نسبة الفعل إلى الدولة منحصرة في أربع حالات:

الحالة الأولى: عندما يكون الهدف من نسبة الفعل إلى الدولة هو إدانة الدولة علناً "Name and Shame" فيكون التصريح بمسؤولية الدولة علناً، وبأنها قد انتهكت القانون الدولي. مثال ذلك ما قامت به بريطانيا في 2018 فقد صرح المركز الوطني للأمن السيبراني البريطاني (NCSC) قيام جهاز المخابرات العسكرية الروسية بعدد من الهجمات الإلكترونية العشوائية والمتهورة التي استهدفت المؤسسات السياسية، والشركات، ووسائل الإعلام، والرياضة، وأن في تنفيذ هذه الهجمات انتهاك صارخ للقانون الدولي؛ لأن الهجمات أثرت على المواطنين في عدد كبير من البلدان، وكلفت الاقتصادات الوطنية ملايين الجنيهات[2].

[1] Kuerbis, B. (2022). Understanding transnational cyber attribution: Moving from "whodunit" to who did it. In *Cyber Security Politics: Socio-Technological Transformations and Political Fragmentation* (1st ed., pp. 220–239). Retrieved from https://www.taylorfrancis.com/chapters/oa-edit/10.4324/9781003110224-17/understanding-transnational-cyber-attribution-brenden-kuerbis-farzaneh-badiei-karl-grindal-milton-mueller

[2] National Cyber Security Centre. (2018, October 3). *Reckless campaign of cyber attacks by Russian military intelligence service exposed* [Press release]. Retrieved from https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed

وتنبثق من هذه الحالة ملحوظتان: أولاهما: أن مثل هذه التصريحات لها وزن لا يستهان به في ردع الهجمات السيبرانية العدوانية، وإن كانت مجرد تصريحات فإنه عندما تخضع نتيجة التنسيب إلى القانون الدولي وتوصم الدولة أنها تتصرف تصرفًا غير مشروع، فقد يكون لذلك تأثير أكبر من بعض الإجراءات المضادة. والثانية: وفقا لـ Liis Vihul أنه مثل هذا التصرف قانوني دائمًا وإن خلا من قوة الدليل، الكذب ليس غير قانوني أو ليس هناك مستوى معين من الثقة مطلوب في مجال التصريحات والإدانات. قد يكون ذلك صحيحا فالتصريح الكاذب غير أخلاقي لكن وفقا للقانون الدولي فليس هناك قاعدة قانونية تمنعه.

الحالة الثانية: تطرح السؤال الآتي: هل ثمة حاجة إلى اليقين لبدء إجراءات المساعدة الذاتية مثل الدفاع عن النفس والإجراءات المضادة. هنا أيضا القانون الدولي يتسع لعدم اليقين أو الإثبات القاطع في التنسيب؛ لأن هذه الإجراءات مرتبطة بحالة الضرورة، وليس اليقين التام. أما عن نسبة الهجوم السيبراني الضار لدولة معينة ومن ثم الرد عليها بناء على ضرورة فأكثر الدارسون يذهبون إلى كفاية أن يكون "الاستنتاج معقولا"[1] بناء على الظروف المحيطة، أي لو كانت دولة أخرى في الظروف نفسها هل ستصل إلى النتيجة نفسها عن مصدر الهجمات، فهل هذا الاستنتاج معقول؟ إن كان معقولا فهو كاف، وليس مطلوبا أن يكون الاستنتاج أكيدا ويقينياً.

الحالة الثالثة هي طريق الدعاوى القضائية، وفيه يطرح السؤال الآتي: هل هناك حاجة إلى اليقين في الإثبات لتؤخذ القضية إلى محكمة العدل الدولية. إذا كان الأمر كذلك فإن محكمة العدل ستطبق معاييرها الخاصة في الإثبات، وهي متعددة منها: معيار "الشك المعقول" أو "السيطرة الفعالة" وغيرها. أما المحكمة الجنائية الدولية أو غيرها من المحاكم الجنائية فلها معاييرها الجنائية الخاصة التي عادة ما تكون أكثر تطلبا. كأن تفحص المحكمة الدليل بمعيار "الدليل القاطع غير القابل لإثبات العكس".[2] لذلك فمدى اليقين المطلوب يختلف بحسب الجهة القضائية التي ستنظر في القضية وبحسب كل قضية وفقا لما تراه المحكمة.

---

[1] Lin, H. (2014). Attribution of malicious cyber incidents: from soup to nuts. *Journal of International Affairs, 70*(1). Retrieved from https://jia.sipa.columbia.edu/attribution-malicious-cyber-incidents

[2] beyond a reasonable doubt. (2020). In *Legal Information Institute*. Cornell Law School. Retrieved from https://www.law.cornell.edu/wex/beyond_a_reasonable_doubt

الحالة الرابعة: إذا كانت القضية بصدد التفاوض، لجبر الضرر الذي تسببت به الهجمات السيبرانية كإجراءات رد الحالة أو التعويض فإن معيار الإثبات سيكون ما يتفق عليه الطرفان.

يتبين من الحالات الأربع –التي هي ردود على الهجمات السيبرانية– أن القانون الدولي فيه سعة لعدم حصول اليقين، تختلف باختلاف الموقف. لذلك فإن طبيعة الهجمات السيبرانية وضعف اليقين القاطع في إثباتها لا يعني صعوبة تطبيق قواعد مسؤولية الدولة عليها.

وبما أن نطاق الدراسة هو الهجمات السيبرانية على ضوء قانون اللجوء إلى الحرب، لذلك تستبعد كل ما يتعلق بالقانون الدولي الإنساني وبالتالي المحاكم الجنائية الدولية، وكذلك تستبعد الحالة الأولى من الحالات الأربع وهي الإدانة العلنية للدولة كونها خارجة عن نطاق القانون الدولي ومتعلقة بالسياسة الدولية. لكن هذه الدراسة معنية بالحالات الأخرى. فقد سبق تغطية الرد بالدفاع عن النفس وسيتم في المبحثين القادمين مناقشة إجراءات المساعدة الذاتية كرد على الهجمات السيبرانية والتعويض وإمكانية اللجوء لمحكمة العدل الدولية.

المطلب الثالث

بعض الحلول المستقبلية المقترحة للتصدي لمشكلة الإثبات وضعف الأدلة التقنية

خلص دليل (تالين) 2.0 في سياق الرد على الهجمات السيبرانية إلى الآتي "الحقيقة هي أن الدول يجب أن تتخذ قرارات مسبقة –من جانب واحد– فيما يتعلق بإسناد عملية إلكترونية إلى دولة أخرى، قبل الرد، وأن مثل هذه القرارات قد تخضع للمراجعة اللاحقة لتطبيق عبء الإثبات. وبالتالي، يُتوقع من الدول أن تتصرف بموضوعية معقولة مقارنة بدولة أخرى في الظروف نفسها أو ظروف مماثلة، المعقولية تعتمد دائما على السياق الذي أتت فيه الهجمات السيبرانية، مع الأخذ في الحسبان العوامل التراكمية مثل: الموثوقية، والكمية، والمباشرة، والطبيعة، وخصوصية الدليل عند النظر إليه على ضوء الظروف المصاحبة، ويمكن تعويض القصور في الذكاء التقني بذكاء بشري موثوق به[1].

[1] Tallinn Manual 2.0, pp. 81-83

تتضح المشكلة في عملية منهجية الإسناد الحالية أنها قرار أحادي من الدول بخصوص أمر ليس فيه تيقن، وهذا القرار تتخذ –بناءً عليه– ردود وإجراءات كبيرة، تؤثر في العلاقات الدولية، وصحة هذا القرار ستخضع للمراجعة والفحص لاحقا من قبل الخبراء الباحثين والأهم منهم المجتمع الدولي.

وهناك بعض المقترحات التي يمكن أن تخفف من أحادية القرار، وبالتالي توفر المزيد من الحياد، والمزيد من الثقة في مدى صحته، وقبول أكثر لتبعاته. كما أنها يمكن أن تساعد في الجانب التقني لتوفر أفضل تقنيات وتكتيكات التعقب التي قد لا تتوافر في جميع الدول. هذه المقترحات هي: 1القطاع الخاص 2–لجان التحقيق الدولية 3–وحدة تحقيق دولية لنسبة حوادث الهجمات السيبرانية. المقترح الأول والثاني يقبلان التطبيق المباشر، للتصدي لأي عمليات سيبرانية اليوم. أما المقترح الأخير فهو نوع من الطموح المستقبلي لكن قد لا يطول الأمر قبل أن يتحقق بسبب كثرة دعوة الباحثين إلى تحقيقه. نعالج الثلاثة مقترحات بشيء من التفصيل.

الفرع الأول: القطاع الخاص

على مدى العقد الماضي، طورت شركات الأمن السيبراني –في القطاع الخاص– قدرات متقدمة إلى حدٍّ يمكنهم من عزو النشاط السيبراني الضار إلى الدول أو الجهات الفاعلة التي ترعاها الدولة. قد تنافس هذه القدرات قدرات بعض وكالات الاستخبارات الحكومية[1]، وتقدم قدرات جديدة فيها تغيير للوضع التاريخي وهو أن الدولة هي الوحيدة التي لديها القدرة على ربط الأعمال العدائية بجهات أجنبية معينة. يمكن أخذ تلك القدرات في الحسبان وذلك للاستفادة من القطاع الخاص بفتح المجال له للمساهمة في عمليات التنسيب والاستفادة من نتائج التحقيقات التي يجريها[2].

---

[1] Romanosky, S., & Boudreaux, B. (2020). Private-Sector Attribution of Cyber Incidents: Benefits and Risks to the U.S. Government. *International Journal of Intelligence and CounterIntelligence*, *34*(3), 463-493 [p. 482]. https://doi.org/10.1080/08850607.2020.1783877

[2] من أشهر شركات القطاع الخاص ذات السمعة العالية في القدرة على تنسيب الهجمات السيبرانية، شركتا: MandiantFootnote9 و CrowdStrikeFootnote10 فهما من الشركات الخاصة المعروفة بقدرتها على عملية الإسناد ونشر تفاصيل التحقيق.

McWhorter, D. (n.d.). *APT1: Exposing One of China's Cyber Espionage Units*. Mandiant. Retrieved from https://www.mandiant.com/resources/apt1-exposing-one-of-chinas-cyber-espionage-units

NH (2021b, September 2). Hat-tribution to PLA Unit 61486. Retrieved from https://www.crowdstrike.com/blog/hat-tribution-pla-unit-61486/

وهناك الكثير من المزايا التي يتمتع بها القطاع الخاص، نذكر منها:

أولا: الفعالية، فهناك بعض السوابق في الولايات المتحدة التي تشهد بتفوق قدرة القطاع الخاص على التعقب من الحكومة الفيدرالية[1]. فالعمليات السيبرانية أدواتها الحواسيب، والإنترنت والبرامج الضارة، وبرامج وتقنيات التعقب، هذه الأمور ليست كالأسلحة التقليدية، فهي متاحة تماما للقطاع الخاص الذي قد يكون أكثر مهارة في استخدامها، والسبب في ذلك أن مميزات القطاع الخاص أقدر على جذب أصحاب المهارات العالية في القرصنة الإلكترونية من القطاع الحكومي، مما ينعكس على الفاعلية في تنسيب الهجمات السيبرانية. مثلا بخصوص التجسس الصيني الأمريكي اعتمد تقرير الحكومة الأمريكية "نتائج التحقيق في الأفعال والسياسات والممارسات الصينية المتعلقة بنقل التكنولوجيا والملكية الفكرية والابتكار بموجب القسم 301 من قانون التجارة لعام 1974" وقد أشار هذا التقرير الحكومي إلى المعلومات التي أصدرتها شركة FireEye الخاصة[2].

ثانيا: قد يكون القطاع الخاص أقدر على التصرف السريع من القطاع الحكومي. فالعمل الحكومي يتقيد بالحصول على التصريحات اللازمة للقيام بعمليات التعقب بينما القطاع الخاص حر من هذه الإجراءات[3].

ثالثا: الاستعانة بالقطاع الخاص قد تضفي المصداقية على استنتاجات القطاع العام. التقرير النهائي للقطاع الخاص عندما يؤكد شكوك أجهزة الدولة المبدئية يضفي عليها الكثير من المصداقية وثقة الجمهور في البيانات العامة، تلك الثقة التي تستطيع الحكومات الاستفادة منها لتسويغ اتخاذها الإجراءات المضادة[4].

رابعا: يعفي الحكومات من الكشف عن المصادر والأساليب.[5] لطالما اتهمت الدول التي تكون ضحية لهجمات سيبرانية دولاً أخرى دون أن تكشف عن طرقها في التعقب، بسبب ما قد يكون في طرق

---

[1] المرجع السابق – Romanosky, S., & Boudreaux, B. ص463-464

[2] Office of the United States Trade Representative (USTR). (2018, March). *Report on China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation*. Retrieved from https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF

[3] Derian-Toth, G., et al. (2021). Tallinn Paper: Opportunities for Public and Private Attribution of Cyber Operations. *The 12th Tallinn Paper (Young Scholar Edition)*, p. 16. Retrieved from https://ccdcoe.org/uploads/2021/08/Tallinn_Papers_Attribution_18082021.pdf

[4] المرجع السابق

[5] المرجع السابق

التعقب من انتهاك لسيادة الدول الأخرى، وبسبب عدم رغبة الدول في الكشف عن تقنياتها الخاصة في التعقب، فإسناد الأمر للقطاع الخاص يعفي الدولة من ذلك.

خامسا: الردع. فحينما يكون هناك أكثر من جبهة في الدولة تشارك الدفاع السيبراني والإسناد الرقمي يكون ذلك رادعا للهجمات؛ لأنه أقرب إلى إظهار الجهة المتسببة في الهجوم وما يتبعه من تسمية وتشهير للدولة المهاجمة يتحقق فيه عنصر الردع[1].

أما عن مسؤولية الدولة عن أعمال القطاع الخاص فتعتمد على ما يقوم به القطاع الخاص أَمِن تلقاء نفسه؟ أم بموجب تفويض من الدولة؟ أم تعليمات؟ أم توجيهات؟ أم رقابة الدولة؟ إذا لم يكن ذلك ولم يكن هناك ظرف استثنائي يعطل الحكومة عن القيام بمهامها، فإنه لا يمكن نسبة أعمال القطاع الخاص للدولة.

يجب ألا يقلل الاعتماد على القطاع الخاص من مسؤولية الدولة عن الأعمال التي تدخل في اختصاصها، أي الأعمال الحكومية، بما في ذلك مسؤولياتها عن الأمن السيبراني المحلي، والاستخبارات، والردع في الفضاء السيبراني، والسياسة الخارجية الفعالة، كل ذلك يجب أن يظل من مسؤولية الدولة تأمينه بأفضل وجه. والاستفادة من القطاع الخاص لا يعني أن للدولة أن تتراخى في هذه المهام. لذلك من الأفضل أن يتم الاستفادة من القطاع الخاص في إطار التفويض، أو على الأقل التنسيق مع الحكومة. خصوصا إذا كان موضوع التعاون أحد الأعمال التي تدخل في صلاحيات الحكومة؛ وذلك لأن التعاون يسهم في التقليل من مخاطر اللجوء إلى القطاع الخاص كالتداخل في عمليات التحقيق التي تجريها الحكومة وإثباتها أو الادلاء بمعلومات متضاربة للجمهور، وهناك خطورة على العاملين في القطاع الخاص الذين يعملون في عمليات إسناد دولية[2].

تجدر الإشارة إلى أنه بالرغم من الفوائد المذكورة ترفض بعض الآراء هذه الفكرة، بحسبان أن مسألة الإسناد من مسائل السياسة الخارجية للدولة. فضلًا عن أن المعايير العالية التي قد يوفرها القطاع الخاص في الإثبات والأدلة الرقمية تصعب على الجهات الحكومية موازاتها وتظهرها بشكل بطيء ومتخلف[3].

---

[1] المرجع السابق
[2] المرجع السابق – Romanosky & Boudreaux – ص483
[3] المرجع السابق

ولا يقتصر اللجوء إلى القطاع الخاص في الهجمات السيبرانية، شركات الأمن السيبراني فقط. فمثلا بعض البرامج المضادة للفيروسات تقوم بجمع المعلومات عن الجهاز المستخدم، والشبكات التي ترتبط به، وأنواع الملفات الموجودة فيه، حتى لو لم يكن هذا الجهاز يحتوي على أي فايروس أو برنامج خبيث[1]. ولذلك فإن هناك دعوات للتعاون مع الشركات الكبيرة الرائجة المصنعة لهذه البرامج في عمليات التنسيب. وأي شركة خاصة في أي تخصص يمكن أن تساعد في عملية التنسيب، حتى لو لم تكن ذات طبيعة تقنية كأن تكون استخباراتية أو قانونية.

الفرع الثاني: لجان تقصي الحقائق الدولية

نصت اتفاقية لاهاي (1) لعام 1899 على إنشاء محكمة التحكيم الدائمة في لاهاي للتسوية السلمية للنزاعات، وهي هيئة لا تزال تعمل اليوم[2]. كذلك نصت الاتفاقية على فكرة لجان تحقيق دولية مستقلة؛ لتسهيل حل خلافات في الرأي من خلال توضيح الحقائق بحيادية والتحقيق النزيه [3]". فيودور مارتينز الدبلوماسي الروسي المعروف الذي قدم أحكام لجان التحقيق الدولية خلال مؤتمر السلام لعام 1899، ووصفها بأنها "آلية طوعية لتقصي الحقائق، يمكن أن تتجنب المعلومات المضللة الملتهبة حول أسباب نزاع دولي مع كسب الوقت لحل المسألة."[4] وان لم يكن واضحا بصراحةً في هذا التعريف لكنه موجود ضمنيا إن أهم ما يميز هذه اللجان أنها مقتصرة على مسالة معينة. لكن لم يتم الاتفاق حينها على أن يكون التحقيق في مسائل المسؤولية الدولية من مهام تلك اللجان؛ لأنه يمكن أن يتعدى على مجال التحكيم. ومع ذلك، في عام 1904، تم إنشاء لجنة تقصي حقائق للتحقيق في حادث بحري في بحر الشمال، وتم تفويضها في تحديد المسؤولية عن الحادث وتحديد درجة اللوم[5].

---

[1] Batt, S. (2020, March 10). Is Your Antivirus Tracking You? Here's What You Need to Know. *MUO*. Retrieved from https://www.makeuseof.com/tag/antivirus-tracking-youd-surprised-sends/

[2] المحكمة الدائمة للتحكيم (د. ت.) مقدمة عن المحكمة الدائمة للتحكيم. استرجع من https://pca-cpa.org/ar/about/introduction/

[3] Permanent Court of Arbitration (The Hague), *Convention (I) For The Pacific Settlement Of International Disputes*, 18 October 1907, available at: https://docs.pca-cpa.org/2016/01/1899-Convention-for-the-Pacific-Settlement-of-International-Disputes.pdf

[4] المرجع السابق - Shany & Schmitt – المرجع السابق – ص202

[5] Lemnitzer, J. M. (2016). *International Commissions of Inquiry and the North Sea Incident: A Model for a MH17 Tribunal?* European Journal of International Law, 27(4), 923–944. https://doi.org/10.1093/ejil/chw056

إن لجان تقصي الحقائق أو لجان التحقيق الدولية اليوم من الآليات التي يتزايد اللجوء إليها غالبا في حالات الانتهاكات الجسيمة للقانون الدولي، وبالأخص حقوق الإنسان. قد تُعيَّن هذه اللجان من قبل الأمم المتحدة أي من بعض أجهزتها الرئيسة كمجلس الأمن، أو الجمعية العامة، أو مجلس حقوق الإنسان. أو قد تعين لجنة من قبل مجموعة من الدول للتحقيق في قضية معينة أو من قبل دولة واحدة. بيد أنه يمكن أن ينظر للجان تقصي الحقائق المعنية، أو المدعومة من الحكومات على أنها ذات غرض دعائي خصوصا إذا ما تعلقت بالتحقيق في انتهاكات حقوق الانسان[1]. ويفترض بهذه اللجان أن تعمل وفق معايير دولية تم توصيفها من قبل الأمم المتحدة، منها الحياد، وعدم الانحياز، والشفافية والموضوعية، والسرية، والمصداقية، والنزاهة المهنية[2]. هو أهم ما يميز عمل لجان تقصي الحقائق ويعطيها قبولا يصل لحد القوة الإثباتية. وهذا ما يمكن الاستفادة منه في مشكلة الإثبات في الفضاء السيبراني.

فالاجتهاد القضائي لمحكمة العدل الدولية يؤكد أن المحكمة كانت قد أعطت احترامًا لنتائج هيئات التحقيق الدولية[3]. فعلى سبيل المثال في قضيتي: البوسنة والهرسك ضد صربيا، والجبل الأسود وكرواتيا ضد صربيا، قبلت المحكمة النتائج التي توصلت إليها المحكمة الجنائية الدولية ليوغوسلافيا بشأن نية الإبادة الجماعية[4] كذلك في قضية الأنشطة المسلحة الكونغو ضد يوغندا، أولت محكمة العدل الدولية اهتمامًا للأدلة التي جمعتها لجنة "بورتر"، وهي لجنة قضائية عينتها حكومة أوغندا. بل ذهبت المحكمة إلى حد الإشارة إلى أن مثل هذه النتائج كانت مقبولة، لأنه تم الحصول عليها من خلال "استجواب الأشخاص المعنيين مباشرة، والذين تم استجوابهم فيما بعد من قبل القضاة"[5] .

---

[1] Robertson, G., QC. (2010). Human Rights Fact-Finding: Some Legal and Ethical Dilemmas. *UCL Human Rights Review, 3*, 15-43 [p. 19]. Retrieved from https://www.ucl.ac.uk/human-rights/sites/human-rights/files/robertson.pdf

[2] الأمم المتحدة، مفوضية حقوق الإنسان. (2015). *لجان التحقيق وبعثات تقصي الحقائق المعنية بالقانون الدولي لحقوق الإنسان والقانون الدولي الإنساني - توجيهات وممارسات* (ص. 32–33). نيويورك وجنيف.HR/PUB/14/7 استرجع من https://www.ohchr.org/sites/default/files/Documents/Publications/CoI_Guidance_and_Practice_AR.pdf

[3] Williams, P. (2020, October 29). Admitting evidence of fact-finding missions: To be continued? Retrieved from https://www.publicinternationallawandpolicygroup.org/lawyering-justice-blog/2020/1/21/admitting-evidence-of-fact-finding-missions-to-be-continued

[4] *Genocide* judgement, para. 238, p. 140; para. 136, p. 63

[5] *Armed Activities* judgement, p. 201, para. 61

يكشف الفحص الدقيق للسوابق القضائية أن محكمة العدل الدولية حاولت صياغة مبادئ توجيهية؛ لتحديد القيمة الإثباتية لتقارير الطرف الثالث، أي لجان التحقيق المستقلة[1]. لقد أوضحت المحكمة في حكم البوسنة ضد صربيا أن قيمة الدليل تعتمد على مصدر الدليل (أهو متحيز إلى أحد الأطراف أم لا؟)، وعلى نوع المعلومات المنقولة (هل فيها تجريم أو إدانة؟)، والعملية التي تم بها جمعها (هل تم الحصول عليها من خلال استجواب دقيق؟)[2]مع ذلك يجب الانتباه أن هذا النوع من الإثبات يمكن أن يكون قيما أمام محكمة العدل الدولية، أما المحكمة الجنائية الدولية فلها معاييرها الخاصة في الإثبات والتي عادة ما تكون أكثر صرامة.

لذلك يمكن الاستفادة من فكرة اللجان الدولية في الهجمات السيبرانية الجسيمة، وتعيين خبراء تقنيين وقانونيين يتوفر فيهم الحياد والمهنية فإذا ما مارست اللجنة اختصاصها وفق معايير المحكمة المطلوبة فقد تكون لها قوة الدليل، حتى لو لم تتوصل إلى الدولة المسؤولة، فإنه يمكن للأدلة فقط أن تفعل الكثير؛ وإن لم تثبت هوية الأفراد المسؤولين عن إطلاق الهجمات، ولم يثبت تواطؤ الدولة.

هذا ولا يقصد بالأدلة التي يجمعها التحقيق تلك الأدلة المحصورة داخل الفضاء السيبراني فحسب. بل يمكن استخدام أي دليل تم جمعه في العالم الحقيقي أن يكون حاسماً أو ذا صلة، في تحديد الحقائق وإسناد العملية الإلكترونية. وقد تتكون الأدلة من أدلة وثائقية، وأدلة مادية، أو شهادة الخبير، أو شهادات الشهود وغيرها[3]. كما أشارت هيئة الأمم المتحدة UNGGE في تقريرها لعام 2015 إلى ذلك بالنص الآتي: "في حالة تكنولوجيا المعلومات والاتصالات الحوادث، "يجب على الدول النظر في جميع المعلومات ذات الصلة، بما في ذلك السياق الأكبر للحدث، تحديات الإسناد في تكنولوجيا المعلومات والاتصالات، وطبيعة البيئة ومدى العواقب"[4].

الفرع الثالث: جهاز دولي مستقل لإسناد العمليات السيبرانية

هناك دعوات عديدة سواء من باحثين قانونيين أو مبادرات رعتها شركات أو منظمات متخصصة لإنشاء جهاز دولي مستقل يضفي مصداقية على الإسناد في عالم الفضاء الإلكتروني. تتلخص وظيفته الأساسية في التحليل الفني للهجوم وإثبات الإسناد. الفكرة الرئيسة هي أن تتألف هذه المنظمة من خبراء

---

[1] المرجع السابق – Williams, P.

[2] *Genocide* judgement, para. 227, p. 135

[3] المرجع السابق – Shany, Y., & Schmitt, M. N. – ص213

[4] المرجع السابق – A/70/174 – الفقرة 13(ب) – ص7

تقنيين من مختلف الحكومات، والقطاع الخاص، والأوساط الأكاديمية، والمجتمع المدني؛ للوصول إلى أكبر قدر ممكن من التمكن، وأفضل التقنيات والإجراءات المستخدمة في تعقب الهجمات السيبرانية التي تتعرض لها الدول. بالإضافة إلى الاتفاق على المؤشرات التي تشير إلى أن هجوماً معيناً تم بواسطة دولة. مما يؤدي في النهاية إلى بناء معايير دولية متفق عليها في عملية الإسناد.

آلية تحديد المصدر الدولية من شأنها تعزيز ثقة الجمهور في ادعاءات الإسناد الخاصة بوكالات الأمن الوطني، وشركات الأمن السيبراني الخاصة. وعلى الرغم من أن هذين القطاعين: العام والخاص لديهما خبرة مهنية كبيرة، فإن عملها يميل إلى الافتقار إلى الشفافية. كذلك الانتماء الحكومي أو المصالح التجارية قد تجعل نتائجها أشبه ما يكون بالادعاءات المشبوهة، بينما مصداقية مثل هذا الجهاز الدولي لا تشوبها شائبة[1]. كذلك قد تتفوق فكرة الجهاز الدولي على لجان تقصي الحقائق كون الأخيرة تعتمد بشدة على موافقة الدولة التي يشتبه بمسؤوليتها في التعاون، وفي كثير من الأحيان ترفض الدول التعاون مع لجان التحقيق الدولية المشتركة؛ لعدم ثقتها في مصداقية الطرف الآخر. أما مصداقية منظمة دولية مستقلة –على غرار العمل الذي تقوم به الوكالة الدولية للطاقة الذرية، أو هيئة التفتيش في منظمة حظر الأسلحة الكيميائية[2]– فإنها أقوى مما يحد من قدرة الدول المسؤولة على رفض المشاركة في عملية الإسناد الجماعي. مع ذلك كل إيجابيات الجهاز المستقل الدولي للإسناد ظل حبيس الأفكار ولم تلق اهتماما أو رعاية كافية من الدول. فلقد كانت الحكومات مترددة في تمكين منظمة مستقلة للتوصل إلى نتائج قد تكون مهمة ومشحونة سياسياً.

تم إطلاق العديد من المبادرات الهادفة إلى تعزيز آلية تحديد المصدر في الهجمات السيبرانية الدولية في السنوات الأخيرة. مثلا في عام 2016 نشرت Microsoft اقتراحًا للإسناد قائمًا على التحقيق في الحوادث من قبل خبراء دوليين يتألفون من خليط من القطاعين العام (ويكون فيه للدول تمثيل) والخاص[3]. إن الخاصية التي يركز عليها اقتراح مايكروسوفت هي الدمج بين قدرات القطاع الخاص –ليس في النطاق الوطني داخل الدولة الواحدة– بل أن تتعاون الشركات العملاقة الخاصة في نطاق تعاون دولي، وتجري المنظمة تحقيقًا تقنيًا في بعض العمليات التي تقع في نطاق اختصاصها، وتبلغ

---

[1] المرجع السابق – Shany, Y., & Schmitt, M. N. – ص215

[2] منظمة حظر الأسلحة الكيميائية (د. ت) هيئة التفتيش. استرجع من https://www.opcw.org/ar/mn-nhn/alamant-alfnyt/alaqsam/hyyt-altftysh

[3] Charney, S., et al. (2016). *From Articulation to Implementation: Enabling progress on cybersecurity norms.* Microsoft. Retrieved from https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVmc8

المعنيين بالنتائج التي تتوصل إليها بما في ذلك أدلة الإسناد. ونتائج التحقيقات لن تنشر على العامة إلا في حالات استثنائية. وهم يجادلون بأن الآلية المقترحة ستوجد تآزرًا بين خبرات الدول والجهات الفاعلة في القطاع الخاص والأكاديميين، من أجل العمل معا لتعرف مرتكبي العمليات السيبرانية الخبيثة على نموذج آلية التحقيق الذرية الدولية (وكالة الطاقة (IAEA)) حيث قد يكون في تعاون الدول احتمالا أكبر للنجاح في الكشف عن مرتكبي الهجمات الخبيثة.

وعام 2018 اقترحت مؤسسة راند RAND إنشاء منظمة عديمة الجنسية تحت مسمى "اتحاد عالمي لتحديد مصدر الهجمات الإلكترونية"، وتقضي مهمة المنظمة "بإجراء فريق واسع –من الخبراء الدوليين– تحقيقات مستقلة في الحوادث الإلكترونية الكبرى بغية تحديد مصدرها[1]". وتشمل عضويتها خليطا من قطاعين: خبراء القطاع التقني وتكنلوجيا المعلومات والأمن السيبراني، وخبراء قطاع القانون، والسياسة الدولية، والقانونيين، والأكاديميين. إن ما يميز مبادرة راند عن مايكروسوفت هو تشديدها على أهمية ألا يكون في المنظمة أي تمثيل دولي؛ لكيلا تتأثر مصداقية المنظمة بالأغراض السياسية والمصالح الوطنية، ولكي تتمكن من تلافي ضغوط الدول بعدم كشف أدلة معينة أو عدم قبول حالات تحقيق معينة[2].

وقبل ذلك في عام 2014 اقترح المجلس الأطلسي –وهو مركز أبحاث مقره واشنطن العاصمة الأمريكية[3]– إنشاء مجلس متعدد الأطراف للتحكيم والإسناد السيبراني[4] ويعمل المركز على أساس أنه جهاز مشترك بين الدول يُعهد إليه بالتحقيق في الهجمات السيبرانية، بهدف إسناد المسؤولية إلى الدول عند الاقتضاء. ويمكنه بعد ذلك إصدار توصيات؛ لخفض التصعيد، وربما إصدار حكم يحدد تكاليف إصلاح الضرر الذي يلحق بالمعتدي، أو إحالة ملف الاتهام إلى هيئات سياسية أو قضائية أخرى. وقد اعتُقِد أن اقتراح المجلس الأطلسي في التطوير التدريجي لمثل هذه الآلية سيعتمد على قدرات

---

[1] إديفيس الثاني، جون إس، وآخرون – المرجع السابق – ص25

[2] إديفيس الثاني، جون إس، وآخرون – المرجع السابق – ص27-29

[3] Atlantic Council. (2022, May 10). About the Atlantic Council. Retrieved from https://www.atlanticcouncil.org/about/

[4] Healey, J., et al. Atlantic Council of the United States. Brent Scowcroft Center on International Security, Försvarshögskolan. Institutet för högre totalförsvarsutbildning, North Atlantic Treaty Organization. Science for Peace and Security Programme. (2014). *Confidence-Building Measures in Cyberspace*. Washington, United States of America: Atlantic Council, p. 10. Retrieved from https://www.atlanticcouncil.org/wp-content/uploads/2014/11/Confidence-Building_Measures_in_Cyberspace.pdf

التحقيق في المجلس، وأنها في الغالب تأتي من الدول ذات الإسناد الإلكتروني الأعلى وقدرات الطب الشرعي الرقمي أساسًا، لكن ذلك لا يمنع التعاون مع جهات خاصة في بعض الأحيان[1].

هذه وجهات نظر متنوعة لما يمكن أن تكون عليه آلية الإسناد الدولية المركزية، بعضها يرجح القطاع الخاص، وبعضها يرجح منظمة ذات تمثيل دولي فقط، وبعضها الآخر يجمع بين الأمرين. ويبدو أن النهج الأخير هو الأقرب إلى الصواب؛ لأن وجود ممثلين للدول وأشخاص مستقلين يمثلون أنفسهم أمر يجمع بين كفاءة القطاعين ويسمح للدول أن تكون شريكا في القرارات دون أن يترك القرار كله وفقا لمصالحها الوطنية.

إن أهمية وجود جهاز مركزي لجمع جهود التقنيين. لابد له من قاعدة بيانات لرصد وقياس سلوك وتصريحات الدول في النطاق السيبراني، وهذا يتطلب من الدول أن تكون أكثر شفافية في كشف تحركاتها وقدراتها السيبرانية. ويمكن أن يتم الجمع بين الجهازين: التنسيب والتقنين.

المطلب الرابع

آثار المسؤولية الدولية عن الهجمات السيبرانية

الهدف أو السبب من سعي الدولة الضحية لإقامة المسؤولية الدولية هو حصولها على استعادة الوضع القانوني بما لا يتعرض حقوقها للانتهاك، ويتم جبر الأضرار التي نجت من الانتهاك. فإذا نجحت الدولة الضحية في تكييف الفعل بوصفه خرقًا قانونياً، واستطاعت نسبته إلى دولة معينة، تمكنت أن تحمل الدولة المسؤولة بعض الآثار القانونية المترتبة على الخرق، وهذا ما أكدته قواعد مسؤولية الدولة التي وضعت نتائج قانونية لانتهاك مسؤولية الدولة وهي بمنزلة حقوق للدولة الضحية، والواجب على الدولة المسؤولة تنفيذها، وهي الكف والتأكيدات والضمانات بعدم التكرار وأخيرا جبر الضرر.

الفرع الأول: الكف عن الفعل غير المشروع

الكف هو الخطوة الأولى لأنهاء حالة الفعل غير المشروع دولياً. ويقصد به الكف عن الفعل السيبراني غير المشروع، وواجب الدولة المسؤولة قانونًا بوقف عملية سيبرانية جارية غير مشروعة دوليًا[2]. الالتزام

[1] المرجع السابق – ص10-12

[2] Tallinn Manual 2.0, commentary to rule 27, para. 3, p. 142

بالكف قد يكون سلبياً، وذلك في حالة صدور الهجمات السيبرانية غير المشروعة من أحد أجهزة الدولة، ونسبتها إلى الدولة بموجب قواعد مسؤولية الدولة، فتقوم هذه الدولة المعتدية بوقف هذه الهجمات السيبرانية. وقد يكون الكف التزاما إيجابياً، وذلك إذا كان الفعل غير المشروع إهمالًا أو إغفالًا عن واجب الدولة ببذل العناية. فهنا يتحتم على الدولة أن تتحرك وتبذل العناية المطلوبة، لتمنع الفاعلين غير الحكوميين –على إقليمها– من إطلاق تلك الهجمات[1].

وجبر الضرر –وإن كان هو الخطوة النهائية– فإنه ليس أساسياً في خلافات الدول حول المسؤولية الدولية مثل الكف. لذلك نرى أن مطالبة الدولة المسؤولة بالكف دائما ما يكون المحور المقدم، ليس فقط في مطالبات الدول، بل حتى في مطالبات المجتمع الدولي كالمنظمات الدولية مثل: الأمم المتحدة، ومجلس الأمن، فهذه دائما ما تكون محور مطالبتها للدولة المسؤولة الكف عن السلوك الذي يخترق القانون الدولي[2].

أهمية الكف –لا تكمن فقط– في وضع حد للانتهاك القانوني الواقع على دولة معينة، بل في حماية القاعدة القانونية نفسها، وهو بذلك لا يحمي القاعدة القانونية في نطاق العلاقة بين الدولة المسؤولة والدولة المتضررة فقط، بل يحمي القاعدة القانونية عامةً، ويعيد إليها احترامه، وبالتالي فوائده تعود على كل الدول، بل وكل المجتمع الدولي[3].

الفرع الثاني: تقديم التأكيدات والضمانات بعدم التكرار

بعكس الكف عن الفعل غير المشروع فإن التأكيدات والضمانات بعد التكرار ليست مطلوبة في كل حالة انتهاك لفعل غير مشروع، ولكن فقط في حالات محددة عندما تشعر الدولة الضحية أن العودة إلى العلاقة السابقة لن يكون كافيا لحمايتها[4]. الحقيقة إنه من الصعب الاتفاق على الوقت الصحيح لاستخدام أداة التأكيد، والضمان بعدم التكرار إلا أن لجنة القانون الدولي توصي باستخدام أداة الضمان بعدم التكرار بوصفها قاعدة عامة تكون وسيلة لتعزيز العلاقة القانونية مستقبلا، وإعادة الثقة فيها[5] فكأن تلك الأداة مخصصة للدول التي تتطلع للمزيد من العلاقات المستقبلية. مع ذلك، فهناك بعض السوابق

[1] Tallinn Manual 2.0, commentary to rule 27, para. 2, p. 142

[2] التعليق على المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دولياً، التعليق على المادة 30، الفقرة (4)، ص114

[3] المرجع السابق – التعليق على المادة 30 – الفقرة (5) – ص 114-115

[4] المرجع السابق – التعليق على المادة 30 – الفقرة (9) – ص115

[5] المرجع السابق، التعليق على المادة 30 – الفقرة (9) – ص115

التي ذكرتها التعليقات على قواعد مسؤولية الدولة التي استخدمت فيها الضمانات بعدم التكرار في إطار العاقبة القانونية لفعل غير مشروع فقد حكمت بها محكمة العدل الدولية بسبب فعل غير مشروع دوليا[1]، أو أن تأتي في إطار الترضية للدولة المتضررة[2].

التأكيدات بعدم التكرار عادة ما تكون شفوية، في الخطابات العامة أو في الاتصالات الدبلوماسية، لكن ليس هناك ما يمنع من أن تكون كتابية. أما الضمانات بعدم التكرار فلها بعد عملي، فإن الدولة تعرض الخطوات والإجراءات التي اتخذتها، للتحقق من أن أمرا كهذا لن يحدث مستقبلا[3]. إن الضمانات بعدم التكرار لها أهمية خاصة في الجانب السيبراني فإن مجرد التأكيد بعدم التكرار لن يكون مطمئناً بقدر استعداد الدولة المسؤولة لاعتماد وسائل تقنية أو تشريعية لضمان عدم حدوث مثل تلك الهجمات السيبرانية مستقبلا.

ويقترح دليل (تالين) في السياق السيبراني أن تستخدم أداة التأكيد والضمان بعدم التكرار في الحالة التي تكون الدولة المتضررة لديها قلق معقول بأن مجرد إيقاف الفعل غير المشروع دوليًا لن يكون كافياً لحمايتها،[4]وبعبارة أخرى عندما يكون الكف غير كاف للضمان، كأن يكون لدى الدولة المسؤولة سمعة معينة أو سلوك متكرر لاستخدام العمليات السيبرانية لانتهاك سيادة الدول، لذلك من المنطقي ألا تقتصر الدولة المتضررة على الوثوق بمسار الكف، ووقف السلوك وحسب، بل ستسعى إلى الحصول على ضمانات من الدولة المسؤولة بعدم تكرار ذلك.

إن إمكان الحصول فعلا على التأكيدات والضمانات بعدم التكرار يصعب وضعها في شروط محددة! فذلك يعتمد جدا على السياق الذي حدث فيه الفعل غير المشروع، هل حدث لأول مرة؟ وهل هو ذو طبيعة ثانوية؟ ففي هذه الحالة سيكون من المبالغة الإصرار على الحصول على الضمانات[5]. كذلك الأمر يعتمد على أهمية العلاقة بين الدولة المسؤولة والدولة المتضررة، فلا يتصور الحصول على التأكيدات بعدم التكرار في العداوات التاريخية أو العلاقات الضعيفة عامة.

---

[1] في قضية لاغراند بين ألمانيا والولايات المتحدة أعطت المحكمة ألمانيا طلبها وألزمت الولايات المتحدة بتقديم ضمانات بعد التكرار برغم اعتراف الوليات المتحدة بالتقصير واتخاذها إجراءات ضامنة لعدم حدوثه في المستقبل.
انظر: المرجع السابق – التعليق على المادة 30 – الفقرة (10) – ص115-116

[2] التعليق على المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دولياً – التعليق على المادة 30 – الفقرة (11) – ص116

[3] المرجع السابق، التعليق على المادة 30 – الفقرة (12) – ص116

[4] Tallinn Manual 2.0, commentary to rule 27, para. 6, p. 143

[5] Tallinn Manual 2.0, commentary to rule 27, paras. 7-8, pp. 143-144

وتجدر الإشارة إلى أن قبول استمرار قيام العلاقة القانونية –التي تم انتهاكها بالفعل غير المشروع– شرط لإمكان تطبيق التأكيد والضمان بعدم التكرار؛ لأن العلاقة المنتهية لن تحتاج إلى تأكيدات وضمانات بعدم التكرار. هذا الأمر أكدته لجنة القانون الدولي في تعليقها على المادة 30 على النحو الآتي:

"يعد استمرار نفاذ الالتزام الأساسي افتراضاً ضرورياً في كلتا الحالتين (الكف والتأكيدات والضمانات بعدم التكرار)، لأنه إذا توقف الالتزام بعد خرقه فلا تنشأ مسألة الكف ولا يمكن أن تكون التأكيدات والضمانات ذات صلة بالموضوع"[1]

الفرع الثالث: جبر الضرر

تميل بعض الآراء إلى التقليل من قدرات الهجمات السيبرانية على إحداث هجوم مسلح حركي، وترى أن موضوع جبر الضرر بصوره الثلاث (الرد– التعويض– الترضية) من المرجح أن يكون خيارا جذابا للدول المتضررة من هجوم سيبراني، لأنهم يرون بعد احتمال استخدام الوسيلة السيبرانية لتنفيذ هجوم مسلح حركي قاتل للأرواح، ومدمر للممتلكات، وبالتالي يستبعدون الحاجة إلى التصعيد ردا على هجمات سيبرانية، وبمعنى آخر لن يكون هناك حاجة لاجتياح بري، والرد بالدفاع عن النفس بهجوم مسلح. ودليلهم على ذلك أن الغالبية العظمى من أضرار الهجمات السيبرانية تبدأ في البعد الاقتصادي وتنتهي فيه؛ مما يجعل التعويض أهم من أي نتيجة أخرى ترغب الدول في الوصول إليها بإثارة مسئولية دولة عن هجوم سيبراني[2].

وإن كان يصعب الاتفاق على فكرة محدودية قدرات الهجمات السيبرانية فإنه من الواقعي أن غالبية الأضرار التي تسببها الهجمات السيبرانية (حتى الآن) هي أضرار اقتصادية[3]. كهجمات منع الوصول للخدمة التي تشل الدولة في جوانب عدة، وتؤثر في الاقتصاد، أو حتى الهجمات التجسسية التي تسرق معلومات اقتصادية أو صناعية حساسة، أو الهجمات السيبرانية التي تقع على المصارف سارقةً ملايين

---

[1] التعليق على المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دولياً – التعليق على المادة 30 – الفقرة (1) – ص114

[2] Payne, C., & Finlay, L. (2017). Addressing Obstacles to Cyber-Attribution: A Model Based on State Response to Cyber-Attack. *The George Washington International Law Review*, *4*(3), 535-568 [p. 548–549]. Retrieved from https://gwilr.org/wordpress/wp-content/uploads/2017/05/ILR-Vol-49.3_Panye-Finlay.pdf

[3] Yadav, H., & Gour, S. (2017). Cyber Attacks: An impact on Economy to an organization. *International Journal of Information & Computation Technology*, *4*(9), 937–940. Retrieved from https://www.ripublication.com/irph/ijict_spl/ijictv4n9spl_11.pdf

الدولارات، كما وقع على المصرف المركزي لسنغافورة. لذلك يمكن الاتفاق على أن التعويض سيأخذ بعدا مهما في موضوع الهجمات السيبرانية الدولية.

وقد ناقشت قواعد مسؤولية الدولة جبر الضرر في قسمين منفصلين أولهما: بوصفها إحدى النتائج القانونية للفعل غير المشروع، مع الكف والتأكيدات بعدم التكرار. وثانيهما: في فصل منفصل تحت عنوان أشكال الجبر وهي الرد والتعويض والترضية. وفيما يأتي نحاول التعريج على أهم الخطوط الرئيسية في موضوع جبر الضرر كما جاء في القسمين مع تطبيقه على حالة الضرر الذي تم بهجمات سيبرانية.

أولا: جبر الضرر بوصفه نتيجة قانونية للعمليات السيبرانية غير المشروعة

أولًا: إن من الأمور البديهة مما يجب البدء بها أن الحديث عن جبر الضرر، لن يكون ممكنا إلا إذا سببت العملية السيبرانية خسائر معينة. وهنا في سياق المسؤولية الدولية لا يعني أن الضرر يجب أن يصيب الدولة فقط، بل حتى الضرر الذي تسببه الهجمات السيبرانية –غير المشروعة– على الأفراد والمواطنين، والجهات غير الحكومية، كالشركات الخاصة، والمؤسسات الأهلية فكل ذلك يعد ضررا للدولة[1] طالما أن الهجمات السيبرانية فعل غير مشروع دوليا صادر من الدولة. والضرر في نطاق المسؤولية الدولية يتسع لأي ضرر مادي أو معنوي، يتضح ذلك من المادة 31 من قواعد مسؤولية الدولة التي نصت على أن:

1– على الدولة المسؤولة الالتزام بجبر كامل الأضرار الناجمة عن الفعل غير المشروع دولياً.

2–تشمل الخسارة أي ضرر –سواء كان مادياً أم معنوياً– ينجم عن الفعل غير المشروع دولياً مرتكبًا من الدولة.

الضرر المادي الذي سببته العملية السيبرانية يكمن تصوره في الممتلكات التي تتعرض للتخريب، بفعل العملية السيبرانية كالحواسيب التي تتلف، وتصبح غير صالحة للاستخدام (وهذا أمر شائع في العمليات

[1] التعليق على المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دولياً – التعليق على المادة 31 – الفقرة (5) – ص118

السيبرانية)[1] أو السيرفرات، بل الأمر أكبر من ذلك كما في حالة أن تتسبب الهجمة السيبرانية بانفجار في المبنى وتدميره، أو إسقاط طائرة أو التلاعب بخط سير القطارات، والتسبب بحوادث مختلفة. فالاحتمالات المدعومة بتجارب الأمن السيبراني[2] لا حصر لها. لكن الضرر المادي أيضا كامن في حالات فقد البيانات، بشرط أن ينجم عنه خسائر مادية، أو حتى حالة منع الوصول إلى الخدمة إذا ارتبط بخسائر اقتصادية يمكن قياسها. أما إذا كان فقد البيانات أو عدم القدرة المؤقتة على الوصول إليها غير مرتبط بخسائر مادية تذكر فلن يكون من الممكن طلب التعويض على أساس الأضرار المادية[3].

أما الضرر الأدبي فهو ذو طبيعة أخلاقية، سياسية وقانونية، ناتج عن إهانة كرامة الدولة المتضررة وهيبتها.[4] وهو أمر ممكن في الهجمات السيبرانية فكل هجمة تفشل الدولة في اكتشافها وصدها حتى تصل إلى التأثير على حياة الناس يكون فيها تقويض الثقة في الحكومة، وبالتالي يمكن أن تعد ضررا معنوياً وان لم تتسبب بأي ضرر مادي يذكر.

الأمر الذي يمكن الاتفاق عليه في موضوع جبر الضرر هو وجود ضرر أدبي أو مادي يستحق الجبر، أما مقدار الجبر فهو مسالة تقنية صعبة، تختلف من حالة لأخرى، وتختلف بحسب نوع الجبر أهو رد عيني؟ أم تعويض؟ أم ترضية؟ لكن يمكن الاتفاق على أن تحديد مقدار الجبر –سواء تم في مفاوضات بين الدولتين أو عن طريق هيئة تحكيم أو عن طريق محكمة دولية– يبدأ من عملية "تقييم الضرر". وهنا تورد قواعد مسؤولية الدولة بعض المبادئ التي تحكم عملية تقييم الضرر، منها العلاقة المباشرة

---

[1] Pot, J. (2015, March 11). Can A Cyberattack Cause Physical Damage To Your Hardware? Retrieved from https://www.makeuseof.com/tag/can-cyberattack-cause-physical-damage-hardware/

Parker, S. (2017, October 3). Understanding The Physical Damage Of Cyber Attacks. Retrieved from https://www.infosecurity-magazine.com/opinions/physical-damage-cyber-attacks/

[2] Tam, K. et al. (2022). Case Study of a Cyber-Physical Attack Affecting Port and Ship Operational Safety. *Journal of Transportation Technologies*, *12*(01), 1–27. https://doi.org/10.4236/jtts.2022.121001

Peng, Y. et al. (2015). Cyber-Physical Attack-Oriented Industrial Control Systems (ICS) Modeling, Analysis and Experiment Environment. *2015 International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP)*, 322–326. Adelaide, Australia: IEEE. https://doi.org/10.1109/iih-msp.2015.110

[3] Tallinn Manual 2.0, commentary to rule 27, para. 2, p. 144

[4] Rainbow Warrior (NZ v. Fr.), 20 RIAA 217 (Arb.Trib. 1990), para. 109-110, p. 267

بين الفعل غير المشروع والضرر[1]. كذلك "إمكانية التنبؤ بالضرر"[2] فإذا كان الضرر يمكن التنبؤ به بشكل معقول مقارنة بدولة أخرى في نفس الظروف فإن ذلك يستوجب على الدولة اتخاذ خطوات استباقية، لتحمي نفسها، ولا تكون في مرمى الهدف. قد يجادل أحدهم بأن الهجمات السيبرانية ذات الطبيعة المفاجئة لا يمكن توقعها؛ لأنها لا تعبر الحدود الإقليمية أو المجال الجوي أو البحري، ويتفاجأ الضحية بآثارها بعد أن تصيب النظام، لكن تشير تجارب الدول في هذا الصدد أن بعض الهجمات يمكن توقعها، كأن تصرح الدولة بنيتها على استخدام سلاح الهجمات السيبرانية ضد دولة أخرى، أو أن يكون هناك نمط وقتي، أو يكون لها وقت ذروة معتاد في الهجمات السيبرانية، كأن تكون مكثفة مثلا في عطلة أعياد الميلاد دوريًا. وهذا ما يحدث في بلدان مثل هولاندا والولايات المتحدة فإن السلطات فيها تحرص –قبل يوم من عطلة أعياد الميلاد– على رصد ومصادرة الخدمات التي تسمح بإجراء هجمات منع الوصول DDoS بسبب التقليد السنوي لاستخدام تلك الهجمات لشن هجمات على شركات العاب الفيديو[3].

ومن المعايير التي تؤثر في تقييم الضرر وبالتالي مقدار الجبر هو "واجب التخفيف"[4] وهو الخطوات اللاحقة للهجوم السيبراني التي يمكن أن تقوم بها الدولة لتخفيف الضرر. على سبيل المثال، إذا كان من الممكن أن تكون الدولة المتضررة قد نقلت الأنظمة الإلكترونية المتأثرة إلى وضع عدم الاتصال بالإنترنت وهو أمر يمكن القيام به بسهولة من قبل أي دولة مهما كان نظام دفاعها السيبراني غير متطور، ومن شأنه منع المزيد من الضرر الناجم عن عملية إلكترونية مدمرة، لذلك فالضرر الذي بدأ عند تلك النقطة التي كان من الممكن للدولة الضحية منعه بشكل معقول لم يحتسب جزءًا من حساب التعويضات[5].

---

[1] التعليق على المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دولياً – التعليق على المادة 31 – الفقرة (10) – ص119

[2] المرجع السابق – التعليق على المادة 31 – الفقرة (10) – ص120

[3] Cimpanu, C. (2019, January 21). Law enforcement shut down DDoS booters ahead of annual Christmas DDoS attacks. Retrieved from https://www.zdnet.com/article/law-enforcement-shut-down-ddos-booters-ahead-of-annual-christmas-ddos-attacks/

[4] التعليق على المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دولياً – التعليق على المادة 31 – الفقرة (11) – ص120

[5] Tallinn Manual 2.0, commentary to rule 28, para. 8, p. 146

ولا مناص من تأكيد أن "إمكانية التنبؤ" بالضرر أو "واجب التخفيف" ليس واجبا قانونيا –على الدولة الضحية– تحاسب عليه إذا تم إهمالهما أو التقصير فيهما، أو تثار مسؤوليتها القانونية حيالهما، فإنه إذا تم إهمالهما أو التقصير فيهما فذلك قد يؤثر على الحق في التعويض أو في مقدار التعويض[1].

أخيرا لا بد من التنبيه على أنه لتفعيل الحق في جبر الضرر لابد من إخطار يصدر من الدولة المتضررة إلى الدولة المسؤولة. فلا يكفي حدوث الخرق ونسبته لدولة معينة في سجلات الدولة المتضررة ليصبح التعويض واجبا على الدولة المسؤولة، بل على الدولة المتضررة أن تخطر الدولة المسؤولة بالانتهاك القانوني الذي حدث من جانبها، وبالأضرار التي أصابتها، مع توضيح نوع الجبر الذي يجب أن تتم تأديته[2]. ولا يعني ذلك إعفاء الدولة المسؤولة من مسؤوليتها في حالة عدم صدور مثل ذلك الإخطار. لكنه يمثل أداة للاحتجاج بتقصير الدولة المسؤولة في حال عدم تجاوبها[3].

ثانيا: أشكال جبر الضرر

أما بخصوص أشكال الجبر فكما تمت الإشارة إليها أن هناك ثلاث صور لجبر الضرر: الرد العيني والتعويض اللذين يمكن ملاحظة جذورهما في القانون المدني، وهما صورتان والصورة الثالثة: الترضية التي ترسخت في القانون الدولي بوصفها صورة لجبر الضرر غير المادي، الذي ألم بالدولة الضحية. والقاعدة العامة في الجبر هي وجوب التدرج في صورها، فيجب البدء بالرد، فإذا لم يكن الرد ممكنا، يتم اللجوء إلى التعويض، فإن لم يكن الرد أو التعويض ممكنين أو كافيين، فإنه يتم اللجوء إلى خيار الترضية. مع ذلك هناك مراعاة لما تفضله الدولة المتضررة فقد تفضل التعويض بدلا من الرد[4]. نناقش الحالات الثلاث تِباعاً مع التنبيه للاختلافات التي تفرضها الطبيعة السيبرانية إن وجدت.

أولا: جبر ضرر الهجمات السيبرانية عن طريق الرد (إعادة الحالة إلى ما كانت عليه)

---

[1] المرجع السابق
التعليق على المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دولياً – التعليق على المادة 31 – الفقرة (11) – ص120

[2] المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دولياً – المادة 43 – ص12

[3] Tallinn Manual 2.0, commentary to rule 28, para. 12, p. 148

[4] التعليق على المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دولياً – التعليق على المادة 36 – الفقرة (3) – ص127-128

تتضح أهمية الرد في حكم محكمة العدل الدولية في قضية مصنع شورزو حينما عرفت المحكمة جبر الضرر ووضعت شكل الرد أنه هو الهدف الأساسي والأول الذي يجب أن تبتغيه عملية جبر الضرر وذلك على النحو الآتي:

"مبدأ الجبر يقضي بوجوب أن يمحو الجبر–قدر الإمكان– كل عواقب الفعل غير المشروع وأن يعيد الحالة إلى ما كان يمكن أن تكون عليه، وفقاً لأرجح الاحتمالات، لو لم يرتكب هذا الفعل[1]."

إذن الأصل الذي تبتغيه عملية الجبر هو الرد العيني، أي رد الحالة إلى ما كانت عليه قبل العملية السيبرانية الضارة. في النطاق السيبراني قد تعني حالة الرد العديد من الأمور. مثلا، في حالة الهجمات التعطيلية فالرد يعني إعادة اتاحة الخدمات التي أوقفها الهجوم السيبراني، أو إعادة المعلومات التي تم حجبها مع إعادة السيطرة بيد الجهة التي كانت تملكها قبل الهجوم السيبراني. الرد في الهجمات السيبرانية التجسسية يعني الخروج من النظام. لكن قد يتعدى الأمر أكثر من ذلك بحيث تتطلب حالة الرد تعاون الدولة المسؤولة عن الهجوم مع الدولة المتضررة بتوفير معلومات عن البرامج الخبيثة التي تم استخدامها ليتم إبطال عملها في النظم السيبرانية للدولة المتضررة والتحصن منها مستقبلا[2].

تشترط المادة 35 من قواعد مسؤولية الدولة شرطين لإمكان إعمال حالة الرد:

(أ) غير مستحيل مادياً.

(ب) غير مستتبع لعبء لا يتناسب إطلاقاً مع المنفعة المتأتية من الرد بدلاً من التعويض.

بالفعل هناك حالات يكون فيها الرد مستحيلاً أو صعباً. من الحالات التي يمكن أن يكون الرد فيها مستحيلً استحالة مادية الحالة التي تكون مهمة الهجوم السيبراني مسح قواعد المعلومات الخاصة بجهات حكومية، فإذا لم يتم نسخ تلك المعلومات فإن الجبر بالرد يكون مستحيلا. كذلك حالة الهجمات السيبرانية التي تهدف إلى سرقة المعلومات، ونشرها على الملأ، فإعادة السرية بعد النشر أمر مستحيل في هذا الوقت.

[1] *Factory at Chorzow* judgement, p. 47

[2] Tallinn Manual 2.0, commentary to rule 29, para. 3, p. 149

انظر أيضا: التعليق على المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دولياً – التعليق على المادة 30 – الفقرة (7) – ص115

وقد يكون الرد العيني صعبا وإن كان غير مستحيل، مثل الحالات التي تدمر البنية التحتية السيبرانية أو غير السيبرانية ويكون من غير الممكن إعادتها إلى ما كانت عليه بينما يمكن أن يؤدي التعويض مهمة الجبر الكامل[1]. مثلا هجوم Stuxnet الذي وقع على منشأة نطنز النووية في إيران –وأدى إلى تدمير أجهزة الطرد المركز– يصعب فيه إعادة أجهزة الطرد المركزي إلى الحالة التي كانت عليها قبل الهجوم، لكن من الممكن جبر الضرر الذي تعرضت له بالتعويض المالي.

مع ذلك ينبغي تذكر أن حالة الرد هي الأساس الذي يهدف إليه جبر الضرر، ولعدم المبالغة في تجنب الرد بدعوى صعوبته، يتوجب قياس صعوبة الرد من جهة، والمنفعة المتأتية من الرد مقارنة بالتعويض، فإذا كان عبء الرد العيني لا يتناسب مع المنفعة المتأتية مقارنة بالتعويض فإنه يمكن القول بصعوبة الرد واللجوء إلى التعويض[2]. فمثلا بالعودة إلى المثال الأخير عبء إصلاح أجهزة الطرد المركزي – برغم صعوبته– قد لا يكون مفيدا مقارنة بالتعويض وإبدال أجهزة جديدة بها، لذلك يتم اللجوء إلى التعويض.

ثانيا: جبر ضرر الهجمات السيبرانية عن طريق التعويض المالي

لا يمكن اللجوء إلى التعويض إلا عندما يتعذر جبر الضرر بالرد، مع ذلك فإنه أكثر أشكال الجبر شيوعاً[3]. التعويض يهدف إلى معالجة الخسارة الفعلية للهجوم الإلكتروني، لذلك يشترط فيه التناسب مع الضرر الذي سببته العملية السيبرانية. والقاعدة العامة في التعويض تشمل الخسائر التي تسبب بها الهجوم السيبراني بالفعل، والمكاسب، والأرباح التي فوتها الهجوم السيبراني على الدولة المتضررة على أن تكون تلك قابلة للتقدير والقياس[4].

فالأضرار التي سببها الهجوم السيبرانية يمكن أن تكون أي ضرر –يمكن تقييمه مالياً– مما تعرضت له ممتلكات الدولة، أو أي ضرر تعرض له أحد موظفيها، أو أحد المواطنين، أو الشركات الخاصة[5]. وقد يكون الضرر هو قيمة الأجهزة، أو البرامج التي أتلفت، أو المبنى الذي تضرر، وقد يكون تكلفة

---

[1] المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دولياً – المادة 35 – ص9-10

[2] Tallinn Manual 2.0, commentary to rule 29, paras. 4-5, pp. 149-150
وانظر: المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دولياً – المادة 32 – ص9؛ المادة 32(ب) – ص12

[3] التعليق على المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دولياً – التعليق على المادة 35 – الفقرة (2) – ص124

[4] المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دولياً – المادة 36(2) – ص10

[5] Tallinn Manual 2.0, commentary to rule 29, para. 7, p. 150

"واجب تخفيف الضرر"[1] مثل كلفة الدفاع السيبراني سواء أكانت تكلفة التقنيات التي استخدمتها الحكومة للتصدي للعملية السيبرانية؟ أم قيمة الشركات الخاصة أم الأشخاص الذين تم استشارتهم في التصدي لهذه المهمة؟ هذا ويدخل في قيمة التعويض ما استخدمته الدولة في عملية التعقب، وتنسيب الهجمات السيبرانية إلى فاعلها.

أما بخصوص التعويض –عما فات من كسب بسبب العملية السيبرانية– فإن دليل (تالين) يشترط أن تكون تلك الأضرار قابلة للقياس، ولا تعتمد على احتمالات مستقبلية يصعب التحقق من واقعيتها[2]. وهناك حالتان أوردتهما لجنة القانون الدولي يمكن قياسهما على الكسب الفائت من العملية السيبرانية أولاهما: فقدان القدرة مؤقتا على استخدام الممتلكات بسبب الهجوم السيبراني[3] مثال ذلك أن يشل الهجوم موقعاً يدر الأرباح؛ بسبب اعتماده المستمر على الإعلانات، فيقطع الهجوم كسبه لعدة أسابيع. والحالة الثانية هي حالة الكسب الفائت بسبب الاستيلاء غير المشروع على الممتلكات[4]، مثلا تصميم لمحرك سيارة بصدد التصنيع فتسرقه العملية السيبرانية، وتبدأ بتصنيعه قبل الدولة الضحية وتستفيد من أرباحه. في الحالتين كلتيهما هناك كسب فائت بسبب العملية السيبرانية قابل للتقدير ويمكن أن يكون أساسا للتعويض[5].

وعادة ما يأخذ التعويض شكلا نقديا، لكن يمكن الاتفاق على غير ذلك بين الأطراف[6]. وغالبا ما يتم الاتفاق على التعويض عن طريق المحاكم الدولية، أو هيئات تسوية المنازعات، لكن يمكن أن يتفاوض الطرفان للوصول إلى اتفاقية تعويض استنادا على قواعد مسؤولية الدولة[7]، وقد سبق أن حدث مثل هذا التفاوض.

ثالثا: جبر ضرر الهجمات السيبرانية عن طريق الترضية

[1] المرجع السابق

[2] Tallinn Manual 2.0, commentary to rule 29, para. 7, p. 150

[3] التعليق على المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دولياً – التعليق على المادة 36 – الفقرة (29) – ص136

[4] المرجع السابق – التعليق على المادة 36 – الفقرة (30) – ص136

[5] هناك حالة ثالثة أوردتها لجنة القانون الدولي وهي الكسب الفائت من عقود الامتياز
انظر: المرجع السابق – التعليق على المادة 36 – الفقرة (31) – ص136

[6] المرجع السابق – التعليق على المادة 36 – الفقرة (4) – ص128

[7] المرجع السابق – التعليق على المادة 36 – الفقرة (11) و(12) – ص130

أخيرا يأتي خيار الترضية والذي يمكن فهم معناه من المادة 37 (2) من قواعد مسؤولية الدولة " إقرار بالخرق، أو تعبير عن الأسف، أو اعتذار رسمي، أو أي شكل آخر مناسب." ويتم اللجوء إليها فقط عندما يكون الرد والتعويض غير ممكنين، أو غير كافيين. هذا يعني أنه يمكن أن تنضم الترضية إلى الرد العيني، أو تنضم الترضية إلى التعويض لجبر الضرر عن الفعل السيبراني غير المشروع، إذا لم يكن أي منهما كافيا لوحده.

ومن أهم الأمور التي تميز الترضية أنه يتم اللجوء إليها عندما يكون الضرر ذا طبيعة غير قابلة للتقييم المالي[1] كالأضرار الأدبية، أو تهديد السلامة دون التسبب بخسائر. إهانة رمز الدولة، أو علمها، أو انتهاك السيادة، أو انتهاك السلامة الإقليمية دون حصول ضرر مادي، مثل العبور غير المشروع للطائرات على إقليمها، أو لسفن في مياهها، أو تعريض طائراتها أو سفنها التي تمر مرورا قانونيا للتشويش[2]. فكل هذه أضرار ناتجة عن أفعال غير مشروعة لا يمكن تقييمها بالمال.

الأمثلة التي أوردتها المادة 37 للترضية (إقرار بالخطأ–تعبير عن الأسف–اعتذار) ليست حصرية، بل هناك عدة أشكال أقل مباشرة يمكن أن تقبل بوصفها أحد صور الترضية. كأن تقوم الدولة بالتحقيق في ملابسات الهجمات السيبرانية الضارة التي صدرت من إقليمها، وكأن تحقق إداريا مع وكلاء الدولة وتأدب المسؤولين الحكوميين، خصوصا في حالة تجاوز الصلاحيات المعطاة لهم. أو أن تصدر محاكمها أحكاما قضائية بتجريم ومعاقبة قراصنة الانترنت غير الحكوميين على إقليمها والذين قاموا بالهجمات السيبرانية الضارة على الدولة المتضررة. أو أن تصدر الدولة تشريعا يجرم قيام الأفراد بشن هذا النوع من الهجمات السيبرانية[3].

تجدر الإشارة إلى أن الترضية يمكن أن تكون مقابلًا نقدياً، أو غير ذلك مما ورد في تعريف الترضية فعبارة "أو أي شكل آخر مناسب" وردت في تعريف الترضية تستوعب حتى الترضية النقدية فتكون هنا مبلغا رمزيا عن أمر لا يمكن تقدير قيمته بالمال[4]. وهذا هو الفرق بين المبلغ الذي يمكن أن يدفع بوصفه ترضية والذي يمكن أن يدفع على أنه تعويض عن خسائر فعلية يمكن قياسها[5].

---

[1] المرجع السابق – التعليق على المادة 37 – الفقرة (3) و(4) و(6) – ص137-139

[2] المرجع السابق – التعليق على المادة 37 – الفقرة (4) – ص137

[3] Tallinn Manual 2.0, commentary to rule 29, para. 10, p. 151

[4] التعليق على المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دولياً – التعليق على المادة 37 – الفقرة (5) – ص138

[5] المرجع السابق – التعليق على المادة 36 – الفقرة (4) – ص128

ومما لا شك فيه أن أهم عنصر لصحة الترضية، هو الهدف منها، وهو جبر الضرر فحسب. فيجب ألا يكون الهدف من الترضية إهانة الدولة المتسببة بالفعل غير المشروع، أو النيل من كرامتها[1]، كذلك ليس الهدف من الترضية أن تكون نوعا من العقاب، بل هي نوع من أنواع جبر الضرر تهدف إلى جبر ضرر الأذى أو الخسارة التي تعرضت لها الدولة المتضررة فقط.

المبحث الثاني

الاستجابة الدولية الممكنة رداً على الهجمات السيبرانية

(عدا الدفاع عن النفس)

يقصد بالمواجهة الدولية للهجمات السيبرانية كيف سيتعامل القانون الدولي معها حين تحدث؟ بل كيف يمنع حدوثها من الأساس؟ وكيف يتحقق عنصر الردع الذي يمنع الدولة المرتكبة للهجمات السيبرانية الخبيثة من إعادة الأمر؟ بل ويمنع أي دولة من أن تتخذ سلوكا غير مشروع في الفضاء السيبراني.

سبق في الفصل الثاني الوقوف على الإجابة عن سؤال متى تعد الهجمات السيبرانية هجوماً مسلحاً يتبعه الرد بالدفاع عن النفس؟ وتم التفصيل في أن الهجمات التي تصل لدرجة الهجوم المسلح يتم مواجهتها بالدفاع الشرعي عن النفس. لكن إذا كانت أدنى من مستوى الهجوم المسلح فماهي الأدوات القانونية التي تمكن الدول للتصدي لها.

[1] المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دولياً – المادة 37(3) – ص10

ومالم يكن ذلك كله واضحًا فإن الحديث عن الأفعال غير المشروعة، والنتائج التي تترتب على الدولة المسؤولة قانونا، لن يكون ذا قيمة في دحر الهجمات السيبرانية، إن لم تلتزم الدول به ولم تضعه موضع التطبيق. فماذا لو لم تلتزم الدولة المسؤولة أو المخطئة بعواقب فعلها غير المشروع، ورفضت الكف عن الهجمات السيبرانية غير المشروعة، أو رفضت جبر الضرر. التساؤل المنطقي التالي بعد إخضاع قواعد القانون الدولي على الفضاء السيبراني هو كيف يمكن فرض الالتزامات الدولية الناشئة في الفضاء السيبراني؟ فإنه يجب التحقق من أن المخالفات التي ترتكبها الدول في الفضاء السيبراني لن تمر دون عقاب.

في هذا القسم سيناقش البحث الأدوات المتوافرة في القانون الدولي للتصدي للمخالفات في الفضاء السيبراني ويمكن تصنيفها في قسمين: قضائي وغير قضائي. فأما القسم القضائي فإنه يعرض ما يمكن أن يقدمه القضاء الدولي للتصدي للهجمات السيبرانية، ليس المقصود هنا، القضاء الجنائي الدولي فإنه ليس موضع اهتمام هذا البحث. في القانون الدولي العام فإن أهم هيئة قضائية دولية هي محكمة العدل الدولية لذلك ستعنى الدراسة بكيفية إمكان أن تفصل المحكمة في دعاوى الهجمات السيبرانية بين الدول.

أما القسم غير القضائي فهو يُعنى بطرق المساعدة الذاتية، وهي الإجراءات التي تستطيع الدول أن تتخذها منفردة وفي إطار قانوني. فمن المتوقع أن تبقى فكرة تحرك المجلس ضد الهجمات وقد تمت مناقشتها في الفصل السابق– السيبرانية فكرة نظرية، أما وسائل المساعدة الذاتية التي تستطيع أن تتخذها الدول منفردة وهي (التدابير القانونية، والتدابير المضادة، وتدابير الضرورة) فهي الملجأ الأكثر واقعية لردع الهجمات السيبرانية، وذلك يستوجب مزيدًا من الاهتمام بتأصيلها القانوني وإطارها الشرعي.

هذا مع تذكر أنه –ونظرا لعجز مجلس الأمن في التحرك لحفظ السلم والأمن الدولي– يمكن تفعيل قاعدة الـ Erga Omne وهي الالتزامات التي تمس المجتمع الدولي ككل والتي إذا ما تم انتهاكها يمكن لأي دولة في المجتمع الدولي أن تتصدى لها بتدابير قانونية. فقاعدة Erga Omne يمكن أن تحمي المصالح الكبرى التي تمس المجتمع الدولي، أما الانتهاكات الثانوية التي تهم أو تمس دولة أو بضع دول وليس المجتمع الدولي ككل فإنه يتم باللجوء إلى طرق المساعدة الذاتية للتصدي لها.

وعليه ينقسم هذا المبحث إلى مطلبين، يناقش المطلب الأول منهما: طرق المساعدة الذاتية باستثناء الدفاع عن النفس (التدابير القانونية، والتدابير المضادة، وتدابير الضرورة). ويناقش المطلب الثاني الهجمات السيبرانية أمام محكمة العدل الدولية.

المطلب الأول

مواجهة الهجمات السيبرانية باتخاذ إجراءات المساعدة الذاتية

يشير مصطلح "المساعدة الذاتية" في السياقات القانونية، إلى شكل من أشكال الانتصاف خارج العملية القانونية العادية التي تشرف عليها السلطة المختصة، والتي بموجبها يأخذ الشخص بزمام الأمور ويستخدم الوسائل المشروعة في محاولة لحماية حقه القانوني أو استعادته دون أمر من المحكمة، فإنه قد يحمي مصالحه بمبادرة شخصية مستندة إلى أفعال مشروعة قانوناً. مثال على هذه المساعدة الذاتية هو استعادة الملكية حينما لا يتم تسديد الثمن. وما لم ينطوِ ذلك على أعمال غير قانونية فإن المساعدة الذاتية مشروعة[1]. أما إذا انطوى أعمال المساعدة الذاتية على استخدام للعنف وتسبت بإصابات للطرف الآخر فإنها تكون غير مشروعة. ذلك لأن أخذ الحق باليد بوسائل غير مشروعة ممنوع في القوانين الداخلية، لكنه –كما سيتبين في هذا المطلب– أحد الركائز الأساسية في القانون الدولي. وإن لم ينص ميثاق الأمم المتحدة على عبارة "المساعدة الذاتية" فإن قواعد مسؤولية الدولة قد ذكرتها في عدة مواضع[2] بوصفها إجراءات تأخذ بها الدول، لتحقيق هدف معين، وقد تكون تلك الإجراءات قانونية كأصل وقد تكون غير قانونية لولا الحالة أو السياق الذي جاءت فيها.

فهناك ما يعرف بالتدابير القانونية –وهي غير ودية، لكنها لا تخالف أي قاعدة في القانون الدولي– يمكن أن تلجأ إليها الدول بوصفها وسيلة من وسائل المساعدة الذاتية، لأهداف متعددة، كأن تتخذها احتجاجا رمزيا، أو محاولة للضغط، أو ومحاولة لمعالجة موقف معين. إلا أنه في ظروف معينة، قد تحتاج الدولة إلى اتخاذ تدابير أكثر صرامة مثل الإجراءات المضادة، والإجراءات المتخذة بدافع

---

[1] Self-help. (2021). In *Legal Information Institute*. Retrieved from https://www.law.cornell.edu/wex/self-help

[2] المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دولياً – المادة 5 – الفقرة (7) – ص55
انظر أيضا: التعليق على المادة 22 – الفقرة (3) – ص97
انظر أيضا: التعليق على المادة 48 – الفقرة (2) و(3) – ص166
انظر أيضا: التعليق على المادة 52 – الفقرة (2) – ص176

الضرورة، أو الدفاع عن النفس في مواجهة العمليات السيبرانية غير المشروعة. كل رد من هذه الردود الثلاثة الأخيرة لو لم تكن جاءت في إطار الرد على فعل غير مشروع لكانت انتهاكا للقانون الدولي، فإن القانون الدولي يتسع لاستخدامها في نطاق الرد على فعل غير مشروع خصوصا العمليات السيبرانية غير مشروعة[1].

والسبب في جعل موضوع المساعدة الذاتية مهما بوجه خاص –على نطاق الهجمات السيبرانية– هو أن تحديد الحقائق على الأرض قد يكون أكثر صعوبة في سياق العمليات السيبرانية، حيث أدت التطورات التكنولوجية والاتصالات الشبكية للدول إلى إخفاء أفعالها بسهولة أكبر، وذلك مما يتيح أن تظل أعمالها العدائية دون المستوى الذي من شأنه أن يثير استجابة واسعة النطاق[2]، كإعلان الحرب أو تحريك صلاحيات مجلس الأمن بموجب الفصل السابع.

وبعبارة أخرى موضوع الهجمات السيبرانية مليء بعدم اليقين، أو ما يعرف بالمنطقة الرمادية ليس فقط بسبب عدم التيقن من هوية الفاعل، بل عدم التيقن من قاعدة قانونية محددة يتم انتهاكها، وبالتالي ما هو الرد الصحيح عليها. مثلا الهجمات التي تبلغ مرحلة استخدام القوة –لكنها لا تصل إلى الهجوم المسلح– لا يمكن الرد عليها بالدفاع عن النفس، ولا يمكن أن تترك دون حساب وكذلك الهجمات التي تقتصر على الآثار الاقتصادية –متجنبة تماما أي أثر حركي– قد يصعب تصنيفها استخدامًا للقوة.

يؤكد Michael N. Schmitt –في عدد من أوراقه– أن المنطقة الرمادية ليست مشكلة افتراضية، بل هي فعلا منطقة مفضلة للدول التي لا تحترم القانون –ويعني روسيا والصين– بهدف شل الدول التي تحترم القانون –ويعني الولايات المتحدة– عن التحرك والرد[3]. فإنهم يأملون في تجنب عواقب وخيمة لانتهاك القوانين الواضحة التي تطورت من خلال المعاهدات والعرف. وأهم الجهود في التصدي

---

[1] Johnson, D. E., & Schmitt, M. N. (2021). Responding to Proxy Cyber Operations Under International Law. *The Cyber Defense Review*, *6*(4), 15–30 [p. 23]. Retrieved from https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/2843482/responding-to-proxy-cyber-operations-under-international-law/

[2] المرجع السابق – ص20

[3] Schmitt, M. N. (2018). "Virtual" Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law. *Chicago Journal of International Law*, *19*(1), 30–67. Retrieved from https://chicagounbound.uchicago.edu/cjil/vol19/iss1/2/

لما يحدث في المنطقة الرمادية، أن يتم الاعتماد على الرد بإجراءات المساعدة الذاتية، لمنع الالتباسات القانونية التي تمنع استجابات الدولة حالًا والسماح للمخالفين بالفرار من التداعيات.

سبق الحديث عن الدفاع عن النفس باستفاضة في الفصل السابق وهو رد– تتخذه الدولة من تلقاء نفسها– على فعل غير مشروع متمثل في استخدام جسيم للقوة يصل إلى حد الهجوم المسلح. أعطاه ميثاق الأمم المتحدة الشرعية المطلوبة، وذكرته قواعد مسؤولية الدولة بوصفه أحد الظروف النافية لعدم المشروعية. يكفي القول إن الجانب الأوسع من الفقه يعد الدفاع عن النفس أحد إجراءات المساعدة الذاتية[1]، ومع ذلك فإن حالة الدفاع عن النفس يجب أن تكون لها خصوصيتها، لأنها تنطوي على استخدام للقوة، بينما باقي إجراءات المساعدة الذاتية لا تنطوي على استخدام للقوة[2]. ولما سبق التفصيل في حالة الدفاع عن النفس ومتطلباتها الخاصة، فالاهتمام يكون هنا بالوقوف على الأنواع الأخرى من أنواع المساعدة الذاتية التي لا تنطوي على استخدام للقوة، وهي التدابير القانونية، والتدابير المضادة، والتدابير المتخذة بموجب حالة الضرورة.

يجب الإشارة إلى أن تقسيمات إجراءات المساعدة الذاتية تختلف من مصدر لآخر. فالبعض يجعل منها (العقوبات، والتدابير المتبادلة، وتعليق المعاهدات، أو إنهاءها، وغيرها)[3]. بيد أنه يمكن القول: إن الأنواع التي تم اخيارها هنا وهي: (التدابير القانونية، والتدابير المضادة، وتدابير الضرورة) تشمل في مضمونها كل تلك المصطلحات. مثلا العقوبات إذا اتخذت بطريقة لا تخالف أي التزام دولي فإنها تدابير قانونية، وإذا اتخذت بطريقة تخالف التزام دولي، فإنها تدخل في حالة الإجراءات المضادة. أما حالة الضرورة فلها من الخصائص ما يتوجب عرضها مستقلةً.

وقبل البدء في استخدام إجراءات المساعدة الذاتية يلزم أولا وجود هجوم سيبراني، نسب بنهج المعايير الشاملة –الذي تم التفصيل فيه– إلى دولة معينة. ثم يلزم قراءة في مستوى الهجوم السيبراني، وقوته، لتحديد ما إذا كان ينتهك أي قاعدة قانونية، وهل يصل إلى عتبة الهجوم المسلح؟ وذلك للبدء بالدفاع عن النفس، أما إذا استبعد الهجوم المسلح، وبالتالي الرد بالدفاع عن النفس فإن للدول الخيار فيما تراه مناسبا من إجراءات المساعدة الذاتية على أن تنطبق شروطها إن وجدت.

[1] Noortmann, M. (2005). *Enforcing International Law*, p. 20. Aldershot, England: Ashgate

[2] المرجع السابق

[3] المرجع السابق – ص33-45

الفرع الأول: التدابير القانونية غير الودية "Retorsion"

هي إجراءات –وإن كانت غير ودية– مشروعة؛ لذلك لا ينظمها القانون الدولي[1]. مثالها تأجيل لزيارات مرتقبة بين البلدين، أو تقليص الدبلوماسيين، أو سحب برامج المساعدات، أو تعليق، أو تقليص، أو إنهاء التمثيل الدبلوماسي، أو العقوبات الاقتصادية، أو تعليق العمل باتفاقيات مما يتماشى مع قانون المعاهدات، أو منع رعايا الدولة المسؤولة من دخول إقليم الدولة المتضررة.

عادة ما يشار إلى التدابير القانونية بمصطلح "الرد بالمثل"، لكن في الحقيقة لا يوجد تماثل بين التدبير القانوني المتخذ، والفعل الذي كان سببا لاتخاذ التدبير. خصوصا في صدد استخدامها ردًّاً على هجوم سيبراني فإن التدبير القانوني –عندئذ– غالبا ما سيكون من طبيعة غير سيبرانية، لأن حصر إمكانية الرد على هجوم سيبراني بمثل الوسيلة يحصر التدابير القانونية في نطاق ضيق جدا، بل إن دليل (تالين) لم يقدم سوى مثال واحد على التدبير القانوني السيبراني، ونصه هو: "استخدام قائمة الوصول إلى الإنترنت لمنع الاتصالات من دولة أخرى"[2]. لذلك من الأفضل درءًا للحيرة –أن يعتمد مصطلح التدابير القانونية بدل الرد بالمثل لما في الأول من مقاربة للمعنى الحقيقي لتلك الإجراءات أكثر من الأخير.

وتعد التدابير القانونية الاستجابة الأكثر شيوعاَ للعمليات العدائية السيبرانية[3] بوصفها أحد أنواع المساعدة الذاتية أحادية الجانب، على الرغم من أنها "غير ودية من منظور الكيان الذي يتم توجيهها ضده. فضلًا عن أن التدابير القانونية تعد وسيلة قوية لدفع الدولة للرجوع عن الفعل أو ردعه مستقبلا، فقد يؤمَّل من اتخاذها أن تراجع الدولة المسؤولة نفسها، وتكف عن الأعمال التي تقوم بها، أو لا تكرر

---

[1] ورد ذكرها مرة واحدة في التعليق على قواعد مسؤولية الدولة بعبارة "التصرف غير الودي" لتمييزها عن الإجراء المضاد وتم الاكتفاء بالقول: انها إذا لم تخالف أي التزام قانوني قائم فهي لا تنطوي على تدابير مضادة. انظر:
التعليق على المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دولياً – في التعليق على الفصل الثاني "التدابير المضادة" – الفقرة (3) – ص166

[2] مثلا لم يرد أي تفصيل ينظم التدابير القانونية في قواعد مسؤولية الدولة، وإنما جاء ذكرها في أثناء تمييز التدابير المضادة حيث نصت المسودة على:" وتختلف التدابير المضادة عن الرد بالمثل، أي التصرف "غير الودي" الذي لا يتسق مع أي التزام دولي للدولة التي تقوم به، حتى لو كان رداً على فعل غير مشروع دولياً، ومهما تكن دوافع مثل هذه الأفعال، فما دامت غير متعارضة مع الالتزامات الدولية -للدول التي تقوم بها تجاه الدولة المستهدفة- فإنها لا تنطوي على تدابير مضادة، ولا تدخل ضمن نطاق هذه المواد"
انظر: التعليق على المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دولياً – في التعليق على الفصل الثاني "التدابير المضادة" – الفقرة (3) – ص166

[3] Arimatsu, L., & Schmitt, M. N. (2021). The Plea of Necessity: An Oft Overlooked Response Option to Hostile Cyber Operations. *International Law Studies*, *97*, 1171-1199 [p. 1173]. Retrieved from https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=2983&context=ils

الأمر في المستقبل. وعلى سبيل المثال، يذكر ملف ردة إدارة أوباما على التدخل الروسي السيبراني العدائي في الانتخابات الرئاسية لعام 2016 بطرد الدبلوماسيين، وفرض الضرائب لتكون عقوبات اقتصادية على المنتجات الروسية[1].

وتعد خيارات التدابير القانونية استجابة مفيدة بخاصة للرد على عملية إلكترونية لا تنتهك القانون الدولي، أو تكون ذات طابع قانوني غامض بدلاً من المخاطرة في المواقف التي يطغى فيها عدم اليقين، بشأن ما إذا كانت العملية الإلكترونية التي تعرضت لها الدولة مشروعة؟ أو أنها غير قانونية، أو إذا كانت غير قانونية فماهي القاعدة التي تنتهكها على وجه الدقة؟ هنا يمكن الرد بالتدابير القانونية[2]. فهي خيار قانوني عند الرد على العمليات السيبرانية التي لا تنتهك القانون الدولي، وهي تقلل من التبعات السياسية والقانونية للرد المتخذ.

بالإضافة إلى ذلك، لا تحتاج الدولة من الناحية القانونية إلى إسناد العملية السيبرانية إلى دولة أخرى قبل الانخراط في أعمال التدابير القانونية، فقد يكون من الصعب الحصول على دليل واقعي للإسناد ويجب الرد على العملية السيبرانية قبل اكتمال نتائج التحقيق فيها والتي قد تستغرق عدة أشهر، فهنا شبهة التورط تكفي للرد. على افتراض أن ذلك يتوافق مع القانون المحلي للدولة[3]. ببساطة فإن أفعال التدابير القانونية هي دائما خيار استجابة متاح؛ لأنها إجراءات قانونية؛ غير مقيدة بالمتطلبات القانونية الدولية التي تصاحب إجراءات المساعدة الذاتية الأخرى، كالدفاع عن النفس، أو الإجراءات المضادة. مع ذلك، فإنه يتوجب على الدولة التي تختار السلوك المسؤول –أمام التزاماتها القانونية– أن تتخذ التدابير القانونية فقط عندما يكون ذلك معقولاً في ظل الظروف وبحسن نية[4]. كذلك يجب تذكر أن التدابير القانونية لها استخدام محدود؛ لأنها على عكس التدابير المضادة؛ فإنها يجب أن تظل ضمن حدود القانون الدولي بشكل صارم.

قد يجدر التوقف عند التجربة الأوروبية الفريدة في هذا المجال، فقد تم الإعلان عن "صندوق أدوات الدبلوماسية الإلكترونية" لأول مرة عام 2017. يشتمل صندوق الأدوات على تدابير دبلوماسية ضمن

---

[1] The White House. (2016, December 29). Statement by the President on Actions in Response to Russian [Press release]. Retrieved from https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/statement-president-actions-response-russian-malicious-cyber-activity

[2] المرجع السابق – Johnson, D. E., & Schmitt, M. N. – ص22-23

[3] المرجع السابق – ص22

[4] المرجع السابق – ص22

السياسة الخارجية والأمنية المشتركة للاتحاد الأوروبي، والتي يمكن استخدامها ضد العمليات السيبرانية الخبيثة الموجهة ضد الدول الأعضاء في الفضاء الإلكتروني[1]. يرى الاتحاد الأوروبي أن اتباع نهج مشترك وشامل للدبلوماسية الإلكترونية يمكن أن يسهم في منع نشوب النزاعات، والتخفيف من تهديدات الأمن السيبراني وزيادة الاستقرار في العلاقات الدولية[2].

أما عن ماهية التدابير الدبلوماسية المطروحة فقد وصفت أنها تدابير "مقيدة" دون تحديد ماهيتها تماما إلا أنها استجابة لعمليات سيبرانية خبيثة "ستكون متناسبة مع نطاق النشاط السيبراني، وحجمه، ومدته، وكثافته، وتعقيده وتطوره وتأثيره"[3]. وهذا الوصف للأدوات الدبلوماسية يمكن أن يكون أي شيء بين الإدلاء ببيانات إدانة، إلى ما هو أكثر قسرية، مثل فرض بعض العقوبات. وفي عام 2020، استخدم مجلس الاتحاد الأوروبي صندوق أدوات الدبلوماسية الإلكترونية" لأول مرة؛ لفرض حظر سفر وتجميد أصول بالإضافة إلى ذلك، يُحظر على الأشخاص والكيانات في الاتحاد الأوروبي إتاحة الأموال لأولئك المدرجين في قائمة مكونة من ستة أفراد وثلاثة كيانات مسؤولة عن هجمات إلكترونية مختلفة أو متورطة فيها. وتشمل هذه الهجمات محاولة الهجوم السيبراني ضد منظمة حظر الأسلحة الكيميائية (OPCW) وهي المعروفة باسم "WannaCry" و"NotPetya" و" Operation Cloud Hopper"[4].

الفرع الثاني: التدابير المضادة

تُعَرِّف لجنة القانون الدولي التدابير المضادة أنها "التدابير التي كانت لتتعارض مع الالتزامات الدولية لدولة متضررة تجاه دولة مسؤولة، **لو لم** تتخذها الدولة الأولى رداً على فعل غير مشروع دولياً – ارتكبته الدولة الأخيرة– من أجل ضمان الكف عن هذا الفعل أو جبر الضرر"[5] وترى لجنة القانون

---

[1] NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). (n.d.). European Union Equipping Itself against Cyber Attacks with the Help of Cyber Diplomacy Toolbox. Retrieved from https://ccdcoe.org/incyder-articles/european-union-equipping-itself-against-cyber-attacks-with-the-help-of-cyber-diplomacy-toolbox/

[2] المرجع السابق

[3] المرجع السابق

[4] European Council. (2020, July 30). *EU imposes the first ever sanctions against cyber-attacks* [Press release]. Retrieved from https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/

[5] التعليق على المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دولياً – في التعليق على الفصل الثاني "التدابير المضادة" – الفقرة (1) – ص166

الدولي أنها تستخدم في نظام لا توجد فيه سلطة مركزية تحاول بواسطته الدولة المتضررة حماية حقها، واستعادة الوضع القانوني بينها وبين الدولة المسؤولة[1]. ومن أمثلة التدابير المضادة وقف الفوائد التي تعود على الدولة من اتفاقية نقل جوي وقفاً لا تسمح به الاتفاقية نفسها أو قانون المعاهدات عامةً. أو تجميد أرصدة الدول المسؤولة برغم وجود معاهدات لا تسمح بمثل هذا التصرف، أو تعليق حقوق العبور، لكن أهم مثال للتدابير المضادة في نطاق الرد على الهجمات السيبرانية هو الرد بالمثل Hack Back، أي القيام بعملية سيبرانية مضادة لا تصل في آثارها إلى مستوى استخدام القوة. مثل تلك العملية غير مشروعة ابتداءً لولا انها تأتي في إطار الرد على هجوم سيبراني غير مشروع.

ليس هناك شك –فيما يخص الهجمات السيبرانية– في أن قانون مسؤولية الدولة عن التدابير المضادة ينطبق في الفضاء الإلكتروني. فإنه يجوز للدولة المتضررة –بفعل غير مشروع دولياً– اللجوء إلى تدابير مضادة متناسبة، بما في ذلك التدابير المضادة السيبرانية، ضد الدولة المسؤولة". ويمكن الوصول إلى هذا الاستنتاج بسهولة بالاعتماد على المبادئ المنصوص عليها في المواد المتعلقة بمسؤولية الدولة. وهذا استنتاج مهم بسبب شيوع العمليات الإلكترونية الضارة التي لا يمكن الرد عليها باستخدام القوة، فهي تعطي الدولة الحق في أن تحفظ مصالحها وأمنها وكرامتها، وأن وترد بالتدابير المضادة. مع ذلك –ونظرًا للقيود الواسعة المفروضة على استخدامها– قد لا يكون فيها الدواء الشافي لردع العلميات السيبرانية الضارة بقدر ما هو موجود في التدابير القانونية.

يتبين من تعليق لجنة القانون الدولي –المصاحب للمواد– أن الإجراءات المضادة هي إجراءات وإن كانت غير مشروعة أساسا – لكنها تصبح مشروعة بسبب مخالفة من الدولة المسؤولة، أو صدور اعتداء منها. وبعبارة أخرى، تكون الدولة التي تلجأ إليها في تلك الظروف منطلقة من سبب معقول، أو تكون معذورة بموجب القانون الدولي على الرغم من أنها أعمال غير قانونية من الناحية الفنية البحتة. وفي ذلك ذكرت محكمة العدل الدولية في قضية مشروع غابتشيكوفو – ناغيماروس:

"أن التدابير المضادة قد تبرر تصرفاً – غير مشروع لولا أنه – تم القيام به رداً على فعل غير مشروع دولياً قامت به دولة أخرى، وكان موجها ضد تلك الدولة المتضررة"[2]

[1] المرجع السابق – في التعليق على الفصل الثاني "التدابير المضادة" – الفقرة (1) – ص166

[2] Gabčíkovo-Nagymaros Project (Hungary/Slovakia), Judgment, I.C.J. Reports 1997, p. 7 [p. 42, para. 55]

وكانت الإجراءات المضادة –تاريخًا– تسمى في الأصل عمليات الثأر المشروعة، فالثأر والانتقام كان ممارسة مقبولة، لعدة قرون في القانون الدولي.[1] مثلا في القرن الثامن عشر وصف فقيه القانون الدولي Emer de Vattel الأعمال الانتقامية بأنها ضرورية "لنظام الإدارة الذاتية للعدالة بين الدول"[2]. ذلك لأنه كان شائعا –عبر التاريخ– أن ينخرط أصحاب السيادة من الدول والممالك في أعمال انتقامية مثل الاستيلاء على الممتلكات الأجنبية الخاصة؛ من أجل الوفاء بديون غير مدفوعة أو عقود مخالفة أو مع مرور الوقت، تم التخلي عن الغرض الأصلي من التدابير الوقائية وهو الانتقام أو التعويض، وتحولت إلى وسيلة للإكراه القانوني، تهدف إلى التأثير على سلوك الدولة المخالفة للقانون[3]. فاليوم لا يجوز للدولة المتضررة أن تستخدم التدابير المضادة؛ للانتقام، أو لمعاقبة الدولة المسؤولة والهدف المشروع الوحيد هو تنفيذ التدابير المضادة لحمل الدولة المسؤولة على الامتثال لالتزاماتها الدولية، فقط[4]. وقد يكون ذلك عن طريق الكف عن الفعل غير المشروع، أو اصدار التأكيدات والضمانات بعدم التكرار أو التعويضات.

لا يمكن للتدابير المضادة أن تنطوي على استخدام القوة أو من باب أولى لا يمكن أن تصل إلى درجة الهجوم المسلح، حتى لو كانت ردا على استخدام القوة. هذا أمر لا خلاف فيه وإلا ضاعت الخطوط بين الرد بالدفاع عن النفس والرد بالإجراءات المضادة. يتوافق هذا الموقف مع فقه محكمة العدل الدولية[5] ويتم تكراره في المادة 50 (1) (أ) من المواد المتعلقة بمسؤولية الدولة[6].

ومع ذلك لا بد من ذكر أن هناك نقاشا فقهيا متزايدا حول إمكانية وجود تدابير مضادة قد يكون فيها استخدام للقوة المسلحة؛ لسد الفراغ أو المنطقة الرمادية؛ وذلك حين يعد الهجوم الذي تعرضت له الدولة استخدامًا للقوة، لكنه لا يصل إلى حد الهجوم المسلح. وذلك عندما تبدو الإجراءات المضادة التي لا

---

[1] التعليق على المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دولياً – التعليق على المادة 22 – الفقرة (3) – ص97

[2] Schmitt, M. N., & Watts, S. (2021). Collective Cyber Countermeasures? *National Security Journal by Harvard Law School, 12,* 373–411 [p. 380]. Retrieved from https://harvardnsj.org/2021/06/collective-cyber-countermeasures/

[3] المرجع السابق – ص381

[4] المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دولياً – المادة 49(1) – ص14

[5] *Corfu Channel* judgement, para.35, p. 17; *Nicaragua* judgement, para. 149, p. 127

[6] "الالتزامات التي لا تتأثر بالتدابير المضادة ١ -لا تمس التدابير المضادة بالالتزامات التالية: (أ) الالتزام المنصوص عليه في ميثاق الأمم المتحدة بالامتناع عن التهديد باستعمال القوة أو استعمالها فعلاً؛"
انظر: المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة – المادة 50(1)(أ)

تنطوي على استخدام القوة غير كافية[1]. لكن لأغراض هذا البحث فالتدابير المضادة –كما قررت محكمة العدل الدولية وقواعد مسؤولية الدولة– هي تدابير لا تنطوي على استخدام القوة.

هنا لا بد من العودة إلى الخلاف حول أي الهجمات السيبرانية تدخل في إطار استخدام القوة، فالدول التي عدت الهجمات السيبرانية ذات الأثر غير الحركي قوة – وقد تم تعداد مواقف ست منها في المبحث الأول من الفصل الثاني في مطلب مدى اعتبار الهجوم السيبراني هجوما مسلحا– لن تتمكن من استخدام تلك الهجمات –التعطيلية ذات الأثر غير الحركي– كتدابير مضادة. فكما تمت الإشارة إليه في المبحث الأول من الفصل الثاني إن العديد من الدول صرحت بأن الهجمات التي تؤثر على اقتصادها أو تتسبب بتعطيل جسيم لخدمات ومرافق الدولة تعتبرها قوة تؤهل حق الدفاع عن النفس، تلك الدول حرمت على نفسها استخدامها في إطار التدابير المضادة. وكان ذلك أحد مسوغات الفريق الذي يشجع على عَدِّ الهجمات التعطيلية قوة تؤهل للرد بالدفاع عن النفس، وهو أنها ستدخل في دائرة المنع وفقا للمادة 2(4).

فالرأي القائل بتكييف الهجمات السيبرانية التعطيلية ذات الأضرار الاقتصادية استخداما غير مشروع للقوة له أسباب تشجيعيه ومنها: إخراج هذا النوع من الهجمات من نطاق التدابير المضادة وبالتالي التقليل من إمكانية اللجوء إليها. ويمكن الرد على ذلك بالقول: إن كان تصنيف الهجمات السيبرانية التعطيلية بوصفها استخداما للقوة يقيد اللجوء إليها بوصفها تدبيرا مضادا، فإنها تفتح المجال للرد بالدفاع عن النفس بشكل كبير، لانتشار الهجمات ذات الأثر التعطيلي أكثر من الهجمات ذات الأثر الحركي. والأولى بالتضييق هو الدفاع عن النفس–لا الهجوم السيبراني ذو الآثار الاقتصادية–الذي قد تستخدم فيه أسلحة فتاكة أكثر من السلاح السيبراني. ثم إن ترك المجال لاستخدام الهجمات السيبرانية ذات الأثار التعطيلية الاقتصادية فيه حل لمشكلة الفراغ بين استخدام القوة والهجوم المسلح – والتي عادة ما تستخدم مسوغاً للجوء لمذهب الهجوم المسلح التراكمي، أو فتح المجال أمام استخدام القوة في التدابير المضادة– وينفي الحاجة إلى تحويل التدابير المضادة إلى النطاق القسري.

إن التدابير المضادة وحدودها تناولتها المواد 22 و49–54 من قواعد مسؤولية الدولة عن الأفعال غير المشروعة دولياً وأن التعامل فيها يكون مع التدابير المضادة على أنها أحد "الظروف النافية لعدم المشروعية". وتنظيم التدابير المضادة بالكيفية التي وضعتها لجنة القانون الدولي يعكس القانون الدولي

[1] انظر لموقف القاضي سيما في محكمة العدل الدولة في قضية المنصات النفطية ورأيه المنفصل في ذلك الموضوع:
Oil Platforms judgement, separate opinion of Judge Simma, para. 13, p. 333

العرفي في معظمة إلا أن هناك بعض الشروط المتشددة التي وضعتها لجنة القانون الدولي مازالت محل جدل، ومازالت بحاجة إلى تأكيد قبولها أو رفضها من قبل الدول.

القسم الأول: شروط التدابير المضادة

وصف البروفيسور جيمس كروفورد عمل لجنة القانون الدولي –بشأن مسؤولية الدولة تجاه الإجراءات المضادة– بأنها "ربما كانت الجانب الأكثر صعوبة، وإثارة للجدل في كامل نظام مسؤولية الدولة " كدليل على مخاوف اللجنة بشأن التوسع في استخدام التدابير المضادة[1]. ذلك أن الإجراءات المضادة يمكن أن تؤدي إلى التصعيد، أو تدهور في العلاقات الدولية، وربما وصلت إلى نشوب الحرب إذا لم تستخدم وفق غرضها الصحيح. لذلك عددت لجنة القانون الدولي شروطا واسعة، إجرائية وموضوعية، على الدول الامتثال لها في لجوئها إلى التدابير المضادة. فعلى الرغم من أن الإجراء المضاد فعل غير مشروع من الناحية الفنية البحتة، إلا أن الحدود المنصوص عليها في المواد المتعلقة بمسؤولية الدولة هي بمنزلة إطار لمشروعية الفعل المضاد، إذا ما تمت مراعاتها في أثناء اللجوء إلى التدبير المضاد، يستبعد عدم مشروعية التدبير المضاد. وفي المقابل إذا لم يتم مراعاتها؛ فإن ذلك من شأنه أن يحول الموقف القانوني للدولة التي قامت به من دولة متضررة إلى دولة مسؤولة عن فعل غير مشروع. ولسوف نعرض تلك الشروط تباعاً.

أولا: أن يكون الهدف من الإجراء المضاد تصحيح وضع مخالف للقانون

المطلوب في نطاق الهدف ألا يكون هو الانتقام أو العقاب، فلا بد أن الإجراءات المضادة دائما تكون بغية الحق لا العقاب[2]. ويبدو اشتراط مثل هذا الهدف منطقيا خصوصًا إذا ما قورن بحالة الدفاع عن النفس، ويكون الهدف وقف الهجوم المسلح، وليس الانتقام والتصعيد. كذلك الإجراءات المضادة هدفها إصلاح المخالفة القانونية، أو إعادة العلاقة القانونية بين الدولة المتضررة والدولة المسؤولة. جاء في تسويغ اشتراط هدف معين في التدابير المضادة في قضية تحكيم Air Service الآتي: "[ج] الإجراءات

[1]المرجع السابق – Schmitt, M. N., & Watts, S. – ص382

[2] التعليق على المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دولياً – التعليق على المادة 49 – الفقرة (7) – ص169

المضادة ... يجب أن تكون رهانًا على الحكمة، وليس على ضعف الطرف الآخر. ويجب استخدامها بروح الاعتدال الكبير وأن تكون مصحوبة بجهد حقيقي في حل مشكلة نزاع.[1]"

على سبيل المثال، إذا نفذت الدولة "أ" عملية إلكترونية استهدفت الدولة "ب" وتسببت في إتلاف جزء كبير من البنية التحتية الصناعية لها، فتقوم الاخيرة بإجراء مضاد، يهدف إلى إحداث أضرار مماثلة للبنية التحتية للدولة "أ". مثل هذا الإجراء المضاد لا رجوع فيه، وهو مدفوع بالانتقام بدلاً من إجبار الدولة المسؤولة على وقف انتهاك التزام قانوني، وبالتالي يعد الإجراء المضاد غير مشروع[2].

تكمن أهمية الهدف أيضا في تحديد وقت التوقف عن التدابير المضادة. فالتدبير المضاد يجب أن يتوقف إذا تحقق الهدف، وهو تنفيذ الدول المسؤولة التزامها القانوني[3]. وهنا تقدم التدابير المضادة مجالا أوسع للدفاع عن النفس، فالدفاع عن النفس يتوقف بمجرد ردع الهجوم المسلح. أما التدابير المضادة فلا يشترط أن تتوقف إذا توقفت الدولة عن الفعل غير المشروع دولياً، لأن التزامها القانوني قد يكون متواصلا، مثل تقديم التأكيدات والضمانات بعدم التكرار في بعض الأحيان أو جبر الضرر إن وجد، وبالتالي يمكن للدولة المتضررة أن تستمر في التدابير المضادة حتى تحصل على تعويض عن الضرر، أو على الأقل تبدأ عملية المفاوضات بخصوص التعويض.

قد يكون التدبير المضاد مصمما لإعطاء الدولة الخيار أن تعود إلى التزامها القانوني بنفسها، أو يكون مصمما لإجبارها–ودون خيار منها– على تصحيح مخالفتها القانونية. ويعطي دليل (تالين) مثالاً موضحاً تلك الفكرة. فلنفترض أن هناك دولتين أنهتا للتو نزاعًا مسلحًا دوليًا. تملك الدولة الأولى قاعدة بيانات، بشأن أسماء ومواقع المدنيين الذين شردهم المسلحون في المنطقة الحدودية بين الدول، وتقوم بتحديثها باستمرار. وفي سلوك يخالف قانون النزاع المسلح –بخصوص واجب تسهيل إعادة توحيد العائلات عقب النزاع المسلح[4]– ترفض الدولة الأولى الإفصاح عن المعلومات إلى الدولة الثانية. ومن باب التدبير المضاد، يمكن للدولة الثانية أن تقوم باختراق شبكة الكمبيوتر الحكومية للدولة الأولى، وتنسخ قاعدة البيانات لاستخدامها لتمكين لم شمل العائلات. وعلى ضوء استمرار رفض الدولة الأولى

[1] *Air Service* arbitral award, p. 2, para. 91; Tallinn Manual 2.0, commentary to rule 21, para. 2, p. 117

[2] Tallinn Manual 2.0, commentary to rule 21, para. 2, p. 117

[3] المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دولياً – المادة 52 – ص14-15

[4] اتفاقية جنيف الرابعة بشأن حماية الأشخاص المدنيين في وقت الحرب – مادة 26

انظر أيضا: الملحق (البروتوكول) الأول الإضافي إلى اتفاقيات جنيف والمتعلق بحماية ضحايا المنازعات الدولية المسلحة – المادة 74

لتقديم المعلومات تستمر الدولة الثانية في سرقة المعلومات المحدثة من قاعدة البيانات بانتظام[1]. مثل هذا التدبير مصمم لوقف المخالفة جبرا وليس باختيار الدولة المسؤولة وليس في هذا النوع من التدابير ما يجعله غير مشروع.

إذا كان التدبير المضاد هو إنهاء معاهدة دولية أو تعليقها، فإن لجنة القانون الدولي توجه النظر إلى التمييز بين الحق في إنهاء أو تعليق المعاهدة لان الطرف الآخر أخل بالتزام جوهري فيها بمقتضى المادة 60 من اتفاقية فيينا، وبين تعليق المعاهدة كتدبير مضاد الذي يكون هنا وقتياً ومرتبطاً بهدف محدد، ففي الحالة الثانية إذا تحقق الهدف من التدبير المضاد –وهو إعادة الوضع القانوني إلى ما كان علية قبل الفعل غير المشروع– ينتهي مبرره وبالتالي تنتهي مشروعية الاستمرار في تعليق المعاهدة.[2] وليس هناك ما يمنع أن تجمع الدولة بين الأمرين، فتنهي الدولة التزامها بالمعاهدة اعتمادا على المادة 60 من اتفاقية فيينا لكن تستمر في اتخاذ إجراءات مضادة حتى حصولها على التعويض.

ثانيا: أن يكون التدبير من دولة متضررة ضد دولة خالفت القانون الدولي ونسبت المخالفة إليها

يجب قبل البدء في تنفيذ التدابير المضادة أن تكتمل عناصر مسؤولية الدولة، بموجب قواعد مسؤولية الدولة، من فعل غير مشروع، ينسب إلى دولة معينة. ذلك لأن الفعل غير المشروع هو الذي يحول التدبير المضاد من تدبير غير مشروع إلى فعل مشروع، فهو يأتي في سياق الرد على خرق أولي وتصحيح مخالفة للقانون[3].

كذلك لابد من نسبة الفعل إلى دولة. فوفقًا للجنة القانون الدولي، يجوز للدولة **المتضررة فقط**[4] اتخاذ إجراءات مضادة ضد **الدولة المسؤولة فقط**[5]، فلا يمكن توجيه الإجراءات المضادة إلا ضد دول ذات سيادة، فلا يمكن اتخاذ إجراءات مضادة ضد أشخاص، أو كيانات خاصة، ولا تصدر الإجراءات المضادة من دولة ضد جماعات فاعلة من غير الدول. لكنها تكون موجهة ضد الدولة المسؤولة، حتى

[1] التعليق على المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دولياً – التعليق على المادة 21 – الفقرة (3) – ص95
[2] المرجع السابق – في التعليق على الفصل الثاني "التدابير المضادة" – الفقرة (4) – ص167
[3] المرجع السابق – التعليق على المادة 49 – الفقرة (2) – ص169
[4] لمعرفة راي لجنة القانون الدولي في إمكان اتخاذ تدابير من غير الدولة المتضررة انظر: المرجع السابق – في التعليق على الفصل الثاني "التدابير المضادة" – الفقرة (8) – ص168
[5] المرجع السابق – التعليق على المادة 49 – الفقرة (4) – ص169

لو وقعت على أصول الجماعات الفاعلة غير الحكومية[1]. إذا لا بد من كون الفعل صادرًا من دولة في مواجهة دولة.

إن عبارة: "لا يحق سوى للدولة المتضررة أن تلجأ للتدابير المضادة" لا تعني اشتراط حدوث ضرر من الفعل غير المشروع، لتتمكن الدولة من اتخاذ التدابير المضادة، وقد مر تفصيل ذلك في بداية هذا الفصل، وتقرر أن المسؤولية الدولية لا تتطلب ضررا، بل فعلًا غير مشروع منسوبًا إلى دولة ولا، يشترط الضرر إلا في مجال جبر الضرر. لكن" يقصد بكلمة الدولة المتضررة هنا هو أن "تكون الدولة متضررة إذا كان الالتزام الذي خرق واجباً تجاهها بمفردها[2].

إن قصر حصر الحق في اتخاذ التدابير المضادة على الدولة المتضررة من أكبر القيود التي تفرضها طبيعة التدابير المضادة مقارنة بالدفاع عن النفس، حيث هناك مبدأ الدفاع الجماعي عن النفس.[3] لذلك بالعودة إلى "صندوق أدوات الدبلوماسية الإلكترونية" الذي أنشأه الاتحاد الأوروبي، نرى أن تلك الأدوات الدبلوماسية لا يمكن أن تتخطى التدابير القانونية؛ وصولا إلى التدابير المضادة؛ لأن هناك عائقًا وهو أنه يحق فقط للدولة المتأثرة بالنشاط السيبراني الضار اللجوء إلى الإجراءات المضادة، مما يحد من إمكانية قيام دول أعضاء أخرى في الاتحاد الأوروبي بمساعدة الدولة المتضررة، نظرًا لأن استجابتهم يجب ألا تصل إلى مستوى الإجراءات المضادة. لذلك سيبقى صندوق الأدوات الدبلوماسية الإلكترونية مقتصرا على التدابير القانونية[4].

---

[1] Stockburger, P. Z., & Schmitt, M. N. (2018, June). *Due Diligence in Cyberspace - CyCon 2018*. Panel discussion presented at the 10th International Conference on Cyber Conflict, Tallinn, Estonia. Retrieved from https://youtu.be/YOIuiNfaZU8

[2] التعليق على المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دولياً – التعليق على المادة 42 – الفقرة (6) – ص153

[3] المرجع السابق – Arimatsu, L., & Schmitt, M. N. – ص1181

[4] تجدر الإشارة أن رئيسة إستونيا في خطابها الافتتاحي لمؤتمر CyCon 2019 أن إستونيا اعتبرت أن اتخاذ تدابير مضادة من دول غير الدول المتضررة يعتبر قانوني، وذلك تطبيقا للتعاون الدولي الذي تطلبه طبيعة الهجمات السيبرانية فهي تتطلب تعاوناً دوليا ويجب ان تساعد الدولة القادرة على اتخاذ إجراءات مضادة الدول المتضررة غير القادرة على الرد على الهجمات السيبرانية الخبيثة. لكن فرنسا في إعلانها الصادر في 9 سبتمبر 2019 بشأن كيفية تطبيق القانون الدولي على الإنترنت، عارضت موقف استونا واعتبرته غير قانوني. لذلك حتى الآن الأمر الوحيد المتفق عليه هو ان الدولة المتضررة من حقها اتخاذ إجراءات مضادة، اما غير الدولة المتضررة فالأمر غير متفق عليه، ولم يقترب من نطاق الشرعية بعد. للمزيد عن ذلك انظر الورقة

Roguski, P. Ł. (2020). *Collective Countermeasures in Cyberspace – Lex Lata, Progressive Development or a Bad Idea?* Presented at the 2020 12th International Conference on Cyber Conflict. Retrieved from https://ccdcoe.org/uploads/2020/05/CyCon_2020_2_Roguski.pdf

انظر أيضا: المرجع السابق – Schmitt, M. N., & Watts, S.

متطلبات المسؤولية الدولية من الفعل غير المشروع المنسوب إلى دولة نفسها تنطبق في سياق الهجمات السيبرانية. فقط عندما يكون النشاط السيبراني يتخطى خط الشرعية يكون اللجوء إلى الإجراءات المضادة مسموح بها؛ لذلك يعد التمييز بين الحقوق والمصالح أمرًا بالغ الأهمية، فالمصالح واسعة تختلف باختلاف الدولة. "ونظام الحكم فيها، أما الحق فهو المحمي بقاعدة من قواعد القانون الدولي، أيا كان مصدرها العرف أو المعاهدة أو المبادئ العامة[1].

أما ما يتعلق بالشق الثاني من المسؤولية الدولية (وهو نسبة الفعل إلى دولة) من المهم التأكيد أن التدابير المضادة ليست متاحة استجابة لعملية إلكترونية ما لم تُنسب العملية إلى دولة. فلا يمكن لدولة كانت ضحية عمليات سيبرانية من شركة أجنبية معينة، أن تطلق إجراءات مضادة ضد تلك الشركة، ما لم يكن الفعل غير المشروع الذي قامت به الشركة يمكن أن يُعزى إلى دولة معينة (القاعدتان 15 و17) أو كان بسبب فشل تلك الدولة في السيطرة على أنشطة الشركة، وبالتالي خرق التزام العناية الواجبة للسيطرة على ما يصدر من إقليمها بمجرد علمها بالعمليات[2].

أما بخصوص احتمالية الخطأ المرتفعة في عملية التنسيب السيبراني، وما يتبعها من احتمالية توجيه إجراءات مضادة ضد الدولة، فينبغي التنبيه هنا، على أن الإجراءات المضادة تتطلب تدرجا اجرائيا معينا في التنفيذ يقلل نسبة الخطأ في التنسيب السيبراني، ومن هذه الإجراءات: الإخطار وسيناقش لاحقا (في الشرط السادس)، لكن المشكلة في التدابير التي تتخذ بصفة الاستعجال وهو قانونية – وتعفى فيها الدولة من الإخطار– فإمكانية الخطأ في التنسيب السيبراني دائما قائمة بسبب الطبيعة السيبرانية، وبالتالي –ومن دون اجراء الإخطار– قد يتم مباشرة الإجراء المضاد لتتفاجأ به جهة لا تستحقه. هنا يمكن التذكير بالنتيجة التي تم التوصل إليها عند الحديث عن تنسيب الفعل السيبراني، وهي أنه إذا كانت النتيجة التي توصلت إليها الدولة معقولة مقارنه بأي دولة أخرى في نفس ظروفها، فإن التدبير المضاد الذي ستتخذه بناء على تلك النتيجة الخاطئة لا يعد عندئذ غير قانوني، مع عدم الإضرار بحق الدولة ضحية التدابير الخاطئة بالتعويض.

تجدر الإشارة إلى أن المكان الذي ينطلق منه التدبير المضاد السيبراني أو غير السيبراني لا يؤثر عادة على مشروعية الإجراء المضاد. لكن أحيانا يمكن أن يؤثر الموقع على جوانب أخرى في القانون

[1] Schmitt, M. N., & Pitts, M. C. (2015). Cyber Countermeasures and Effects on Third Parties: the International Legal Regime. *International Law from a Baltic Perspective, 14*, 258–280 [p. 261]. https://doi.org/10.1163/9789004433151_011

[2] Tallinn Manual 2.0, commentary to rule 20, p. 113, para. 7

الدولي. مثلا أن يسافر عملاء الدولة "أ" المتضررة إلى الدولة "ب" –وهي دولة محايدة– لإطلاق عملية إلكترونية ضد الدولة "ج" المسؤولة، إذا حدث ذلك بدون إذن الدولة "ب" فإن وكلاء الدولة "أ" يكونوا قد انتهكوا سيادة الدولة "ب" وقد يكون ذلك سببا لإثارة مسؤولية الدولة "أ" ومع ذلك، يكون التدبير المضاد قانونياً فيما يتعلق بالدولة "ج".[1]

ثالثا: أن يكون التدبير المضاد قابلاً للإلغاء

يجب اتخاذ تدابير مضادة مؤقتة أو قابلة للإلغاء أو لإعادة الحالة إلى ما كانت عليه. يمكن فهم الحكمة من هذا الشرط حينما أكدت محكمة العدل الدولية أنه:

"لا يلزم التجاوز عن شرط آخر من أجل شرعية تدبير مضاد، وهو أنه يجب أن يكون الغرض منه حمل الدولة المرتكبة للفعل غير المشروع على امتثال التزاماتها بموجب القانون الدولي، ولهذا يجب أن يكون التدبير قابلاً للإلغاء[2]"

الطبيعة الضاغطة للتدابير المضادة التي تستهدف تصحيح وضع مخالف تستلزم أن يكون التدبير المضاد ذا أثر غير دائم، أو قابل لإعادة الحالة إلى ما كانت عليه. مع ذلك ترى لجنة القانون الدولي أن هذا الشرط ليس مطلقا؛ لذلك كانت عبارة "قدر الإمكان"[3] فمن الممكن أن تلحق التدابير المضادة أضرارا –لا يمكن التراجع عنها– بحق الدولة المسؤولة، وبالتالي تصل إلى مستوى العقاب أو الجزاء[4]. لذلك تشير لجنة القانون الدولي –في تعليقها– إلى أن المقصود هنا أنه إذا كانت هناك خيارات مطروحة من الإجراءات المضادة يجب على الدولة المتضررة اختيار التدابير التي تسمح بإعادة الوضع القانوني بينها وبين الدولة المسؤولة، أو إعادة الدولة المسؤولة استئناف إلزامها[5].

الأمر نفسه في المجال السيبراني خاصية القابلية لإعادة الحال إلى ما كانت عليه لها بعد مهم في التدابير المضادة المتخذة ضد هجمات سيبرانية ضارة؛ لأنها تهدف إلى إجبار الدولة المخالفة على الامتثال بالتزاماتها بدلاً من معاقبتها، لكن الحقيقة أنه غير ممكن دائما. يمكن القول –عامة– إن عكس الهجمات السيبرانية بأنواعها المختلفة يتمثل في إيقافها، لكن أحيانا قد تكون مسببةً آثارًا لا يمكن

---

[1] Tallinn Manual 2.0, commentary to rule 20, para. 17, p. 116

[2] *Gabčíkovo-Nagymaros* judgement, para. 87, pp. 56-57

[3] المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دولياً – المادة 49(3) – ص15

[4] التعليق على المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دولياً – التعليق على المادة 49 – الفقرة (9) – ص170

[5] المرجع السابق – التعليق على المادة 49 – الفقرة (9) – ص170

العودة عنها. مثلاً لا يمكن التراجع عن مسح أو حذف البيانات التي لم يتم نسخها احتياطيا من قبل الدولة التي تتخذ الإجراءات المضادة. فإن إجراءً مضادًا لـ DDoS يمكن إنهاؤه واستعادة الخدمة، ولكن الأنشطة التي تم تعطيلها قد لا يكون من الممكن إجراؤها في وقت لاحق. بعبارة أخرى، حتى لو تم ايقاف هجمات DDoS، فإن آثارها المترتبة في شكل خسائر اقتصادية، أو الصعوبات الأخرى التي سببها توقف الخدمة لا يمكن عكسها دائمًا[1].

اتفق فريق الخبراء في دليل (تالين) على أن شرط إعادة الحالة إلى ما قبل الإجراء المضاد ليس مطلقًا، وعدم القابلية للإلغاء لا يمنع الإجراء المضاد، بل إنه –في حالة اختيار تدبير غير قابل للإلغاء برغم وجود خيارات أخرى– يرى أغلبية الخبراء صحته مادام الإجراء يمتثل للمتطلبات الأخرى للتدبير المضاد[2]. فبدلا من الاهتمام بقابلية الإلغاء يجب النظر إلى ما يهدف إليه الإجراء المضاد أكثر من النظر إلى قابليته للانعكاس؛ لتقرير سلامته. فسبب تقرير خاصية عدم الانعكاس هو منع التدبير المضاد من إلحاق ضرر جسيم بالدولة المسؤولة، ويبدو أنه انتقام عقابي، وليس إجراءً يهدف إلى إجبار الدولة المسؤولة للامتثال بالتزاماتها بموجب القانون الدولي. على سبيل المثال، إذا نفذت الدولة "أ" عملية إلكترونية تستهدف عددا من المصانع المهمة في اقتصاد الدولة "ب" وتسببت في أضرار جسيمة أثرت على الإنتاج بشدة، والدولة الأخيرة أخذت إجراء سيبرانياً مضاداً يهدف إلى إحداث أضرار مماثلة للبنية التحتية الصناعية للدولة "أ". مثل هذا الإجراء المضاد لا رجوع فيه، مع التوجه إلى الانتقام بسبب الخسارة بدلاً من إجبار الدولة المسؤولة، وبالتالي قد يعد غير مشروع. لكن إذا قامت الدولة بعملية سيبرانية –استحوذت فيها على بعض المعلومات الصناعية المهمة للدولة "أ" من أجل الضغط عليها لتغيير سلوكها، أو لوحت بعقوبات اقتصادية على الدولة "أ" حتى تعوض الأضرار التي تعرضت لها الدولة "ب"– يكون التدبير صحيحا[3].

رابعاً: ألا يكون موضوع التدبير المضاد مخالفا لبعض الالتزامات الحصرية التي نصت عليها قواعد مسؤولية الدولة

حددت لجنة القانون الدولي بعض الالتزامات التي لا يجوز للتدابير المضادة أن تنتقص منها، فلا يجوز في التدابير المضادة انتهاك (القواعد القطعية أو الآمرة في القانون الدولي العام)، ولا أحكام

[1] Tallinn Manual 2.0, commentary to rule 21, para. 8, p. 119
[2] Tallinn Manual 2.0, commentary to rule 21, paras. 8-9, p. 119
[3] Tallinn Manual 2.0, commentary to rule 21, para. 9, p. 119

القانون الدولي (للأعراف الدبلوماسية)، أو (حقوق الانسان الأساسية)، أو الالتزامات بمقتضى ميثاق الأمم المتحدة بخصوص (قاعدة منع استخدام القوة أو التهديد بها) أو تتهرب الدولة من (التزاماتها بموجب هيئات تسوية المنازعات)[1]. إن الالتزام الأخير واضح في سببه، وهو ألا تجد الدولة المتضررة باباً للتهرب من تنفيذ الأحكام القضائية ولقد سبق الكلام مفصلا في الفصل السابق على: التزام عدم التعرض لقاعدة منع استخدام القوة. أما الالتزامات الثلاث الأخرى فإنها قد تحتاج إلى بعض التوضيح.

أولا: الأعراف الدبلوماسية: الإجراءات المضادة التي يمكن أن تمس الحرمة الدبلوماسية أو القنصلية محظورة[2]. على سبيل المثال لا يمكن إطلاق برامج الفدية ضد نظام حاسوب سفارة معينة ثم مطالبة الدولة المرسلة عن كف فعل غير مشروع دوليًا كإجراء مضاد[3]. يشمل هذا الحظر الحالات التي قد تتعرض فيها امتيازات الدبلوماسيين وحصاناتهم للانتهاك، كإجراء عملية سيبرانية على حاسوب أحد الدبلوماسيين المبتعثين[4] أو الحالات المعاكسة حيث يستغل الدبلوماسي حصاناته وامتيازاته ليقوم بتدبير مضاد ضد الدولة التي هو على إقليمها.

ثانياً: القواعد القطعية: لا يجوز أن تشمل التدابير المضادة إجراءات تنتهك القواعد القطعية، أو في ترجمات أخرى القواعد الآمرة (Jus Cogen) للقانون الدولي العام، مثل حظر الإبادة الجماعية. والقواعد القطعية قواعد مقبولة، ومعترف بها من قبل المجتمع الدولي للدول قاطبةً، لا يجوز مخالفتها، ولا يُسمح بأي انتقاص منها تحت أي ظرف، كما لا يمكن تعديلها إلا بوساطة قاعدة لاحقة من قواعد القانون الدولي العام لها نفس الطابع[5]. ومن ثم، فإن استخدام الوسائل السيبرانية للتحريض على الإبادة الجماعية مثلا من خلال التلاعب بمحتوى التقارير الإخبارية التي يتم توزيعها بالوسائل الإلكترونية، فلا يمكن قبوله إجراءً مضادًا، بل يمكن أن يكون اعتداء على قاعدة دولية قطعية[6].

ثالثا: حقوق الانسان الأساسية: ليس من السهل تقرير المقصود بحقوق الإنسان الأساسية التي لا يجوز للتدابير المضادة مسها. فحقوق الإنسان كثيرة منها ما يمتد في المعاهدات الدولية والإقليمية، ومنها ما

---

[1] المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دولياً – المادة 50 – ص14

[2] United Nations, *Vienna Convention on the Law of Treaties*, 23 May 1969, United Nations, Treaty Series, vol. 1155, p. 331, available at: https://www.refworld.org/docid/3ae6b3a10.html [accessed 17 September 2022]

Tallinn Manual 2.0, commentary to rule 39, p. 212; commentary to rule 41, p. 219

[3] Tallinn Manual 2.0, commentary to rule 22, para. 8, p. 125

[4] Tallinn Manual 2.0, commentary to rule 22, para. 8, p. 125

[5] Tallinn Manual 2.0, commentary to rule 12, para. 7, p. 71

[6] Tallinn Manual 2.0, commentary to rule 22, para. 4, p. 123-124

هو عرفي. بالرغم من أنه دائما ما يذكر عن خصائص حقوق الإنسان أنها وحدة واحدة غير قابلة للتجزئة والمفاضلة بينها، أي أنها جميعا في مستوى واحد من الأهمية، وليس هناك أي هرمية بينها في الأهمية والتطبيق[1]، إلا أنه –بحكم القانون والعرف– هناك مفاضلة، ذلك أن بعض الحقوق تكون أقوى من غيرها.

فمثلا من الحقوق التي اكتسبت قوة عرفية دولية كحرمة للتعذيب، أو العبودية من القواعد القطعية التي لا يمكن المساس بها تحت أي ظرف، سواء أكانت الدولة تعترف بها أم لا؟ وسواء أكانت الدولة طرفا في اتفاقيات تحميها؟ أم لم تكن كذلك فلها قوة ملزمه لجميع الدول، وفي كل الظروف لا يجوز مخالفتها.

كذلك –بمقتضى نص المعاهدات– هناك بعض الحقوق التي لا يجوز الانتقاص منها من خلال أوقات الطوارئ الوطنية، أو النزاع المسلح.[2] بالإضافة إلى ذلك كل نظام إقليمي يحدد بعض الحقوق الأساسية التي لا يجوز المساس بها حتى في الظروف الطارئة، فالنظام الأمريكي[3] والأوروبي[4] والعربي[5] لحقوق الإنسان جميعها لديها قائمة خاصة من الحقوق التي لا يجوز المساس بها تحت أي ظرف. فتكون

---

[1] الأمم المتحدة، مكتب المفوض السامي لحقوق الإنسان (د. ت). ما هي حقوق الإنسان؟ استرجع من https://www.ohchr.org/ar/what-are-human-rights

[2] UN General Assembly, *International Covenant on Civil and Political Rights*, 16 December 1966, United Nations, Treaty Series, vol. 999, p. 171, available at: https://www.refworld.org/docid/3ae6b3aa0.html [accessed 17 September 2022]
Article 4: "2. No derogation from articles 6, 7, 8 (paragraphs I and 2), 11, 15, 16 and 18 may be made under this provision."

[3] Organization of American States (OAS), *American Convention on Human Rights, "Pact of San Jose", Costa Rica*, 22 November 1969, available at: https://www.refworld.org/docid/3ae6b36510.html [accessed 17 September 2022]
Article 27: "2. The foregoing provision does not authorize any suspension of the following articles: Article 3 (Right to Juridical Personality), Article 4 (Right to Life), Article 5 (Right to Humane Treatment), Article 6 (Freedom from Slavery), Article 9 (Freedom from Ex Post Facto Laws), Article 12 (Freedom of Conscience and Religion), Article 17 (Rights of the Family), Article 18 (Right to a Name), Article 19 (Rights of the Child), Article 20 (Right to Nationality), and Article 23 (Right to Participate in Government), or of the judicial guarantees essential for the protection of such rights."

[4] Council of Europe, *European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14*, 4 November 1950, ETS 5, available at: https://www.refworld.org/docid/3ae6b3b04.html [accessed 17 September 2022]
Article 15: "2. No derogation from Article 2, except in respect of deaths resulting from lawful acts of war, or from Articles 3, 4 (paragraph 1) and 7 shall be made under this provision."

[5] انظر الميثاق العربي لحقوق الإنسان 2004 ، االمادة 4(2) تنص على: يجوز في حالات الطوارئ الاستثنائية مخالفة أحكام المواد الآتية، المادة 5 والمادة 8 والمادة 9 والمادة 10 والمادة 13 والمادة 14 فقرة "6" والمادة 15 والمادة 18 والمادة 19 والمادة 20والمادة 22والمادة 27 والمادة 28 والمادة 29 والمادة 30، كما لا يجوز تعليق الضمانات القضائية اللازمة لحماية تلك الحقوق. امتوفر على موقع جامعة الدول العربية: http://www.leagueofarabstates.net/ar/humanrights/Committee/Pages/CommitteeCharter.aspx

تلك الحقوق التي أقر بها العرف، أو القانون من الحقوق الأساسية التي لا يجوز المساس بها بالتدابير المضادة. بعض النصوص التي تتناول ما لا يجوز المساس به، آثرت أن انقلها من أصلها بلغتها؛ لتكون واضحة.

أما بقية الحقوق فليس من الواضح ما يعد منها أساسيا وما لا يعد أساسيا، وما يمكن المساس به، وما لا يمكن المساس به[1]. فمثلا الحق في الخصوصية من الحقوق المتصور جدا أن تكون عرضة للانتهاك بالإجراءات السيبرانية، وليس هناك اتفاق على عده حقا أساسيا فهل يمكن المساس به؟ لم يتفق فريق دليل (تالين) على ذلك[2]. لكن قد يكون من الواقعي والأقرب إلى المنطق ألا تدخل جميع حقوق الانسان في قائمة المنع من المساس في التدابير المضادة، وإلا فلن يمكن فرض أي تدبير مضاد؛ لأنه لابد أن يتعرض إلى جزئية معينة من حقوق الانسان، لذلك فالرأي أن يكتفى بمنع الحقوق التي تعد أساسية بالعرف، أو القانون، وهو ما يتناسب مع جوهر هذا الشرط؛ فإن جميع الالتزامات ذات درجة غير عادية من الأهمية.

خامساً: أن يكون التدبير المضاد متناسبا مع الضرر[3]

من أهم شروط سلامة التدابير المتخذة شرط التناسب. شرط التناسب يعنى بالمقدار الصحيح، والكيفية الصحيحة لتنفيذ التدابير المضادة[4]، وعدم مراعاة التناسب قد ينتج عنها المسؤولية الدولية للدولة التي قامت بالتدبير المضاد. نصت المادة 51 من قواعد مسؤولية الدولة على الآتي:

---

[1] Tallinn Manual 2.0, commentary to rule 22, para. 4, pp. 123-124

[2] Tallinn Manual 2.0, commentary to rule 22, para. 4, pp. 123-124

[3] بخلاف الدفاع عن النفس يوجد هنا شرط التناسب فقط دون شرط الضرورة، وقد اختلفت المصادر في اشتراط عنصر الضرورة في التدابير المضادة فبعضها يؤكد أن الإجراء لابد أن يكون ضروريا لإعادة الوضع القانوني، لكن مراجع أخرى منها دليل (تالين) لا يذكر الضرورة في التدابير المضادة. ونرى صحة موقف الفريق الثاني؛ وذلك لأن أولا قواعد مسؤولية الدولة لم تضع الضرورة شرطا مستقلا للتدابير المضادة إنما أدخلتها في معنى التناسب .
انظر: التعليق على المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دولياً – التعليق على المادة 51 – الفقرة (7) – ص175

ثانيا الضرورة تتناسب مع حجم الدفاع عن النفس فإن الدولة الضحية ستستخدم، القوة المسلحة لأنها تحت هجوم مسلح. لكنها لا تتناسب مع طبيعة الأفعال التي تؤهل للرد بالتدابير المضادة، والتي تكون أبسط من الهجوم المسلح ولا تكون تهديدا وجودياً، مع ذلك هناك مخالفة للقانون لا يجب أن تترك دون حساب. فإذا تم وضع شرط الضرورة للجوء للتدابير المضادة سيكون في ذلك مصادرة لاستخدمها، لأنها غالبا تأتي في نطاق أبسط من حالة الضرورة.

[4] التعليق على المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دولياً – التعليق على المادة 51 – الفقرة (6) – ص175

"يجب أن تكون التدابير المضادة متناسبة مع الضرر المتكبد، على أن يوضع في الحسبان جسامة الفعل غير المشروع دولياً والحقوق المعنية".

وفقا لهذا النص يمكن القول: إن هناك ثلاثة أسس للتناسب في التدابير المضادة، أولها: هو تناسب التدبير المتخذ مع الضرر الذي تعرضت له الدولة نتيجة إخلال الدولة المسؤولة بالتزامها القانوني. ثم بالدرجة الثانية يجب أن يكون التدبير متناسبا مع خطورة الفعل غير المشروع دوليًا، أي وزن القاعدة القانونية التي تم انتهاكها، وأخيرا أن يكون أن يكون التدبير متناسبا مع أهمية الحقوق المعنية التي يتعرض لها الفعل غير المشروع[1].

ونلاحظ هنا الاختلاف الجوهري بين التناسب في الدفاع عن النفس والتناسب في الإجراءات المضادة ذلك أن التناسب في الدفاع عن النفس لا يعنى الضرر، بل التناسب مع الغرض من الدفاع عن النفس وهو وقف حالة الهجوم. بينما في التدابير المضادة لا يرتبط التناسب بالغرض من التدابير المضادة وهو، وقف الوضع المخالف للقانون[2].

القاعدة العامة نفسها –في تناسب التدبير المضاد مع الضرر– تنطبق في حال اتخاذ تدبير مضاد ضد هجوم سيبراني، فلا ينال من التناسب الاختلاف الكمي بين التدابير المضادة المتخذة والمخالفة التي ارتكبتها الدولة فقد ترتكب الدولة مخالفة واحدة متمثلة في نسخ معلومات مهمة في حواسيب منشأة صناعية في الدولة ويكون الرد عليها بسلسلة مستمرة من الهجمات السيبرانية ذات الأثر التعطيلي، حتى توافق الدولة على توقيع مذكرة تفاهم، تتعهد فيها بالكف، وعدم تكرار ذلك السلوك[3]. كذلك لا ينال من التدابير المضادة كونها اتخذت في حقل بعيد عن موضوع المخالفة القانونية، كأن تتعرض الدولة إلى عملية سيبرانية بسرقة معلومات معينة من حواسيب حكومية، فترد بمنع الدولة التي ارتكبت ذلك الهجوم من العبور فوق أراضيها أو مياهها الإقليمية إذا كانت دولة مجاورة، حتى تتعهد الدولة بعدم تكرار ذلك[4].

بيد أن التناسب ردا على هجوم سيبراني في الإجراءات المضادة يختلف عن التناسب في الدفاع عن النفس في نقطة مهمة، وهي الخطوة الأولى في الهجمات المضادة. ففي الدفاع عن النفس ينصح

---

[1] المرجع السابق – التعليق على المادة 51 – الفقرة (6) – ص175

[2] المرجع السابق – Schmitt, M. N. – "Below the Threshold" Cyber Operations – ص724

[3] Tallinn Manual 2.0, commentary to rule 23, para. 8, p. 129

[4] Tallinn Manual 2.0, commentary to rule 23, para. 7, p. 127

الفقهاء أن تحاول الدولة تقوية منظومتها الدفاعية قبل اتخاذ إجراء بحجم الدفاع عن النفس. لكن في التدابير المضادة –ردا على هجمات سيبرانية– لا يقتضي البدء بالإجراءات الدفاعية السيبرانية قبل الرد بالتدابير المضادة، بل يمكن البدء مباشرة بالتدابير المضادة سواء أكانت ذات طبيعة سيبرانية مماثلة أم من طبيعة أخرى اقتصادية أو سياسية؟ السبب في عدم اشتراط محاولة الدفاع أو تخفيف الفعل غير المشروع قبل البدء بالتدبير المضاد هو أن قواعد مسؤولية الدولة لم تشترط أمرا كهذا[1].

إذا كان تناسب الإجراء المضاد يقاس على الضرر الذي تعرضت له الدولة بحسبانه قاعدة عامة فإن الوضع يختلف في قاعدة بذل العناية. وذلك إذا كانت الإجراءات المضادة تتخذ بسبب فشل الدولة في منع جعل إقليمها مصدرا لإضرار الدول الأخرى باتخاذها كل الإجراءات الممكنة، فإن القياس لن يكون بالضرر الذي سببه الهجوم السيبراني الصادر من الفاعل غير الحكومي، بل بمستوى الإغفال أو الإهمال الذي ارتكبته الدولة[2]. ويجب ألا يغفل أبداً تذكر أن التدابير المضادة موجهة ضد الدولة، وليس الفاعلين غير الحكوميين على إقليمها، فلا يمكن تخطي سيادة دولة ومعاقبة أشخاص محليين على إقليمها لكن يمكن محاسبة الدولة على فشلها في التزامها ببذل العناية، لذلك فقياس التناسب يكون بين التدبير ومدى إهمال الدولة، وليس الهجمات السيبرانية التي قام بها الفاعل غير الحكومي.

سادسا: شروط إجرائية سابقة على اتخاذ الإجراء المضاد: (الدعوة إلى الوفاء بالالتزام)، (الإخطار بالإجراء المضاد) و(الدعوة إلى التفاوض)

بهدف وضع التدابير المضادة في تدرج إجرائي معقول واحتواء خطر استخدامها جزاءً تتطلب مواد مسؤولية الدولة من الدولة المتضررة أولا دعوة الدولة المسؤولة إلى الوفاء بالتزاماتها (بدء التنفيذ)[3] فتوضح الدولة المتضررة للدولة المسؤولة أنها تقوم بانتهاك لالتزام يضر بحقوقها وتطلب منها التوقف عنه والعودة إلى حالة السلامة القانونية. ثم إن لم ينفع ذلك على الدول المتضررة إخطار الدولة المسؤولة بنيتها في اتخاذ تدابير مضادة ضدها، وتعرض عليها التفاوض[4]. هذا ولم تحدد قواعد مسؤولية الدولة ولا التعليق المصاحب لها إن كان يكفي في الإخطار أن تنذر بتدابير مضادة عامةً أو يحدد – بوضوح– ماهية التدبير التي سوف يتم اتخاذه. لكن لا يشترط أن يكون بين الدعوة إلى الوفاء والإخطار

[1] Tallinn Manual 2.0, commentary to rule 23, para. 9, p. 129
[2] Tallinn Manual 2.0, commentary to rule 23, paras. 11-12, p. 130
[3] المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دولياً – المادة 52(1)(أ) – ص14
[4] المرجع السابق – المادة 52(1)(ب) – ص14

مدة زمنية، وقد يمكن أن يحدث ذلك في الجلسة نفسها، ويكفي أن يصدر الإخطار لمرة واحدة فقط قبل اتخاذ الإجراء المضاد[1].

هذا التدرج في الإجراءات جاء لأن الإجراءات المضادة قد يكون لها عواقب جسيمة على الدولة المسؤولة، ويجب أن تحصل على فرصة لإعادة النظر في موقفها، على ضوء إمكانية اتخاذ إجراءات مضادة ضدها[2]. مع ذلك تتفق لجنة القانون الدولي على أن هناك ظروفا استثنائية تسمح للدول باتخاذ التدابير المضادة دون إخطار[3]، وذلك إذا كان الإخطار يمكن أن يؤثر على القدرة على تنفيذ الإجراء المضاد، كأن تباشر الدولة التي تم إخطارها بسحب أرصدتها من بنوك الدولة المتضررة[4].

جاءت ردود فعل الدول متباينة حول هذه القيود الإجرائية للجنة القانون الدولي على التدابير المضادة. فعلى سبيل المثال، قدمت الولايات المتحدة تعليقات مستفيضة على مسودة المواد وقد وصفت العديد من القيود الإجرائية على التدابير المضادة، بأنها غير مدعومة بممارسات الدولة. وعلى وجه التحديد، اعترضت الولايات المتحدة على شرط التفاوض[5]. حتى بعض الفقه يروى أن هذه الإجراءات تعكس التطور التدريجي الطموح للقانون الذي تبتغيه لجنة القانون الدولي أكثر من كونها تعكس القانون الدولي العرفي حقيقة[6]. بالرغم من أن لجنة القانون الدولي اعتمدت على حكم تحكيم سابق في اشتراك وجوب أن تطلب الدولة المتضررة من الدولة المسؤولة بالوفاء بالتزامها قبل اتخاذ التدبير المضاد، وهي قضية الاتفاق بشأن الخدمات الجوية[7] إلا أن شرط الإخطار بالفعل يمثل رأي وطموح اللجنة أكثر من عرف ملزم[8]. ولا مناص من القول: إن الموضوع من عام 2001 حتى اليوم لايزال مثارًا للخلاف حتى في

---

[1] التعليق على المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دولياً – التعليق على المادة 54 – الفقرة (4) و(5) – ص180

[2] المرجع السابق – التعليق على المادة 52 – الفقرة (2) – ص176

[3] المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دولياً – المادة 52(2) – ص15

[4] التعليق على المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دولياً – التعليق على المادة 52 – الفقرة (6) – ص176-177

[5] U.S. Comments on ILC Draft Articles on State Responsibility. (2001). *The American Journal of International Law, 95*(3), 626–628. https://doi.org/10.2307/2668497

[6] المرجع السابق – Schmitt, M. N., & Watts, S. – ص383

[7] *Air Services* arbitral award, paras. 91, 94-96, pp. 445-446,

[8] يتبين ذلك بوضوح من تبرير اللجنة في:
التعليق على المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دولياً (مرجع 7)، التعليق على المادة 52، الفقرة (4)، ص176

النطاق السيبراني. فمثلا عام 2018 في خطاب حول موقف المملكة المتحدة من انطباق القانون الدولي في الفضاء السيبراني قال المدعي العام Jeremy Wright:

"المنطقة الوحيدة التي تخرج فيها المملكة المتحدة عن العمل المتقن للجنة القانون الدولي هي الوضع الذي تستجيب فيه المملكة المتحدة للهجوم السيبراني بإجراءات مضادة. في مثل هذه الظروف، لن نتفق على أننا دائمًا ملزمون قانونياً بإعطاء إشعار مسبق للدولة المعادية قبل اتخاذ الإجراءات المضادة ضدها.... إنه لا يمكن أن يكون من الصواب أن يطلب القانون الدولي إجراء مضاد لفضح قدرات حساسة للغاية في الدفاع عن بلد في الساحة الإلكترونية"[1]

من المستغرب أن يعرض الأمر بهذه الطريقة المخالفة للجنة القانون الدولي بينما في الواقع أن الأمر مقنن في المادة 52 (2) من المواد الخاصة بمسؤولية الدولة، وهي تهدف إلى تقديم حل للدولة المتضررة التي قد يعرض الإخطار –بإجراء التدبير المضاد– حقوقها للخطر[2].

ولا يمكن الاختلاف على أن بعض الظروف تدعو إلى اتخاذ إجراءات عاجلة. لكن ليست مسألة العجلة الوقتية فقط هي ما يمكن أن يسقط واجب الإخطار، بل عندما يعتمد نجاح الإجراء المضاد على عنصر المفاجأة. لذلك يمكن أن يتم التنازل عن شرط الإخطار في مثل هذه الظروف[3]. إلا أن اشتراط دعوة الدولة المسؤولة للوفاء بالتزامها بالتعويض قبل اتخاذ إجراءات التدابير المضادة لا خلاف عليه وعلى استقراره بوصفه التزاما دوليا لأهميته في إعطاء الدولة الفرصة للعودة عن السلوك وأهميته في تقليل إمكانية الخطأ في التنسيب.

القسم الثاني: التدابير المضادة ضد إخلال بالتزام يمس المجتمع الدولي ككل Erga Omnes

تم الحديث عن الإجراءات المضادة ضد الإخلال بالتزامات تمس المجتمع الدولي ككل، وأن لجنة القانون الدولي لا تشجع اتخاذ تدابير مضادة، بل مجرد تدابير قانونية ضد تلك الأفعال. إن أفعالًا مثل الإبادة الجماعية أو التطهير العرقي –في الوضع القانوني المثالي– تقع مسؤولية التصدي لها على مجلس الأمن لاتصالها بالسلم والأمن الدوليين، لكن ماذا لو أعيق مجلس الأمن بحق النقض الفيتو،

[1] المرجع السابق – Wright, J. – Cyber and International Law
[2] المرجع السابق – Delerue, F. – ص221
[3] المرجع السابق – Johnson, D. E., & Schmitt, M. N. – ص24-25

هل يقف العالم شاهدا على مذبحة ولا يستطيع القيام بأي شيء. يبدو منطقيا السماح للدول غير المتضررة أن تصنع نوعا من الضغط بتدابير مضادة لا تنطوي على استخدام للقوة.

هناك ممارسات كثيرة في هذا الصدد[1]، مثلا، الولايات المتحدة ادعت في عام 1978 ان رئيس أوغندا آنذاك عيدي أمين داد يقوم بإبادة جماعية ضد شعبة، ووقع الرئيس كارتر على قانون حظر التجارة التام، وإعلان الحرب الاقتصادية[2]. طبقت حالة الأحكام العرفية في بولندا عام1991، مما ترتب عليه ادعاءات جادة بوجود انتهاكات لحقوق الإنسان في بولندا؛ مما جعل بعض الدول الغربية تفرض عقوبات على بولندا[3]. كذلك الاجتياح العراقي للكويت، قامت الولايات المتحدة ودول أخرى غربية بتجميد أرصدة العراق، وحظرت التجارة معها قبل أن يتحرك مجلس الأمن، ويفرض عقوبات أخرى[4]. أما أوضح مثال نراه اليوم فهو الكم الهائل من العقوبات الذي فرضه الاتحاد الأوروبي على روسيا؛ بسبب حربها على أوكرانيا الذي بلغ في المجموع (مع الأخذ في الحسبان أيضًا العقوبات السابقة التي فُرضت بعد ضم شبه جزيرة القرم في عام 2014) عقوبات على 98 كيانًا و1158 فردًا[5].

بالرغم من أنه يبدو منطقيا أن تتحرك الدول في انتهاك يؤثر على المجتمع الدولي ككل فإن للموضوع أبعادا أخرى فقد يكون الموضوع أكثر تعقيدا من مجرد فرض القانون. الممارسات تشير إلى أن القوى الغربية هي المستفيدة من التحرك تحت مبدأ المصلحة التي تمس المجتمع الدولي ككل فيستخدم ذلك المبدأ كقوة أخرى، كقوة الفيتو التي تكتسبها الدول الغربية القادرة على فرض العقوبات لتصبح أقوى[6]. كان من الممكن أن يتم التحرك ضد الولايات المتحدة على ممارسات التعذيب التي حدثت في سجون أبو غريب؛ لأن الامتناع عن التعذيب من القواعد القطعية والالتزام بها يعني المجتمع الدولي ككل،

---

[1] هناك عدد من الممارسات رصدتها لجنة القانون الدولي
انظر: التعليق على المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دولياً – التعليق على المادة 54 – الفقرة (3) – ص178-180

[2] Ullman, R. H. (1978). Human Rights and Economic Power: The United States versus Idi Amin. *Foreign Affairs*, *56*(3), 529-543. https://doi.org/10.2307/20039917

[3] التعليق على المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دولياً – التعليق على المادة 54 – الفقرة (3) – ص178-180

[4] انظر الأمر التنفيذي رقم 12722 للرئيس بوش بتاريخ 2 أغسطس 1990
George Bush, Executive Order 12722—Blocking Iraqi Government Property and Prohibiting Transactions with Iraq Online by Gerhard Peters and John T. Woolley, The American Presidency Project https://www.presidency.ucsb.edu/node/269016

[5] European Council. (2022, June 28). EU sanctions against Russia explained. Retrieved from https://www.consilium.europa.eu/en/policies/sanctions/restrictive-measures-against-russia-over-ukraine/sanctions-against-russia-explained/

[6] المرجع السابق – Pr. Pierre d'Argent

لكن ضعف إمكانية حدوث مثل هذا التحرك تعطي فكرة عن سبب تخوف لجنة القانون الدولي من تشريع التدابير المضادة ومحاولة تقييد الإجراءات المتخذة بموجب مبدأ الالتزامات التي تمس المجتمع الدولي كلًا بالإجراءات القانونية التي لا تنطوي على مخالفة للقانون الدولي.

الفرع الثالث: تدابير بمقتضى حالة الضرورة

يسمح للدولة باتخاذ إجراء –هو في الأساس غير مشروع بموجب القانون الدولي– استنادًا إلى انطباق حالة الضرورة وهي" صون مصلحة أساسية من خطر جسيم ووشيك يهددها"[1]. أوردت قواعد مسؤولية الدولة الضرورة بوصفها أحد الظروف النافية لعدم المشروعية مع ظروف أخرى كالقوة القاهرة وحالة الشدة والدفاع عن النفس والإجراءات المضادة. وبالتالي فإن تدابير الضرورة هي تدابير غير قانونية لولا حالة الضرورة. وقد استخدمت الدول عذر الضرورة للقيام بأفعال غير مشروعة كمصادرة ممتلكات رعايا دول أخرى رغم وجود اتفاقات تجارية بين البلدين تمنع ذلك[2]، ومثل ذلك التأخر في سداد الديون، وفرض حظر لصيد أنواع معينة من الحيوانات في أعالي البحار للمحافظة عليها من خطر الانقراض[3] وغيرها. وكلما حدث تنازع بين مصلحة الدولة والتزام قانوني يقيد تلك المصلحة تحتج الدول بالضرورة.

أولا: شروط حالة الضرورة

هناك ثلاثة شروط يجب توافرها لانطباق حالة الضرورة، بعضها يخص الخطر الذي تسبب في حالة الضرورة، وبعضها يخص الحق الذي وقع عليه الاعتداء، وبعضها يخص فعل الرد باستخدام حالة الضرورة.

أولا: في حالة الفعل الذي تسبب بحالة الضرورة يشترط أن يكون الخطر " جسيما ووشيكاً". جسيما أي له تأثير بالغ على المصلحة المحمية. ويمكن أن يستوفى هذا المعيار حتى بالتأثر الجزئي للمصلحة الأساسية، فلا يشترط أن تتعطل المصلحة تماما. ويجب أن يكون وشيكا –هذا بالطبع إن لم يكن

---

[1] التعليق على المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دولياً – التعليق على المادة 25 – الفقرة (1) – ص103

[2] في نزاع نشب بين بريطانيا والبرتغال عام 1832 احتجت حومة البرتغال بالضرورة التي فرضها نقص المواد الغذائية بين صفوف القوات التي مسؤولة عن قمع الاضطرابات أن تصادر ممتلكات بعض الرعاة البريطانيين.
انظر: المرجع السابق – التعليق على المادة 25 – الفقرة (4) – ص104

[3] حينما منعت روسيا صيد الفقمة ذا الفراء في أعالي البحار ودفعت بالضرورة حيث ان ذلك غير مشروع بسبب عدم وجود اختصاص لروسيا في أعالي البحار، لكنها دفعت ان ذلك ضروري بسبب الصيد الجائر لهذا النوع من الحيوان الذي جعلت عرضة لخطر الانقراض ولأن موسم الصيد كان على وشك أن يبدأ.
انظر: المرجع السابق – التعليق على المادة 25 – الفقرة (6) – ص104-105

حالاً بالفعل– يقوم على سند مضوعي، وليس مجدر تكهنات، أو تخوف عام من أن يقع. وعلى عاتق الدولة أن تثبت موضوعيا وشاكة الخطر، وأنه حقيقي وأن الأمر يتعدى مجرد التخوف من إمكان وقوعه في المستقبل[1].

ثانياً: يجب أن تكون المصلحة –والمطلوب هنا مجرد مصلحة وليس حقا بمقتضى القانون الدولي– أساسية. والمصلحة الأساسية مصطلح فضفاض في القانون الدولي، وقد تم الاحتجاج بحالة الضرورة، لحماية طائفة متنوعة من المصالح، مثل "الحفاظ على البيئة، وصون ذات وجود الدولة، وشعبها في حالات الطوارئ العامة، أو لضمان سلامة السكان المدنيين وغيرها"[2].

وأما الشروط المطلوبة –في الإجراء المتخذ بموجب الضرورة– فيجب أن يكون إجراء الضرورة "السبيل الوحيد" المتاح لحماية المصلحة. فلا يقبل أن يكون السبيل الأقل تكلفة، أو الأسهل أو الأكثر ملائمة فكل ذلك لا يخلق حالة ضرورة؛ فلكي يكون الإجراء ضروريا لابد أن يكون خيارا وحيدا، وأن يظل على هذا النحو طوال مدة اتخاذه. فإذا كان التدبير المتخذ هو السبيل الوحيد بداية ثم ظهرت سبل أخرى لحماية المصلحة يسقط عذر الضرورة[3].

بالرغم من أن قواعد مسؤولية الدولة ترى أن الشروط المصاحبة لحالة الضرورة " لن تتاح إلا فيما ندر لتسويغ عدم أداء التزام"[4] فهناك توسع ليس من الدول، بل من جانب الفقه في عرض حالة الضرورة خيارًا أمام الدول خصوصا، في النطاق السيبراني[5]. لأن الملاحظ أن حالة الضرورة لا تشترط وقوع فعل غير مشروع دوليا، ولا تشترط أن يتعرض حق بمقتضى القانون الدولي للانتهاك، بل تكتفي بعبارة المصلحة الأساسية، وهي مصطلح يختلف تفسيره من دولة لأخرى. والأهم أنها لا تشترط نسبة الفعل أو الخطر إلى دولة معينة. وفي مدى انطباق المصلحة الأساسية جانب تقديري كبير من الدول فتوافر

---

[1] المرجع السابق – التعليق على المادة 25 – الفقرة (15) و(16) – ص107-108
[2] المرجع السابق – التعليق على المادة 25 – الفقرة (14) – ص107
[3] المرجع السابق – التعليق على المادة 25 – الفقرة (15) – ص107
[4] المرجع السابق – التعليق على المادة 25 – الفقرة (2) – ص103
[5] مثال على تعامل الفقه مع حالة الضرورة كخيار للرد على العمليات السيبرانية:
المرجع السابق – Arimatsu, L., & Schmitt, M. N. – ص1199
مثال على تعامل الدول (دولة ألمانيا) مع حالة الضرورة كخيار للرد على العمليات السيبرانية:
German Federal Foreign Office, German Federal Ministry of Defence, & German Federal Ministry of the Interior, Building and Community. (2021, March). *On the Application of International Law in Cyberspace*. The Federal Government of Germany. Retrieved from https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf

الشروط قرارات أحادية من الدول –وإن كانت ستخضع لرقابة المجتمع الدولي لاحقا– فإنه ابتداء تستطيع الدول اللجوء إلى حالة الضرورة للتعامل مع خطر الهجمات السيبرانية بسهولة أكثر من لجوئها إلى الدفاع عن النفس أو التدابير المضادة.

ويمكن أن يكون اللجوء إلى تدابير الضرورة –أحيانا– خياراً أفضل للدولة الضحية من التدابير المضادة. أولا: قد يكون من الأسهل اللجوء إلى حالة الضرورة في سبيل الرد على الهجمات السيبرانية، لأن في التدابير المضادة يجب أن يتوافر ركنا المسؤولية الدولية من فعل غير مشروع، منسوب إلى دولة معينة، في حين أن الضرورة ليس لها مثل هذا الشرط. بعبارة أخرى، الفعل الذي يترتب عليه اتخاذ إجراء مضاد يجب أن يُنسب إلى دولة ما، في حين أن الأفعال بناء على الضرورة قد يتم اتخاذها ردًا على العمليات السيبرانية التي تقوم بها جهات فاعلة من غير الدول (أو حتى عندما يكون صاحب الفعل مجهول الهوية). ثانيا: في حالة الضرورة يمكن اللجوء إلى تدابير الضرورة استباقيا، وهذا ما يفهم من وجوب أن يكون الخطر جسيمًا ووشيكًا، وكلمة "وشيك" تشير إلى أنه يُسمح للدولة المستهدفة بالاستجابة الاستباقية. بينما في حالة التدابير المضادة لا يمكن إلا بعد وقوع الفعل غير المشروع فلا يمكن البدء بفعل غير مشروع ردا على فعل غير مشروع لم يحدث بعد. ثالثا، هناك بعض المعاهدات التي قد تمنع التدابير المضادة في مواقف معينة، وبدلاً من ذلك تفرض شرطًا باللجوء إلى وسائل محددة؛ لتسوية المنازعات على سبيل المثال: معاهدة ثنائية قد تحظر التدابير المضادة ردا على انتهاكات شروط المعاهدة، وتتطلب اللجوء إلى منظمة إقليمية محددة لمعالجة الانتهاكات. هنا يمكن استبدال التدابير المضادة بتدابير الضرورة مع عدم الإخلال بأهمية وجود شروط حالة الضرورة[1].

من ناحية أخرى قد يكون اللجوء إلى استخدام حالة الضرورة أصعب من التدابير المضادة؛ لأنه لا يجوز إلا عندما يرقى الوضع إلى خطر جسيم ووشيك لمصلحة أساسية للدولة. بينما يكفي مجرد الإخلال بالتزام تعاهدي أو عرفي لإطلاق الحق في اتخاذ تدابير مضادة. الحالة الثانية قد تكون أيسر في الإثبات وبالتالي أكثر إقناعا لموقف الدولة الضحية عند المحاسبة اللاحقة من قِبل الرأي العام والمجتمع الدولي.

[1] التعليق على المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دولياً – التعليق على المادة 50 – الفقرة (10) – ص172

ثانيا: تطبيق التصرف بناء على حالة الضرورة في النطاق السيبراني

الرد بمقتضى الضرورة يمكن أن يكون مفيداً جدا بوصفه خيارًا للرد على العمليات السيبرانية، خصوصا في حالة عدم اليقين بشأن ماهية الالتزام الذي تنتهكه العملية الإلكترونية، كأن يكون عدم اليقين بين وجود خرق قاعدة احترام السيادة، أو الامتناع عن التدخل، أو عدم اليقين من وجود خرق قاعدة قانونية أصلا، بل قد يقتصر الأمر على التضييق على مصلحة غير محمية بموجب قاعدة قانونية[1]. وأكثر ما يمكن أن تستفيد منه الدول في استخدام حالة الضرورة هو حالة تعرضها لهجمات ترقى في آثارها أن تكون استخداما للقوة، فيمكن أن تستخدم عذر الضرورة؛ لتتخذ إجراءات لولا حالة الضرورة لكانت غير قانونية[2].

وينبغي التحذير أنه من غير المستقر عليه ما إذا كانت التدابير القائمة على نداء الضرورة يمكن أن تنطوي على عمل قسري. انقسم فريق الخبراء الدولي حول هذه المسألة. فبعضهم يرى أنه ليس مشروعا استخدام القوة ردا على عملية إلكترونية ضارة إلا وفقًا لقانون الدفاع عن النفس، فالقانون الدولي يحظر استخدام القوة لاستثناءات حصرية محددة وهي إذن من مجلس الأمن والدفاع عن النفس. لكن هناك آراء أخرى ترى أن حظر التدابير القسرية بمقتضى الضرورة قد يعني أن الدول التي تواجه العمليات السيبرانية ذات آثار تصل لآثار استخدام القوة قد تجد نفسها في موقف يكون فيه الخيار الوحيد الفعال لصد تلك الهجمات هو اتخاذ بعض الإجراءات القسرية، بمقتضى الضرورة، لكنها ستكون عاجزة عن صد الهجمات وعليها التحمل والانتظار حتى تبلغ الهجمات السيبرانية مستوى الهجوم المسلح[3]. فالأمر مخلف فيه وغير واضح إلى الآن وهو متروك إلى تطبيق الدول ونقاشها وما ستتبناه من سياسات في هذا السيناريو.

بالمثل، التصرف بناءً على الضرورة في نطاق العمليات السيبرانية مفيد في حالة عدم اليقين من الفاعل؛ لأنه ليس من الضروري نسبة العملية السيبرانية العدائية قانونًا إلى دولة قبل الرد على أساس الضرورة. لذلك يمكن أن يستخدم عذر الضرورة للرد على الهجمات السيبرانية التي تقوم بها الجماعات

---

[1] Schmitt, M. N. (2018a). Peacetime Cyber Responses and Wartime Cyber Operations Under International Law: An Analytical Vade Mecum. *Harvard National Security Journal*, *8*, 239-280 [pp. 251–252]. Retrieved from https://harvardnsj.org/wp-content/uploads/sites/13/2017/02/Schmitt-NSJ-Vol-8.pdf

[2] Tallinn Manual 2.0, commentary to rule 26, paras. 9-10, pp. 137-138

[3] Tallinn Manual 2.0, commentary to rule 26, para. 18, p. 140

الفاعلة من غير الدول كالأفراد أو الشركات والجماعات المسلحة. المطلوب فقط هو تحديد واقعي للعملية السيبرانية العدائية التي حدثت أو من المحتمل أن تحدث أفيها تهديد خطير لمصلحة أساسية للدولة المستهدفة؟ وهل الرد أو الاستجابة المقترحة هي الوسيلة الممكنة الوحيدة لمنع الاعتداء على المصلحة؟[1]

فمثلا عملية إلكترونية تستهدف البنية التحتية الإلكترونية الأساسية: كالنظام المالي الوطني، أو نظام المواصلات الوطني، تم إطلاقها من دولة يشتبه في نسبتها إليها، ولكن لا يمكن التحقق من ذلك تماماً. وقد يكون من غير الواضح إمكان إعمال قاعدة بذل العناية؛ لأن الدولة الضحية غير متأكدة من قدرة الدولة المصدر على وضع حد للعملية، كأن تكون الدولة المصدر غير متقدمة رقمياً. والرد المقترح من الدولة الضحية من شأنه أن ينتهك السيادة الإقليمية للدولة المسؤولة إن لم يصعد الانتهاك إلى قواعد أكثر من ذلك. في هذه الحالة، عدم قانونية ذلك الرد يعد قانونيًا طالما استوفيت المعايير الصارمة لحالة الضرورة[2].

فيجب أولا: أن تكون العملية العدائية السيبرانية جسيمة وإن لم تكن قائمة أو وشيكة، قبل أن تستجيب الدولة المستهدفة بتدابير الضرورة. تشير كلمة "جسيمة" إلى عملية إلكترونية عدائية مهدّدة أو مستمرة لها عواقب استثنائية شديدة، أو ضارة، أو لها تأثير حاد على مصلحة أساسية للدولة. ثم يجب ان تكون العملية السيبرانية حالة أو وشيكة. كلمة حالة تعني قائمة وأضرارها قائمة، وتعني أن تكون الهجمات مستمرة، أي تكون سلسلة من الهجمات التي تبدأ وتتوقف، أو أن تكون قد حدثت الهجمات واكتملت إلا أن آثارها الضارة ما زالت مستمرة، واللجوء إلى تدابير الضرورة هي الطريقة الوحيدة لمنع حدوث مزيد من الأضرار[3]. أما ما يعد وشيكًا فإن قواعد مسؤولية الدولة تتطلب أن يكون الفعل وشيكا وفقا للمعيار الموضوعي، أي عندما تكون أي دولة أخرى –في الظروف المماثلة نفسها– من شأنها أن تتصرف بدافع الضرورة، قبل ظهور الضرر الذي سوف يحدث بسبب العملية السيبرانية[4]. وبالإضافة إلى العنصر الموضوعي سبقت الإشارة إلى دليل (تالين) أنه لا يرجح القرب الزماني معيارًا للخطر الوشيك، بل يهتم بالفعالية، وهل سيكون الإجراء فعالا إذا تم الانتظار حتى يصبح الهجوم السيبراني

[1] المرجع السابق
[2] المرجع السابق – Johnson, D. E., & Schmitt, M. N. – ص27
[3] Tallinn Manual 2.0, commentary to rule 26, para. 16, p. 139
[4] Tallinn Manual 2.0, commentary to rule 26, para. 13, p. 138

قريباً. أو ما يسميه دليل (تالين) "الفرصة الأخيرة"[1] لاتخاذ إجراء يمنع الهجمات السيبرانية، وهذه الفرصة على وشك الانتهاء. فمثلا إذا كانت الدولة لديها معلومات استخباراتية موثوقة عن جماعة تستعد لإطلاق عمليات سيبرانية عليها –في تاريخ محدد– تدهور البنية التحتية الحيوية بشدة. فهذه الدولة قد تتصرف استباقياً ضد المجموعة؛ لأنها إن لم تقم بذلك ستخسر فرصة مع العمليات السيبرانية من الحدوث[2].

كما تم الانتهاء إليه في النقاش حول الدفاع الاستباقي عن النفس يمكن التأكيد عليه هنا في استخدام حالة الضرورة استباقيا: إن الإلغاء التام لاشتراط القرب الزمني –من وجهة نظر الباحثة– ليس صحيحا! فلابد قبل البدء في إجراءات مضادة أن تكون هناك مدة معقولة لوقوع لفعل، فلا تحرك ضد أمر سيحدث خلال سنوات أو عقود تغلب عليه الصفة العدوانية أكثر من كونه إحدى طرق المساعدة الذاتية المشروعة وفقا للقانون[3]، لذلك لا بد أن يكون القرب الزمني المعقول أحد المعايير التي يقاس عليها الخطر الوشيك.

ثانياً: يجب أن تتأثر المصلحة الأساسية. وتجدر الإشارة إلى أن دليل (تالين) يقر بعدم وضوح مصطلح المصلحة الأساسية في القانون الدولي، وبالتالي إمكان اختلافه من دولة لأخرى بحجة أنه مصلحة "لها أهمية أساسية وعظيمة للدولة المعنية". لكنه يقترح حسبان تعرض المرفق العام الحيوي –الذي عرض في الفصل الثاني– بمنزلة العرض لمصلحة أساسية[4]. من الواضح أن بعض الأنشطة تعد ضرورية لجميع الدول نحو كل ما يتعلق بالاستقرار الاقتصادي، والصحة، والسلامة العامة، والاتصالات، وتوليد الطاقة، والأمن القومي. هذه الأمور عامةً مصالح أساسية في كل دولة، لكن هناك الكثير من المجالات التي تختلف في أهميتها من دولة لأخرى فمثلا السياحة قد تكون ركيزة اقتصادية في دولة ما، وفي بلدان أخرى تكون سببا غير مؤثر في الاقتصاد. وفقًا لذلك، فإن العمليات السيبرانية

---

[1] تمت مناقشة فكرة الفرصة الأخيرة في المادة 73 من دليل (تالين)
Tallinn Manual 2.0, commentary to rule 73, p. 350

[2] Tallinn Manual 2.0, commentary to rule 26, para. 15, p. 139

[3] وإلا لكانت الحرب الروسية على أوكرانيا مشروعة حيث بررها الرئيس الروسي بأنها دفاع استباقي ضد خطر سيتشكل في المستقبل وسكون الأوان قد فات إذا تم الانتظار حتى ذلك الوقت للدفاع عن النفس
European Commission. (2022, March 1). *Speech by President von der Leyen at the European Parliament Plenary on the Russian aggression against Ukraine* [Press release]. Retrieved from https://ec.europa.eu/commission/presscorner/detail/en/speech_22_1483

[4] Tallinn Manual 2.0, commentary to rule 26, para. 2-5, pp. 135-136

التي تستهدف صناعة السياحة في البلدان السابقة قد تكون مؤهلة على أنها موجهة إلى مصلحة أساسية، ولكن ليس في تلك الأخيرة[1].

أخيرا: لابد من التحقق من أن العملية غير القانونية التي سيتم اتخاذها تحت حالة الضرورة هي مسار العمل الوحيد الممكن لإنهاء الخطر السيبراني الجسيم الحال أو الوشيك. فإذا كانت تدابير الاستجابة الأقل –مثل التدابير القانونية أو إجراءات الدفاع السيبراني، يمكن أن تحمي المصلحة– فإنه لا يجوز للدولة المستهدفة أن تتصرف بدافع الضرورة.

المطلب الثاني

المواجهة القضائية للهجمات السيبرانية أمام محكمة العدل الدولية

حتى الآن لم يصل موضوع الهجمات السيبرانية إلى محكمة دولية، لكن لا بد أن يحدث ذلك في مرحلة ما، وعندئذٍ ستوضع كل محاولات تطبيق القانون الدولي على الهجمات السيبرانية تحت مجهر الاختبار الحقيقي.

ولمعالجة هذا الموضوع فإنه من المهم جدا التفرقة بين معايير الإثبات، وطرق الإثبات من جهة، وقواعد الإسناد في القانون الدولي من الجهة الأخرى. في حين أن معيار الإثبات يتعامل مع ماهية الأدلة المطلوبة وكميتها؛ لإثبات الدعوى، فإن قواعد الإسناد تتناول نسبة الفعل إلى الدولة، فوظيفتها تأكيد العلاقة بين الفاعل والدولة، وأمور مثل مستوى السيطرة التي تمارسها الدولة على جهة فاعلة غير حكومية تسببت في الانتهاك[2]. وقد تم تناول موضوع الإسناد في المبحث الأول من هذا الفصل. هنا نتناول إمكان رفع موضوع الهجمات السيبرانية –بعد تنسيبها إلى دولة معينة– إلى محكمة دولية، وفيها يكون للأدلة المستخدمة في الوصول إلى الفاعل أهمية كبيرة. وفي الواقع عادة ما تكون الخطوة التالية لتحديد الجاني هي المطالبة بسبل الانتصاف، ولا يمكن القيام بذلك إلا عندما تكون الدولة الضحية قادرة على إثبات ادعاءاتها وفقًا لمعايير الإثبات في القانون الدولي.

---

[1] المرجع السابق – Johnson, D. E., & Schmitt, M. N. – ص26

[2] Aravindakshan, S. (2020). Cyberattacks: a look at evidentiary thresholds in International Law. *Indian Journal of International Law*, *59*(1–4), 285-299 [p. 287]. https://doi.org/10.1007/s40901-020-00113-0

وفي هذا الصدد، ينبغي توجيه النظر إلى أنه لا يوجد في الوقت الحاضر اتفاق عالمي على مجموعة متماسكة من القوانين التي يمكن وصفها بأنها قانون الإثبات الدولي[1]. فلكل جهاز قضاء دولي معاييره الخاصة للاستنتاج وتقييم الأدلة، وبعضها ثابت في أنظمتها الأساسية أو قواعد إجراءاتها، في حين يطور البعض الآخر معاييره من خلال الممارسة والفصل في كل قضية تطرح[2].

وقد أدى تطور نظام العدالة الدولي بداية من لجان تقصي الحقائق التي تصدر قرارها تجاه موضوع معين وصولا إلى القضاء الدولي، إلى جعل المجتمع الدولي يطالب بمعايير إثبات أعلى بدرجة متزايدة[3]. لذلك فقد نصح بعض العلماء بعدم تخفيض معيار الإثبات في السياق السيبراني في قضايا مثل قضايا تحديد الهوية والإسناد؛ وذلك تحسبا للإسناد الخاطئ، وهو خطر قائم للغاية في المجال السيبراني[4].

فهناك بعض المقترحات "بعكس عبء الإثبات"، فتقدم الدولة الضحية أدلة مبدئية تشير إلى مسؤولية دولة أخرى لينتقل عبء الإثبات على تلك الدولة، لتثبت عدم مسؤوليتها[5] في ذلك تناسب مع خصوصية موضوع الإثبات في المجال السيبراني، الذي يعاني من مشكلات النقص العام في الأدلة، وعندما يكون الدليل موجودًا لا يكون في متناول الدولة الضحية، بل يتم التحكم في الدليل من قبل إقليم دولة أخرى. لكن رد بعضهم على ذلك بأن عكس الإثبات في الفضاء السيبراني وهو الإثبات يمكن يؤدي بسهولة إلى نتائج خاطئة، بل قد تكون سخيفة نظرًا لإمكان أن يوجه الإنترنت عمليات من خلال العديد من البلدان تجعل بإمكاننا تصور ما سيحدث، وهو إلقاء الدولة المسؤولة اللوم على غير المتورطين تماما وإدانة والدول الأبرياء –لما حصل– على سبيل المثال في الهجمات على إستونيا 2007، تضمنت الروبوتات أجهزة كمبيوتر موجودة ليس فقط في روسيا، ولكن أيضاً في الولايات المتحدة وأوروبا وكندا والبرازيل وفيتنام ودول أخرى[6].

---

[1] Mikanagi, T., & MačÁk, K. (2020). Attribution of cyber operations: an international law perspective on the Park Jin Hyok case. Cambridge International Law Journal, 9(1), 51–75 [p. 54]. https://doi.org/10.4337/cilj.2020.01.03

[2] المرجع السابق

[3] المرجع السابق – Delerue, F. – ص91

[4] Roscini, M. (2014). Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations. *Texas International Law Journal*, *50*, 233–273. Retrieved from https://ssrn.com/abstract=2611753

[5] Kuner, C. (2013). Transborder Data Flows and Data Privacy Law. Oxford, United Kingdom: Oxford University Press, pp. 11-14. https://doi.org/10.1093/acprof:oso/9780199674619.001.0001

انظر أيضا: المرجع السابق – Roscini, M. – Evidentiary Issues in International Disputes – ص247

[6] المرجع السابق – ص248

ما يمكن قوله بخصوص الدليل في قضية الهجمات السيبرانية أمام محكمة العدل الدولية أنه سيتكون من خليط من الأدلة التقنية: وهي الأدلة المباشرة، والظرفية –أو البشرية– وهي: الأدلة غير المباشرة مثل عوامل السياسة والتاريخ والاستخبارات التي تستخدم للوصول إلى نتيجة معينة والسؤال هو هل سيكون مثل هذا الدليل مقبولا في قضية منظورة أمام محكمة العدل الدولية.

الفرع الأول: معيار محكمة العدل الدولية في الإثبات

لا يتطلب النظام الأساسي لمحكمة العدل الدولية وقواعد المحكمة، معايير محددة للإثبات، ولا تشير إلى طرق الإثبات التي ستعدها المحكمة كافية؛ من أجل تلبية معيار معين، أو طرق الإثبات التي يتعين على محكمة العدل الدولية تجنبها[1]. لذلك تتبع معايير الإثبات في محكمة العدل الدولية مهمة تنتهي عادة بالإحباط[2]. فالحقيقة أنه بتتبع وجهة نظر محكمة العدل الدولية نجدها تتشدد تارة وتتراخى تارة أخرى في قبول الأدلة. والمشكلة عندئذٍ أنه لن يتمكن الخصوم من معرفة معيار الإثبات الذي استخدمته المحكمة إلا في مرحلة الحكم، يكون الوقت متأخرا بالطبع بالنسبة للأطراف لأخذها في الاعتبار.[3] ولسوف تعرض بعض نصوص أحكام محكمة العدل الدولية بخصوص معايير الإثبات التي استخدمتها المحكمة؛ لقبول أو رفض الأدلة في بعض القضايا، وما إذا مكان من الممكن استنتاج نمط معين في الإثبات. وفيما يأتي بعض الأمثلة على ذلك:

قضية المنصات النفطية: "ومع ذلك لا يوجد **(دليل مباشر)** في القاعدة الأولى من نوع الصاروخ الذي أصاب مدينة سي آيل؛ الأدلة إلى طبيعة الصواريخ الأخرى التي أطلقت على الأراضي الكويتية في هذه المدة **(أدلة موحية)**، وحسب، لا أكثر... يجب على المحكمة أن تأخذ علما بهذا النقص في الأدلة المتاحة[4]"

قضية قناة كورفو: "بخصوص شهادة الشاهد كوفاسيتش... تعدها المحكمة ادعاءات لا ترقى إلى مستوى **(الأدلة القاطعة)**. تهمة بهذه الجسامة الاستثنائية ضد دولة تتطلب **(درجة من اليقين)** الذي لم

---

[1] الأمم المتحدة، النظام الأساسي لمحكمة العدل الدولية، صدر في 18 أبريل 1946

[2] Singh, A. H. S. (2021, March 5). A Clear Standard of Proof in Disputes Before the ICJ: Are We There Yet? – Cambridge International Law Journal. Retrieved from http://cilj.co.uk/2021/03/05/a-clear-standard-of-proof-in-disputes-before-the-icj-are-we-there-yet/

[3] المرجع السابق – Roscini, M. – Evidentiary Issues in International Disputes – ص249

[4] *Oil Platforms* judgement, para. 59, p. 189

يتم التوصل إليه هنا في هذه الشهادة"[1] لكن في موقع لاحق قالت المحكمة إنه يمكن استخلاص الدليل من **(استنتاجات الحقيقة ... التي لا تترك مجالًا للشك المعقول)**.[2]

قضية نيكاراجوا: "استخدام مصطلح (ترضي نفسها) في النص الإنكليزي للنظام الأساسي للمحكمة يعني أن المحكمة يجب أن تفعل ذلك للحصول على **(درجة اليقين**" .... "**مدعومة بأدلة مقنعة)**[3]. في موقع لاحق طلبت المحكمة دليلًا واضحًا "لكن على الرغم من الإعانات الكبيرة وغيرها من الدعم المقدم من قبل الولايات المتحدة، لا يوجد "**دليل واضح**" على أن الولايات المتحدة كانت تمارس بالفعل درجة من التحكم في جميع المجالات لاعتبار الكونترا تتصرف نيابة عنها."[4]

قضية الأنشطة المسلحة في إقليم الكونغو: "يجب على المحكمة أولاً تحديد **الحقائق** (ذات الصلة) **التي تم إثباتها بشكل مقنع من خلال الأدلة**[5]"

"تعتمد أوغندا على بعض الوثائق التي أرفقتها جمهورية الكونغو الديمقراطية ... ومع ذلك، فإن المحكمة لا تجد هذه **(الأدلة ثقيلة ومقنعة)**. وهي تتكون من مجموعة تقارير إخبارية متغيرة الموثوقية"[6]

يتبين من هذا التنوع في مفردات طلب قوة الأدلة عدد من الأمور:

أولا: لا توجد معايير إثبات ثابتة لمحكمة العدل الدولية، تصنف الأدلة على أساسها، لكنها يجب أن تقنع نفسها للحصول على درجة اليقين المطلوبة من الأدلة المطروحة. تميل المحكمة إلى تقرير معيار الإثبات في أثناء النظر في القضية المطروحة وهذا يعطي كل قضية خصوصيتها في الإثبات[7].

ثانيا: هناك نوعان من الأدلة المباشرة والأدلة غير المباشرة أو الظرفية. الدليل المباشر هو الذي يرتبط بالوقائع ويدلل عليها مباشرة. أما الدليل غير المباشر فهو الذي يستخدم لاستنتاج الحقيقة، وليس التدليل عليها مباشرة[8].

---

[1] *Corfu Channel* judgement, p. 17
[2] *Corfu Channel* judgement, p. 18
[3] *Nicaragua* judgement, para. 29, p. 24
[4] *Nicaragua* judgement, para. 109, p. 62
[5] *Armed Activities* judgement, para. 72, p. 205
[6] *Armed Activities* judgement, para. 56, p. 199
[7] المرجع السابق – Roscini, M. – Evidentiary Issues in International Disputes – ص149
[8] المرجع السابق – Aravindakshan, S. – ص292

ثالثا: نهج محكمة العدل الدولية –وإن كان غالبا ما يطلب الدليل "المباشر" "القاطع" "الواضح"– فإن المحكمة تقبل في حالات خاصة الدليل الظرفي غير المباشر. يتضح لك من عبارات "استنتاجات الحقيقة"، و"الحقائق التي تم إثباتها من خلال الأدلة"، و"استنتاجات الحقيقة ... [التي] لا تترك مجالًا للشك المعقول".

يعرف قاموس كورنيل القانوني الدليل الظرفي أنه "دليل غير مباشر لا يؤسس حقيقة بمفرده، لكنه يمكن أن يؤدي إلى استنتاج منطقي بوجود الحقيقة. الأدلة الظرفية تحتاج إلى أن تلحق باستنتاجات منطقية لتدعم المطالبة"[1] هذا الأمر يرتبط ارتباطًا وثيقًا بإمكان معالجة القضاء الدولي موضوع الهجمات السيبرانية. فكرة الدليل غير المباشر أو الدليل الظرفي هي التي تم الاعتماد عليها في مرحلة نسبة الفعل إلى الدولة، وبالتالي هي الفكرة التي يجب أن تصمد أمام محكمة العدل الدولية. متى ترفض المحكمة الأدلة الظرفية؟ ومتى ترفضها؟

الفرع الثاني: متى تقبل محكمة العدل الدولية الدليل الظرفي؟ ومتى ترفضه؟

قضية قناة كورفو هي أول قضية تنظر فيها محكمة العدل الدولية، وهي قضية لإثبات المسؤولية الدولية بموجب قاعدة بذل العناية، وكان أساسها إثبات العلم المفترض لدولة ألبانيا، وهي من أشهر الأمثلة التي بنت المحكمة حكمها على القرائن والأدلة الظرفية[2].

تتلخص وقائع قضية قناة كورفو –وهي مضيق مائي بين ألبانيا واليونان– أنه في أكتوبر 1946 مرت سفن حربية بريطانية عبر القناة واصطدمت سفينتان بالألغام، مما ألحق بهما أضراراً بالغة. رفعت المملكة المتحدة قضية أمام محكمة العدل الدولية ضد ألبانيا، مدعية أن ألبانيا كانت مسؤولة عن الألغام الموجودة في القناة[3]. لإثبات أن ألبانيا كانت على علم بوجود الألغام، تم الاعتماد على أدلة غير مباشرة. وقد كان حكم المحكمة في صالح بريطانيا إلى حد كبير، فقد خلصت المحكمة إلى الآتي: أولاً: أن ألبانيا تراقب مياهها عن كثب فيمكنها أن تراقب زرع الألغام من الساحل، كان هناك انتهاك

[1] circumstantial evidence. (2022) In *Legal Information Institute*. Cornell Law School. Retrieved from https://www.law.cornell.edu/wex/circumstantial_evidence

[2] عبد الله، نايف. (2014). المبررات الموضوعية لعدم قبول الدعوى أمام محكمة العدل الدولية. مجلة جامعة تكريت للعلوم القانونية، (22)، 205-233 (ص217). استرجع من https://www.iasj.net/iasj/download/5c31e6bbbbeb84a9

[3] *Corfu Channel* judgement, p. 17

للقانون الدولي من قبل ألبانيا لأنها فشلت في تحذير المملكة المتحدة[1]. ثانيا: لا يمكن أن تكون المملكة المتحدة قد انتهكت القانون الدولي، فقد رفضت المحكمة ادعاء ألبانيا بأن المملكة المتحدة انتهكت السيادة الألبانية بإرسال سفن حربية عبر القناة.[2] ثالثا: سمحت المحكمة للمملكة المتحدة برفض تقديم تقارير معينة على أساس السرية[3]. رابعا وقالت المحكمة: إن الأدلة المباشرة الأخرى التي قدمتها المملكة المتحدة تتعارض مع مطالبة ألبانيا في ترجيح أدلة المملكة المتحدة وموقفها على صالح ألبانيا[4].

من الواضح هنا أنه تم تطبيق معيار إثبات أقل من اللازم لصالح المملكة المتحدة عندما سمحت المحكمة "باللجوء الليبرالي إلى استنتاجات الحقائق". في البحث في نصوص الحكم نجد أن المحكمة سوغت تساهلها في قبول الأدلة غير المباشرة بالآتي:

"من ناحية أخرى، فإن حقيقة التحكم الزماني الحصري –الذي يمارس من قبل دولة داخل حدودها– له تأثير على طرق الإثبات المتاحة ... بسبب هذه السيطرة الحصرية فإن الدولة الأخرى –ضحية خرق القانون الدولي– تكون في كثير من الأحيان غير قادرة على تقديم دليل مباشر للحقائق التي أدت إلى المسئولية الدولية. مثل هذه الدولة يجب أن تكون حرة أكثر للجوء إلى استنتاجات الحقائق والأدلة الظرفية. هذه الأدلة غير المباشرة تعد مقبولة في جميع أنظمة القانون، واستخدامها معترف به في القرارات الدولية. يجب أن يؤخذ في الحسبان أن لها وزنًا خاصًا عندما تكون مبنية على سلسلة من الحقائق المرتبطة معًا ويؤدي منطقيًا إلى استنتاج واحد[5]"

لذلك، يمكن استنتاج أن الاعتماد على الأدلة الظرفية يعد مقبولًا من قبل المحكمة عندما: (أ) يعمل الدليل الظرفي بالتوازي مع الأدلة المباشرة المتاحة والحقائق، و(ب) الدليل المباشر تحت السيطرة الخاصة للطرف الآخر[6]. من هنا يمكن حسبان تساهل المحكمة في معايير الإثبات تجاه المملكة المتحدة سليماً؛ لأن المملكة المتحدة، لم يكن لديها الفرصة للحصول على دليل مباشر قانوني، بينما كان لدى ألبانيا القدرة على جمع الأدلة المتعلقة بمرور السفن البريطانية عبر القناة.

---

[1] المرجع السابق – ص10
[2] المرجع السابق – ص12
[3]المرجع السابق – ص32
[4] المرجع السابق
[5] المرجع السابق – ص18
[6] المرجع السابق – ص18

كذلك قضية الإبادة الجماعية في البوسنة حين لم تقبل المحكمة الأدلة الظرفية فقد ادعت البوسنة والهرسك أن صربيا انتهكت اتفاقية الإبادة الجماعية لعام 1948[1] وفشلت أيضًا في التزامها بمنع مرتكبي الإبادة الجماعية ومعاقبتهم. وكانت القضية الأساسية التي تحاول البوسنة إثباتها هي وجود نية للإبادة الجماعية لدى صربيا[2]. والحالة هنا مشابهة لقضية قناة كورفو؛ لأن صربيا لديها سيطرة إقليمية حصرية على الإقليم، مما يجعل من المستحيل تقريبًا تقديم دليل مباشر يظهر التواطؤ الصربي، وأن المحكمة يجب أن تسمح للبوسنة بإجراء استنتاجات حرة للحقائق والظروف من أنماط الأدلة لتحميل صربيا المسؤولية، وكذلك امتلاكها النية المحددة لتنفيذ الإبادة الجماعية، لكن المحكمة[3] بالرغم من ذلك كله رفضت القيام بذلك ورأت أنه من أجل إثبات النية المطلوبة، يجب أن يكون أي نمط من السلوك "بحيث يشير فقط إلى وجود مثل هذه النية.[4]"

رفض المحكمة الأدلة الظرفية في هذه القضية ارتبط بعدد من العوامل. كاعتماد محكمة العدل الدولية على أحكام المحكمة الجنائية الدولية ليوغوسلافيا السابقة، التي تضمنت نتائج تتعارض مع ما كانت البوسنة تحاول إثباته.[5] لكن أهم عامل هو أن صربيا قدمت الكثير من الأدلة المباشرة مثل إفادات الشهود، على عكس ما كانت البوسنة تحاول القيام به.[6]

من الواضح أن المحكمة تفضل الدليل المباشر، هذا أمر متوقع أمام أي جهة قضائية، ولكن هذا لا يعني أنه في الحالات التي قد يكون فيها مثل هذا الدليل المباشر غائبا، إما بسبب صعوبات فنية، وإما بسبب رفض أحد الأطراف تقديمه، لن تلجأ المحكمة إلى أدلة ظرفية. طالما أنه من الصعب أو غير الممكن الوصول إلى أدلة المباشرة، وأن الأدلة الظرفية ستسفر عن سلسلة من الحقائق المرتبطة بعضها ببعض وتؤدي منطقيًا إلى استنتاج واحد لا يترك مجالًا للشك المعقول كما في قضية قناة كورفو.

[1] Genocide convention (1948)

[2] المرجع السابق – Singh, A. H. S.

[3] المرجع السابق – Aravindakshan, S. – ص294

[4] *Genocide* judgment, para. 376, p. 198

[5] المرجع السابق – Aravindakshan, S. – ص295

[6] المرجع السابق – ص295

الفرع الثالث: الأدلة الظرفية في سياق الهجمات السيبرانية

إن جمع الأدلة الظرفية، وملاحظتها أمر صعب، ولكن لا مناص من أن نتطرق إلى بعض المحاولات العملية من جانب الفقه لوضع الأدلة الظرفية السيبرانية موضع الاختبار أمام محكمة العدل الدولية. فمثلا ورقة " Cyber-Attacks: A Look at Evidentiary Thresholds in International Law" حاولت وضع الدليل الظرفي في المجال السيبراني موضع التطبيق العملي، وذلك بالنظر في هجمات سيبرانية ضارة وقعت بالفعل في أحد المفاعلات النووية الهندية في كودانكولام، وجمع الأدلة الظرفية ومحالة توقع رأي محكمة العدل فيها. فقد كشفت التحقيقات في الواقعة المذكورة عددا من الأمور المهمة وهي:

(1) تم تتبع الهجوم إلى نموذج حاسوبي تم إنتاجه واستخدامه فقط في كوريا الشمالية[1].

(2) تحمل عناوين MAC و IP توقيعات كورية شمالية.[2]

(3) اللغة الكورية قد استخدمت في "كود" (شفرة) البرامج الخبيثة.[3]

(4) الرمز الخبيث يتوافق مع هجوم إلكتروني سابق على بنوك كوريا الجنوبية، وقد نُسب إلى كوريا الشمالية.[4]

(5) إن الشفرة هي أحد أشكال البرامج الضارة "Dtrack" المعروفة بأنها مرتبطة بمجموعة Lazarus التي يُعتقد أنها تتكون من كوريين شماليين[5].

(6) وتقارير استخباراتية عن محاربين إلكترونيين دربتهم حكومة كوريا الشمالية استخدموا لتنفيذ عمليات تجسس إلكتروني مماثلة في بلدان مختلفة[6].

بناءً على هذه المعلومات فإن الأدلة المستخدمة في نسبة الفعل إلى كوريا الشمالية يغلب عليها البعد التقني، لكنها مزيج من عمل الاستخبارات، والقراءة للتاريخ والحوادث السابقة المماثلة، وهي أفضل

[1] المرجع السابق – ص297
[2] المرجع السابق
[3] المرجع السابق
[4] المرجع السابق
[5] المرجع السابق
[6] المرجع السابق

نتيجة يمكن أن يصل إليها منهج التنسيب المطروح حاليا. فنرى أن الأدلة توجه الاتهام إلى كوريا الشمالية فهل تصمد تلك الأدلة أمام قضية في محكمة العدل الدولية تتهم فيها الهند حكومة كوريا الشمالية بشأن هجوم كودانكولام الإلكتروني.

فيرى الكاتب Aravindakshan أنه من غير المحتمل أن تحقق هذه الأدلة بحد ذاتها الكثير في إقناع المحكمة. وفي أحسن الأحوال، قد يُنظر إلى هذه التقارير على أنها أدلة داعمة، ومن غير المرجح أن تصمد في التدقيق أمام أي جهة قضائية دولية.[1] فقد تتمكن تلك الأدلة من إثبات أن البرامج الضارة المستخدمة تتبع كوريا الشمالية، لكن هل هذا يعني أنه لا يوجد طرف آخر يمكنه استخدام تلك البرامج؛ بغرض التمويه، وتحويل الأنظار نحو المدعى عليها. قد تستطيع الهند إثبات أن كوريا الشمالية هي المستفيد من تخريب برنامجها النووي، لكن هل سيكون ذلك كافيا أمام المحكمة؟ أم أنها ستطلب من الهند إثبات أن كوريا الشمالية هي المستفيد الوحيد لاستبعاد أية دولة أو جهة دولية أخرى؟

بل يتوقع الكاتب أنه سيُطلب من الهند أيضًا إبطال احتمالات انتحال بروتوكول الإنترنت، ومحاكاة الشفرات، وأنماط الإخفاء والتمويه الأخرى في الفضاء الإلكتروني؛ لأنها ستتحمل عبء نفي وجودها. وقد يُطلب من الهند أيضًا إثبات حقائق مثل البرمجيات الخبيثة من النوع الذي تمتلكه وتستخدمه حكومة كوريا الشمالية فقط مع عدم وجود إمكانية معقولة لأي جهة فاعلة أخرى، الأمر الذي يراه الكاتب عبئا ثقيلا على أي دولة.[2] [3]

كما تمت مناقشته في المبحث الأول من هذا الفصل يبدو أن أحد الطرق القابلة للتطبيق يتمثل في التراكم السليم للأدلة غير المباشرة أو الظرفية واستخدامها، وهو الشكل الرئيس للأدلة المتوافرة حاليًا في المجال السيبراني. بالنظر إلى أن معظم الأدلة من المرجح أن تكون تحت السيطرة الحصرية للدولة المهاجمة، هناك احتمال أن تسمح المحكمة باللجوء الليبرالي إلى الحقائق والظروف. إلا أنه يجب على تلك الأدلة الظرفية أن تؤدي إلى استنتاج واحد بحيث "لا تترك مجالاً للشك المعقول" بعكسها. وهذا المعيار المرتفع، هو أصعب تحدٍ أمام أدلة الإثبات السيبرانية. ولما لم تكن هناك –حتى الآن– أي

---

[1] المرجع السابق – ص298

[2] المرجع السابق – ص298-299

[3] كذلك تجدر الإشارة إلى أن ورقة بحثية أخرى كتبت بالاشتراك بين خبير في القانون الدولي وخبير في الأمن السيبراني قامت بتقييم الأدلة الظرفية التي عرضتها السلطات الفيدرالية في الولايات المتحدة والتي بناء عليها تم وضع بعض القراصنة الكوريين الشمالبين على قوائم المطلوبين بتهمة القيام بهجمات الكترونية منها هجمات سوني. وانتهت أيضا إلى نفس النتيجة أنه من الصعب أن تقبل محكمة العدل تلك الأدلة لبناء دعوى قانونية.

للمزيد انظر: المرجع السابق – Mikanagi, T., & Mačák, K.

قضية أمام محكمة العدل الدولية أو غيرها من المحاكم الدولية التي تخاطب الدولة المسؤولية الناشئة عن العمليات السيبرانية، ستظل الإجابة عن ذلك غير معروفة برغم السوابق التي تبين أن ذلك ممكن.

الحقيقة أنه لا بد أن تتكيف المحكمة مع خصوصية الطبيعة السيبرانية والتعامل بمعايير جديدة تتلاءم معها. والقول بغير ذلك يعني القول باستحالة إخضاع هذا النوع من الأفعال لعدالة القضاء، وبالتالي فيه إنكار للعدالة. والقدرة على التكيف مع الطبيعة السيبرانية أمر متوقع من محكمة العدل فهي لم تلزم نفسها بمعايير جامدة، بل الملاحظ أنها كانت تميل إلى التشدد في القضايا ذات الطبيعية الجنائية، مثل قضية الإبادة الجماعية بين البوسنة وصربيا، وتميل إلى التساهل في القضايا ذات الطبيعة المدنية، مثل قضية قناة كورفو. لذلك فالمرجح أن تستمر المرونة لدى المحكمة، وهي مرونة مستمدة من مرونة قواعد القانون الدولي التي تمددت لتشمل الفضاء السيبراني. وإن كانت هناك صعوبة لوصول قضايا الهجمات السيبرانية أمام محكمة العدل الدولية، فلن تكون بسبب معايير الإثبات، بل الاحتمال صعب جدا وبعيد؛ بسبب صعوبة إحضار دول أمام المحكمة لمحاسبتها على أعمال من طبيعة الهجمات السيبرانية.

الخاتمة

بعد أن ناقشت هذه الأطروحة انطباق القانون الدولي على الهجمات السيبرانية في ضوء قانون اللجوء إلى الحرب يتبين أن الكثير من المناطق بقيت مفتوحة دون جزم وسيبقى الأمر كذلك حتى يحسم بمعاهدة أو ممارسة دولية واضحة ومتكررة تلاقي قبول من مجتمع الدول. ولأن الخيار الأول مستبعد حاليا فمن المهم تقريب وجهات النظر للاتفاق على تفسير القانون الدولي في النطاق السيبراني. برغم تعرض الدول لهجمات سيبرانية باستمرار إلا أن المشكلة أن الدول لا تصرح بموقفها القانوني تجاهها، فلا يكفي ان تصرح الدولة أنها تعرضت لهجوم سيبراني أو أنها تعرضت لهجوم سيبراني وتشير دلائل قوية أن روسيا مثلا تقف خلفه، بل المهم هو التكييف القانوني للهجوم السيبراني كأن تعتبره (مع التسبيب القانوني) خرقا لمبدأ السيادة أو تدخلا في الشأن الداخلي أو في حكم الهجوم المسلح. إذا حدث ذلك بشكل متكرر سيكون القانون الدولي السيبراني أكثر صلابة. ذلك لأنه مهما غزرت المراجع الفقهية التي تتصدى لتكييف الهجمات السيبرانية فأنها لن تصنع قانوناً، فالآراء الفقهية لا تصنع القاعدة الدولية الملزمة، بل الدول هي من يفعل ذلك.

كذلك من الأمور المهمة المستفادة في هذا البحث هي مرونة القانون الدولي وقدرته على ضبط أي ظاهرة مستجدة. فالمواضيع القانونية التي لم تحسم في النطاق السيبراني هي نفسها التي لم تحسم في القانون الدولي بشكل عام مثل عتبة الهجوم المسلح والدفاع عن النفس الاستباقي أو الدفاع عن النفس ضد جماعات مسلحة مستقلة أو مدى قبول محكمة العدل الدولية للدليل الظرفي، كل تلك المواضيع مازالت غير محسومة حتى خارج الطبيعة السيبرانية وبالتالي امتد الخلاف على الهجمات السيبرانية. فيما عدا ذلك فإن القانون انطبق بسهولة في نفس المناطق المتفق عليها في القانون كانطباق قاعدة منع استخدام القوة اذا كانت آثار الهجوم السيبراني تضاهي آثار استخدام القوة، وشروط الضرورة والتناسب والمسؤولية الدولية وغيرها. هنا درس مهم يجب استيعابه ان مبادئ القانون الدولي قادرة على استيعاب الجديد من الأسلحة والظواهر المختلفة، لذلك نقطة البدء يجب ان تكون **كيف** ينطبق القانون الدولي على الموقف؟، وليس هل ينطبق القانون الدولي؟

أخيرا هذه الدراسة استخدمت في مراجعها المراجع الغربية غالبا وذلك لنقص المراجع الشرقية بشكل عام. ليس المقصود الوطن العربي فقط، بل حتى روسيا والصين والهند، وهذا يطرح تساؤلا حقيقيا عن

مدى القبول الدولي للطرح الغربي كما جاء في دليل (تالين). هذا يؤكد الحاجة الملحة لاهتمام الدول الشرقية بهذا الموضوع وقد تكون نقطة بداية جيدة هي قراءة في دليل (تالين) فإما الاتفاق أو الاختلاف معه أو التعديل عيه.

وتأسيساً على ما تقدم، فقد توصلت هذه الدراسة إلى جملة من النتائج والتوصيات، نورد أهمها على النحو الآتي:

الاستنتاجات:

1- الاستخدام العدواني للهجمات السيبرانية ممنوع في القانون الدولي؛ لأن قاعدة منع استخدام القوة كما هي موجود في المادة 2(4) من الميثاق، تنطبق على الهجمات السيبرانية، وذلك بالنظر أنه لا خلاف على انطباقها على الأسلحة البيولوجية والكيميائية وهذين النوعين يدخلان في نطاق القوة الممنوعة بسبب الآثار التي تماثل أو تفوق آثار السلاح التقليدي؛ لذلك يمكن اعتبار الهجمات السيبرانية سلاحاً لاحتواء قدراتها التدميرية في نطاق المادة 2(4).

2- يمكن ان يعتبر الهجوم السيبراني في حكم الهجوم المسلح إذا كانت الآثار التي تسبب بها تشابه آثار الهجوم بالسلاح التقليدي. والأثر المقصود هو الأثر الحركي أي ان يؤدي الهجوم السيبراني إلى الإصابة أو موت الأشخاص أو تدمير الممتلكات. وبالتالي يمكن الرد على هذا النوع من الهجمات بالدفاع عن النفس.

3- لا يمكن اعتبار الهجوم السيبراني في حكم الهجوم المسلح إذا ظلت آثاره حبيسة العالم الرقمي كتعطيل الخدمة أو فقدان المعلومات أو حتى لو ظهرت آثاره في شكل خسائر اقتصادية واسعة يجب تذكر ان ذلك يخالف الميثاق حيث تم رفض اقتراح ادخال البعد الاقتصادي في معنى القوة أثناء الصياغة. بالتالي لا يمكن الرد على مثل هذا النوع من الهجمات بالدفاع عن النفس والقول بغير ذلك فيه منحى خطير نحو التصعيد في استخدام القوة ومخالفة لروح الميثاق. لكن يمكن مواجهة هذا النوع من الهجمات بالتدابير المضادة أو التدابير القانونية الغير ودية أو تدابير حالة الضرورة اذا انطبقت شروطها.

4- في الدفاع عن النفس ضد هجوم مسلح سيبراني لا بد من مراعاة الطبيعة الخاصة لعنصر الضرورة. فالدفاع عن النفس يكون **ضرورياً** إذا لم تكن الدفاعات الإلكترونية السلبية (محاولة تعزيز الدفاع وسد الثغرات التي تستغلها الهجمات السيبرانية) أو الدفاعات الإلكترونية النشطة (الدفاع بالوسيلة السيبرانية لإيقاف الهجوم) التي تقل عن عتبة استخدام القوة كافية لتحييد الهجوم السيبراني المسلح.

5- كذلك لا بد من مراعاة الطبيعة الخاصة لعنصر التناسب. فيكون الدفاع عن النفس متناسباً إذا كان مصمما في مقداره وحجمه لتحقيق هدف الدفاع وهو دحر الهجوم السيبراني، وليس تحقيق نفس الاضرار التي خلفها الهجوم السيبراني المسلح لأن ذلك يدخل في الانتقام غير المشروع. كما ينبغي تذكر أن التماثل في الرد بنفس الوسيلة السيبرانية دفاعاً عن النفس غير مطلوب فإذا كان الرد بالوسيلة السيبرانية غير كاف لإيقاف الهجوم السيبراني المسلح يمكن اللجوء للسلاح التقليدي إذا كان سيحقق هدف الدفاع.

6- الدفاع عن النفس ضد **تهديد** بهجمات سيبرانية محتمله غير مستقر في مشروعيته، حتى لو كان ذلك التهديد السيبراني وشيكا أو قريب الحدوث وذلك لأن معنى التهديد الوشيك غير متفق عليه بعد. لذلك الدولة الحريصة على البقاء في إطار المشروعية لا تستخدم الدفاع عن النفس ضد تهديد بهجوم سيبراني إلا إذا كانت هناك خطوات اتخذت لتنفيذ التهديد السيبراني أي يكون بدأ في مرحلة التنفيذ وليس التخطيط والتحضير، فإذا بدأت مرحلة التنفيذ يمكن اعتراضه دفاعاً عن النفس أما إذا لم يبدأ بعد لكن هناك مؤشرات على قرب حدوثه فالأمر مازال غير مستقر في مشروعيته.

7- إذا لم يصل الهجوم السيبراني لمرحلة استخدام القوة فلا يمكن الرد بالدفاع عن النفس لكن يمكن الرد بالتدابير المضادة أو التدابير القانونية أو تدابير حالة الضرورة. لكن يجب الانتباه ان هذه الردود يجب ان لا تهدف إلى مجرد الرد بهدف الانتقام، بل يجب ان تهدف إلى الكف عن الفعل غير المشروع أو تقديم الضمانات بعدم التكرار أو جبر الضرر الي احدثته الهجمات السيبرانية.

8-لا يمكن استخدام الدفاع الشرعي عن النفس ضد هجمات سيبرانية إلا إذا صدرت من دولة أو بدعم أو رعاية دولة. وعليه يمكن الدفاع عن النفس ضد الجماعات غير الحكومية إذا تبين بعملية التنسيب أنها كانت بمثابة امتداد لأجهزة الدولة أو مدعومة من الدولة. اما الهجمات السيبرانية التي تتبناها جماعات مستقلة فلا يمكن الدفاع عن النفس ضدها دون موافقة الدولة التي تنطلق تلك الهجمات منها.

أفضل تعامل قانوني مع هذه الحالة هو عرض المساعدة على دولة الإقليم التي تنشأ منها الهجمات فإذا لم توافق يمكن إلزام الدولة بإيقاف الهجمات بقاعدة بذل العناية Due Diligence، فإذا فشلت الدولة في إيقاف الهجمات السيبرانية يمكن الضغط عليها بموجب قواعد مسؤولية الدولة لتقصيرها في التزام بذل العناية واستخدام الإجراءات المضادة ضد إقليم تلك الدولة أو الإجراءات القانونية أو تدابير حالة الضرورة.

9- تكون الدولة مسؤولة عن الهجوم السيبراني بموجب قواعد مسؤولية الدولة إذا نسبت الهجمات السيبرانية اليها بموجب قواعد مسؤولية الدولة وإذا شكلت الهجمات السيبرانية خرقا لالتزام دولي. الالتزام الدولي قد يكون معاهدة دولية عامة أو ثنائية أو قاعدة عرفية ويبدو أن أكثر القواعد القانونية ملامسة للسلوك غير القانوني في الفضاء السيبراني في قانون اللجوء إلى الحرب هي (الاستخدام غير المشروع للقوة- عدم التدخل في الشأن الداخلي- سيادة الدولة - واجب بذل العناية).

10- الاثبات التقني في المجال السيبراني يعطي نتائج غير قطعية فدائما هناك مجال لتزوير الهوية، لكن الاثبات في القانون الدولي (في المواضيع ذات طبيعة غير جنائية) يعتمد على المعقولية وليس القطعية لذلك طالما ان نتيجة نسبة العملية السيبرانية تعتبر استنتاجا معقولا في ظروف الدولة سيكون التصرف الذي يتبعها أكثر قبولا في مشروعيته. ولكي يكون الاستنتاج معقولا يجب ان لا يتم الاكتفاء بنتيجة التنسيب التقني وحده، بل يجب ان تضاف آلية ادلة استخباراتية وظرفية وتاريخية وغيرها لزيادة عنصر المعقولية.

التوصيات:

1- ضرورة استمرار الدول على ان يكون لها استراتيجيات أمن سيبراني تجيب فيه عن موقفها بشأن كيفية انطباق القانون الدولي على الفضاء السيبراني. خصوصا القواعد التي مازالت مثارا للخلاف مثل متى تعتبر الهجمة السيبرانية استخداما للقوة ومتى تعتبر في حكم الهجوم المسلح. ومتى تعتبر خرقا السيادة وكيف يتم تنفيذ واجب بذل العناية في منظورها. تلك المواقف يجب ان تخضع لتدقيق ونقد الفقه لعدم الحياد عن المشروعية الموجودة في الميثاق.

2- ضرورة الاهتمام بعملية رصد وتجميع سلوك ومواقف الدول في القانون الدولي السيبراني. هناك قاعدة مركز التميز للدفاع السيبراني التابع لحلف الناتو وهذا أمر جيد لكن من الضروري أن تظل

خاضعة للتحديث المستمر وأن تتاح بعدة لغات، لأن تلك القواعد تساعد على إبراز التفسير الأكثر قبولا لانطباق القانون الدولي على الفضاء السيبراني.

3- ضرورة تفعيل الدول للقانون الدولي في حوادث الهجمات السيبرانية الدولية. فاذا تعرضت دولة لهجوم سيبراني فلا يكفي إعلان أن دولة ما تقف وراء الهجوم، بل يجب ومن الضروري ان تشير الدولة أي قاعدة تم خرقها بهذا الهجوم السيبراني، لو تكررت هذه المواقف ستكون قيمة جدا في ترجيح تفسير كيفية انطباق القانون الدولي على الهجمات السيبرانية.

4- نهيب بالمجتمع الفقهي بالتمسك بمعنى الهجوم المسلح في الفضاء السيبراني كما جاء في الميثاق ومقاومة محاولات التوسع في تشريع استخدام القوة وذلك عن طريق:

- عدم اعتبار الهجمات السيبرانية التي تولد خسائر اقتصادية في حكم الهجوم المسلح واعتبار التماثل مع أثر الأسلحة التقليدية (إصابة أو موت أو تدمير) شرطاً للهجوم المسلح السيبراني.
- بضرورة مراجعة مخاطر نظرية الهجوم المسلح بشكل تجميعي أو تراكمي لأنها تتعارض مباشرة مع الميثاق الذي تطلب وقوع هجوم مسلح بشكل غير مجزأ.
- ضرورة بقاء التدابير المضادة خارج دائرة استخدام القوة وإلا فأين الخط الفاصل بينها وبين الدفاع عن النفس. ويجب الانتباه أن مما يمكن أن يتحقق به سد الحاجة إلى تدابير مضادة تنطوي على استخدام القوة هو إبقاء الهجمات التعطيلية ذات الأثر غير الحركي خارج نطاق استخدام القوة، ليتسنى استخدامها كتدبير مضاد.

5- التشجيع على التعاون الدولي لإنشاء وحدة تحقيق دولية لنسبة حوادث الهجمات السيبرانية، واقعية مثل هذه المبادرة تعتمد على الأداة القانونية التي تنظم عملها. فالنظام الأساسي الذي ينظم عمل وحدة التحقيق الدولة يجب أن يعرض مزايا عديدة لمنفعة الدولة العضو حتى يسهل في المقابل الحصول على رضاء الدولة وتقديمها بعض الالتزامات كالتعاون وتبادل الخبرات والتعهد بالاستخدام السلمي القانوني للفضاء السيبراني. ويمكن الاستفادة من تجربة الوكالة الدولية للطاقة الذرية في هذا المجال.

6- التشجيع على الأخذ بإلزامية البعد الوقائي لقاعدة بذل العناية إن لم يكن كقاعدة ملزمة فكسلوك الدولة المسؤولة فمع التسليم بعدم قدرة الدولة على معرفة كل استخدام ضار للإنترنت على اقليمها والتسليم بتعارض مراقبة جميع استخدامات الانترنت مع حقوق الانسان وخصوصا الحق في

الخصوصية، لكن هناك بعض الإجراءات الوقائية التي تعتبر في متناول أي دولة بحكم سيادتها، كتشريع قوانين تجرم الهجمات السيبرانية وحملات التثقيف والتوعية من مخاطر مثل هذا السلوك ووضع سياسات عامة تجبر شركات الاتصال على التعاون في حال معرفتها بارتكاب هجمات سيبرانية ضارة.

7- الدعوة إلى الاهتمام بقاعدة الالتزامات تجاه المجتمع الدولي ككل؛ لما فيها من مؤهلات تسد الحاجة إلى دور مجلس الأمن المتعطل. فالمعلوم أن هذا النوع الالتزام موجود لكن ماهي بالضبط تلك الالتزامات التي تمس المجتمع الدولي ككل؟ وكيف يمكن حماية المبدأ من سوء الاستخدام والتدخل في الشؤون الداخلية؟ هذه أسئلة لم تتضح الإجابة عليها بعد، وهي- كما تمت الإشارة إلية- تستحق البحث.

8-محكمة العدل الدولية يجب ان تكون مستعدة لتقديم معيار إثبات يتناسب مع الطبيعة السيبرانية، والاهتمام بالكتابات الفقهية التي تعنى بهذا الموضوع خطوة في الاتجاه الصحيح، وهذا أمر يجب أن يشترك فيه الخبراء من الحقلين التقني والقانوني.

المصادر والمراجع

الكتب

الجمل، حازم (2015). الحماية الجنائية للأمن الإلكتروني (الطبعة الأولى). المنصورة، جمهورية مصر: دار الفكر والقانون للنشر والتوزيع.

جلال، يحي (2014) التاريخ الأوروبي الحديث والمعاصر حتى الحرب العالمية الأولى (الطبعة الثالثة). الإسكندرية: جمهورية مصر: المكتب الجامعي الحديث.

عبد الصادق، عادل .(2009) .الارهاب الالكتروني: القوة في العلاقات الدولية نمط جديد وتحديات مختلفة (الطبعة الأولى). جمهورية مصر: مركز الدراسات السياسية والاستراتيجية بالأهرام.

Anghie, A. (2004). The Bush Administration Preemption Doctrine and the United Nations. Proceedings of the 115th ASIL Annual Meeting, 98, 326–331. https://doi.org/10.1017/s0272503700061565

Brownlie, I. (1991). International Law and the Use of Force by States (1st ed.), p. 250. Oxford, England: Clarendon Press.

Buchan, R., & Navarrete, I. (2020). Cyber Espionage. Oxford Bibliographies in International Law. https://doi.org/10.1093/obo/9780199796953-0212

Bussolati, N. (2015). 6 The Rise of Non-State Actors in Cyberwarfare. In Cyber War: Law and Ethics for Virtual Conflicts (pp. 102–126). Oxford, United Kingdom: Oxford University Press. https://doi.org/10.1093/acprof:oso/9780198717492.003.0007

Chayes, A. (2015). 10 - Cyber Attacks and Cyber Warfare: Framing the Issues. In Borderless Wars: Civil Military Disorder and Legal Uncertainty (pp.

130–143). Cambridge, United Kingdom: Cambridge University Press. https://doi.org/10.1017/CBO9781316271551.011

Clarke, R. A., & Knake, R. (2010). Cyber War: The Next Threat to National Security and What to Do About It. Harper Collins.

Clarke, R. A., & Knake, R. K. (2020). The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats. Penguin Random House.

Corten, O. (2021b). The Law Against War: The Prohibition on the Use of Force in Contemporary International Law. In Do the Prohibition of the Use of Force and Self-Defence Apply to Non-State Actors? (pp. 137–203). Oxford, United Kingdom: Hart Publishing. https://doi.org/10.5040/9781509949021.ch-003

Crawford, J. (2012). Brownlie's Principles of Public International Law (8th ed.). Oxford, United Kingdom: Oxford University Press. https://doi.org/10.1093/he/9780199699698.001.0001

Crawford, J. (2013). State Responsibility: The General Part. Cambridge, United Kingdom: Cambridge University Press.

Curtin, P. A., & Gaither, K. T. (2007). International Public Relations: Negotiating Culture, Identity, and Power (1st ed.). SAGE Publications. https://doi.org/10.4135/9781452224817

Delerue, F. (2020). Cyber Operations and International Law. Cambridge, United Kingdom: Cambridge University Press. https://doi.org/10.1017/9781108780605

Dinniss, H. H. (2014). Cyber Warfare and the Laws of War (Cambridge Studies in International and Comparative Law, Series Number 92) (Illustrated ed.). Cambridge: Cambridge University Press.

Dinstein, Y. (2012). War, Aggression and Self-Defence. Cambridge, United Kingdom: Cambridge University Press.

Dinstein, Y., & Dahl, A. W. (2020c). Section II: Cyber Operations. In Oslo Manual on Select Topics of the Law of Armed Conflict: Rules and Commentary (pp. 19–29). Springer, Cham. https://doi.org/10.1007/978-3-030-39169-0_2

Foster, C. E. (2021). Global Regulatory Standards in Environmental and Health Disputes: Regulatory Coherence, Due Regard, and Due Diligence. Oxford, United Kingdom: Oxford University Press.

Gardam, J. (2009). Necessity, Proportionality and the Use of Force by States. Cambridge, United Kingdom: Cambridge University Press. https://doi.org/10.1017/CBO9780511494178

Geiss, R., & Lahmann, H. (2013). Freedom and Security in Cyberspace: Shifting the Focus away from Military Responses towards Non-Forcible Countermeasures and Collective Threat-Prevention. In Peacetime Regime for State Activities in Cyberspace (pp. 621–657). Tallinn, Estonia: NATO CCD COE Publications.

Glennon, M. J. (2003). Limits of Law, Prerogatives of Power: Interventionism after Kosovo (2001st ed.) London, United Kingdom: Palgrave Macmillan.

Gray, C. (2018). International Law and the Use of Force (Foundations of Public International Law) (4th ed.). Oxford, United Kingdom: Oxford University Press.

Green, J. R. (2009). The International Court of Justice and Self-Defence in International Law. London, United Kingdom: Hart Publishing.

Green, J.A. (Ed.). (2016). Cyber Warfare: A multidisciplinary analysis: Routledge Studies in Conflict, Security and Technology (1st ed.). Routledge.

Guzman, A. T. (2009). Rethinking International Law as Law. Proceedings of the 115th ASIL Annual Meeting, 103, 155–157. https://doi.org/10.1017/s0272503700033978

Hannas, W. C., Mulvenon, J., & Puglisi, A. B. (2013). Chinese Industrial Espionage: Technology Acquisition and Military Modernisation (Asian Security Studies) (1st ed.). Retrieved from https://www.routledge.com/Chinese-Industrial-Espionage-Technology-Acquisition-and-Military-Modernisation/Hannas-Mulvenon-Puglisi/p/book/9780415821421

Healey, J., & Grindal, K. (Eds.). (2013). A Fierce Domain: Conflict in Cyberspace, 1986 to 2012 (Illustrated ed.). Vienna, Virginia: Cyber Conflict Studies Association (CCSA).

Higgins, R. (1995). Problems and Process: International Law and How We Use It (Reprint ed.). Oxford, United Kingdom: Clarendon Press. https://doi.org/10.1093/law/9780198764106.001.0001

Hyde, R., & Kolb, R. (2008). The Separation Between Jus Ad Bellum and Jus in Bello in Modern International Law: Equality of the Belligerents and Just War. An introduction to the international law of armed conflicts (pp. 21–28). Hart Publishing.

Janczewski, L. J., & Colarik, A. M. (2007). Cyber Warfare and Cyber Terrorism (1st ed.). Hershey, Pennsylvania: IGI Global.

Jayakumar, S. (2020). Cyber Attacks by Terrorists and other Malevolent Actors: Prevention and Preparedness. In Handbook of Terrorism Prevention and Preparedness (pp. 898–954). Hague, Netherlands: ICCT Press. https://doi.org/10.19165/2020.6.01

Jennings, R., & Watts, A. (2008). Oppenheim's International Law: Volume 1 Peace (9th ed.). Oxford University Press.

Jessup, P. C. (1948). Modern Law of Nations - An Introduction, p. 166. New York, United States: Macmillan Publishers.

Kampmann, C. (2021). The Treaty of Westphalia As Peace Settlement and Political Concept: From a German Security System to the Constitution of International Law. In Marc Weller, M. Retter, & A. Varga (Eds.), International Law and Peace Settlements (pp. 64–85). Cambridge University Press. https://doi.org/10.1017/9781108627856.005

Kittichaisaree, K. (2017). Public International Law of Cyberspace. In Law, Governance and Technology Series, 32. Cham, Switzerland: Springer.

Kuerbis, B. (2022). Understanding transnational cyber attribution: Moving from "whodunit" to who did it. In Cyber Security Politics: Socio-

Technological Transformations and Political Fragmentation (1st ed., pp. 220–239). Retrieved from https://www.taylorfrancis.com/chapters/oa-edit/10.4324/9781003110224-17/understanding-transnational-cyber-attribution-brenden-kuerbis-farzaneh-badiei-karl-grindal-milton-mueller

Kuner, C. (2013). Transborder Data Flows and Data Privacy Law. Oxford, United Kingdom: Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199674619.001.0001

McLean, A. T. (1993). WWI: Technology and the weapons of war. In Tar heel junior historian (Vols. 32, No. 2, pp. 25–30). Raleigh, North Carolina: North Carolina Museum of History. Retrieved from https://digital.ncdcr.gov/digital/collection/p16062coll9/id/521069

National Research Council. (2009). Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities. (W. A. Owens, K. W. Dam, & H. S. Lin, Eds.) (Illustrated ed). Washington, DC: National Academies Press, https://doi.org/10.17226/12651

National Research Council. (2010). Proceedings of a Workshop on Deterring Cyberattacks. Washington, DC: The National Academies Press. https://doi.org/10.17226/12997

NATO and Cyber Terrorism. (2008). In Responses to Cyber Terrorism (NATO Science for Peace and Security Series-E: Human and Societal Dynamics ed, (pp. 118–126). Ankara, Turkey: Centre of Excellence Defence Against Terrorism.

Nichols, T. M. (2008). Eve of Destruction: The Coming Age of Preventive War. University of Pennsylvania Press.

Nolte, G., & Randelzhofer, A. (2012). Ch.VII Action with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression, Article 51. In The Charter of the United Nations: A Commentary, Volume II (3rd Edition) (3rd ed., p. 1409). Oxford, United Kingdom: Oxford University Press.

Noortmann, M. (2005). Enforcing International Law. Aldershot, England: Ashgate

Noortmann, M., Reinisch, A., & Ryngaert, C. (Eds.). (2017). Non-State Actors in International Law (Studies in International Law) (Reprint ed.), p. 86. Oxford, United Kingdom: Hart Publishing.

O'Brien, J. (2001). International Law (1st ed.), p. 682. Abingdon, United Kingdom: Routledge.

Off Target: The Conduct of the War and Civilian Casualties in Iraq. (2003), p. 138. Human Rights Watch. Retrieved from https://www.hrw.org/reports/2003/usa1203/usa1203.pdf

Orford, A. (2009). Reading Humanitarian Intervention: Human Rights and the Use of Force in International Law. Cambridge, United Kingdom: Cambridge University Press.

Perkovich, G., & Levite, A. E. (Eds.). (2017). 5 Cyber War and Information War à la Russe. In Understanding Cyber Conflict: 14 Analogies (pp. 81–98). Washington, DC: Georgetown University Press.

Pitropakis, N., et al. (2018). An Enhanced Cyber Attack Attribution Framework. In S. Furnell, H. Mouratidis, & G. Pernul (Eds.), Trust, Privacy

and Security in Digital Business (pp. 213–228). Regensburg, Germany. https://doi.org/10.1007/978-3-319-98385-1_15

Reichberg, G. M., Syse, H., & Begby, E. (Eds.). (2008). The Ethics of War: Classic and Contemporary Readings (1st ed.).

Roscini, M. (2016). Cyber Operations and the Use of Force in International Law (1st ed.). https://doi.org/10.1093/acprof:oso/9780199655014.001.0001

Rosenzweig, P. (2013). Chapter 6: The Fundamental Problem of Identity. In Cyber Warfare: How Conflicts in Cyberspace Are Challenging America and Changing the World (Illustrated, pp. 75–84). Praeger. Retrieved from http://publisher.abc-clio.com/A3670E

Ruys, T., Corten, O., & Hofer, A. (Eds.). (2018). The Use of Force in International Law: A Case-Based Approach. Oxford, United Kingdom: Oxford University Press. https://doi.org/10.1093/law/9780198784357.001.0001

Ruys, T., Corten, O., & Hofer, A. (Eds.). (2018). The Use of Force in International Law: A Case-Based Approach. Oxford, United Kingdom: Oxford University Press. https://doi.org/10.1093/law/9780198784357.001.0001

Schmitt, M. N. (2010). Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts. In Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy (pp. 151–178). Washington, DC: National Academies Press.

Schmitt, M. N. (2010b). Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts. In Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy (pp. 151–178). Washington, DC: National Academies Press. https://doi.org/10.17226/12997

Schmitt, M.N. (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (2nd ed.). Cambridge University Press. https://doi.org/10.1017/9781316822524

Shaw, M. N. (2022). International Law 6th (sixth) edition (6th ed.). Cambridge, United Kingdom: Cambridge University Press.

Stevens, K. R. (1989). Border Diplomacy: The Caroline and McLeod Affairs in Anglo-American-Canadian Relations, 1837-1842 (1st ed.). University Alabama Press.

The Open University. (2017). The use of force in international law. University course. Retrieved from https://www.open.edu/openlearn/society-politics-law/the-use-force-international-law/altformat-word

Wedgwood, R. (1992). Proportionality and Necessity in American National Security Decision Making. Proceedings of the ASIL (American Society of International Law) Annual Meeting, 86, 58–67. https://doi.org/10.1017/s0272503700094295

Weller, M., Rylatt, J. W., & Solomou, A. (Eds.). (2015). The Oxford Handbook of the Use of Force in International Law, p. 115. Oxford, United Kingdom: Oxford University Press.

Wessendorf, N., Simma, B., Khan, D., Nolte, G., & Paulus, A. (Eds.). (2012). The Charter of the United Nations: A Commentary (Oxford Commentaries on International Law). In Oxford Commentaries on International Law (3rd ed., Vol. 1). Oxford, United Kingdom: OUP Oxford. https://doi.org/10.1093/law/9780199639762.001.0001

الدوريات

أحمد، مبخوتة. (2021). التطورات المتلاحقة على العرف الدولي باعتباره مصدرا للقانون الدولي. مجلة الحقوق والعلوم الإنسانية، 14(1)، 71–89. استرجع من https://www.asjp.cerist.dz/en/article/149162

الصائغ، محمد. (2009). أسانيد الولايات المتحدة بشأن الحرب الاستباقية. الرافدين للحقوق – جامعة الموصل كلية الحقوق، 11(40)، 229–282. استرجع من https://alaw.mosuljournals.com/pdf_160567_2a6b05cf1b8832033c63b55f687c42c3.html

إيهاب، خليفة. (2020). هجمات حرجة: الاستهداف السيبراني للأقمار الصناعية والمنشآت النووية اتجاهات الأحداث – مركز المستقبل للأبحاث والدراسات المتقدمة. استرجع من https://platform.almanhal.com/Details/Article/241951

حتوت، فوزي. (1439 هـ). التفويض الاداري في ضوء النصوص القانونية وأحكام القضاء الاداري "دراسة مقارنة". المجلة القضائية الصادرة عن وزارة العدل السعودية، (14)، 58–152. استرجع من https://adlm.moj.gov.sa/Alqadaeya/attach/955.pdf

رياحي، الطاهر. (2014). حظر استخدام القوة في العلاقات الدولية: بين شرعية النص ومشروعية الضرورة. التواصل في العلوم الإنسانية والاجتماعية، 38، 193–212. استرجع من https://www.asjp.cerist.dz/en/article/41790

سندل، مصطفى. (2017). مبدأ عدم التدخل في الشؤون الداخلية للدول بين النصوص والمتغيرات الدولية. مجلة القانون والعلوم السياسية، 3(1)، 211–232. استرجع من https://www.asjp.cerist.dz/en/article/78875

طاع، زهيرة. (2019). العقوبات الاقتصادية كأداة سياسية في العلاقات الدولية "العراق نموذجا ". مجلة المفكر للدراسات القانونية والسياسية، 2(2)، 148–164. استرجع من https://www.asjp.cerist.dz/en/article/123345

طالب، ياسين. (2018). الشركات العسكرية والأمنية الخاصة ودورها كفاعل مؤثر في العلاقات الدولية. Annales de l’université d’Alger، 32(4)، 38–59(ص44). استرجع من https://www.asjp.cerist.dz/en/downArticle/18/32/4/69946

طلال العيسى، وعدي عيسى. (2019). المسؤوليّة الدّوليّة النّاشئة عن الهجمات السّيبرانيّة في ضوء القانون الدّولي المعاصر. مجلة الزرقاء للبحوث والدراسات الإنسانية، 19(1). استرجع من https://zujournal.zu.edu.jo/index.php/2017-2/16-3-2024/864-2019-04-29-12-30-47

عبد الله، نايف. (2014). المبررات الموضوعية لعدم قبول الدعوى أمام محكمة العدل الدولية. مجلة جامعة تكريت للعلوم القانونية، (22)، 205–233. استرجع من https://www.iasj.net/iasj/download/5c31e6bbbbeb84a9

علام، وائل. (2012). تدرج قواعد القانون الدولي العام. مجلة الحقوق – جامعة البحرين، (1)، 9–59. استرجع من https://journal.uob.edu.bh/handle/123456789/3288

Aloupi, N. (2015). The Right to Non-intervention and Non-interference. Cambridge Journal of International and Comparative Law, 4(3), 566–587. https://doi.org/10.7574/cjicl.04.03.566

Aravindakshan, S. (2020). Cyberattacks: a look at evidentiary thresholds in International Law. Indian Journal of International Law, 59(1–4), 285-299. https://doi.org/10.1007/s40901-020-00113-0

Arimatsu, L., & Schmitt, M. N. (2021). The Plea of Necessity: An Oft Overlooked Response Option to Hostile Cyber Operations. International Law Studies, 97, 1171-1199. Retrieved from https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=2983&context=ils

Assumpção, C. (2020, May 11). The Problem of Cyber Attribution Between States. Retrieved from https://www.e-ir.info/2020/05/06/the-problem-of-cyber-attribution-between-states/

Badr, G. (1980). The Exculpatory Effect of Self-Defense in State Responsibility. Georgia Journal of Comparative and International Law, 10(1), 1–28. Retrieved from https://digitalcommons.law.uga.edu/gjicl/vol10/iss1/2/

Banks, W. C. (2017). Cyber Espionage and Electronic Surveillance: Beyond the Media Coverage. Emory Law Journal, 66(3), 513–525. Retrieved from https://scholarlycommons.law.emory.edu/elj/vol66/iss3/3/

Bethlehem, D. (2012). Self-Defense Against an Imminent or Actual Armed Attack By Nonstate Actors. American Journal of International Law, 106(4), 770–777 [para. 8, p. 6]. https://doi.org/10.5305/amerjintelaw.106.4.0769

Brunnée, J., & Toope, S. J. (2017). Self-defence against non-state actors: Are powerful states willing but unable to change international law? International and Comparative Law Quarterly, 67(2), 263–286. https://doi.org/10.1017/s0020589317000458

Buchan, R. (2012). Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions? Journal of Conflict and Security Law, 17(2), 212–227 [p. 217]. https://doi.org/10.1093/jcsl/krs014

Budnitsky, S., & Jia, L. (2018). Branding Internet sovereignty: Digital media and the Chinese–Russian cyberalliance. European Journal of Cultural Studies, 21(5), 594–613. https://doi.org/10.1177/1367549417751151

Burra, S. (2018). Use of Force as Self Defence against Non-State Actors and TWAIL Considerations: A Critical Analysis of India's State Practice. Asian Yearbook of International Law, 24, 106–127 [p. 107]. Retrieved from https://www.jstor.org/stable/10.1163/j.ctv1sr6j7f.9

Cassese, A. (2007). The Nicaragua and Tadic Tests Revisited in Light of the ICJ Judgment on Genocide in Bosnia. European Journal of International Law, 18(4), 649–668 [p. 652]. https://doi.org/10.1093/ejil/chm034

Christopher, B., & Tikk-Ringas, E. (in press). Hack or Attack? Shamoon and the Evolution of Cyber Conflict. James a. Baker III Institute for Public Policy of Rice University.

Corn, G. P., & Taylor, R. (2017). Sovereignty in the Age of Cyber. AJIL Unbound, 111, 207–212. https://doi.org/10.1017/aju.2017.57

Corten, O. (2021). Chapter 2. What Do 'Use of Force' and 'Threat of Force' Mean? In The Law Against War: The Prohibition on the Use of Force in Contemporary International Law (French Studies in International Law) (pp. 61–136). Oxford, United Kingdom: Hart Publishing. https://doi.org/10.5040/9781509949021.ch-002

Couzigou, I. (2016). The Right to Self-Defence against Non-State Actors: Criteria of the Unwilling or Unablee Test. Heidelberg Journal of International Law, 77, 53–55. Retrieved from https://www.zaoerv.de/77_2017/77_2017_1_a_53_55.pdf

Dinstein, Y. (2002). Computer Network Attacks and Self-Defense. International Law Studies, 76(1), 99–119 [p. 109]. Retrieved from https://digital-commons.usnwc.edu/ils/vol76/iss1/20/

Eaton, T. (2021). Self-Defense to Cyber Force: Combatting the Notion of 'Scale And Effect. American University International Law Journal, 36(4), 697–772. Retrieved from https://digitalcommons.wcl.american.edu/auilr/vol36/iss4/1/

Finnemore, M., & Hollis, D. B. (2016). Constructing Norms for Global Cybersecurity. American Journal of International Law, 110(3), 425–479. https://doi.org/10.1017/s0002930000016894

Foltz, A. C. (2012). Stuxnet, Schmitt Analysis, and the Cyber Use-of-Force Debate. Joint Force Quarterly (JFQ), 67, 40–48. Retrieved from https://apps.dtic.mil/sti/citations/ADA618715

Garg, U, et al. (2012). MAC and Logical addressing (A Review Study). Journal of Engineering Research and Applications (IJERA), 2(3), 474-480. Retrieved from https://www.ijera.com/papers/Vol2_issue3/CB23474480.pdf

Garrie, D. B. (2012). Cyber Warfare, What Are The Rules? Journal of Law and Cyber Warfare, 1(1), 1–7. Retrieved from https://www.jstor.org/stable/26441232

Goldsmith, J. (2013). How Cyber Changes the Laws of War. European Journal of International Law, 24(1), 129–138. https://doi.org/10.1093/ejil/cht004

Green, J. A., & Grimal, F. (2011). The Threat of Force as an Action in Self-Defense Under International Law. Vanderbilt Journal of Transnational Law, 44(2), 285–329. Retrieved from https://scholarship.law.vanderbilt.edu/vjtl/vol44/iss2/2

Greenwood, C. (2003). International Law and the Pre-emptive Use of Force: Afghanistan, Al-Qaida, and Iraq. San Diego International Law Journal, 4(7), 7–38. Retrieved from https://digital.sandiego.edu/ilj/vol4/iss1/3/

Haataja, S. (2017). The 2007 cyber attacks against Estonia and international law on the use of force: an informational approach. Law, Innovation and Technology, 9(2), 159–189 [p. 161]. https://doi.org/10.1080/17579961.2017.1377914

Haslam, E. (2000). Information Warfare: Technological Changes and International Law. Journal of Conflict and Security Law, 5(2), 157–175 [p. 163]. https://doi.org/10.1093/jcsl/5.2.157

Hathaway, O. et al. (2012). The Law of Cyber-Attack. California Law Review, 100(4), 817–886. Retrieved from https://www.californialawreview.org/print/2the-law-of-cyber-attack/

Helmersen, S. T. (2014). The Prohibition of the Use of Force as Jus Cogens: Explaining Apparent Derogations. Netherlands International Law Review, 61(02), 167–193. https://doi.org/10.1017/s0165070x14001168

Herzog, S. (2011). Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. Journal of Strategic Security, 4(2), 49–60. https://doi.org/10.5038/1944-0472.4.2.3

Jain, A. G. (2014). Rationalising International Law Rules on Self-Defence: The Pin-Prick Doctrine. Chicago-Kent Journal of International and Comparative Law, 14(2), 23–70 [p. 47-58]. Retrieved from https://scholarship.kentlaw.iit.edu/ckjicl/vol14/iss2/2

Jensen, E. T., & Watts, S. (2021). Cyber Due Diligence. Oklahoma Law Review, 73(4), 645–710. Retrieved from https://digitalcommons.law.ou.edu/cgi/viewcontent.cgi?article=2215&context=olr

Jiang, M. (2010). Authoritarian Informationalism: China's Approach to Internet Sovereignty. SAIS Review of International Affairs, 30(2), 71–89. https://doi.org/10.1353/sais.2010.0006

Johnson, D. E., & Schmitt, M. N. (2021). Responding to Proxy Cyber Operations Under International Law. The Cyber Defense Review, 6(4), 15–30. Retrieved from https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/2843482/responding-to-proxy-cyber-operations-under-international-law/

Jolley, J. D. (2017). Attribution, State Responsibility, and the Duty to Prevent Malicious Cyber-Attacks in International Law. SSRN Electronic Journal, p. 25. https://doi.org/10.2139/ssrn.3056832

Joyner, C. C. (2001). Information Warfare as International Coercion: Elements of a Legal Framework. European Journal of International Law, 12(5), 825–865. https://doi.org/10.1093/ejil/12.5.825

Joyner, C. C., & Lotrionte, C. (2001). Information Warfare as International Coercion: Elements of a Legal Framework. European Journal of International Law, 12(5), 825–865. https://doi.org/10.1093/ejil/12.5.825

Kesler, B. (2011). The Vulnerability of Nuclear Facilities to Cyber Attack. Strategic Insights, 10(1), 15–25. Retrieved from https://core.ac.uk/download/pdf/36718376.pdf

Kolton, M. (2017). Interpreting China's Pursuit of Cyber Sovereignty and its Views on Cyber Deterrence. The Cyber Defense Review, 2(1), 119–145. Retrieved from https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/1588940/interpreting-chinas-pursuit-of-cyber-sovereignty-and-its-views-on-cyber-deterre/

Kozlowski, A. (2014). Comparative analysis of cyberattacks on Estonia, Georgia and Kyrgyzstan. European Scientific Journal (ESJ), 3, 237–245. Retrieved from https://eujournal.org/index.php/esj/article/view/2941

Kretzmer, D. (2013). The Inherent Right to Self-Defence and Proportionality in Jus Ad Bellum. European Journal of International Law, 24(1), 235–282. https://doi.org/10.1093/ejil/chs087

Kuru, H. (2018). Evolution of War and Cyber Attacks in the Concept of Conventional Warfare. Journal of Learning and Teaching in Digital Age, 3(1), 12–20. Retrieved from https://www.learntechlib.org/p/209516/

Lachow, I. (2011). The Stuxnet Enigma: Implications for the Future of Cybersecurity. Georgetown Journal of International Affairs, 118–126. Retrieved from http://www.jstor.org/stable/43133820.

Lemnitzer, J. M. (2016). International Commissions of Inquiry and the North Sea Incident: A Model for a MH17 Tribunal? European Journal of International Law, 27(4), 923–944. https://doi.org/10.1093/ejil/chw056

Liivoja, R. (2008). The Scope of the Supremacy Clause of the United Nations Charter. International and Comparative Law Quarterly, 57(3), 583–612. https://doi.org/10.1017/s0020589308000389

Lin, H. (2014). Attribution of malicious cyber incidents: from soup to nuts. Journal of International Affairs, 70(1). Retrieved from https://jia.sipa.columbia.edu/attribution-malicious-cyber-incidents

Lotrionte, C. (2022). Bringing the Law In: Unlearned Lessons for Diplomats and Others. The Cyber Defense Review, 7(1), 23-31. Retrieved from https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/2882573/bringing-the-law-in-unlearned-lessons-for-diplomats-and-others/

Madubuike-Ekwe, J. N. (2021). Cyberattack and the Use of Force in International Law. Beijing Law Review, 12(02), 631–649. https://doi.org/10.4236/blr.2021.122034

Mikanagi, T., & MačÁk, K. (2020). Attribution of cyber operations: an international law perspective on the Park Jin Hyok case. Cambridge International Law Journal, 9(1), 51–75. https://doi.org/10.4337/cilj.2020.01.03

Milanovic, M. (2006). State Responsibility for Genocide. European Journal of International Law, 17(3), 553–604 [p. 577]. https://doi.org/10.1093/ejil/chl019

Moore, S. (2013). Cyber Attacks and the Beginnings of an International Cyber Treaty. North Carolina Journal of International Law, 39(1), 223-257. Retrieved from https://scholarship.law.unc.edu/ncilj/vol39/iss1/7

Moynihan, H. (2020). The vital role of international law in the framework for responsible state behaviour in cyberspace. Journal of Cyber Policy, 6(3), 394–410 [p. 403]. https://doi.org/10.1080/23738871.2020.1832550

Mueller, M., Grindal, K., Kuerbis, B., & Badiei, F. (2019). Cyber Attribution: Can a New Institution Achieve Transnational Credibility? The Cyber Defense Review, 4(1), 107–122. Retrieved from https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/1830029/cyber-attribution-can-a-new-institution-achieve-transnational-credibility/

Murphy, S. D. (2005). The Doctrine of Preemptive Self-Defense. Villanova Law Review, 50(3), 699–748. Retrieved from https://digitalcommons.law.villanova.edu/vlr/vol50/iss3/9/

Nguyen, R. (2013). Navigating "Jus Ad Bellum" in the Age of Cyber Warfare. California Law Review, 101(4), 1079–1129. Retrieved from https://www.californialawreview.org/print/4navigating-jus-ad-bellum-in-the-age-of-cyber-warfare/

O'Connell, M. E. (2012). Cyber Security without Cyber War. Journal of Conflict & Security Law, 17(2), 187–209. https://doi.org/10.1093/jcsl/krs017

Ochoa-Ruiz, N., & Salamanca-Aguado, E. (2005). Exploring the Limits of International Law relating to the Use of Force in Self-defence. European

Journal of International Law, 16(3), 499–524 [p. 523]. https://doi.org/10.1093/ejil/chi128

Olivier, M. (2012). Cyber Warfare: The Frontline of 21st Century Conflict. LBJ Journal of Public Affairs, 20, 23–42. Retrieved from https://repositories.lib.utexas.edu/handle/2152/17903

Payne, C., & Finlay, L. (2017). Addressing Obstacles to Cyber-Attribution: A Model Based on State Response to Cyber-Attack. The George Washington International Law Review, 4(3), 535–568 . Retrieved from https://gwilr.org/wordpress/wp-content/uploads/2017/05/ILR-Vol-49.3_Panye-Finlay.pdf

Pegna, O. L. (1998). Counter-claims and Obligations Erga Omnes before the International Court of Justice. European Journal of International Law, 9(4), 724–736. https://doi.org/10.1093/ejil/9.4.724

Posner, E. A., & Goldsmith, J. L. (1999). A Theory of Customary International Law. Chicago Unbound, 66, 1113–1177. Retrieved from https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=2767&context=journal_articles

Provost, R. (1992). Starvation as a Weapon: Legal Implications of the United Nations Food Blockade Against Iraq and Kuwait. Columbia Journal of Transnational Law, 30, 577–639. Retrieved from https://ssrn.com/abstract=1332012

Richardson, J. (2011). Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield. UIC John Marshall Journal of Information Technology

& Privacy Law, 29(1), 1–28. Retrieved from https://repository.law.uic.edu/jitpl/vol29/iss1/1/

Robertson, G., QC. (2010). Human Rights Fact-Finding: Some Legal and Ethical Dilemmas. UCL Human Rights Review, 3, 15-43. Retrieved from https://www.ucl.ac.uk/human-rights/sites/human-rights/files/robertson.pdf

Rogoff, M. A., & Collins, E. Jr. (1990). The Caroline Incident and the Development of International Law. Brooklyn Journal of International Law, 16, 493.

Romanosky, S., & Boudreaux, B. (2020). Private-Sector Attribution of Cyber Incidents: Benefits and Risks to the U.S. Government. International Journal of Intelligence and CounterIntelligence, 34(3), 463-493. https://doi.org/10.1080/08850607.2020.1783877

Roscini, M. (2007). Threats of Armed Force and Contemporary International Law. Netherlands International Law Review, 54(02), 229–277. https://doi.org/10.1017/s0165070x0700229x

Roscini, M. (2014). Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations. Texas International Law Journal, 50, 233–273. Retrieved from https://ssrn.com/abstract=2611753

Sadurska, R. (1988). Threats of Force. The American Journal of International Law, 82(2), 239–268. https://doi.org/10.2307/2203188

Samuel, K. L. H. (2018). The Legal Character of Due Diligence: Standards, Obligations, or Both? Central Asian Yearbook of International Law. https://doi.org/10.2139/ssrn.3264764

Schmitt, M. N. (1999). Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework. Columbia Journal of Transnational Law, 37, 887–937. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1603800

Schmitt, M. N. (2011). Cyber Operations and the Jus Ad Bellum Revisited. Villanova Law Review, 56, 569–606. Retrieved from https://digitalcommons.law.villanova.edu/vlr/vol56/iss3/10

Schmitt, M. N. (2013). "Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law. Virginia Journal of International Law, 54(3), 698-732 [p.702]. Retrieved from https://centaur.reading.ac.uk/89821/1/SSRN-id2353898.pdf

Schmitt, M. N. (2015). In Defense of Due Diligence in Cyberspace. The Yale Law Journal, 125 (Forum 68), 68–81. Retrieved from https://www.yalelawjournal.org/forum/in-defense-of-due-diligence-in-cyberspace

Schmitt, M. N. (2018). "Virtual" Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law. Chicago Journal of International Law, 19(1), 30–67. Retrieved from https://chicagounbound.uchicago.edu/cjil/vol19/iss1/2/

Schmitt, M. N. (2018a). Peacetime Cyber Responses and Wartime Cyber Operations Under International Law: An Analytical Vade Mecum. Harvard National Security Journal, 8, 239-280. Retrieved from https://harvardnsj.org/wp-content/uploads/sites/13/2017/02/Schmitt-NSJ-Vol-8.pdf

Schmitt, M. N., & Pitts, M. C. (2015). Cyber Countermeasures and Effects on Third Parties: the International Legal Regime. International Law from a Baltic Perspective, 14, 258–280. https://doi.org/10.1163/9789004433151_011

Schmitt, M. N., & Watts, S. (2021). Collective Cyber Countermeasures? National Security Journal by Harvard Law School, 12, 373–411. Retrieved from https://harvardnsj.org/2021/06/collective-cyber-countermeasures/

Shany, Y., & Schmitt, M. N. (2020). An International Attribution Mechanism for Hostile Cyber Operations. International Law Studies, 96(1), 196–222 [p. 213-214]. Retrieved from https://digital-commons.usnwc.edu/ils/vol96/iss1/8/

Sheraz, M. M., & Dayan, F. (2018). Cyber Warfare And Protection Of Civilian Under International Humanitarian Law. Ilkogretim Online - Elementary Education Online, 17(3), 1790–1803. Retrieved from https://www.ilkogretim-online.org/fulltext/218-1638043863.pdf

Singh, A. H. S. (2021, March 5). A Clear Standard of Proof in Disputes Before the ICJ: Are We There Yet? – Cambridge International Law Journal. Retrieved from http://cilj.co.uk/2021/03/05/a-clear-standard-of-proof-in-disputes-before-the-icj-are-we-there-yet/

Sofaer, A. D. (2003). On the Necessity of Pre- emption. European Journal of International Law, 14(2), 209–226. Retrieved from http://ejil.org/pdfs/14/2/411.pdf

Stergiopoulos, G., Gritzalis, D. A., & Limnaios, E. (2020). Cyber-Attacks on the Oil & Gas Sector: A Survey on Incident Assessment and Attack Patterns.

IEEE Access, 8, 128440–128475. https://doi.org/10.1109/access.2020.3007960

Subramaniam, T. K., & Deepa, B. (2015). A Review Towards DDoS Prevention and Detection Methodology. International Journal of Computational Science and Information Technology, 3(1/2/3), 1–9. https://doi.org/10.5121/ijcsity.2015.3301

Sulek, D., & Moran, N. (2009). What Analogies Can Tell Us About the Future of Cybersecurity. Cryptology and Information Security Series, Volume 3: The Virtual Battlefield: Perspectives on Cyber Warfare, 118–131. Retrieved from http://195.222.11.251/uploads/2018/10/08_SULEK_What-Cyber-Analogies-Can-Tell-Us.pdf

Sullivan, C. (2016). The 2014 Sony Hack and the Role of International Law. Journal of National Security Law and Policy, 8(3), 437–468. Retrieved from https://jnslp.com/wp-content/uploads/2017/10/The-2014-Sony-Hack-and-the-Role-of-International-Law_2.pdf

Sun, Y. (2022). The Future of Due Diligence in Cyberspace. New York University Journal of International Law and Politics, 54(2), 753–764. Retrieved from https://www.nyujilp.org/wp-content/uploads/2022/05/nyi_54-2-449-460_Sun.pdf

Tam, K. et al. (2022). Case Study of a Cyber-Physical Attack Affecting Port and Ship Operational Safety. Journal of Transportation Technologies, 12(01), 1–27. https://doi.org/10.4236/jtts.2022.121001

The Use of Nonviolent Coercion: A Study in Legality under Article 2(4) of the Charter of the United Nations. (1974). University of Pennsylvania Law

Review, 122(4), 983–1011. Retrieved from https://scholarship.law.upenn.edu/penn_law_review/vol122/iss4/13

Trapp, K. N. (2007). Back to Basics: Necessity, Proportionality, and the Right of Self-Defence Against Non-State Terrorist Actors. International and Comparative Law Quarterly, 56(1), 141–156. https://doi.org/10.1093/iclq/lei153

Tsagourias, N. (2012). Cyber attacks, self-defence and the problem of attribution. Journal of Conflict and Security Law, 17(2), 229–244. https://doi.org/10.1093/jcsl/krs019

U.S. Comments on ILC Draft Articles on State Responsibility. (2001). The American Journal of International Law, 95(3), 626–628. https://doi.org/10.2307/2668497

Ullman, R. H. (1978). Human Rights and Economic Power: The United States versus Idi Amin. Foreign Affairs, 56(3), 529-543. https://doi.org/10.2307/20039917

Wallace, D. A., McCarthy, A. H., & Visger , M. (2019). Peeling Back the Onion of Cyber Espionage after Tallinn 2.0. Maryland Law Review, 78(2), 205–246 [p. 205-209]. Retrieved from https://digitalcommons.law.umaryland.edu/mlr/vol78/iss2/2/

Waxman, M. C. (2011). Cyber Attacks as "Force" under UN Charter Article 2(4). International Law Studies, 87, 43–57. Retrieved from https://digital-commons.usnwc.edu/ils/vol87/iss1/5/

Waxman, M. C. (2011b). Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4). The Yale Journal of International Law, 36, 421–459 [pp. 426-430]. Retrieved from https://openyls.law.yale.edu/handle/20.500.13051/6629

Yadav, H., & Gour, S. (2017). Cyber Attacks: An impact on Economy to an organization. International Journal of Information & Computation Technology, 4(9), 937–940. Retrieved from https://www.ripublication.com/irph/ijict_spl/ijictv4n9spl_11.pdf

Yifeng, C. (2014). Chapter 13: The customary nature of the principle of non-intervention: a methodological note. In Renmin Chinese Law Review (Vol. 2, pp. 319–340). https://doi.org/10.4337/9781783473793.00018

Yusuf Imam, M. A., & Biswas, P. K. (2019). MAC ADDRESS CLONING TECHNIQUE RESULTS. International Journal of Engineering Applied Sciences and Technology, 4(1), 1–5. https://doi.org/10.33564/ijeast.2019.v04i01.001

المؤتمرات

جلسات المؤتمرات

Lotrionte, C., Corcoran, T., Lewis, J., & Rosenzweig, P. (2018, April). Bringing Order to Chaos: The Development of Nation-State Cyber-Norms. Presentation presented at the RSA Conference, San Francisco, California [Video file]. Retrieved from https://youtu.be/nMJLjy2Y1T4

The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) [natoccdcoe]. (2018, June 20). Due Diligence in Cyberspace - CyCon 2018, 14: 00 [Video file]. Retrieved from https://youtu.be/YOIuiNfaZU8?t=840

London School of Economics. (2010, December 9). Can International Law Change the World? 32:00 [Video file]. Retrieved from https://youtu.be/gH8yIqcG13c?t=1920

natoccdcoe. (2017, November 7). Tallinn Manual 2.0 & Gray Zones in International Law - CyCon 2017 [Video file]. Retrieved from https://youtu.be/w38HSUlnX6U

Stockburger, P. Z., & Schmitt, M. N. (2018, June). Due Diligence in Cyberspace - CyCon 2018. Panel discussion presented at the 10th International Conference on Cyber Conflict, Tallinn, Estonia. Retrieved from https://youtu.be/YOIuiNfaZU8

Security Council [United Nations - UN Web TV]. (2021, June 29). Cyber security - Security Council, VTC Open debate [Video file]. Retrieved from https://media.un.org/en/asset/k1e/k1egd92tkq

بحوث المؤتمرات

Applegate, S. D. (2013). The Dawn of Kinetic Cyber. In K. Podins, J. Stinissen, & M. Maybaum (Eds.). Presented at the 5th International Conference on Cyber Conflict, Tallinn, Estonia. Retrieved from https://ccdcoe.org/uploads/2018/10/10_d2r1s4_applegate.pdf

Cunche, M., & Matte, C. (2016, November). On Wi-Fi Tracking and the Pitfalls of MAC Address Randomization. Presented at the Journée Nationale

de l'Internet des Objets Nouveaux défis de l'Internet des Objets: Interaction Homme-Machine et Facteurs Humains, Cité de l'Innovation, Nokia Paris-Saclay. Retrieved from https://ido2016.sciencesconf.org/122873/Privacy_v4.pdf

Dixon, W., & Eagan, N. (2019, June). 3 ways AI will change the nature of cyber-attacks. Article presented at the Annual Meeting of the New Champions 2019, Dalian, People's Republic of China. Retrieved from https://www.weforum.org/agenda/2019/06/ai-is-powering-a-new-generation-of-cyberattack-its-also-our-best-defence/

Final Document - Disarmament and International Security. (2006, September), 1–68. Presented at the 14th Summit Conference of Heads of State or Government of the Non-Aligned Movement, Havana, Cuba. Retrieved from http://cns.miis.edu/nam/documents/Official_Document/14NAMSummit-Havana-Compiled.pdf

Giles, K. (2012). Russia's Public Stance on Cyberspace Issues. In C. Czosseck, R. Ottis, & K. Ziolkowski (Eds.), Chapter 2 Cyber Policy & Strategic Options, 63–76. Tallinn, Estonia. Retrieved from https://ccdcoe.org/uploads/2015/04/CyCon_2012_book_web_sisu.indd_.pdf

Iasiello, E. (2013). Cyber Attack: A Dull Tool to Shape Foreign Policy. In K. Podins, J. Stinissen, & M. Maybaum (Eds.) (p. 8). Presented at the 5th International Conference on Cyber Conflict, Tallinn, Estonia. Retrieved from https://ccdcoe.org/uploads/2018/10/24_d3r1s3_Iasiello.pdf

Lemay, A., Fernandeza, J. M., & Knight, S. (2010). Pinprick attacks, a lesser included case? In C. Czosseck & K. Podins (Eds.) (pp. 183–194). Presented at the Conference on Cyber Conflict, Tallinn, Estonia. Retrieved from https://ccdcoe.org/uploads/2018/10/Lemay-Pinprick-attacks-a-lesser-included-case.pdf

O'Connell, M. E., & Arimatsu, L. (2012, May). Cyber Security and International Law. Presented at the International Law: Meeting Summary, London, United Kingdom: Chatham House. Retrieved from https://www.chathamhouse.org/sites/default/files/public/Research/International%20Law/290512summary.pdf

Peng, Y. et al. (2015). Cyber-Physical Attack-Oriented Industrial Control Systems (ICS) Modeling, Analysis and Experiment Environment. 2015 International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 322–326. Adelaide, Australia: IEEE. https://doi.org/10.1109/iih-msp.2015.110

Roguski, P. ł. (2020). Collective Countermeasures in Cyberspace – Lex Lata, Progressive Development or a Bad Idea? Presented at the 2020 12th International Conference on Cyber Conflict. Retrieved from https://ccdcoe.org/uploads/2020/05/CyCon_2020_2_Roguski.pdf

Schmitt, M. N. (2012). "Attack" as a Term of Art in International Law: The Cyber Operations Context. In C. Czosseck, R. Ottis, & K. Ziolkowski (Eds.). Presented at the 4th International Conference on Cyber Conflict, Tallinn, Estonia. Retrieved from https://ccdcoe.org/uploads/2012/01/5_2_Schmitt_AttackAsATermOfArt.pdf

Svabensky, V., & Vykopal, J. (2018). Gathering Insights from Teenagers' Hacking Experience with Authentic Cybersecurity Tools. 2018 IEEE Frontiers in Education Conference (FIE), 1–4. https://doi.org/10.1109/fie.2018.8658840

Swiss Federal Department of Foreign Affairs (FDFA), & Eggenschwiler, J. (2018, November). Geneva Dialogue on Responsible Behaviour in Cyberspace: Private Sector. Presented at the Geneva Dialogue on Responsible Behaviour in Cyberspace, Geneva, Switzerland. Retrieved from https://genevadialogue.ch/wp-content/uploads/Geneva-Dialogue-Role-of-the-Private-Sector.pdf

التقارير

ديفيس الثاني، جون إس، وآخرون (2017). تهديدات مجهولة المصدر: نحو مسائلة قانونية في الفضاء الإلكتروني. سانتا مونيكا، كاليفورنيا: مؤسسة RAND. استرجع من https://www.rand.org/content/dam/rand/pubs/research_reports/RR2000/RR2081/RAND_RR2081z1.arabic.pdf

The Shanghai Cooperation Organization (SCO). (n.d.). Annex 1 to the Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of Information Security. Retrieved from https://ccdcoe.org/uploads/2018/10/SCO-090616-IISAgreement.pdf

Defence Education Enhancement Program (DEEP) eAcademy. (2020, May). MEDIA – (DIS)INFORMATION – SECURITY. North Atlantic Treaty Organization (NATO). Retrieved from

https://www.nato.int/nato_static_fl2014/assets/pdf/2020/5/pdf/2005-deepportal4-information-warfare.pdf

"Frequently Asked Questions on International Law Aspects of Countering Terrorism", United Nations Office on Drugs and Crime (UNODC), (Vienna, 2009). Retrieved from https://www.unodc.org/documents/terrorism/Publications/FAQ/English.pdf

Schreier, F. (2014, May). On Cyberwarfare: DCAF Horizon 2015 Working Paper No. 7. The Geneva Centre for the Democratic Control of Armed Forces (DCAF). Retrieved from https://www.dcaf.ch/sites/default/files/publications/documents/OnCyberwarfare-Schreier.pdf

North Atlantic Treaty Organization. (2019, February). NATO Cyber Defence. Retrieved from https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_02/20190208_1902-factsheet-cyber-defence-en.pdf

CrowdStrike. (2019). The Global Threat Report: Adversary Tradecraft and the Importance of Speed. Retrieved from https://www.africacybersecurityconference.com/document/CrowdStrike_GTR_2019.pdf

Austin, G., Tay, K. L., & Sharma, M. (2022, February). Great-Power Offensive Cyber Campaigns: Experiments in Strategy. International Institute for Strategic Studies (IISS). Retrieved from https://www.iiss.org/blogs/research-paper/2022/02/great-power-offensive-cyber-campaigns

Lee, R. M., Assante, M., & Conway, T. (2014, November). ICS CP/PE (Cyber-to-Physical or Process Effects) case study paper – Media report of the Baku-Tbilisi-Ceyhan (BTC) pipeline Cyber Attack. SANS Industrial Control Systems. Retrieved from https://www.yumpu.com/en/document/view/36490959/media-report-of-the-btc-pipeline-cyber-attack

Lee, R. M., Assante, M. J., & Conway, T. (2014b, December). ICS CP/PE (Cyber-to-Physical or Process Effects) case study paper – German Steel Mill Cyber Attack. SANS Industrial Control Systems. Retrieved from https://dokumen.tips/documents/ics-cppe-case-study-2-german-steelworks-facility.html

King, A., & Gallagher, M. (2020, March). CSC Report. Cyberspace Solarium Commission (CSC). Retrieved from https://cybersolarium.org/wp-content/uploads/2022/05/CSC-Final-Report.pdf

Harry, C. (2015, July). A Framework for Categorizing Disruptive Cyber Activity and Assessing Its Impact. University of Maryland, p. 4-5. Retrieved from https://spp.umd.edu/research-impact/publications/framework-categorizing-disruptive-cyber-activity-and-assessing-its

Swedish Security and Defense Industry Association (SOFF). (2018, March). State sponsored cyber attack. Retrieved from https://soff.se/wp-content/uploads/2018/03/Cybersecurity_statsunderst%C3%B6dda-akt%C3%B6rer.pdf

Ashmore, W. C. (2009, May). Impact of Alleged Russian Cyber Attacks (Monograph). School of Advanced Military Studies, United States Army

Command and General Staff College. Retrieved from https://apps.dtic.mil/sti/citations/ADA504991

Tikk, E., Kaska, K., & Vihul, L. (2010). International Cyber Incidents: Legal Considerations. Tallinn, Estonia: Cooperative Cyber Defence Centre of Excellence (CCD COE). Retrieved from https://ccdcoe.org/uploads/2018/10/legalconsiderations_0.pdf

Ottis, R. (2018, October). Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective. Cooperative Cyber Defence Centre of Excellence (CCD COE), p. 2. Retrieved from https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf

Independent International Fact-Finding Mission on the Conflict in Georgia (IIFFMCG). (2009, September). Report of the Independent International Fact-Finding Mission on the Conflict in Georgia (Volume II), p. 4. Retrieved from https://www.mpil.de/files/pdf4/IIFFMCG_Volume_II1.pdf

Gazula, M. B. (2017, May). Cyber Warfare Conflict Analysis and Case Studies. Cybersecurity Interdisciplinary Systems Laboratory (CISL), Massachusetts Institute of Technology (MIT), p. 38. Retrieved from https://web.mit.edu/smadnick/www/wp/2017-10.pdf

White, Sarah P. (2018, March). Understanding Cyberwarfare: Lessons from the Russia-Georgia War. Modern War Institute. Retrieved from https://mwi.usma.edu/wp-content/uploads/2018/03/Understanding-Cyberwarfare.pdf

Cyber Conflict Studies Association. (2012, June). The History of Stuxnet: Key Takeaways for Cyber Decision Makers. AFCEA International. Retrieved

from https://www.afcea.org/committees/cyber/documents/TheHistoryofStuxnet.pdf

Albright, D., Brannan, P., & Walrond, C. (2010, December). Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Institute for Science and International Security. Retrieved from https://isis-online.org/uploads/isis-reports/documents/stuxnet_FEP_22Dec2010.pdf

Harold, S. W., Libicki, M. C., & Cevallos, A. S. (2016). Getting to Yes with China in Cyberspace. RAND Corporation, p. 36. https://doi.org/10.7249/RR1335

Rollins, J. W., Lawrence, S. V., Rennack, D. E., & Theohary, C. A. (2015, October). U.S.-China Cyber Agreement. Library of Congress, Congressional Research Service. Retrieved from https://digital.library.unt.edu/ark:/67531/metadc795686/m1/1/high_res_d/IN10376_2015Oct16.pdf

Atlantic Council. (2019, May). Ukrainian Election Task Force Foreign Interference in Ukraine's Democracy - Ukrainian Election Task Force Report. Retrieved from https://www.atlanticcouncil.org/wp-content/uploads/2019/05/Foreign_Interference_in_Ukraines_Election.pdf

U.S. Office of the Director of National Intelligence (ODNI). (2017, January). Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution. Retrieved from https://www.dni.gov/files/documents/ICA_2017_01.pdf

Mueller, R. S. (2019a, March). Report On The Investigation Into Russian Interference In The 2016 Presidential Election (Volume I of II). U.S.

Department of Justice. Retrieved from https://www.justice.gov/archives/sco/file/1373816/download

Mueller, R. S. (2019b, March). Report On The Investigation Into Russian Interference In The 2016 Presidential Election (Volume II of II). U.S. Department of Justice. Retrieved from https://www.justice.gov/storage/report_volume2.pdf

Korzak, E. (2021). Russia's Cyber Policy Efforts in the United Nations. NATO Cooperative Cyber Defence Centre of Excellence, Tallinn Paper No. 11. Retrieved from https://ccdcoe.org/uploads/2021/06/Elaine_Korzak_Russia_UN.docx.pdf

Kurowska, X. (2019, December). What does Russia want in cyber diplomacy? A primer. Central European University. Retrieved from https://eucd.s3.eu-central-1.amazonaws.com/eucd/assets/a4jdTSQp/13-kurowska_rif-final.pdf

Mr. Richard Kadlčák Special Envoy for Cyberspace Director of Cybersecurity Department. (2020, February). Czech Republic at the 2nd substantive session of the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security of the First Committee of the General Assembly of the United Nations, p. 2. Retrieved from https://www.nukib.cz/download/publications_en/CZ%20Statement%20-%20OEWG%20-%20International%20Law%2011.02.2020.pdf

Maliha, N. (2020). Cyber Warfare: Challenges In The Application Of International Humanitarian Law To Virtual Conflict. University of Dhaka. Retrieved from https://www.researchgate.net/publication/343979992_Cyber_Warfare_Chall

enges_In_The_Application_Of_International_Humanitarian_Law_To_Virtual_Conflict

Czech Republic, The National Cyber and Information Security Agency (NÚKIB), Czech Republic Statement at the 2nd substantive session of the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security of the First Committee of the General Assembly of the United Nations (11 February 2020). Retrieved from https://www.nukib.cz/download/publications_en/CZ%20Statement%20-%20OEWG%20-%20International%20Law%2011.02.2020.pdf

Finland, Finish Ministry of Foreign Affairs, International law and cyberspace - Finland's national positions (19 October 2020). Retrieved from https://um.fi/documents/35732/0/Cyber+and+international+law%3B+Finland%27s+views.pdf/41404cbb-d300-a3b9-92e4-a7d675d5d585?t=1602758856859

Federal Republic of Germany, German Federal Foreign Office and the German Federal Ministry of Defence, On the Application of International Law in Cyberspace (March 2021). Retrieved from https://www.auswaertiges-amt.de/blob/2446304/2ae17233b62966a4b7f16d50ca3c6802/on-the-application-of-international-law-in-cyberspace-data.pdf

Moynihan, H. (2019, December). The Application of International Law to State Cyberattacks: Sovereignty and Non-intervention. Chatham House. Retrieved from https://www.chathamhouse.org/sites/default/files/publications/research/2019-11-29-Intl-Law-Cyberattacks.pdf

Dias, T., & Coco, A. (2022). Cyber due diligence in international law. Oxford Institute for Ethics, Law and Armed Conflict. Retrieved from https://www.elac.ox.ac.uk/wp-content/uploads/2022/03/finalreport-bsg-elac-cyberduediligenceininternationallawpdf.pdf

International Committee of the Red Cross. (2019, November). International humanitarian law and cyber operations during armed conflicts. Retrieved from https://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts

Melzer, N. (2011). Cyberwarfare and International Law. United Nations Institute for Disarmament Research. Retrieved from https://unidir.org/sites/default/files/publication/pdfs//cyberwarfare-and-international-law-382.pdf

Department of Defense Cyberspace, USA. (2011, November). A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934 (Policy Report). Retrieved from https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-059.pdf

Advisory Council on International Affairs (AIV) & Advisory Committee on Public International Law (CAVV). (2011, December). Cyber Warfare (No 77, AIV / No 22, CAVV). Retrieved from https://cyberwar.nl/d/20120426_cavv-advies-nr-22-digitale-oorlogsvoering-en.pdf

Ministry of Foreign Affairs and Trade. (2020, December). The Application of International Law to State Activity in Cyberspace. New Zealand. Retrieved from https://dpmc.govt.nz/sites/default/files/2020-12/The%20Application%20of%20International%20Law%20to%20State%20Activity%20in%20Cyberspace.pdf

Garcia, M. J., & Elsea, J. K. (2014, September). U.S. Military Action Against the Islamic State: Answers to Frequently Asked Legal Questions. Library of Congress - Congressional Research Service. Retrieved from https://digital.library.unt.edu/ark:/67531/metadc461904/

Meer, S. (2020, June). How states could respond to non-state cyber-attackers (Policy Report). Netherlands Institute of International Relations Clingendael. Retrieved from https://www.clingendael.org/sites/default/files/2020-06/Policy_Brief_Cyber_non-state_June_2020.pdf

Gori, B. (2022, February). From Kinetic to Cyber Attacks and Back: the Israeli Approach to Deterrence In Cyberspace and the Multi-Dimensional Threat of Hamas. University of Florence (Università degli Studi di Firenze). Retrieved from https://www.cssii.unifi.it/upload/sub/Pubblicazioni/2022_Gori_Beatrice.pdf

Alexander Klimburg (Ed.), New Conditions and Constellations in Cyber, The Hague Centre for Strategic Studies, The Hague 2021. Retrieved from https://cyberstability.org/wp-content/uploads/2021/12/Cyberstability-Paper-Series.pdf

Ruhl, C., Hollis, D., Hoffman, W., & Maurer, T. (2020). Cyberspace and geopolitics: Assessing global cybersecurity norm processes at a crossroads. Carnegie Endowment for International Peace. Retrieved June 14, 2022, from https://carnegieendowment.org/2020/02/26/cyberspace-and-geopolitics-assessing-global-cybersecurity-norm-processes-at-crossroads-pub-81110

Charney, S., et al. (2016). From Articulation to Implementation: Enabling progress on cybersecurity norms. Microsoft. Retrieved from https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVmc8

United Nations, General Assembly, Open-ended working group on developments in the field of information and telecommunications in the context of international security (Final OWEG report), A/AC.290/2021/CRP.2 (10 March 2021). Available from https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

Healey, J. (2012, February). Beyond Attribution: Seeking National Responsibility in Cyberspace. Atlantic Council. Retrieved from https://www.files.ethz.ch/isn/142271/022212_ACUS_NatlResponsibilityCyber.pdf

Manshu, X. (2022). Beyond Public Cyber Attribution: Reflections and Responses. In Managing U.S.-China Tensions Over Public Cyber Attribution (pp. 25–32). Retrieved from https://carnegieendowment.org/files/Perkovich_et_al_Cyber_Attribution_web.pdf

AO Kaspersky Lab. (2021). The power of threat attribution. Retrieved from https://media.kaspersky.com/en/business-security/enterprise/threat-attribution-engine-whitepaper.pdf

Carter, R. A., & Enoizi, J. (2021). Mapping a Path to Cyber Attribution Consensus. The Geneva Association. Retrieved from https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf_public/cyber-attribution_web_final.pdf

Mueller, P., & Yadegari, B. (2012). The Stuxnet Worm. University of Arizona. Retrieved from

https://www2.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/2012/topic9-final/report.pdf

Davis, J. (2022). Tallinn Paper: Developing Applicable Standards of Proof for Peacetime Cyber Attribution. The 13th Tallinn Paper. Retrieved from https://ccdcoe.org/uploads/2022/03/Jeremy-K.-Davis-Standards_of_Attribution.pdf

Office of the United States Trade Representative (USTR). (2018, March). Report on China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation. Retrieved from https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF

Derian-Toth, G., et al. (2021). Tallinn Paper: Opportunities for Public and Private Attribution of Cyber Operations. The 12th Tallinn Paper (Young Scholar Edition). Retrieved from https://ccdcoe.org/uploads/2021/08/Tallinn_Papers_Attribution_18082021.pdf

Healey, J., et al. Atlantic Council of the United States. Brent Scowcroft Center on International Security, Försvarshögskolan. Institutet för högre totalförsvarsutbildning, North Atlantic Treaty Organization. Science for Peace and Security Programme. (2014). Confidence-Building Measures in Cyberspace. Washington, United States of America: Atlantic Council. Retrieved from https://www.atlanticcouncil.org/wp-content/uploads/2014/11/Confidence-Building_Measures_in_Cyberspace.pdf

George Bush, Executive Order 12722—Blocking Iraqi Government Property and Prohibiting Transactions with Iraq Online by Gerhard Peters and John T.

Woolley, The American Presidency Project https://www.presidency.ucsb.edu/node/269016

German Federal Foreign Office, German Federal Ministry of Defence, & German Federal Ministry of the Interior, Building and Community. (2021, March). On the Application of International Law in Cyberspace. The Federal Government of Germany. Retrieved from https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf

المقالات الإخبارية

الأمم المتحدة (7 ديسمبر 2021) منتدى حوكمة الإنترنت يروج لمستقبل رقمي شامل للجميع. استرجع من https://news.un.org/ar/story/2021/12/1089192

شؤون الأمم المتحدة. (يناير 25، 2022). الأمين العام يأمل في أن تقوم جميع البلدان بإخماد نيران عالمية مستعرة. استرجع من https://news.un.org/ar/story/2022/01/1092282

صحيفة العرب (16 فبراير 2019). "الإنترنت ذات السيادة": موسكو تغلق حدودها الرقمية. استرجع من https://alarab.app/الإنترنت-ذات-السيادة-موسكو-تغلق-حدودها-الرقمية

Abad-Santos, A. (2022, May 12). China Is Winning the Cyber War Because They Hacked U.S. Plans for Real War. The Atlantic. Retrieved from https://www.theatlantic.com/international/archive/2013/05/china-hackers-pentagon/314849/

Ackerman, S., & Ross, A. (2016, January 29). Airstrike targeting British hacker working for Isis killed three civilians instead, US admits. The Guardian. Retrieved from https://www.theguardian.com/us-

news/2016/jan/29/sis-airstrike-syria-civilians-killed-us-military-junaid-hussain

Bamford, J. (2020, January 8). Edward Snowden: The Untold Story. Wired. Retrieved from https://www.wired.com/2014/08/edward-snowden/

Banka, N. (2021, June 30). Explained: The story of how North Korea hackers stole $81 million from Bangladesh Bank. The Indian Express. Retrieved from https://indianexpress.com/article/explained/bangladesh-bank-robbery-north-korea-lazarus-heist-7375441/

Berthiaume, L. (2021, December 20). Canada blames China for widespread attack on email servers. Retrieved September 6, 2022, from https://www.nationalobserver.com/2021/07/19/news/canada-blames-china-widespread-attack-email-servers

Bocev, P. (2008, April 28). Le patron de l'espionnage allemand est sur la sellette. LEFIGARO. Retrieved from https://www.lefigaro.fr/international/2008/04/29/01003-20080429ARTFIG00010-le-patron-de-l-espionnage-allemand-est-sur-la-sellette.php

Connor, R. (2022, January 26). Chinese hackers targeting companies, says Germany. DW. Retrieved from https://www.dw.com/en/chinese-apt-27-hackers-targeting-companies-says-germany/a-60564091

Culpan, T. (2015, April 13). Decade-Long Cyberspy Attack Hacked Southeast Asian Targets. Bloomberg. Retrieved from https://www.bloomberg.com/news/articles/2015-04-12/decade-long-cyber-spying-campaign-hacked-southeast-asia-targets

Davidson, H., & Ni, V. (2022, August 6). Taiwan says China making simulated attack on main island. Retrieved September 6, 2022, from https://www.theguardian.com/world/2022/aug/06/taiwan-says-china-making-simulated-attack-main-island-military-drills

Davis, J. (2007, August 21). Hackers Take Down the Most Wired Country in Europe. Wired. Retrieved from https://www.wired.com/2007/08/ff-estonia/

Declaration of General Staff of the Armed Forces of the Islamic Republic of Iran Regarding International Law Applicable to the Cyberspace. (2020, August 17). Young Journalists Club (YJC). Retrieved from https://www.yjc.news/en/news/47482/declaration-of-general-staff-of-the-armed-forces-of-the-islamic-republic-of-iran-regarding-international-law-applicable-to-the-cyberspace

Eddy, M., & Perlroth, N. (2020, September 19). Cyber Attack Suspected in German Woman's Death. NY Times. Retrieved from https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html

European Council. (2022, June 28). EU sanctions against Russia explained. Retrieved from https://www.consilium.europa.eu/en/policies/sanctions/restrictive-measures-against-russia-over-ukraine/sanctions-against-russia-explained/

Finkle, J. (2013, February 26). Researchers say Stuxnet was deployed against Iran in 2007. Reuters. Retrieved from https://www.reuters.com/article/us-cyberwar-stuxnet-idUSBRE91P0PP20130226

Greenemeier, L. (2011, June 11). Seeking Address: Why Cyber Attacks Are So Difficult to Trace Back to Hackers. Scientific American. Retrieved from https://www.scientificamerican.com/article/tracking-cyber-hackers/

How German Spies Eavesdropped on an Afghan Ministry. (2008, April 28). Spiegel International. Retrieved from https://www.spiegel.de/international/germany/bnd-scandal-how-german-spies-eavesdropped-on-an-afghan-ministry-a-550212.html

Hurst, D. (2021, July 20). Australia joins allies in accusing China of 'malicious cyber activities.' Retrieved September 6, 2022, from https://www.theguardian.com/world/2021/jul/19/australia-joins-allies-in-accusing-china-of-malicious-cyber-activities

Khalip, A. (2018, February 19). U.N. chief urges global rules for cyber warfare. Retrieved from https://www.reuters.com/article/us-un-guterres-cyber/u-n-chief-urges-global-rules-for-cyber-warfare-idUSKCN1G31Q4

Koetsier, J. (2022, July 8). Apple Offers $2M To Hackers Who Can Break Its New Lockdown Mode. Retrieved from https://www.forbes.com/sites/johnkoetsier/2022/07/07/apple-offers-2m-to-hackers-who-can-break-its-new-lockdown-mode/?sh=ad2ac1a3e591

Kremlin denies involvement in cyber attacks on Estonia. (2007, May 18). The Baltic Times. Retrieved from https://www.baltictimes.com/news/articles/17908/

Mehrotra, K., & Voreacos, D. (2021, February 18). U.S. Calls North Korean Hackers 'World's Leading Bank Robbers'. Bloomberg - Middle East Edition.

Retrieved from https://www.bloomberg.com/news/articles/2021-02-17/u-s-charges-3-north-koreans-linked-to-sony-hack-in-new-scheme

Menn, J. (2022, April 7). Leading security companies Mandiant and CrowdStrike vow to collaborate. The Washington Post. Retrieved from https://www.washingtonpost.com/technology/2022/04/07/mandiant-crowdstrike-cybersecurity-cooperation/

Miller, B. J. (2014, July 31). Israeli Iron Dome firms "infiltrated by Chinese hackers." BBC News. Retrieved from https://www.bbc.com/news/technology-28583283

Mugabe, F. (2021, January 9). How bar fight sparked the 1979 Uganda - Tanzania war. Monitor - Uganda Edition. Retrieved from https://www.monitor.co.ug/uganda/magazines/people-power/how-bar-fight-sparked-the-1979-uganda-tanzania-war-1634552

Murphy, M. (2017, November 13). Boeing 757 controls HACKED remotely while on the runway, officials reveal. The Sun. Retrieved from https://www.thesun.co.uk/tech/4901413/boeing-757-controls-hacked-remotely-while-on-the-runway-officials-reveal/

NATO Cooperative Cyber Defence Center (CCDCOE). (2021). CCDCOE to Host the Tallinn Manual 3.0 Process. Retrieved from https://ccdcoe.org/news/2020/ccdcoe-to-host-the-tallinn-manual-3-0-process/

NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). (n.d.). European Union Equipping Itself against Cyber Attacks with the Help of Cyber Diplomacy Toolbox. Retrieved from https://ccdcoe.org/incyder-

articles/european-union-equipping-itself-against-cyber-attacks-with-the-help-of-cyber-diplomacy-toolbox/

Nichols, M. (2019, August 6). North Korea took $2 billion in cyberattacks to fund weapons program: U.N. report. Retrieved from https://www.reuters.com/article/us-northkorea-cyber-un/north-korea-took-2-billion-in-cyberattacks-to-fund-weapons-program-u-n-report-idUSKCN1UV1ZX

nournews. (2020, August 18). General Staff of Iranian Armed Forces Warns of Tough Reaction to Any Cyber Threat.

Pagliery, J. (2014, October 31). It looks like Russia and smells like Russia . . . but is it Russia? CNN. Retrieved from https://money.cnn.com/2014/10/31/technology/security/russia-hackers/index.html

Reuters. (2021, July 21). French cybersecurity agency warns of China-linked APT31 attacks on French organizations. Retrieved September 6, 2022, from https://www.reuters.com/technology/french-cybersecurity-agency-warns-china-linked-apt31-attacks-french-2021-07-21/

Rising, D. (2022, April 7). Chinese hackers reportedly target India's power grid. Retrieved September 6, 2022, from https://abcnews.go.com/Technology/wireStory/chinese-hackers-reportedly-target-indias-power-grid-83928423

Sanger, D. E., & Shane, S. (2016, December 10). Russian Hackers Acted to Aid Trump in Election, U.S. Says. NY Times. Retrieved from https://www.nytimes.com/2016/12/09/us/obama-russia-election-hack.html

Stokel-Walker, C. (2021, September 28). Planes can be remotely controlled by hackers. Retrieved from https://cybernews.com/security/planes-can-be-remotely-controlled-by-hackers/

Swinhoe, D. (2020, May 1). How much does it cost to launch a cyberattack? Retrieved from https://www.csoonline.com/article/3340049/how-much-does-it-cost-to-launch-a-cyberattack.html

UK condemns Chinese cyber attacks against governments and businesses. (2020, September 16). National Cyber Security Centre (NCSC). Retrieved from https://www.ncsc.gov.uk/news/uk-condemns-chinese-cyber-attacks-against-businesses-governments

United Nations, UN News, Developing countries most vulnerable to cyberattacks, 9 December 2011. Retrieved from https://news.un.org/en/story/2011/12/397922-developing-countries-most-vulnerable-cyberattacks-un

Whitney, L. (2020, March 2). Most common cyberattacks we'll see in 2020, and how to defend against them. ZDNet. Retrieved from https://www.zdnet.com/article/most-common-cyberattacks-well-see-in-2020-and-how-to-defend-against-them/

Winder, D. (2020, May 6). Microsoft Offers $100,000 If You Can Hack This Linux Operating System. Retrieved from https://www.forbes.com/sites/daveywinder/2020/05/06/microsoft-offers-100000-if-you-can-hack-this-linux-operating-system/?sh=4bc19fa819e4

Windrem, R. (2016, December 18). Timeline: Ten Years of Russian Cyber Attacks on Other Nations. NBC News. Retrieved from

https://www.nbcnews.com/storyline/hacking-in-america/timeline-ten-years-russian-cyber-attacks-other-nations-n697111

Winn, P. (2018, June 21). How North Korean hackers became the world's greatest bank robbers. Retrieved from https://gpinvestigations.pri.org/how-north-korean-hackers-became-the-worlds-greatest-bank-robbers-492a323732a6

Xinhua News Agency. (2022, January 17). Full Text: Special Address by Chinese President Xi Jinping at the World Economic Forum Virtual Event of the Davos Agenda [Press release]. Retrieved from http://www.xinhuanet.com/english/2021-01/25/c_139696610.htm

Yui, M., & Kawamoto, S. (2014, December 18). Chinese Criminals Blamed for Record Japan Bank Cybertheft. Bloomberg. Retrieved from https://www.bloomberg.com/news/articles/2014-12-17/chinese-criminals-blamed-for-record-japan-bank-cybertheft

Zetter, K. (2014, November 3). An Unprecedented Look at Stuxnet, the World's First Digital Weapon. Wired. Retrieved from https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

مواقع الانترنت

الأمم المتحدة، مكتب المفوض السامي لحقوق الإنسان (د. ت). ما هي حقوق الإنسان؟ استرجع من https://www.ohchr.org/ar/what-are-human-rights

الأمم المتحدة، مكتب مكافحة الإرهاب (د. ت) أمن الفضاء الإلكتروني. استرجع من https://www.un.org/counterterrorism/ar/cct/programme-projects/cybersecurity

المحكمة الدائمة للتحكيم (د. ت.) مقدمة عن المحكمة الدائمة للتحكيم. استرجع من https://pca-cpa.org/ar/about/introduction/

منظمة حظر الأسلحة الكيميائية (د. ت) هيئة التفتيش. استرجع من https://www.opcw.org/ar/mn-nhn/alamant-alfnyt/alaqsam/hyyt-altftysh

About the Cybersecurity Tech Accord. (2019, October 11). Retrieved from https://cybertechaccord.org/about/

About. Cyberstability (2022, February 28). Retrieved from https://cyberstability.org/about/

Agence nationale de la sécurité des systèmes d'information (ANSSI). (n.d.). The National Cybersecurity Agency of France. Retrieved from https://www.ssi.gouv.fr/en/cybersecurity-in-france/the-national-cybersecurity-agency-of-france/

Akande, D., Coco, A., & Dias, T. (2021, January 5). Old Habits Die Hard: Applying Existing International Law in Cyberspace and Beyond. Retrieved from https://www.ejiltalk.org/old-habits-die-hard-applying-existing-international-law-in-cyberspace-and-beyond/

Anderlini, J. (2010, January 15). The Chinese dissident's 'unknown visitors.' Retrieved from https://www.ft.com/content/c590cdd0-016a-11df-8c54-00144feabdc0

Anderson, N. (2012, June 1). Confirmed: US and Israel created Stuxnet, lost control of it. Retrieved from https://arstechnica.com/tech-policy/2012/06/confirmed-us-israel-created-stuxnet-lost-control-of-it/

Atlantic Council. (2022, May 10). About the Atlantic Council. Retrieved from https://www.atlanticcouncil.org/about/

Batt, S. (2020, March 10). Is Your Antivirus Tracking You? Here's What You Need to Know. MUO. Retrieved from https://www.makeuseof.com/tag/antivirus-tracking-youd-surprised-sends/

Cameron, L. (2022, May 24). IoT Meets the Military. Retrieved from https://www.computer.org/publications/tech-news/research/internet-of-military-battlefield-things-iomt-iobt

CCDCOE - The NATO Cooperative Cyber Defence Centre of Excellence is a multinational and interdisciplinary hub of cyber defence expertise. (n.d.). Retrieved from https://ccdcoe.org/

Charney, S., et al. (2016). From Articulation to Implementation: Enabling progress on cybersecurity norms. Microsoft. Retrieved from https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVmc8

Charter of Trust. (2020, November 2). About. Retrieved from https://www.charteroftrust.com/about/

Cimpanu, C. (2019, January 21). Law enforcement shut down DDoS booters ahead of annual Christmas DDoS attacks. Retrieved from https://www.zdnet.com/article/law-enforcement-shut-down-ddos-booters-ahead-of-annual-christmas-ddos-attacks/

Council on Foreign Relations. (2005, August). Connect the Dots on State-Sponsored Cyber Incidents - Titan Rain. Retrieved from https://www.cfr.org/cyber-operations/titan-rain

Cybersecurity Tutorial For Beginners: IP Addressing. (2021, October 15). Retrieved from https://cybercoastal.com/cybersecurity-tutorial-for-beginners-ip-addressing/

Eichensehr, K. (2020, July 24). Cyberattack Attribution and International Law. Retrieved from https://www.justsecurity.org/71640/cyberattack-attribution-and-international-law/

Estonian Defence League. (n.d.). Estonian Defence League's Cyber Unit. Retrieved from https://www.kaitseliit.ee/en/cyber-unit

Everything You Need To Know About Operation Aurora. (2016, August 8). Retrieved from https://cyware.com/news/everything-you-need-to-know-about-operation-aurora-5c5f5b99

Fischerkeller, M. P. (2021, August 31). Current International Law Is Not an Adequate Regime for Cyberspace. Retrieved from https://www.lawfareblog.com/current-international-law-not-adequate-regime-cyberspace

Forcepoint. (2021, May 5). What is the CIA Triad? Retrieved from https://www.forcepoint.com/cyber-edu/cia-triad

Getchell, M. (n.d.). The League of Nations (article). Retrieved from https://www.khanacademy.org/humanities/us-history/rise-to-world-power/us-in-wwi/a/the-league-of-nations

Gotsiridze, A. (2019, August 9). The Cyber Dimension of the 2008 Russia-Georgia War. Rondeli Foundation, Georgian Foundation for Strategic and International Studies. Retrieved from https://gfsis.org.ge/blog/view/970

Greenberg, A. (2019, August 23). What Is Cyberwar? The Complete WIRED Guide. Retrieved from https://www.wired.com/story/cyberwar-guide/

Hanna, A. (2021, December 16). The Invisible U.S.-Iran Cyber War. Retrieved from https://iranprimer.usip.org/blog/2019/oct/25/invisible-us-iran-cyber-war

Hollis, D. B. (2011, January 25). Could Deploying Stuxnet be a War Crime? Retrieved from http://opiniojuris.org/2011/01/25/could-deploying-stuxnet-be-a-war-crime/

IAB. (2021, January 26). The Mobile Identity Guide for Marketers. Retrieved from https://www.iab.com/insights/themobileidguide/

International Institute for Management Development (IMD). (n.d.). World Competitiveness Rankings - IMD. Retrieved from https://wwwcontent.imd.org/centers/world-competitiveness-center/rankings/world-competitiveness/

K. (2022, April 6). Catch a Hacker: How to Trace an IP Address. Retrieved from https://www.colocationamerica.com/blog/catch-a-hacker-how-to-trace-an-ip-address

Keizer, G. (2009, January 28). Russian "cybermilitia" knocks Kyrgyzstan offline. Retrieved from https://www.computerworld.com/article/2530572/russian--cybermilitia--knocks-kyrgyzstan-offline.html

Kohout, J. (2017, February 7). TeskaLabs Blog · How DDoS Attacks Can Sink Your Business. Retrieved from https://teskalabs.com/blog/how-ddos-can-sink-your-business

Kucera, J. (2014, December 11). U.S. Intelligence: Russia Sabotaged BTC Pipeline Ahead Of 2008 Georgia War. Retrieved from https://eurasianet.org/us-intelligence-russia-sabotaged-btc-pipeline-ahead-of-2008-georgia-war

Lauterbach, A. (2017, April 10). Cyber-security: Full Prevention is not possible. Retrieved from https://www.internationalairportreview.com/article/75245/cyber-security/

Lowry, A. (2018, March 7). "There are only two types of companies: those that have been hacked, and those that will be." Retrieved from https://wecyberup.org/there-are-only-two-types-of-companies-those-that-have-been-hacked-and-those-that-will-be/

Main Page. (2022, July 5). International cyber law: interactive toolkit. Retrieved from https://cyberlaw.ccdcoe.org/wiki/Main_Page

McWhorter, D. (n.d.). APT1: Exposing One of China's Cyber Espionage Units. Mandiant. Retrieved from https://www.mandiant.com/resources/apt1-exposing-one-of-chinas-cyber-espionage-units

Médecins Sans Frontières. (n.d.). القاموس العملي للقانون الإنساني. Retrieved from https://ar.guide-humanitarian-law.org/content/article/5/hrb/

Melnick, J. (2018, May 15). Top 10 Most Common Types of Cyber Attacks. Retrieved from https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/

Milanovic, M. (2022, February 26). What is Russia's Legal Justification for Using Force against Ukraine? Retrieved from https://www.ejiltalk.org/what-is-russias-legal-justification-for-using-force-against-ukraine/

National Air and Space Museum. (2017, April 6). The Technology of World War I. Retrieved from https://airandspace.si.edu/stories/editorial/240-artist-soldiers-technology

NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). (n.d.-b). Cyber security strategies. Retrieved from https://ccdcoe.org/library/strategy-and-governance/

NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). (n.d.-a). About us. Retrieved from https://ccdcoe.org/about-us/

NH (2021b, September 2). Hat-tribution to PLA Unit 61486. Retrieved from https://www.crowdstrike.com/blog/hat-tribution-pla-unit-61486/

North Atlantic Treaty Organization (NATO). (2022, June 11). Collective defence - Article 5. Retrieved from https://www.nato.int/cps/en/natohq/topics_110496.htm

North Atlantic Treaty Organization (NATO). (2022, July 14). Relations with Georgia. Retrieved from https://www.nato.int/cps/en/natohq/topics_38988.htm

Page, M. (2022, March 7). The hypocrisy of Russia's push for a new global cybercrime treaty. Retrieved from https://www.lowyinstitute.org/the-interpreter/hypocrisy-russia-s-push-new-global-cybercrime-treaty

Paltiel, D. (2022, June 02). G20 Communiqué Agrees on Language to Not Conduct Cyber Economic Espionage. Retrieved from https://www.csis.org/blogs/strategic-technologies-blog/g20-communiqu%C3%A9-agrees-language-not-conduct-cyber-economic

Paris Call for Trust and Security in Cyberspace. (n.d.). Retrieved from https://pariscall.international/en/call

Parker, S. (2017, October 3). Understanding The Physical Damage Of Cyber Attacks. Retrieved from https://www.infosecurity-magazine.com/opinions/physical-damage-cyber-attacks/

Pot, J. (2015, March 11). Can A Cyberattack Cause Physical Damage To Your Hardware? Retrieved from https://www.makeuseof.com/tag/can-cyberattack-cause-physical-damage-hardware/

Prohibition of intervention. (2022). In International Cyber Law in Practice: Interactive Toolkit. Retrieved from https://cyberlaw.ccdcoe.org/wiki/Prohibition_of_intervention#cite_ref-5

Schondorf, R. (2020, December 9). Israel's perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations. Retrieved from https://www.ejiltalk.org/israels-perspective-on-key-legal-and-practical-issues-concerning-the-application-of-international-law-to-cyber-operations/

Segal, A. (2016, October 15). The US-China Cyber Agreement: New Beginning or Tactical Pause? Retrieved from https://www.orfonline.org/expert-speak/the-us-china-cyber-agreement-new-beginning-or-tactical-pause/

Sendut, J. H. (2022, August 22). The Unwilling and Unable Doctrine and Syria. Retrieved from https://www.culs.org.uk/per-incuriam/the-unwilling-and-unable-doctrine-and-syria

Singh, V. (n.d.). The Existence of Right To Self-Defense Against The Non-State Actors. Retrieved from https://www.legalserviceindia.com/legal/article-2992-the-existence-of-right-to-self-defense-against-the-non-state-actors.html

Strachan, D. (2014, February 14). 9 Cities With The Best Free Wifi. Retrieved from https://www.businessinsider.com/9-cities-with-the-best-free-wifi-2014-2?international=true&r=US&IR=T

Straub, J. (2019). A cyberattack could wreak destruction comparable to a nuclear weapon. The Conversation. Retrieved from https://theconversation.com/a-cyberattack-could-wreak-destruction-comparable-to-a-nuclear-weapon-112173

Tannery, C. (2019, April 17). Cyber Attribution: Essential Component of Incident Response or Optional Extra. Retrieved from https://www.exabeam.com/incident-response/cyber-attribution-essential-component-of-incident-response-or-optional-extra/ (بتصرف)

The Law Society. (2019, August 28). How to identify a cyber attack. Retrieved from https://www.lawsociety.org.uk/topics/cybersecurity/how-to-identify-a-cyber-attack

The Shanghai Cooperation Organization (SCO). (n.d.). About SCO. Retrieved from http://eng.sectsco.org/about_sco/

Tietsort, J.R. (2022, June 5). 17 Types of Cyber Attacks & Examples (UPDATED FOR 2022). Aura. Retrieved from https://www.aura.com/learn/types-of-cyber-attacks

U.S. Cyber Command. (n.d.). Home USCYBERCOM. Retrieved from https://www.cybercom.mil/

Williams, P. (2020, October 29). Admitting evidence of fact-finding missions: To be continued? Retrieved from https://www.publicinternationallawandpolicygroup.org/lawyering-justice-blog/2020/1/21/admitting-evidence-of-fact-finding-missions-to-be-continued

Williamson, D. (2021, June 1). Cyberattacks are getting faster as prevention stays slow. Retrieved from https://www.americanbanker.com/payments/opinion/cyberattacks-are-getting-faster-as-prevention-stays-slow

Winkler, I. (2005, October 20). Guard against Titan Rain hackers. Retrieved from https://www.computerworld.com/article/2559195/guard-against-titan-rain-hackers.html

Yasar, K., & Cobb, M. (2022, April 28). man-in-the-middle attack (MitM). Retrieved from https://www.techtarget.com/iotagenda/definition/man-in-the-middle-attack-MitM

الاتفاقيات والمعاهدات الدولية

اللجنة الدولية للصليب الأحمر (جنيف)، اتفاقية جنيف الرابعة بشأن حماية الأشخاص المدنيين في وقت الحرب (12 أغسطس 1949) 287 UNTS 75. استرجع من https://www.icrc.org/ar/doc/resources/documents/misc/5nsla8.htm

اللجنة الدولية للصليب الأحمر (جنيف)، الملحق (البروتوكول) الأول الإضافي إلى اتفاقيات جنيف المعقودة في 12 أغسطس 1949 والمتعلق بحماية ضحايا المنازعات الدولية المسلحة (8 يونيو 1977) 3 UNTS 1125. استرجع من https://www.icrc.org/ar/resources/documents/treaty/protocol-i-additional-to-the-geneva-conventions

مجلس أوروبا (بودابست)، الاتفاقية المتعلقة بالجريمة الإلكترونية، رقم 185 (23 سبتمبر 2001). استرجع من https://rm.coe.int/budapest-convention-in-arabic/1680739173

المؤتمر الدولي (لاهاي)، اتفاقية لاهاي الرابعة الخاصة باحترام قوانين وأعراف الحرب البرية ومرفقها اللائحة المتعلقة بقوانين وأعراف الحرب البرية (18 أكتوبر 1907). استرجع من https://www.icrc.org/ar/doc/resources/documents/misc/62tc8a.ht

Council of Europe (Budapest), Convention on Cybercrime, 23 November 2001, ETS No. 185. Available at: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185

Council of Europe (Budapest), Convention on Cybercrime, Chart of signatures and ratifications of Treaty 185. Available at:

https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185

Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5, available at: https://www.refworld.org/docid/3ae6b3b04.html [accessed 17 September 2022]

North Atlantic Treaty Organization (Washington), North Atlantic Treaty, 9 April 1949, available at: https://www.nato.int/cps/en/natohq/official_texts_17120.htm

Organization of American States (OAS), American Convention on Human Rights, "Pact of San Jose", Costa Rica, 22 November 1969, available at: https://www.refworld.org/docid/3ae6b36510.html [accessed 17 September 2022]

Permanent Court of Arbitration (The Hague), Convention (I) For The Pacific Settlement Of International Disputes, 18 October 1907, available at: https://docs.pca-cpa.org/2016/01/1899-Convention-for-the-Pacific-Settlement-of-International-Disputes.pdf

UN General Assembly, Convention on the Prevention and Punishment of the Crime of Genocide, 9 December 1948, United Nations, Treaty Series, vol. 78, p. 277, available at: https://www.refworld.org/docid/3ae6b3ac0.html [accessed 17 September 2022]

UN General Assembly, International Covenant on Civil and Political Rights, 16 December 1966, United Nations, Treaty Series, vol. 999, p. 171, available

at: https://www.refworld.org/docid/3ae6b3aa0.html [accessed 17 September 2022]

United Nations, Vienna Convention on the Law of Treaties, 23 May 1969, United Nations, Treaty Series, vol. 1155, p. 331, available at: https://www.refworld.org/docid/3ae6b3a10.html [accessed 17 September 2022]

القضايا

Air Services arbitral award: Case Concerning the Air Services Agreement of 27 March 1946 (United states v. France), Decision of 9 December 1978, volume XVIII pp. 417-493

Armed Activities judgement: Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda), Judgment, I.C.J. Reports 2005, p. 168

Barcelona Traction judgement: Barcelona Traction, Light and Power Company, Limited,

Certain Activities and Construction of a Road judgement: Certain Activities Carried Out by Nicaragua in the Border Area (Costa Rica v. Nicaragua) and Construction of a Road in Costa Rica along the San Juan River (Nicaragua v. Costa Rica), Judgment, I.C.J. Reports 2015, p. 665

Corfu Channel judgement: Corfu Channel case, Judgment of April 9th, 1949: I.C.J. Reports 1949, p. 4

East Timor judgement: East Timor (Portugal v. Australia), Judgment, I.C.J. Reports 1995, p. 102, para. 29

Gabčíkovo-Nagymaros judgement: Gabčíkovo-Nagymaros Project (Hungary/Slovakia), Judgment, I.C.J. Reports 1997, p. 7

Genocide judgement: Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), Judgment, I.C.J. Reports 2007, p. 43

Judgment, I.C.J. Reports 1970, p. 3.

Nicaragua judgement: Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America). Merits, Judgment. I.C.J. Reports 1986, p. 14

Nuclear Weapons advisory opinion: Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, I.C.J. Reports 1996, p. 226

Obligation to Prosecute or Extradite judgement: Questions relating to the Obligation to Prosecute or Extradite (Belgium v. Senegal), Judgment, I.C.J. Reports 2012, p. 422

Rainbow Warrior arbitral award: Rainbow Warrior (NZ v. Fr.), 20 RIAA 217 (Arb.Trib. 1990)

Trail Smelter arbitral award: Trail Smelter Case (United States v. Canada) (1938 and 1941) 3 R.I.A.A. 1905

Wall advisory opinion: Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, I.C.J. Reports 2004, p. 136

القرارات والتقارير الصادرة عن الأمم المتحدة

الجمعية العامة للأمم المتحدة

الأمم المتحدة، الجمعية العامة ومجلس الأمن، رسالة موجهة إلى رئيسة مجلس الأمن من الممثل الدائم للمكسيك لدى الأمم المتحدة، A/75/766-S/2021/161 (16 مارس 2021). استرجع من https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/066/44/PDF/N2106644.pdf?OpenElement

الأمم المتحدة، الجمعية العامة، تقرير فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي: مذكرة من الأمين العام، A/68/98 (24 يونيو 2013). استرجع من https://undocs.org/A/68/98

الأمم المتحدة، الجمعية العامة، رسالة موجهة إلى الأمين العام من الممثلين الدائمين للاتحاد الروسي وأوزباكستان والصين وطاجيكستان وقيرغيزستان وكازاخستان لدى الأمم المتحدة، A/69/273 (9 يناير 2015). استرجع من https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/014/00/PDF/N1501400.pdf?OpenElement

الأمم المتحدة، الجمعية العامة، فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي: مذكرة من الأمين العام، A/70/174 (22 يوليو 2015). استرجع من https://undocs.org/A/70/174

الأمم المتحدة، لجنة القانون الدولي، تقرير لجنة القانون الدولي إلى الجمعية العامة للأمم المتحدة عن أعمال دورتها الثالثة والخمسين، المجلد الثاني الجزء الثاني (A/CN.4/SER.A/2001/Add.1 (Part 2)). https://legal.un.org/ilc/publications/yearbooks/arabic/ilc_2001_v2_p2.pdf

الأمم المتحدة، لجنة القانون الدولي، تقرير لجنة القانون الدولي إلى الجمعية العامة للأمم المتحدة عن أعمال دورتها الثالثة والخمسين، المجلد الثاني الجزء الثاني (A/CN.4/SER.A/2001/Add.1

((Part 2)
https://legal.un.org/ilc/publications/yearbooks/arabic/ilc_2001_v2_p2.pdf

الأمم المتحدة، لجنة القانون الدولي، تقرير لجنة القانون الدولي إلى الجمعية العامة عن أعمال دورتها الثامنة والخمسين، المجلد الثاني الجزء الثاني ((Part 2) A/CN.4/SER.A/2006/Add.1)
https://legal.un.org/ilc/publications/yearbooks/arabic/ilc_2006_v2_p2.pdf

الأمم المتحدة، مفوضية حقوق الإنسان، لجان التحقيق وبعثات تقصي الحقائق المعنية بالقانون الدولي لحقوق الإنسان والقانون الدولي الإنساني – توجيهات وممارسات،HR/PUB/14/7. استرجع من
https://www.ohchr.org/sites/default/files/Documents/Publications/CoI_Guidance_and_Practice_AR.pdf

قرار الجمعية العامة 52/119، احترام مبدأي السيادة الوطنية وعدم التدخل في الشؤون الداخلية للدول في عملياتها الانتخابية،A/RES/52/119 (12 ديسمبر 1997). استرجع من
https://www.un.org/ar/ga/52/res/res52119.htm

قرار الجمعية العامة 25/2525، اعلان مبادئ القانون الدولي المتعلقة بالعلاقات الودية والتعاون بين الدول وفقا لميثاق الأمم المتحدة، A/RES/2625(XXV) (24 أكتوبر 1970). استرجع من
https://www.undocs.org/A/RES/2625(XXV)

قرار الجمعية العامة 199/58، إرساء ثقافة عالمية لأمن الفضاء الحاسوبي وحماية الهياكل الأساسية الحيوية للمعلومات، A/RES/58/199 (23 ديسمبر 2003). استرجع من
https://undocs.org/A/RES/58/199

قرار الجمعية العامة 243/68، التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، A/RES/68/243 (9 يناير 2014). استرجع من
https://undocs.org/A/RES/68/243

قرار الجمعية العامة 98/68، تقرير فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، A/68/98 (24 يونيو 2013). استرجع من
https://undocs.org/A/68/98

قرار الجمعية العامة 70/237، التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، A/RES/70/237 (30 ديسمبر 2015). استرجع من https://undocs.org/A/RES/70/237

قرار الجمعية العامة رقم 42/22، إعلان زيادة فعالية مبدأ الامتناع عن التهديد باستعمال القوة أو استعمالها في العلاقات الدولية، A/RES/42/22 (17 مارس 1988). استرجع من https://legal.un.org/avl/ha/ga_42-22/ga_42-22.html

قرار الجمعية العامة رقم 2625، اعلان مبادئ القانون الدولي المتعلقة بالعلاقات الودية والتعاون بين الدول وفقا لميثاق الأمم المتحدة، A/RES/2625(XXV) (24 أكتوبر 1970). استرجع من https://www.undocs.org/A/RES/2625(XXV)

قرار الجمعية العامة رقم 13/32، تعزيز وحماية حقوق الإنسان على الإنترنت والتمتع بها، A / HRC/RES/32/13 (1 يوليو 2016). استرجع من https://undocs.org/A/HRC/RES/32/13

General Assembly resolution 2625, Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations, 24 October 1970, A/RES/2625(XXV). Available at: https://www.un.org/ruleoflaw/files/3dda1f104.pdf

General Assembly resolution 3314 (XXIX), Definition of Aggression, 14 December 1974). Retrieved from http://hrlibrary.umn.edu/instree/GAres3314.html

General Assembly resolution 73/266, Advancing responsible State behaviour in cyberspace in the context of international security, A/RES/73/266, available from https://documents-dds-

ny.un.org/doc/UNDOC/GEN/N18/465/01/PDF/N1846501.pdf?OpenElement

General Assembly resolution 73/27, Developments in the field of information and telecommunications in the context of international security, A/RES/73/27, available from https://documents-dds-ny.un.org/doc/UNDOC/GEN/N18/418/04/PDF/N1841804.pdf?OpenElement

Open-Ended Working Group (OEWG). (2020, June). Statement by the representative of the Russian Federation at the online discussion of the second "pre-draft" of the final report of the UN Open-ended Working Group on developments in the field of information and telecommunications in the context of international security (Unofficial translation). Retrieved from https://front.un-arm.org/wp-content/uploads/2020/09/oewg-informal-virtual-meetings-statement-by-the-russian-federation-15-june-2020.pdf

Open-ended Working Group (OWEG), Pre-Draft Report of the OEWG – ICT Comments by Austria (31 March 2020). Retrieved from https://front.un-arm.org/wp-content/uploads/2020/04/comments-by-austria.pdf

Open-ended Working Group (OWEG). (n.d.). Second "Pre-draft" of the report of the OEWG on developments in the field of information and telecommunications in the context of international security. Retrieved from https://front.un-arm.org/wp-content/uploads/2020/05/200527-oewg-ict-revised-pre-draft.pdf

UN Office for Disarmament Affairs. (2021, December). International Law Applied to Operations in Cyberspace (Paper shared by France with the Open-

ended working group established by resolution 75/240). Retrieved from https://documents.unoda.org/wp-content/uploads/2021/12/French-position-on-international-law-applied-to-cyberspace.pdf

United Nations, General Assembly, Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States, A/76/136 (13 July 2021), p. 137. Available from https://undocs.org/en/A/76/136

United Nations, General Assembly, Note by the Secretary General on Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174 (22 July 2015). Retrieved from https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/228/35/PDF/N1522835.pdf?OpenElement

United Nations, General Assembly, UN High Level Panel on Threats, Challenges and Change in 2004, A/59/565 (2 December 2004). available from https://undocs.org/A/59/565

United Nations, UN Office for Disarmament Affairs (UNUDO), International Law Applied to Operations in Cyberspace - paper shared by France with the open-ended working group established by resolution 75/240 (December 2021). Retrieved from https://documents.unoda.org/wp-content/uploads/2021/12/French-position-on-international-law-applied-to-cyberspace.pdf

مجلس الأمن

قرار مجلس الأمن 1540، S/RES/1540 (28 أبريل 2004). استرجع من https://undocs.org/ar/S/RES/1540(2004)

قرار مجلس الأمن 1368، S/RES/1368 (12 سبتمبر 2001). استرجع من https://undocs.org/ar/S/RES/1368(2001)

قرار مجلس الأمن 1373، S/RES/1373 (28 سبتمبر 2001). استرجع من https://undocs.org/ar/S/RES/1373(2001)

قرار مجلس الأمن 1737، S/RES/1737 (23 ديسمبر 2006). استرجع من https://www.un.org/securitycouncil/ar/node/45690

قرار مجلس الأمن 1747، S/RES/1747 (24 مارس 2007). استرجع من https://www.un.org/securitycouncil/ar/node/45693

قرار مجلس الأمن 1803، S/RES/1803 (3 مارس 2008). استرجع من https://www.un.org/securitycouncil/ar/node/45696

قرار مجلس الأمن 1929، S/RES/1929 (9 يونيو 2010). استرجع من https://www.un.org/securitycouncil/ar/s/res/1929-%282010%29

قرار مجلس الأمن 2231، S/RES/2231 (20 يوليو 2015). استرجع من https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/225/25/PDF/N1522525.pdf?OpenElement

قرار مجلس الأمن 2249، S/RES/2249 (20 نوفمبر 2015). استرجع من https://undocs.org/ar/S/RES/2249(2015)

قرار مجلس الأمن 2370، S/RES/2370 (2 أغسطس 2017). استرجع من https://undocs.org/ar/s/res/2370(2017)

UN Security Council, Security Council resolution 186 (1964) [The Cyprus Question], 4 March 1964, S/5575 (1964), available at: http://unscr.com/en/resolutions/186

UN Security Council, Security Council resolution 187 (1964) [The Cyprus Question], 13 March 1964, S/5603 (1964), available at: http://unscr.com/en/resolutions/187

Security Council resolution 326 (1973) [Provocation by Southern Rhodesia], 2 February 1973, S/RES/326 (1973), available at: http://unscr.com/en/resolutions/326

Security Council resolution 411 (1977) [Mozambique-Southern Rhodesia], 30 June 1977, S/RES/411 (1977), available at: http://unscr.com/en/resolutions/411

Security Council resolution 573 (1985) [Israel-Tunisia], 4 October 1985, S/RES/573 (1985), available at: http://unscr.com/en/resolutions/573

U.N. SCOR, 36th Sess., 2314 mtg., U.N. Doc. S/PV.2314 (15 December 1981), available from https://digitallibrary.un.org/record/49211

U.N. SCOR, 37th Sess., 2359 mtg., U.N. Doc. S/PV.2359 (20 May 1982), available from https://undocs.org/en/S/PV.2359

U.N. SCOR, 37th Sess., 2361 mtg., U.N. Doc. S/PV.2361 (21 May 1982), available from https://undocs.org/en/S/PV.2361

U.N. SCOR, 37th Sess., 2365 mtg., U.N. Doc. S/PV.2365 (24 May 1982), available from https://undocs.org/en/S/PV.2365

U.N. SCOR, 37th Sess., 2367 mtg., U.N. Doc. S/PV.2367 (25 May 1982), available from https://undocs.org/en/S/PV.2367

Security Council resolution 487 (1981) [Iraq-Israel], 19 June 1981, S/RES/487 (1981), available at: http://unscr.com/en/resolutions/487

Security Council Report. (2022, January). In Hindsight: The Security Council and Cyber Threats, an Update. Retrieved from https://www.securitycouncilreport.org/monthly-forecast/2022-02/in-hindsight-the-security-council-and-cyber-threats-an-update.php

الأطروحات

بودربالة، صلاح الدين. (2010). استخدام القوة المسلحة في إطار أحكام ميثاق الأمم المتحدة (أطروحة دكتوراه)، ص80–87. جامعة الجزائر. استرجع من http://193.194.83.98/jspui/bitstream/1635/10291/1/BOUDERBALA_SALAH.pdf

داوود، محمود. (نوفمبر 1993). مبدأ حظر استخدام القوة في العلاقات الدولية: دراسة مقارنة بين الشريعة الإسلامية والقانون الدولي العام (رسالة ماجستير). القاهرة، مصر: جامعة الأزهر.

عثمان، محمد. (يناير، 2015). دور القانون الدولي في مواجهة التجسس الدبلوماسي (رسالة دكتوراه). جامعة الشرق الأوسط. استرجع من https://meu.edu.jo/libraryTheses/5879f716c1346_1.pdf

منية، العمري .(2011–2010) .الدفاع الشرعي في القانون الدولي العام (أطروحة ماجستير). كلية الحقوق والعلوم السياسية – جامعة الإخوة منتوري .استرجع من https://bu.umc.edu.dz/theses/droit/AELA3806.pdf

Flemme, M. (2004). Due Diligence in International Law (Master Thesis). Faculty of Law - Lund University. Retrieved from https://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=1557482&file

Jolley, J. D. (2017). Attribution, State Responsibility, and the Duty to Prevent Malicious Cyber-Attacks in International Law. (PhD Thesis). University of Glasgow. https://doi.org/10.2139/ssrn.3056832

O'Meara, C. (2018, July). Necessity and Proportionality and the Right of Self-Defence in International Law (PhD Thesis). Faculty of Laws, University College London. Retrieved from https://discovery.ucl.ac.uk/id/eprint/10057299/1/PhD%20Thesis%20-%20FINAL%20VERSION%20.pdf

البيانات الصحفية

European Commission. (2022, March 1). Speech by President von der Leyen at the European Parliament Plenary on the Russian aggression against Ukraine [Press release]. Retrieved from https://ec.europa.eu/commission/presscorner/detail/en/speech_22_1483

European Council. (2020, July 30). EU imposes the first ever sanctions against cyber-attacks [Press release]. Retrieved from https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/

Israel Defense Forces [@IDF]. (2019, May 5). CLEARED FOR RELEASE: We thwarted an attempted Hamas cyber offensive against Israeli targets. Following our successful cyber defensive operation, we [Tweet]. Retrieved from https://twitter.com/IDF/status/1125066395010699264?s=20&t=XDX57wLgyoX8DghScSYZiw

JON CHANG HYOK. (2021, November 16). [Press release]. Retrieved from https://www.fbi.gov/wanted/cyber/jon-chang-hyok

KIM IL. (2021, November 16). [Press release]. Retrieved from https://www.fbi.gov/wanted/cyber/kim-il

National Cyber Security Centre. (2018, October 3). Reckless campaign of cyber attacks by Russian military intelligence service exposed [Press release]. Retrieved from https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed

North Atlantic Treaty Organization (NATO). (2016, July 9). Warsaw Summit Communiqué: Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8–9 July 2016 [Press release], para. 6. Retrieved from https://www.nato.int/cps/en/natohq/official_texts_133169.htm

North Atlantic Treaty Organization (NATO). (2019, November 4). London Declaration: Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in London 3–4 December 2019 [Press release], para. 31. Retrieved from https://www.nato.int/cps/en/natohq/official_texts_171584.htm

North Atlantic Treaty Organization (NATO). (2021, June 14). Brussels Summit: Communiqué Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels 14 June 2021 [Press release]. Retrieved from https://www.nato.int/cps/en/natohq/news_185000.htm

PARK JIN HYOK. (2021, November 16). [Press release]. Retrieved from https://www.fbi.gov/wanted/cyber/park-jin-hyok

Sky News. (2022, February 21). In full: Russian President addresses the nation [Video file]. Retrieved from https://www.de.com/watch?v=W57I2mzAr9c&feature=youtu.be

The White House. (2016, December 29). Statement by the President on Actions in Response to Russian [Press release]. Retrieved from https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/statement-president-actions-response-russian-malicious-cyber-activity

الخطابات

Hon. Ney, P.C. Jr. (2 March 2020) DOD General Counsel Remarks at U.S. Cyber Command Legal Conference [Speech]. US Department of Defense. Retrieved from https://www.defense.gov/News/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/

Statement by Ambassador Janne Taalas at the second session of the open-ended Working Group (OEWG) on developments in the field of information and telecommunications in the context of international security, February 10 and 11. Retrieved from https://ccdcoe.org/uploads/2018/10/Statement-on-International-Law-by-Finnish-Ambassador-Janne-Taalas-at-2nd-session-of-OEWG.pdf

The Print. (2022, February 24). Full text of Vladimir Putin's speech announcing 'special military operation' in Ukraine. Retrieved from

https://theprint.in/world/full-text-of-vladimir-putins-speech-announcing-special-military-operation-in-ukraine/845714/

Wright, J. (11 January 2017) The Modern Law of Self-Defence [Speech]. EJIL: Talk! Retrieved from https://www.ejiltalk.org/the-modern-law-of-self-defence/

Wright, J. (23 May 2018) Cyber and International Law in the 21st Century [Speech]. GOV.UK. Retrieved from https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century

المحاضرات

الصديقي، سعيد (مارس 29، 2020) القانون الدولي العام 11: مسؤولية الدولة عن أفعالها غير المشروعة دوليا (فيديو) 24:00. استرجع من https://www.youtube.com/watch?v=BG_jl9THDaM&t=1206s

Pr. Pierre d'Argent, Université catholique de Louvain [International Law MOOC]. (2017, January 27). 55 The Notion of Responsibility [Video]. Retrieved from https://youtu.be/9yb2uKgzgok

Neso Academy. (2019, November 17). Basics of MAC Addressing [Video file]. Retrieved from https://www.youtube.com/watch?v=FkiTOMn-XGw

التعريفات

Beyond a reasonable doubt. (2020). In Legal Information Institute. Cornell Law School. Retrieved from https://www.law.cornell.edu/wex/beyond_a_reasonable_doubt

Circumstantial evidence. (2022). In Legal Information Institute. Cornell Law School. Retrieved from https://www.law.cornell.edu/wex/circumstantial_evidence

Cybercrime. (n.d.). In Lexico (Oxford Dictionary). Retrieved from https://www.lexico.com/definition/cybercrime

Cybercrime. (n.d.). In Merriam-Webster. Retrieved from https://www.merriam-webster.com/dictionary/cybercrime

Erga omnes obligation. (2003). In Oxford Dictionary of Law (5th edition, p. 179). Oxford, Great Britain: Oxford University Press.

Self-help. (2021). In Legal Information Institute. Retrieved from https://www.law.cornell.edu/wex/self-help

الاحصائيات

البنك الدولي. (n.d.). الإنفاق العسكري (% من إجمالي الناتج المحلي) – معهد ستوكهولم الدولي لبحوث السلام، الكتاب السنوي: الأسلحة، ونزع السلاح، والأمن الدولي. استرجع من https://data.albankaldawli.org/indicator/MS.MIL.XPND.GD.ZS

Central Intelligence Agency (CIA). (2011). The World Factbook. Retrieved from https://www.cia.gov/the-world-factbook/

Check Point. (n.d.). Live Cyber Threat Map. Retrieved from https://threatmap.checkpoint.com/

Statista Research Department. (2022, July 7). U.S. government: proposed cyber security spending in FY 2017–2021. Retrieved from https://www.statista.com/statistics/675399/us-government-spending-cyber-security/

Abstract

The subject of cyber-attacks amongst states is a serious topic that takes place in all countries' defense and security policies. That is because the potential capabilities of cyber-attacks are not less than a conventional heavy weapon. Therefore, it is vital to be prepared to confront it legally by prohibiting its illegal use and establishing a legal framework for the victim state to respond to it.

This study attempts to address cyber-attacks from the perspective of jus ad Bellum, by applying the rule of prohibition of the use of force on cyber-attacks and exploring the consequences of breaching such a prohibition. Especially the effects of triggering the right of self-defense of the victim state if the cyber-attack extends to the threshold of armed attacks.

In addition, this study applies the rules of state responsibility to cyber-attacks, answers the question of when a cyber-attack will be considered an internationally wrongful act, the consequences of establishing the international responsibility of cyber acts, and the right for a victim state to resort to non-coercive means of self-help.

The study concludes with four available responses for the victim state to respond to cyber aggression. These responses are self-defense, countermeasures, legal measures, and a plea of necessity.

University of Bahrain

College of Law **Department of Public Law**

Responding to Cyber-Attacks Under Public International Law

A Thesis Submitted in Partial Fulfillment of the Requirements for the Ph.D. Degree in Public Law

Submitted by

Mariam Khalid Buqahoos

University Number: 20052267

Supervised by

Prof. Mahmoud El-Sayed Dawood

Professor of International Relations at University of Bahrain

Former Professor of Public International Law at Al-Azhar University

Kingdom of Bahrain
September 2022