مدى انطباق القانون الدولي الإنساني على الهجمات السيبرانية

إعداد

الدكتور/ سلوى يوسف الاكيابي

أستاذ مساعد القانون الدولي العام

كلية الحقوق – جامعة الزرقاء

بريد الكترونى : Salekiaby@yahoo.com

١٢- مدى انطباق القانون الدولي الإنساني على الهجمات السيبرانية

ملخص باللغة العربية

شهد العالم خلال العقدين الأخيرين ثورة في تكنولوجيا المعلومات والاتصالات، امتدت آثارها إلى ساحات القتال، التي امتد فضائها ليشمل الواقع الافتراضي. وتعتمد أغلب نظم الأسلحة الحديثة على البنية التحتية السيبرانية بما في ذلك نظم الكومبيوتر وشبكة الإنترنت، حتى أصبح هذا الاعتماد هو السمة المميزة للنزاعات في الآونة المعاصرة. وحيث أن معاهدات القانون الدولي الإنساني تمت صياغتها في وقت كانت فيه الهجمات السيبرانية مجرد خيال علمي، فالسؤال الذي يطرحه هذا البحث هو هل يستجيب القانون الدولي الإنساني للتحديات التي يطرحها التطور التكنولوجي الحديث؟ بعبارة أخرى، هل القانون الدولي الإنساني -بوضعه الحالي- صالح للتطبيق على الهجمات السيبرانية، أم أنَّ هناك حاجة لتطويع بعض قواعده لتلاحق التطورات التكنولوجية الحديثة؟

يوضح البحث في البداية ماهية الهجمات السيبرانية التي ينطبق عليها القانون الدولي الإنساني على وجه التحديد، ثم ينتقل من ذلك إلى بحث مدى انطباق القانون الدولي الإنساني على الهجمات السيبرانية من زاويتين، الأولى: من حيث استخدام الأسلحة السيبرانية كوسيلة للهجوم السيبراني، وذلك من خلال التعرض لمدى الامتثال للقواعد

التي تنظم اقتناء الأسلحة الجديدة، والثانية: من حيث استخدام الهجمات السيبرانية كأسلوب للقتال، وذلك من خلال بحث مدى انطباق القواعد التي تنظم مشروعية الهجمات عليها.

كلمات مفتاحية: الأسلحة السيبرانية ، الهجمات السيبرانية ، استعراض الأسلحة ، الحرب السيبرانية .

ملخص باللغة الإنجليزية

The Applicability of International Humanitarian Law to cyber attacks

During the last two decades, the world had witnessed a revolution in information and communication technology, the effects of which extended to the battlefields, whose space extended to include virtual reality. Furthermore, the most modern weapons systems depend on cyber infrastructure, including computer systems and the Internet, which became the hallmark of contemporary conflicts. Since International Humanitarian Law (IHL) treaties were drafted at a time when cyber-attacks were just science fiction, the question raised by this research is whether IHL responds to the challenges posed by modern technological development? In other words, is international humanitarian law – in its current state – applicable

to cyber-attacks, or is there a need to adapt some of its rules to cope with modern technological developments?

This research initially clarifies the type of cyber-attacks, which falls under the jurisdiction of IHL, and then moves on to examine the applicability of IHL to cyber-attacks from two angles, the first: in terms of the use of cyber weapons as a means of cyber-attack, through exposure to the extent to which the usage of these weapons complies with the rules regulating the acquisition of new weapons, and the second: in terms of the use of cyber-attacks as a method of combat, by examining the applicability of the rules regulating the legality of attacks on them.

Keywords: cyber weapons – cyber-attacks – weapons review – cyber warfare

١٢- مدى انطباق القانون الدولي الإنساني على الهجمات السيبرانية

مقدمة*

في ٢٤ فبراير ٢٠٢٢، وكجزء من الهجمات الروسية ضد أوكرانيا، شنت روسيا هجمات باستخدام برمجيات خبيثة؛ استهدفت حذف بيانات من حواسيب في وكالات حكومية أوكرانية، بالإضافة إلى استخدام برمجيات الحرمان من الخدمة ضد المواقع الإلكترونية للحكومة الأوكرانية والأنظمة العسكرية.[1] وقد أثرت هذه الهجمات على القطاعات العامة، وقطاعات الطاقة والإعلام، والقطاع المالي والتجاري في أوكرانيا، كما أثرت على توزيع الأدوية والمواد الغذائية، وإمدادات الإغاثة؛ مما حدا بالاتحاد الأوروبي، والولايات المتحدة الأمريكية، وحلف الناتو لإطلاق عدة مبادرات بهدف تقليص أثر هذه الهجمات وحماية البنية التحتية الأساسية لأوكرانيا.[٢]

---

*تود الكاتبة أن تتقدم بالشكر الجزيل للزميل الدكتور محمد موسى على مراجعة هذا البحث لغويًا ونحويًا.

[1] موسكو تلوّح باستخدامه.. سلاح تفادت روسيا استخدامه في العملية العسكرية في أوكرانيا!، جريدة الوطن، ٨ مارس ٢٠٢٢. متاح على: https://alwatannews.net/Life-Style/article/994774/ . كافة المواقع الإلكترونية في هذا البحث تمت زيارتها آخر مرة في ١ نوفمبر ٢٠٢٢.

[٢] كجزء من هذه المبادرات، قام الاتحاد الأوروبي بتنشيط فرق الاستجابة الإلكترونية السريعة (مشروع في إطار التعاون المنظم الدائم في مجال السياسة الأمنية والدفاعية، لدعم الدفاع السيبراني الأوكراني. للمزيد انظر:

ولم تكن هذه الهجمات هي الأولى من نوعها التي تشنها روسيا؛ فعادة ما كان يسبق العمليات العسكرية على الأرض هجمات سيبرانية. فقد سبقت العمليات العسكرية التي تمت ضد جورجيا عام ٢٠٠٨، وفي شبه جزيرة القرم عام ٢٠١٤، هجمات سيبرانية تضمنت نشر معلومات مضللة، وهجمات الحرمان من الخدمة على شبكات الكمبيوتر؛ استهدفت إثارة المعارضة الشعبية لحكومة الخصم، والتأثير على معنوياتها.[1]

على صعيد مماثل، تعرض البرنامج النووي الإيراني إلى هجوم سيبراني معقد عام ٢٠١٠، من خلال استخدام فيروس (دودة كمبيوتر Stuxnet)؛ مما أدى إلى خروج أجهزة الطرد المركزي عن السيطرة، وتعد أجهزة الطرد المركزي ضرورية لإنتاج

Russia's war on Ukraine: Timeline of cyber-attacks, Think Tank, European Parliament, 21-06-2022. Available at: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)733549

[1]وقد أُطلق على هذا النهج اسم "الحرب المختلطة"، واستخدمته روسيا بنجاح في احتلال شبه جزيرة القرم. خالد وليد محمود، كيف يمكن استخدام السلاح السيبراني في الأزمة الروسية الأوكرانية؟، الجزيرة، 21/2/2022. متاح على: https://1-a1072.azureedge.net/opinions/2022/2/21/

اليورانيوم المخصب، الذي يمكن استخدامه في تصنيع وقود المفاعلات النووية. [١] وبالرغم من أن إسرائيل لم تعلن مسئوليتها عن الهجوم، إلا أن صحف إسرائيلية أشارت إلى أن إسرائيل هي المتسببة في الهجوم، كما اتهمت إيران إسرائيل بشن هذا الهجوم.[٢]

وتُشير بعض التقارير إلى وجود هجمات سيبرانية متبادلة بين إيران وإسرائيل؛ إذ تعرضت إسرائيل في ١٤ مارس ٢٠٢٢، لهجوم سيبراني شمل المواقع الإلكترونية لوزارات وهيئات رسمية مختلفة، بما فيها الصحة، والعدل، والرعاية الاجتماعية، والداخلية، ومكتب رئيس الوزراء، وقد وصفته صحف إسرائيلية بأنه الهجوم السيبراني الأكبر ضد إسرائيل واتهمت فيه إيران.[٣] فيما تُشير التقارير إلى تعرض إيران بعدها –

---

[١] Oona A. Hathaway, et al. "The Law of Cyber-Attack", California Law Review, vol. 100, no. 4, 2012, pp. 817-85. JSTOR, http://www.jstor.org/stable/23249823 .

[٢] منشأة نطنز النووية الإيرانية: ما هي وما سر الحوادث المتكررة فيها؟، بي بي سي بالعربي، ٢٢ أبريل/ نيسان ٢٠٢١. متاح على: https://www.bbc.com/arabic/middleeast-56721332

[٣] اتهمت في هذه الهجمات الحكومة الإيرانية، وجهات محسوبة على الحرس الثوري الإيراني مثل مجموعات "بلاك شادو" و"عصا موسى". انظر: خير الدين الجابري، أكبر هجوم سيبراني في تاريخ

في ٢٥ أبريل ٢٠٢٢– إلى هجوم سيبراني واسع النطاق على البنية التحتية للبلاد، شمل اختراق مواقع أكثر من ١٠٠ مؤسسة عامة وخاصة، لكنه قد تم إحباطه في مراحله الأولى، قبل أن يصل إلى المعلومات والبيانات الرئيسة الهامة، واتُهمت فيه إسرائيل.[١]

وقد بدأت بعض الدول بالفعل في إنشاء وحدات داخل قواتها النظامية متخصصة في المحافظة على الأمن السيبراني، ومنها: الجيش الأمريكي، حيث جرى تطوير القيادة القتالية السيبرانية فيه كوحدة مستقلة بذاتها في داخله، والجيش الصيني الأزرق، الذي أنشأته الصين عام ٢٠١٥، لحماية الفضاء السيبراني الصيني، والجيش الروسي، حيث أعلنت روسيا عام ٢٠١٧، عن امتلاكها جيشًا سيبرانيًّا لحماية فضائها السيبراني، وكذلك الجيش الإسرائيلي، وهو وحدة متعددة التخصصات داخل الجيش، ومنها وحدة الإشارة في صحراء النقب، وكذلك الجيش البريطاني، حيث أعلنت

إسرائيل".. ماذا وراء عمليات الاختراق التي شلت وزارات حكومة تل أبيب؟، عربي بوست ١٥/٠٣/٢٠٢٢. متاح على الرابط التالي: https://arabicpost.net/

[١] "وتقول طهران إنها في حالة تأهب قصوى ضد أي هجمات إلكترونية قد تشنّها تل أبيب". انظر: هجوم سيبراني على أكثر من ١٠٠ موقع إلكتروني لمؤسسات إيرانية عامة وخاصة، موقع إيران انترناشيونال 04/25/2022 . متاح على الرابط التالي: https://www.iranintl.com/ar/202204255536

بريطانيا في ٢٠١٥، عن برنامجها للتصدي للهجمات السيبرانية من خلال وحدة متخصصة داخل جيشها.[١]

ومنذ بداية القرن الحالي، زادت الهجمات السيبرانية ضد الدول، وكانت الدول المتقدمة هي الأكثر عرضة لهذه الهجمات، وعلى رأسها الولايات المتحدة الأمريكية وروسيا.[٢] ويثير ذلك العديد من المسائل القانونية في إطار القانون الدولي.

[١] ما هي الحرب السيبرانية وما مدى خطورتها، مقال منشور على CyberOne، متاح على: https://cyberone.co/%D9%85%D8%A7-%D9%87%D9%8A-%D8%A7%D9%84%D8%AD%D8%B1%D8%A8-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9/

[٢] تعرضت الولايات المتحدة في عام ٢٠١٤، لحوالي ١٠٠ ألف هجمة سيبرانية واختراقات متعددة. انظر: ما هي الحرب السيبرانية، وما مدى خطورتها، مقال منشور على CyberOne، متاح على: https://cyberone.co/%D9%85%D8%A7-%D9%87%D9%8A-%D8%A7%D9%84%D8%AD%D8%B1%D8%A8-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9/

إشكالية البحث ونطاقه:

تكمن إشكالية البحث في أن معاهدات القانون الدولي الإنساني تمت صياغتها في وقت كانت فيه الهجمات السيبرانية مجرد خيال علمي، فهل يستجيب القانون الدولي الإنساني للتحديات التي يطرحها التطور التكنولوجي الحديث؟ بعبارة أخرى، هل القانون الدولي الإنساني – بوضعه الحالي – صالح للتطبيق على الهجمات السيبرانية، أم أنَّ هناك حاجة لتطويع بعض قواعده لتلاحق التطورات التكنولوجية الحديثة؟

للإجابة على هذا التساؤل، ينبغي توضيح أن مفهوم "الهجمات السيبرانية" مفهومٌ واسع، ويشمل العديد من الأفعال قد ينطبق عليها القانون الدولي الإنساني، وقد ينطبق عليها قوانين أخرى، ولذلك، ستوضح الدراسة في البداية ماهية الهجمات السيبرانية التي ينطبق عليها القانون الدولي الإنساني على وجه التحديد، ثم تنتقل من ذلك إلى بحث مدى انطباق القانون الدولي الإنساني على الهجمات السيبرانية من زاويتين، **الأولى:** من حيث استخدام الأسلحة السيبرانية كوسيلة للهجوم السيبراني، وذلك من خلال التعرض لمدى الامتثال للقواعد التي تنظم اقتناء الأسلحة الجديدة، **والثانية:** من

حيث استخدام الهجمات السيبرانية كأسلوب للقتال، وذلك من خلال بحث مدى انطباق القواعد التي تنظم مشروعية الهجمات عليها.

أهمية البحث ومنهجه:

شهد العالم خلال العقدين الأخيرين ثورة في تكنولوجيا المعلومات والاتصالات، امتدت آثارها إلى ساحات القتال، التي امتد فضاؤها ليشمل الواقع الافتراضي.[1] وتعتمد أغلب نظم الأسلحة الحديثة على البنية التحتية السيبرانية بما في ذلك نظم الكمبيوتر وشبكة الإنترنت، حتى أصبح هذا الاعتماد هو السمة المميزة للنزاعات في الآونة الأخيرة. ولذلك، فمن الضروري أن يُلاحق التطور القانوني نظيره التكنولوجي، ومن هنا تكمن أهمية هذه الدراسة؛ إذ تتعرض لمدى انطباق القانون الدولي الإنساني على الهجمات السيبرانية حتى تصل لنتيجة حول مدى كفاية التشريع الدولي الحالي لتنظيم الاستخدام المشروع للهجمات السيبرانية.

وللوصول لهذه النتيجة، يستخدم البحث منهجًا وصفيًّا تحليليًّا، مع المقارنة وفقًا لأحكام القضاء الدولي والمعاهدات ذات الصلة – متى كان ذلك لازمًا – في التعرض

[1] خالد وليد محمود، الهجمات عبر الإنترنت: ساحة الصراع الإلكترونيّ الجديدة، سلسلة: دراسات ٢٠١٣، المركز العربي للأبحاث ودراسة السياسات، ص٢٠.

للموضوع من زاويتين: **الأولى:** مدى انطباق القانون الدولي الإنساني على استخدام الأسلحة السيبرانية كوسيلة للقتال، **والثانية:** مدى انطباق القانون الدولي الإنساني على استخدام الهجمات السيبرانية كأسلوب للقتال. وقبل ذلك سيتعرض البحث للمقصود بالسيبرانية، وما يتعلق بها من مفاهيم وتمييزها عن غيرها، ومفهوم الهجمات التي ينطبق عليها القانون الدولي الإنساني.

تقسيم:

في ضوء ما تقدم، سيتم تقسيم البحث على النحو التالي:

الفصل الأول: مفهوم الهجمات السيبرانية وتمييزها عن غيرها

الفصل الثاني: الأسلحة السيبرانية كوسيلة للقتال

الفصل الثالث: الهجمات السيبرانية كأسلوب للقتال

الفصل الأول

مفهوم الهجمات السيبرانية في إطار القانون الدولي الإنساني

تمهيد:

لمعرفة المقصود بـ "الهجمات السيبرانية"، ينبغي التعرض لبعض المصطلحات المرتبطة بهذا المفهوم، وقبلها للمقصود بمصطلح "سيبراني". وعلى الرغم من وجود العديد من المصطلحات المرتبطة بالهجوم السيبراني بوجه عام، فسنُقصر الحديث في هذا الفصل على المصطلحات ذات العلاقة بالهجمات السيبرانية في أوقات النزاعات المسلحة، والتي سيتم استخدامها في هذه الدراسة.

كذلك، فقد لاحظنا وجود خلط في المفاهيم – في بعض الكتابات – ما بين الهجمات السيبرانية، والهجمات الإلكترونية، في حين أن مفهوم كلٍّ منهما يختلف تمامًا عن الآخر. كذلك وجب التعرض أيضًا للتمييز بين الهجمات السيبرانية، وتلك التي تتم باستخدام تكنولوجيا الذكاء الاصطناعي باعتبار أنَّ كليهما يقع ضمن مسائل التكنولوجيا الناشئة.

بعد ذلك سنتعرض لمفهوم "الهجمات السيبرانية" التي ينطبق عليها القانون الدولي الإنساني، وذلك لتمييزها عن غيرها مما لا ينطبق عليها هذا القانون، وقد يخضع تنظيمها لقوانين أخرى كالقوانين الجنائية الداخلية على سبيل المثال. وذلك تمهيدًا للفصول التالية، والتي ستتناول مدى انطباق القانون الدولي الإنساني على هذه الهجمات.

تقسيم:

بناءً على ما تقدم، سنتعرض في هذا الفصل إلى مفهوم السيبرانية، وما يختلط به من مفاهيم وتمييزه عن غيره في مبحث أول، ثم لمفهوم الهجمات السيبرانية التي يُطبق عليها القانون الدولي الإنساني في مبحث ثانٍ، وذلك على النحو التالي.

المبحث الأول: السيبرانية وما يتعلق بها من مفاهيم وتمييزها عن غيرها.

المبحث الثاني: الهجمات السيبرانية الخاضعة للقانون الدولي الإنساني.

المبحث الأول

السيبرانية وما يتعلق بها من مفاهيم وتمييزها عن غيرها

إن كلمة "سايبر" – المشتق منها كلمة "السيبراني" – باللغة العربية هي تعريب لكلمة Cyber باللغة الإنجليزية، والمشتقة بدورها من كلمة Cybernetics، والتي تعني علم التحكم في الآلة. وقد ظهر هذا المصطلح على يد عالم الرياضيات نوربرت وينر Norbert Wiener في أربعينيات القرن الماضي، وعرفها بأنها: "الدراسة العلمية للتحكم والتواصل في الحيوان والآلة".[١]

ويضع دليل تالين[٢] تعريفًا أبسط للسيبرانية، وأكثر دلالة على المقصود بها اليوم، فيُعرَّف السيبرانية بأنها "العلاقة مع تكنولوجيا المعلومات".[١] ولا يوجد مقابل لفظي في

---

[١] "The scientific study of control and communication in the animal and the machine". For more see: https://www.vocabulary.com/dictionary/cybernetics.

[٢] نتيجة للهجمات السيبرانية التي تعرضت لها إستونيا في عام ٢٠٠٧، فقد التفت المجتمع الدولي إلى خطورة هذه الهجمات على الدول وعلى المدنيين. وقد أدى ذلك إلى تسريع إنشاء مركز الناتو للدفاع السيبراني the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) في تالين بإستونيا. وقد كان من أنشطته إجراء دراسة حول الحرب السيبرانية أجراها مجموعة من الخبراء القانونيين في القانون الدولي، وعُرفت باسم "دراسة تالين".

اللغة العربية لكلمة Cyber، ولعل بدائل هذا المصطلح باللغة العربية قد تكون "كمبيوتري" أو "حوسبي"، إذ يشير هذان المصطلحان إلى العمليات التي تتم باستخدام الكمبيوتر أو الحاسوب عن طريق وظائف رياضية معقدة.[٢] ونظرًا لشيوع استخدام كلمة "سيبراني" باللغة العربية في العديد من المؤلفات والتقارير، ودلالتها على المصطلح في اللغة الإنجليزية Cyber، فسوف نستخدمها في دراستنا هذه.

وفيما يلي سنتعرض لمفهوم السيبرانية وما يرتبط بها من مفاهيم في المطلب الأول، ثم تمييزها عما يختلط بها من مفاهيم في المطلب الثاني.

والتي أصبحت دليلاً إرشاديًا للحكومات في جميع أنحاء العالم. صدرت الطبعة الأولى منه عام ٢٠١٣، تحتوي على ٩٥ قاعدة، ثم تم تنقيحها وصدرت طبعة منقحة في عام ٢٠١٧، تحتوي على ١٥٤ قاعدة.

Tallinn Manual 2.0 on the International Law Applicable to Cyber Operation, edited by Michael N. Schmitt, United States Naval War College, Newport, Rhode Island, Cambridge University Press, February 2017, pp.1-7. [hereinafter: Tallinn Manual].

[١] Tallinn Manual, op.cit., p.465.

[٢] انظر في المقصود من مصطلح كمبيوتري أو حوسبي الرابط التالي:
https://www.vocabulary.com/dictionary/computing

المطلب الأول

السيبرانية وما يرتبط بها من مفاهيم

يُستخدم مصطلح "سيبراني" كصفة للعديد من المصطلحات المستخدمة في إطار القانون الدولي الإنساني، وفيما يلي سنتعرض بالتوضيح للمصطلحات المتعلقة بالسيبرانية، والمستخدمة في هذه الدراسة بالقدر اللازم لتوضيحها وفهم المقصود منها.

الفضاء السيبراني Cyberspace:

يعد الفضاء السيبراني – ببساطة – الساحة التي تجري فيها الحرب السيبرانية. ويوصف بأنه "المجال الخامس للحرب، بعد البر والبحر والجو والفضاء".[١] كما يوصف بأنه "نطاق عالمي" global domain يفتقر إلى المادية، وهو افتراضي بطبيعته.[٢]

[١] 'War in the Fifth Domain', The Economist, July 1st of 2010. Available at: https://www.economist.com/briefing/2010/07/01/war-in-the-fifth-domain

[٢] Joint Chiefs of Staff, Joint Publication 1-02, US Department of Defense Military and Associated Terms, at 57 (8 November 2010, as amended through 15 January 2016).

وتُعرِّف وزارة الدفاع الأمريكية الفضاء السيبراني بأنه "مجال عالمي داخل بيئة معلومات تتكون من شبكة معلومات مترابطة البنية التحتية التكنولوجية، بما في ذلك الإنترنت وشبكات الاتصالات السلكية واللاسلكية، وأنظمة الكمبيوتر والمعالجات، ووحدات التحكم المدمجة".[١] ويعرفه ريتشارد كلارك Richard Clarke ، مسئول الأمن السيبراني الأمريكي السابق بأنه: "كل شبكات الكمبيوتر في العالم، وكل شيء يتصل بها ويتحكم فيها، فهو ليس الإنترنت فحسب..... الفضاء السيبراني يشمل الإنترنت، بالإضافة إلى الكثير من شبكات الكمبيوتر الأخرى التي لا يُفترض أن تكون متاحة للوصول إليها من خلال الإنترنت".[٢]

---

[١] "a global domain within the information environment consisting of the technology infrastructures, including interdependent network of information the Internet, telecommunications networks, computer systems, and embedded processors and controllers". Dictionary of Military and Associated Terms, available at: http://www.dtic.mil/doctrine/dod_dictionary/data/c/10160.html

[٢] "Cyberspace is all of the computer networks in the world and everything they connect and control. It's not just the Internet. Let's be clear about the difference. The Internet is an open network of networks. From any network you should be able to communicate with any computer on the Internet, Internet's networks. Cyberspace includes the connected to any of the

وتعرِّف وينجفيلد Wingfield الفضاء الإلكتروني بأنه: "ليس مكانًا ماديًّا – ولا يمكن قياسه في أي بُعد مادي أو مساحة زمنية متصلة، إنه مصطلح مختصر يشير إلى البيئة التي تم إنشاؤها عن طريق التقاء الشبكات التعاونية لأجهزة الكمبيوتر وأنظمة تكنولوجيا المعلومات، والبنى التحتية للاتصالات التي يشار إليها عادة باسم شبكة الويب العالمية".[١]

ووفقًا لدليل تالين، يتكون الفضاء السيبراني من "مكونات مادية وغير مادية لتخزين، وتعديل، وتبادل البيانات باستخدام شبكات الكمبيوتر".[٢] ولذلك، يمكن القول بأن الفضاء السيبراني يتكون من مكون مادي يشمل كل الكابلات، والأسلاك، والألياف الضوئية، أو اللاسلكية المتصلة بالكمبيوتر، ويُطلق عليها "البنية التحتية السيبرانية"،

---

computers that are not supposed to be accessible from the Internet". Internet plus lots of other networks of

R Clarke, Cyber War (Harper Collins, 2010), chapter 3, available at: http://www.richardaclarke.net/cyber_war.php#excerpts

[١] Thomas C. Wingfield, The Law of Information Conflict: National Security Law in Cyberspace, Aegis Research Corp., 2000, p. 17.

[٢] Tallinn Manual, op.cit., p.564.

وهي تضم أجهزة الاتصالات، والتخزين، والحوسبة التي يتم بناء وتشغيل أنظمة المعلومات عليها.[١]

كما يتكون من مكون غير مادي يشمل شبكة الإنترنت، وكل الشبكات غير المتاح الوصول إليها عبر الإنترنت، بالإضافة إلى أنظمة التحكم الإشرافي والحصول على البيانات Supervisory Control and Data Acquisition (SCADA) التي تسمح للآلات فقط بالاتصال مع الأجهزة الأخرى، مثل: لوحات التحكم التي تتحكم في عمل المضخات كالمصاعد، والمولدات الكهربائية وما إلى ذلك.

وبالتالي، فإن الفضاء السيبراني يتكون من مليارات من أجهزة الكمبيوتر، بالإضافة إلى الخوادم، وأجهزة التوجيه والمفاتيح، وكابلات الألياف الضوئية، واللاسلكية الاتصالات التي تسمح للبنى التحتية الحيوية بالعمل.[٢]

ويوضح Schreier أربع خصائص تميز الفضاء السيبراني، وهي:

---

١. Tallinn Manual, op.cit., p.564.

2 Fred Schreier, On Cyberwarfare, Working Paper No. 7, DCAF Horizon, Geneva,2015, P10. Available At: https://www.dcaf.ch/sites/default/files/publications/documents/OnCyberwarfare-Schreier.pdf

١٢- مدى انطباق القانون الدولي الإنساني على الهجمات السيبرانية

أولاً: أنه لا غنى عنه بالنسبة لشبكات تكنولوجيا المعلومات والاتصالات، فبدون الفضاء السيبراني لا يمكن لأي نشاط سيبراني أن يتم، ولا يمكن نقل ملايين المعلومات، ولن تكون تقنيات الاتصالات قادرة على التواصل مع بعضها البعض، كذلك فلن تكون تكنولوجيا المعلومات والاتصالات نفسها قادرة على العمل.

ثانيًا: أن الفضاء السيبراني من صنع الإنسان، مما يجعله فريدًا عند مقارنته ببيئات العمليات العسكرية الأخرى كالأرض والبحر والجو والفضاء. ولذلك، فقد يكون من الأسهل على الدول أن تتحكم فيه، بعكس البيئات الطبيعية. فيحق للدول – وفقًا لمبدأ السيادة – قطع الاتصال بالإنترنت كليًا أو جزئيًا، وكذلك البنية التحتية السيبرانية الموجودة على أراضيها، طالما لم تخل بأية معاهدة أو التزامات بموجب القانون الدولي العرفي، ولا سيما في مجال القانون الدولي لحقوق الإنسان.[١]

ثالثًا: أنه لا توجد حدود لعدد الفضاءات السيبرانية التي يمكن صنعها، وأن كل فضاء سيبراني لا حدود له، على عكس البيئات الأخرى كالأرض والبحر والجو والفضاء.

رابعًا: أن كلفة الدخول إلى الفضاء السيبراني رخيصة نسبيًا، كذلك، فالموارد والخبرات المطلوبة لدخول الفضاء السيبراني، والتواجد فيه، واستغلاله متواضعة نسبيًا مقارنة

[١] Tallinn Manual, op.cit., p.13.

بالمطلوب لاستغلال الفضاءات البرية والبحرية والجوية والفضائية. فعلى سبيل المثال، تستطيع مجموعة صغيرة من المراهقين، بعدد قليل من أجهزة الكمبيوتر المتصلة بالشبكة الدخول إلى الفضاء السيبراني.

العمليات السيبرانية Cyber Operations:

يعرف Adkins العمليات السيبرانية بأنها: "أي عمل يهدف إلى إجبار خصم لتحقيق إرادتنا الوطنية، وتنفيذها ضد عمليات التحكم في البرامج داخل نظام الخصم".[١] ويُعرفها دليل تالين بأنها: "توظيف القدرات السيبرانية لتحقيق الأهداف في أو من خلال الفضاء الإلكتروني". أما النشاط السيبراني فيعرفه بأنه: "أي نشاط يتضمن استخدام البنية التحتية السيبرانية، أو يستخدم الوسائل الإلكترونية؛ للتأثير على تشغيل

[١] 'Any act intended to compel an opponent to fulfill our national will, executed against the software controlling processes within an opponent's system'. BN Adkins, Major USAF, The spectrum of cyber conflict. From hacking to information warfare. What is law enforcement's role, AU/ACSC/003/2001-04, at 34.

هذه البنية التحتية".[١] وبالتالي فإن معنى الأنشطة السيبرانية يشمل، من بين عدة أنشطة، العمليات السيبرانية.

ويرتبط استخدام مصطلح العمليات السيبرانية بمصطلح آخر وهو القوة السيبرانية cyberpower، الذي يستخدم للدلالة على أثر العمليات السيبرانية في الفضاء السيبراني. فإذا كان الفضاء السيبراني هو البيئة التي تتم فيها العمليات السيبرانية، فإنَّ القوة السيبرانية هي جميع الآثار الناتجة عن هذه العمليات في الفضاء السيبراني، وفي البيئة الواقعية. ومن أكثر التعريفات شيوعًا للقوة السيبرانية هي أنه: "القدرة على استخدام الفضاء السيبراني لإنشاء مزايا، والتأثير على الأحداث في البيئات التشغيلية الأخرى وعبر أدوات القوة".[٢] وتتفاوت القوة السيبرانية لكل دولة أو لكل طرف في النزاع على حسب قدرتهم على استخدام الفضاء السيبراني، فالقوة السيبرانية هي دائمًا مقياس للقدرة على استخدام تلك البيئة.

---

١ Tallinn Manual, op.cit., p.465.

٢ "cyberpower is the ability to use cyberspace to create advantages and influence events in other operational environments and across the instruments of power." Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in Fred Schreier, On Cyberwarfare, op.cit., P1٤.

وقد يؤدي استخدام القوة السيبرانية إلى إحداث تأثير داخل الفضاء السيبراني فقط، أو داخله وخارجه؛ أي في البيئات الأخرى مثل الأرض أو البحر أو الجو أو الفضاء. وتعتمد القوة السيبرانية على أداتين: الـ hardware، والتي تشمل على سبيل المثال: وحدة المعالجة المركزية، ومحرك الأقراص، ولوحة مفاتيح، والشاشة، كذلك الكابلات والأقمار الصناعية والموجهات، ورقاقات الكمبيوتر وما شابهها، والـ Software، والتي تشمل على سبيل المثال البرامج الضارة التي تتداخل مع وظائف الكمبيوتر والتطبيقات المستندة إلى الإنترنت، وتعد هذه البرامج سلاحًا رئيسًا في الحرب السيبرانية.[١]

الهجوم السيبراني Cyber Attack:

يُعرف الهجوم السيبراني في دليل العمليات السيبرانية والإرهاب السيبراني للجيش الأمريكي بأنه: "الاستخدام المتعمد للأنشطة التخريبية أو التهديد بها ضد أجهزة الكمبيوتر و/ أو الشبكات، بقصد إحداث ضرر أو تحقيق أهداف اجتماعية، أو إيديولوجية، أو دينية، أو سياسية، أو أهداف مماثلة، أو لتخويف أي شخص من أجل

[١] Fred Schreier, On Cyberwarfare, op.cit., P1 .٤

تحقيق هذه الأهداف".[١] وتتضمن منهجية الهجوم السيبراني إجراءً متعمدًا بغرض "تغيير، أو تعطيل، أو خداع، أو إهانة، أو تدمير أنظمة، أو شبكات الكمبيوتر المعادية أو المعلومات و/ أو البرامج المقيمة في هذه الأنظمة، أو الشبكات أو التي تمر عبرها".[٢] ويعرف البعض الهجوم السيبراني بأنه "أي إجراء يتم اتخاذه لتقويض وظائف شبكة الكمبيوتر لأغراض سياسية، أو أمنية وطنية".[٣]

ويُلاحظ على هذه التعريفات أنها تُقصر الهجوم السيبراني على ما يؤدي إلى تبعات غير عنيفة في الواقع المادي، وتقتصر آثاره على الفضاء السيبراني، في حين يُعرف دليل تالين الهجوم السيبراني بأنه "عملية سيبرانية، هجومية أو دفاعية من المتوقع - بشكل معقول - أن تتسبب في إصابة أو وفاة الأشخاص، أو تلف، أو تدمير

---

[١] "The premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or to further social, ideological, religious, political or similar objectives. Or to intimidate any person in furtherance of such objectives". U.S. Army Training & Doctrine Command, Dcsint Handbook No. 1.02, Critical Infrastructure Threats and Terrorism, at Vii-2 (2006).

[٢] Michael Gervais, Cyber Attacks and the Laws of War (October 1, 2011). Available at: https://ssrn.com/abstract=1939615

[٣] Oona A. Hathaway, et al. "The Law of Cyber-Attack", op.cit., pp. 817-85.

الأشياء".[١] وبالتالي، على عكس التعريفات السابقة، يُقصر الهجمات السيبرانية على ما تؤدي إلى تبعات عنيفة في الواقع المادي مثل: التسبب في إصابة، أو وفاة الأشخاص، أو تلف، أو تدمير الأشياء.

الحرب السيبرانية Cyber Warfare:

بغض النظر عن انتقاد استخدام مصطلح "الحرب"، وتفضيل مصطلح "النزاع المسلح" عوضًا عنه. ففي الواقع يصعب وضع تعريف للحرب السيبرانية، ليس فقط لعدم وجود توافق بين فقهاء القانون الدولي حول مفهومها، وإنما أيضًا لوجود العديد من المصطلحات التي تستخدم بنفس المعنى، وقد تثير لبسًا مثل: "القوة السيبرانية"، و"الهجوم السيبراني"، و"حرب المعلومات".

وفي فقه القانون الدولي، فإن أغلب الكتابات تستخدم مصطلح "الحرب السيبرانية"، فيما تُستخدم مصطلحات أخرى للإشارة إلى نفس المعنى المقصود من الحرب السيبرانية، فتؤكد Wingfield أن الهجوم على شبكات الكمبيوتر (CNA) Computer Network Attack هو نفسه "الحرب السيبرانية"، ويُعرف Schmitt "الهجوم على شبكات الكمبيوتر بأنه: "التصرف المتخذ للتأثير المضاد على معلومات

[١] Tallinn Manual, op.cit., p.415.

أو نظم معلومات الخصم، دفاعًا عن معلومات، أو نظم معلومات الدولة".[١] ونرى أن هذا التعريف أكثر تعبيرًا عن الهجوم السيبراني منه إلى الحرب السيبرانية.

فيما يُفضل Dahl استخدام مصطلح "الحرب المتمحورة حول الشبكة" Network-centric war،[٢] ونرى أنَّ هذا المصطلح صعب، وإن كان يؤدي إلى نفس المعنى المقصود من الحرب السيبرانية. كذلك، يُستخدم مصطلح "حرب المعلومات" Information Warfare للإشارة إلى "توظيف أجهزة الكمبيوتر والتكنولوجيا ذات الصلة لمهاجمة شبكات الكمبيوتر المرتبطة بالموارد المدنية والعسكرية و/ أو الحكومية المستندة إلى المعلومات".[٣] ولكن هذا المعنى واسع، ويشمل الإرهاب السيبراني، والتجسس عبر الإنترنت وهو ما يخرج عن إطار الحرب السيبرانية.

---

[١] Michael N. Schmitt, Computer Network Attack and The Use of Force in International Law: Thoughts on a normative framework, Columbia journal of transnational law, 1998- 1999, Vol. 37, P890.

[٢] Papanastasiou Afroditi, 'Application of International Law in Cyber Warfare Operations', Electronic copy available at: https://ssrn.com/abstract=1673785

[٣] *Ibid.*

كذلك، يعرِّف مايكل هايدن Michael Hayden مدير وكالة الأمن القومي الأمريكي، ووكالة المخابرات المركزية الأمريكية السابق الحرب السيبرانية بأنها: "محاولة متعمدة لتعطيل أو تدمير شبكات الكمبيوتر لدولة أخرى".[١] إلا أن هذا التعريف يشمل في مضمونه الجرائم السيبرانية والهجوم السيبراني والحرب السيبرانية، كما أن هذا التعريف غير دقيق؛ لأنه لا يمكن للحرب أن تُعرف بأنها مجرد مُحاولة.

فيما يرى Mehan أنَّ للحرب السيبرانية مفهومًا واسعًا ينضوي تحته عدة فئات وهي: الفئة الأولى: وتشمل الهجمات ضد أمن المعلومات الشخصية، الفئة الثانية: وتشمل أنشطة التجسس عبر الفضاء السيبراني، الفئة الثالثة: تشمل الأعمال التخريبية ضد مزود الخدمة Distributed Denial of Service (DDoS) والأعمال التخريبية الأخرى، والفئة الرابعة: تتضمن الفئات من الأول إلى الثالث بالإضافة إلى العمليات السيبرانية لدعم الهجوم العسكري.[٢] وينتقد Ashraf هذا التعريف باعتبار أنه يوسع

---

[١] " deliberate attempt to disable or destroy another country's computer networks". Tom Gjelten, Extending the Law of War to Cyberspace, NAT'L PUB. RADIO (Sept. 22, 2010), available at: http://www.npr.org/templates/story/story.php?storyId=130023318

[٢] Julie E. Mehan, CyberWar, CyberTerror, CyberCrime (Ely: IT Governance Publishing, 2008)

بشكل كبير من الحرب السيبرانية، بحيث لا يمكن معرفة أطرافها أو طبيعة الأعمال المرتكبة فيها على وجه التحديد فهي مفتوحة للقراصنة، والأفراد والجماعات، والحركات الاجتماعية، والإرهابيين، والشركات، والدول.[١]

ولعل أكثر التعريفات تداولاً هو تعريف الخبير الأمني الأمريكي ريتشارد كلارك Richard Clarke الذي يعرف الحرب السيبرانية بأنها "أفعال من قبل الدولة لاختراق أجهزة الكمبيوتر أو الشبكات الخاصة بدولة أخرى؛ من أجل إحداث ضرر أو تدمير".[٢]

كما ورد في قرار مجلس الأمن رقم ١١١٣ لعام ٢٠١١، تعريفًا للحرب السيبرانية على أنها: "استخدام أجهزة الكمبيوتر، أو الوسائل الرقمية من قبل الحكومة، أو بمعرفة صريحة، أو الموافقة على ذلك حكومة ضد دولة أخرى، أو ملكية خاصة داخل دولة أخرى، بما في ذلك، الوصول المتعمد إلى البيانات، أو اعتراضها، أو إتلافها رقميًّا أو

---

١ Cameran Ashraf, Defining cyberwar: towards a definitional framework, Defense & Security Analysis, (2021), pp.274-294.

٢ " actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption." Richard A. Clarke & Robert K. Knake, Cyber War: The Next Threat to National Security and What to Do About It, (2010)

إتلاف البنية الأساسية رقميًّا، وإنتاج وتوزيع الأجهزة التي يمكن استخدامها لتخريب الأنشطة المحلية".[١]

ولكننا نميل للتعريف الذي وضعه Greathouse وهو أن الحرب السيبرانية هي "تلك التي تُدار عن طريق استخدام تكنولوجيا الحاسوب وشبكات الإنترنت، وميدانها هو الفضاء الإلكتروني ، وتستهدف منظومة العدو الحاسوبية لتعطيلها أو شل قدرتها، مما يؤدي لأضرار جسيمة بعمل مؤسسات العدو أو البنية التحتية لديه، ويُعرض أمنه القومي للخطر".[٢]

وبذلك، فإنَّ الحرب السيبرانية الناجحة تعتمد على عنصرين: "الوسائل" التي يتم بها شن الحرب، وتشمل الأشخاص، والأدوات، والأسلحة السيبرانية، و"ضعف الخصم"

[١] "Cyber warfare is the use of computers or digital means by a government or with explicit knowledge of or approval of that government against another state, or private property within another state including: intentional access, interception of data or damage to digital and digitally controlled infrastructure. And production and distribution of devices which can be used to subvert domestic activity". UN Security Council, Resolution 1113 (2011), 5 March 2011.

[٢] Craig B. Greathouse, Cyber War and strategic thought: Do the Classic And theorists Still Matter? in J. F Kremer and B. Muller Eds Cyberspace international Relations (Verlog Berlin Heidelberg Spriner 2014), p.22.

ويعتمد على مدى اعتماد الخصم على الإنترنت أو شبكات المعلومات، وقدرة قوته السيبرانية. ولذلك، فإن الدول تسعى أكثر من أي وقت مضى إلى توظيف قوات سيبرانية ماهرة.[١]

القوات السيبرانية/ الجيش السيبراني Cyber force:

سعت عدة دول - في الآونة الأخيرة - إلى إنشاء قسم سيبراني تابع لقواتها العسكرية،[٢] ويُعرف أيضًا بـ "الجيش السيبراني"، ويتكون هذا الجيش من خبراء في مجال البرمجة وتكنولوجيا المعلومات، وعادةً ما يكون عملهم سريًّا، وتركز مهامهم على الدفاع عن أمن الدولة المعلوماتي، وشن هجمات سيبرانية ضد الأعداء في حالة

---

١ James A. Lewis & Katrina Timlin, Cybersecurity and Cyberwarfare 2011, Washington D.C., CSIS, UNIDIR. Available at: https://unidir.org/sites/default/files/publication/pdfs//cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf

٢ Papanastasiou Afroditi, Application of International Law in Cyber Warfare Operations, op.cit., p.8.

الضرورة.[1] وتشير الاتجاهات الحالية إلى أن كل دولة سيكون لها – في المستقبل – "جيش سيبراني" كفرع عسكري مستقل داخل جيوشها النظامية.[٢]

وتُعتَبر الولايات المتحدة، والصين، وروسيا، وإسرائيل من أقوى الدول التي تملك قدرات سيبرانية هجومية قوية، أما الدول التي لا تملك جيوشًا سيبرانية، فتلجأ إلى توظيف مجموعة من المتسللين لتنفيذ الهجمات السيبرانية. ومع ذلك – وإلى الآن – فإنه من الصعب إسناد هجوم سيبراني معين لدولة معينة؛ نظرًا للطبيعة المتخفية للهجمات السيبرانية. فعلى سبيل المثال، يشير العديد من الكتابات إلى أن روسيا هي المتسببة

[1] ومن أقوى الجيوش السيبرانية على مستوى العالم: الجيش الأمريكي، حيث أعلن دونالد ترامب أنه جرى تطوير القيادة القتالية السيبرانية فيه كوحدة مستقلة بذاتها داخل الجيش الأمريكي. وكذلك، الجيش الصيني الأزرق، أنشأته الصين عام ٢٠١٥، لحماية الفضاء السيبراني الصيني. الجيش الروسي، حيث أعلنت روسيا عام ٢٠١٧، عن امتلاكها جيشًا سيبرانيًا لحماية فضائها السيبراني، الجيش الإسرائيلي، وهو وحدة متعددة التخصصات داخل الجيش ومنها وحدة الإشارة في صحراء النقب. الجيش البريطاني، أعلنت بريطانيا في ٢٠١٥، عن برنامجها للتصدي للهجمات السيبرانية من خلال وحدة متخصصة داخل جيشها.
ما هي الحرب السيبرانية، وما مدى خطورتها؟ مقال منشور على CyberOne، متاح على:
https://cyberone.co/%D9%85%D8%A7-%D9%87%D9%8A-%D8%A7%D9%84%D8%AD%D8%B1%D8%A8-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9/

[٢] SJ Lukasik, SE Goodman & DW Longhurst, 'Protecting Critical Infrastructures Against Cyber-Attack', OUP New York, 2003

في الهجمات السيبرانية على إستونيا عام ٢٠٠٧، وجورجيا عام ٢٠٠٨، وأن الصين تسببت في عدد من الهجمات السيبرانية، وأن إسرائيل هي المسئولة عن الهجوم السيبراني على المنشآت النووية الإيرانية، ولكن لم تعلن أي دولة منها عن القيام بأيٍّ من الهجمات المنسوبة إليها، كما لا يوجد دليل جازم على تورط القيادة السياسية لأي من تلك الدول في شن هذه الهجمات.

المطلب الثاني

تمييز السيبرانية عن غيرها من المفاهيم

يختلط مفهوم السيبرانية بغيره من المفاهيم، فالبعض يشير إلى الحرب السيبرانية والحرب الإلكترونية باعتبارهما مترادفين،[١] بالرغم من أن لكل منهما مفهومه المختلف عن الآخر. كذلك الحال، توجد بعض أوجه التشابه والاختلاف بين استخدام الأسلحة السيبرانية وأسلحة الذكاء الاصطناعي. ولذلك، لزم التفريق بين كل منهما، وذلك على نحو ما يلي.

[١] على سبيل المثال: عمر محمود أعمر، الحرب الإلكترونية في القانون الدولي الإنساني، دراسات علوم الشريعة والقانون، المجلد ٤٦، عدد ٣، ٢٠١٩، ص ١٣٤-١٥٥.

أولاً: الحرب السيبرانية والحرب الإلكترونية:

يختلف الاستخدام القانوني لمصطلح "السيبراني" عن مصطلح "الإلكتروني"؛ إذ يشير مصطلح "الإلكتروني" إلى "الآلات والأجهزة التي تتطلب تيارات كهربائية لتشغيلها، والتي تستخدم الرقائق الدقيقة والترانزستورات لتوجيه هذا التيار"، مثل أجهزة الكمبيوتر، وأجهزة الراديو، والتليفزيون، والهواتف المحمولة،[١] ولكنها ليست بالضرورة أجهزة سيبرانية. وفي المجال العسكري، فإنَّ مصطلح "الهجوم الإلكتروني" ينطبق على الاستعمال الحربي للمجال الكهرومغناطيسي، ويتخذ عدة أشكال، منها: التشويش على اتصالات العدو أو الرادار، وتعطيل معداته باستخدام مستويات مرتفعة من الطاقة الميكروويفية.[2]

[١] انظر في المقصود من مصطلح "إلكتروني" بالمعنى اللغوي والفني:
https://www.vocabulary.com/dictionary/electronic

[2] سهيلة هادي، الحروب الإلكترونية في ظل عصر المعلومات، مجلة رؤى استراتيجية، يوليو ٢٠١٧، ص١٢٧. كذلك ففي حين يوجد لدى مصر "سلاح الحرب الإلكترونية"، وهي إدارة تابعة لوزارة الدفاع المصرية، وتم إنشاؤها عام ١٩٦٨، وتتضمن منظومات استطلاع راداري واستطلاع لاسلكي وإعاقة راداري وإعاقة لاسلكي؛ إلا أنه لا توجد أية مصادر تُشير إلى امتلاك مصر سلاح سيبراني.

وتُعرف الحرب الإلكترونية بأنها: "استخدام الطاقة الكهرومغناطيسية أو الموجهة، والقدرات الإلكترونية المتكاملة لتنفيذ المهام العسكرية والاستخباراتية، ويشمل ذلك استخدام الطيف الكهرومغناطيسي الكامل – الموجات الراديوية، والميكروويف، والموجات المليمترية، والأشعة تحت الحمراء، والضوء المرئي، والأشعة فوق البنفسجية، وأشعة جاما".[١]

ومن أشهر أشكال نظم الأسلحة الإلكترونية: الإجراءات المضادة للتهديدات المتقدمة بالأشعة تحت الحمراء (ATIRCM)، أنظمة الحماية الإلكترونية ضد التشويش، الصواريخ المضادة للإشعاع (ARM)، أنظمة التحذير الشائعة من الصواريخ (CMWS)، أنظمة موزع الإجراءات المضادة (CMDS)، أسلحة الطاقة الموجهة، أنظمة التحكم في الانبعاثات (EMCON)، أجهزة استشعار متعددة الأطياف، جهاز استقبال تحذير الرادار (RWR)، مستقبل تحذير الليزر (LWR)، الإجراءات المضادة للترددات الراديوية (RFCM)، وغيرها.[٢] ولذلك، فبدون امتلاك وسائل حرب إلكترونية

---

[١] Tallinn Manual, op.cit., p.565.

[٢] للمزيد حول أشكال الأسلحة ونظم الأسلحة الإلكترونية، انظر: وليد غسان سعيد جلعود، دور الحرب الإلكترونية في الصراع العربي الإسرائيلي، رسالة ماجستير – جامعة النجاح الوطنية، ٢٠١٣، ص ٩٠ وما بعدها. متاح على الرابط التالي:

متطورة، يمكن للعدو أن يشوش على نظام الملاحة الجوية، الذي يعد عاملاً أساسيًّا في عمل القذائف عالية الدقة، كما يمكن أن يؤدي إلى فقدان الصواريخ الموجهة لمسارها، وتقل قدرة الدولة على حماية فضائها الجوي باستخدام وسائل الدفاع الجوي التقليدية، كلما قلت قدرتها على امتلاك الأسلحة الإلكترونية وتوظيفها بالشكل الأمثل.[١]

https://scholar.najah.edu/sites/default/files/%D9%88%D9%84%D9%8A%D8%AF%20%D8%AC%D9%84%D8%B9%D9%88%D8%AF.pdf

[١]وتتكون قوة الحرب الإلكترونية التابعة لأي جيش من ثلاثة أقسام هي: الأولى: وحدات الهجوم الإلكتروني: وتعتمد على بث موجات مركزة تتداخل مع الموجات الخاصة برادارات العدو ووسائل اتصاله، وتؤدي إلى شل قدرتها على تمييز الموجات الخاصة برصد أهداف معادية، إضافة إلى تداخلها مع موجات الاتصال الخاصة بالعدو. والثانية: وحدات الحماية: وسائل الحماية الإلكترونية تقوم بزيادة قوة وسائل الرصد والاستشعار الخاصة بالحرب الإلكترونية، لزيادة قدرتها على مواجهة أي تشويش، أو التقليل من قوته. والثالثة: قوات للدعم، وتقوم بالبحث عن مصدر التشويش الإلكتروني المعادي، ومحاولة اعتراضه والتعرف عليه، تمهيدا لشن هجوم مضا. انظر: الحرب الإلكترونية العسكرية... سلاح "غير مرئي" يصيب الجيوش بـ"شلل تام"، متاح على الرابط التالي: https://sputnikarabic.ae/20191001/%D8%A7%D9%84%D8%AD%D8%B1%D8%A8-%D8%A7%D9%84%D8%A5%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A%D8%A9-%D8%A7%D9%84%D8%B9%D8%B3%D9%83%D8%B1%D9%8A%D8%A9-%D8%B3%D9%84%D8%A7%D8%AD-%D8%BA%D9%8A%D8%B1-%D9%85%D8%B1%D8%A6%D9%8A-

وتتشابه الأسلحة السيبرانية مع الأسلحة الإلكترونية في أن كليهما يُنفذ مهمته بشكل غير مرئي، فلا يمكن رؤية الموجات الكهرومغناطيسية، أو الترددات الراديوية باعتبارها أسلحة إلكترونية، كذلك الحال في الأسلحة السيبرانية فلا يمكن رؤية برامج الفيروسات أو البرامج الضارة malware.

غير أن هناك عددًا من أوجه الاختلاف، ومنها:

أولاً: أن الأسلحة الإلكترونية بعضها محرم دوليًا، لأنها تُسبب آلامًا أو أضرارًا لا مبرر لها، ومنها بعض أسلحة الليزر المحظورة بموجب البروتوكول الرابع لحظر أسلحة الليزر المسببة للعمى لعام ١٩٩٥، الملحق باتفاقية حظر أو تقييد استعمال أسلحة تقليدية معينة يمكن اعتبارها مفرطة الضرر أو عشوائية الأثر لعام ١٩٨٠،

%D9%8A%D8%B5%D9%8A%D8%A8-
%D8%A7%D9%84%D8%AC%D9%8A%D9%88%D8%B4-
%D8%A8%D9%80%D8%B4%D9%84%D9%84-
%D8%AA%D8%A7%D9%85-1043031829.html

بصيغتها المعدلة في ٢١ ديسمبر ٢٠٠١ (اتفاقية الأسلحة التقليدية).[1] في حين أن الأسلحة السيبرانية لم يثبت أنها سببت آلامًا أو أضرارًا لا مبرر لها إلى الآن.

ثانيًا: تعتمد أسلحة الحرب الإلكترونية على توظيف موجات الراديو والرادار، والأشعة تحت الحمراء، ووسائل الرؤية الرقمية، والأشعة فوق البنفسجية، وتقنيات الليزر في مهاجمة العدو، في حين تعتمد الأسلحة السيبرانية على توظيف البرمجيات الخبيثة malware، وهجمات منصات الخوادم Client-Server Platform Attacks، وهجمات رفض الخدمة الموزعة DDOS Distributed Denial of Service في مهاجمة العدو، واستهداف البنى التحتية الحيوية، مثل: حجب الخطوط الأرضية الوطنية أو شبكة الهاتف، أو تعطيل حركة المطار والتسبب في إسقاط طائرة عن طريق قطع الطاقة عن أبراج التحكم في الحركة الجوية. [٢]

---

[1] استعراض الأسلحة الجديدة: نظرة عامة، مقال على الموقع الإلكتروني للجنة الدولية للصليب الأحمر.
https://www.icrc.org/ar/doc/war-and-law/weapons/new-weapons/overview-review-of-new-weapons.htm

[٢] Papanastasiou Afroditi, Application of International Law in Cyber Warfare Operations, op.cit., p.10.

ثالثًا: إنَّ الحرب الإلكترونية تحتاج إلى مقاتلين مدربين على استخدام الأسلحة الإلكترونية، كما أن تكلفة شراء هذه الأسلحة كبير، في حين أن الحرب السيبرانية تكلفتها رخيصة نسبيًّا، فلا تتطلب مقاتلًا ذا مهارات قتالية، وكافة معداتها زهيدة الثمن مقارنة بالأسلحة الإلكترونية، أو حتى الأسلحة التقليدية.

ثانيًا: الأسلحة السيبرانية والأسلحة ذاتية التشغيل:

عرف دليل وزارة الدفاع الأمريكية لعام ٢٠١٢، الأسلحة ذاتية التشغيل بأنها:[١] "منظومات سلاح آلية، تستطيع في حال تشغيلها، أن تختار الأهداف، وتشتبك معها، دون حاجة إلى تدخل إضافي من مشغلها البشري". ويعرفها تقرير فقدان الإنسانية: "القضية ضد الروبوتات القاتلة" الصادر عن منظمة مراقبة حقوق الإنسان، بأنها: [٢]

---

[١] Kenneth Anderson & Matthew C. Waxman, Debating Autonomous Weapon Systems, Their Ethics, And Their Regulation Under International Law, American University Washington College of Law, Washington College of Law Research Paper No. 2017-21

[٢] Losing Humanity: The Case Against Killer Robots, Human Rights Watch (2012), p.2, available at: https://www.hrw.org/report/2012/11/19/losing-humanity/case-against-killer-robots

١. نظم أسلحة يكون العنصر البشري فيها خارج دائرة القرار، بمعنى أن تكون تلك الأسلحة قادرة على اختيار أهدافها، والاشتباك معها بدون أي تدخل بشري؛ أو

٢. نظم أسلحة يكون العنصر البشري فيها ضمن دائرة القرار، بمعنى أن يكون المشغل البشري قادرًا على الإشراف على اختيار الماكينة لأهدافها والاشتباك معها.

ويعرفها دليل وزارة الدفاع بالمملكة المتحدة بأنها:

"أنظمة قادرة على فهم النوايا والاتجاهات ذات المستوى العالي، وبناءً على هذا الفهم وعلى إدراكها للبيئة، تستطيع اتخاذ الإجراء المناسب لتحقيق النتيجة المطلوبة، كما أنها قادرة على تحديد مسار عملها، وانتقائه من بين مجموعة من البدائل بدون الاعتماد على الإشراف أو التحكم البشري".[١]

[١] ترجمة من قبل المؤلف بتصرف، الأصل الإنجليزي:
"An autonomous system is capable of understanding higher-level intent and direction. From this understanding and its perception of its environment, such a system is able to take appropriate action to bring about a desired state. It is capable of deciding a course of action, from a number of alternatives, without depending on human oversight and control,

١٢- مدى انطباق القانون الدولي الإنساني على الهجمات السيبرانية

وتتشابه الأسلحة السيبرانية مع الأسلحة ذاتية التشغيل في أن كلًّا منها يستخدم تكنولوجيا فائقة التطور للاستهداف، أما أوجه الاختلاف، فتتمثل في الآتي:

أولاً: أن استخدام الأسلحة ذاتية التشغيل يؤدي لتبعات عنيفة في الغالب مثل إصابات، أو وفاة بين الأشخاص، أو تدمير للممتلكات، في حين أن استخدام الأسلحة السيبرانية لا يؤدي لتبعات عنيفة في الغالب، فأغلب الخسائر تكون في الفضاء السيبراني، وعادة ما تكون مؤقتة أيضًا.

ثانيًا: أن الأسلحة ذاتية التشغيل تعتمد على الذكاء الاصطناعي بشكل كبير، أما الأسلحة السيبرانية فإن تفعيلها والتحكم فيها يعتمد على التدخل البشري.

---

although these may still be present. Although the overall activity of an autonomous unmanned aircraft will be predictable, individual actions may not be"

United Kingdom Ministry of Defense, 2017, Unmanned Aircraft Systems, Joint Doctrine Publication 0-30.2, p. III, available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/640299/20170706_JDP_0-30.2_final_CM_web.pdf

ثالثًا: أن الأسلحة ذاتية التشغيل كلفتها عالية، وتتطلب قدرًا من الخبرة والمهارة في تشغيلها، في حين أن الأسلحة السيبرانية رخيصة الثمن ومن السهل الوصول إليها، ولذلك قد تمتلكها الدول الغنية والفقيرة.

المبحث الثاني

الهجمات السيبرانية الخاضعة للقانون الدولي الإنساني

سبق وأن عرضنا لبعض الأمثلة على الهجمات السيبرانية الحديثة مثل الهجوم السيبراني ضد جورجيا عام ٢٠٠٨، وضد البرنامج النووي الإيراني عام ٢٠١٠، وفي شبه جزيرة القرم عام ٢٠١٤. وقد تراوحت هذه الهجمات ما بين إثارة المعارضة الشعبية ضد الحكومة، والتسبب في تعطل منشأة عسكرية لفترة عن العمل، ولكن في كل هذه الحالات لم تُسفر الهجمات السيبرانية عن وقوع خسائر بشرية.[١]

[١] كوردولا دوريجي، " لا تقترب من حدود فضائي الإلكتروني: الحرب الإلكترونية والقانون الدولي الإنساني وحماية المدنيين"، المجلة الدولية للصليب الأحمر، مجلد ٩٤ العدد ٨٨٦، صيف ٢٠١٢ ، ص 578 – 533 ، متاح على الرابط التالي: https://cutt.ly/Okp7S5Z

١٢- مدى انطباق القانون الدولي الإنساني على الهجمات السيبرانية

وحيث إن القانون الدولي الإنساني يُطبق في حالة وجود نزاع مسلح،[١] فهل تفي الهجمات السيبرانية بـ "عتبة" النزاع المسلح، وبالتالي ينطبق عليها القانون الدولي الإنساني؟

للإجابة على هذا السؤال ينبغي التفريق بين حالتين:

الحالة الأولى: وجود نزاع مسلح قائم بالفعل، وفي هذه الحالة فإن الهجمات السيبرانية تعد مكونًا أو جانبًا من العمليات العدائية المستمرة داخل هذا النزاع المستمر، ومثال ذلك، الهجمات السيبرانية بين روسيا وجورجيا عام ٢٠٠٨، كانت ضمن نزاع مسلح دولي، وبالتالي فهي خاضعة لقواعد القانون الدولي الإنساني أيًّا كانت تبعاتها، ولا خلاف في ذلك.

---

[١] مصطلح "نزاع مسلح" تم استخدامه لأول مرة في قانون تدوين الحرب في اتفاقيات جنيف لعام ١٩٤٩ ، ولكن لم يتم تعريفه رسميًا. ومع ذلك ، فقد حل محل مصطلح "الحرب" في القانون الدولي. ويشير النزاع المسلح إلى حالة تنطوي على أعمال عدائية، بما في ذلك تلك التي يتم إجراؤها باستخدام الوسائل السيبرانية. مع ملاحظة بعض الحالات التي تنطوي على استثناءات من استخدام أعمال عنف مسلح مثل حالات الاحتلال التي لا يقابلها أي نوع من المقاومة (اتفاقية جنيف الرابعة مادة٢).

Tallinn Manual, op.cit., p. 375.

الحالة الثانية: عدم وجود نزاع قائم بالفعل، في هذه الحالة هل الهجمات السيبرانية – التي تحدث في غياب نزاع مسلح حركي Kinetic Armed Conflict قائم بالفعل – تخضع للقانون الدولي الإنساني؟

بدايةً، فإن القانون الدولي الإنساني لا يطبق إلا في حالة وجود نزاع مسلح، ولم يعرف القانون الدولي الإنساني المقصود بـ "النزاع المسلح"، ولكنه توسع في التمييز بين نوعين من النزاعات المسلحة وهما: النزاع المسلح الدولي، والنزاع المسلح غير الدولي.

وعليه، سنتعرض لتوضيح المقصود بالهجمات السيبرانية التي تُشن في سياق كل نوع من هذين النوعين، لنتتبع إمكانية انطباق القانون الدولي الإنساني على تلك الهجمات في كل سياق منهما، كلٌّ في مطلب مستقل. وبالتالي، نتوصل لمفهوم الهجمات السيبرانية التي ينطبق عليها القانون الدولي الإنساني.

المطلب الأول

الهجمات السيبرانية في إطار النزاع المسلح الدولي

يعرف التعليق الرسمي للجنة الدولية للصليب الأحمر على اتفاقيات جنيف النزاع المسلح الدولي بأنه: "خلاف ناشئ بين دولتين من شأنه أن يُفضي إلى تدخل من

جانب أفراد القوات المسلحة .. حتى وإن أنكر أحد الطرفين وجود حالة حرب .. بما فيها حالات الاحتلال في غياب حالة الحرب".[١] وبالمثل، فإن المحكمة الجنائية الدولية ليوغوسلافيا السابقة تعرف النزاعات المسلحة الدولية بأنها "توجد حيثما يكون هناك لجوء إلى القوة بين الدول".[٢]

وفقًا لذلك، فإن النزاع المسلح يبدأ حينما يكون هناك تبادل في الأعمال العدائية المسلحة بين الدول، بغض النظر عن حجم الأعمال العدائية وآثارها.[٣] وعند تطبيق ذلك على الهجمات السيبرانية، فإنه ينبغي التمييز بين نوعين من الهجمات السيبرانية،

---

[١] J. Pictet, Commentary on the Geneva Conventions of 12 August 1849, p.28. available at: https://www.loc.gov/rr/frd/Military_Law/pdf/GC_1949-I.pdf

[٢] Prosecutor v. Tadic, Case No. IT-94-1-A, Appeals Chamber Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, ¶ 70 (Int'l Crim. Trib. for the Former Yugoslavia Oct. 2, 1995).

[٣] "The International Group of Experts agreed that a conflict is international if two or more States are involved as parties on opposing sides. It also agreed that a conflict is international when an organized armed group that is under the 'overall control' of one State engages in hostilities against another State (see discussion below). As a practical matter, it may be difficult to ascertain whether a State is controlling a non-State actor's cyber activities" Tallinn Manual, op.cit., p. 3. ٨٠.

الأول: الهجمات السيبرانية التي تؤدي إلى تبعات عنيفة، مثل: تلف أو تدمير الأشياء أو إصابة أو وفاة الأفراد في دولة أخرى، **والثاني:** الهجمات السيبرانية التي لا تخلف دمارًا أو إصابات مادية، وإنما يقتصر أثرها على مجرد إزعاج، أو اضطراب، أو تهيج، أو على أقصى تقدير تؤثر على الاقتصاد أو نظام النقل، أو البنية التحتية الحيوية الأخرى. مع العلم أنَّ معظم الهجمات السيبرانية تندرج تحت النوع الثاني من الهجمات.

أولاً: الهجمات السيبرانية التي تؤدي إلى تبعات عنيفة:

تعرف المادة ١/٤٩ من البروتوكول الإضافي الأول[١] الهجمات بأنها: "أعمال العنف الهجومية والدفاعية ضد الخصم". وقد كان المقصود من "أعمال العنف" خلال المؤتمرات التحضيرية لوضع البروتوكول أعمال العنف المادي التي تتم بشكل حركية فقط Kinetic actions. إلا أنه مع التطور العلمي الحديث، واستخدام الأسلحة البيولوجية والكيماوية في النزاعات المسلحة، تم توسيع المقصود من كلمة "أفعال

[١] البروتوكول الإضافي الأول هو بروتوكول عام ١٩٧٧، الإضافي الأول الملحق باتفاقيات جنيف لعام ١٩٨٩، والخاص بحماية ضحايا المنازعات المسلحة الدولية (ويُشار إليه فيما بعد بالبروتوكول الإضافي الأول). انظر لنصوص البروتوكول كاملة:
https://www.icrc.org/ar/resources/documents/treaty/protocol-i-additional-to-the-geneva-conventions

العنف" الواردة بالبروتوكول لتشمل العمليات العسكرية التي تؤدي إلى تبعات عنيفة، حتى وإن كان الفعل المكون لها غير عنيف، وذلك مثل الأسلحة البيولوجية والكيماوية، إذ قد تتم الهجمات من خلال إتيان أفعال غير عنيفة، مثل إطلاق حيوان ملوث بمرض لنشره بين السكان؛ إلا أن آثارها تؤدي إلى الوفاة، أو الإصابات الخطيرة وبالتالي فهي تؤدي إلى تبعات عنيفة.[١]

وبتطبيق هذا المفهوم على الهجمات السيبرانية، فهي هجمات تتم من خلال إتيان أفعال غير عنيفة؛ إذ إنها مجرد دخول في الفضاء السيبراني لإحداث التأثير المطلوب عن طريق برنامج ضار، وهي بذلك أفعال غير عنيفة في طبيعتها، وإنما تؤدي لتبعات عنيفة. فعلى سبيل المثال، فإن الأفعال التي تستهدف إحداث تعطل في نظام الطائرات المُحلقة (أفعال غير عنيفة)، تؤدي لحدوث وفيات، أو إصابات بليغة للأشخاص، أو أضرار بالأعيان (تبعات عنيفة)، وبالتالي فهي تقع ضمن مفهوم الهجوم الوارد في البروتوكول الإضافي الأول. ويتفق ذلك مع التعريف الوارد في دليل تالين للهجوم السيبراني بأنه: "عملية سيبرانية، هجومية أو دفاعية، يتوقع منها بشكل

[١] كوردولا دوريجي، لا تقترب من حدود فضائي الإلكتروني، المرجع السابق، ص٥٤٠.

معقول أن تحدث إصابة أو وفاة في صفوف الأشخاص أو أضرارًا أو دمارًا في الأعيان".[١]

ثانيًا: الهجمات السيبرانية التي لا تؤدي إلى تبعات عنيفة:

إن كافة الهجمات السيبرانية غير عنيفة في طبيعتها، وهذا لا خلاف فيه. أما تبعاتها، ففي معظم الأحوال، هي تبعات غير عنيفة، وغير مباشرة في العالم المادي، ومثال ذلك، الأفعال التي تستهدف إحداث تعطل في تدفق البيانات – على سبيل المثال – قد تؤدي لفقدان القدرة على الاتصال بالعالم الخارجي، أو مباشرة الأنشطة التجارية أو غيرها. فهل تندرج ضمن مفهوم "الهجوم" الوارد في البروتوكول الإضافي الأول؟

يوجد اتجاهان في الفقه في هذا الشأن، يذهب الاتجاه الأول[٢] إلى أنَّ الهجوم الذي لا يؤدي إلى إضرار مادي بالأشخاص سواء كانوا مدنيين أو عسكريين، أو تدمير

[١] " 'Cyber attacks' is a term of art referring to a specific category of cyber operations. Certain cyber operations, such as those affecting the delivery of humanitarian assistance (Rule 145), are governed by the law of armed conflict even if they do not rise to the level of an 'attack'". Tallinn Manual, op.cit., p. 37.

[٢] Prof. Schmitt elaborates that "A cyber operation that is intended, but fails, to generate such results would be encompassed in the concept, in much

الأعيان سواء أكانت أعيانًا مدنية أو عسكرية لا يعد هجومًا بمفهوم المادة ١/٤٩ من البروتوكول الإضافي الأول. ولا يُستثنى من ذلك العمليات السيبرانية، فطالما أنها لا تؤدي إلى معاناة بشرية، ويقتصر تأثيرها على الإزعاج أو تعطيل العمل في الأعيان، فهي ليست هجمات بمفهوم البروتوكول الإضافي الأول.

وهذا الاتجاه يتوافق مع حقيقة أن القانون الدولي الإنساني لا ينطبق إلا بعد أن يصبح النزاع "مسلح"، ولكن على الرغم من ذلك، فهناك أعمال غير مؤذية للأشخاص والأشياء ومع ذلك تعتبر نزاعًا مسلحًا مثل الاحتلال والاحتجاز غير المتنازع عليهما، فكليهما يعتمد على إمكانية التنفيذ بدون استخدام القوة. فيعرف التعليق الرسمي للجنة الدولية للصليب الأحمر على اتفاقيات جنيف النزاع المسلح الدولي بأنه: "خلاف ناشئ بين دولتين من شأنه أن يُفضي إلى تدخل من جانب أفراد القوات المسلحة .. حتى وإن أنكر أحد الطرفين وجود حالة حرب .. بما فيها حالات الاحتلال في غياب حالة

---

the same way that a rifle shot that misses its target is nevertheless an attack in IHL. Similarly, one expected to cause collateral damage to civilian objects or incidental harm to civilians would qualify, even if no harm befell . Michael N. Schmitt, Cyber Operations and "the military objective targeted the Jus in Bello: Key Issues, International Law Studies, Vol. 87, 2011, p. 91.

الحرب".[١] وتنص المادة ١/٢ المشتركة، على أن اتفاقيات جنيف لعام ١٩٤٩، تُطبق في "كل حالات إعلان الحرب الأخرى، أو حالات النزاع المسلح التي يمكن أن تنشأ بين دولتين أو أكثر من الدول السامية المتعاقدة، حتى ولو كانت حالة الحرب غير معترف بها بينها".

وبالتالي، فهناك حالات تعتبر نزاعًا مسلحًا دوليًا ولا تنطوي بالضرورة على أفعال عنف مثل الاحتلال في غياب حالة الحرب مثلاً. وبالقياس على ذلك، فإن الهجمات السيبرانية التي لا تؤدي إلى عنف مثل: استغلال الشبكة والحرمان من الخدمة، قد تعتبر نزاعًا مسلحًا، ويطبق عليها القانون الدولي الإنساني.[٢]

كذلك، هذا الاتجاه مردود عليه بأن أثر "تعطيل العمل في الأعيان" – إذا كان تعطيلًا كليًا أو جوهريًا – يُساوي تدميرها؛ إذ حينها ستصبح العين المدنية أو العسكرية عديمة النفع؛ وبالتالي يتحقق الإضرار بالعدو. من ناحية أخرى، فإن هذا الاتجاه يؤدي إلى استنتاج مفاده أن تدمير منزل واحد عن طريق القصف يعد هجومًا، في حين أن

---

[١] J. Pictet, Commentary on the Geneva Conventions of 12 August 1849, op.cit., p.28.

[٢] Michael N. Schmitt, Cyber Operations and the Jus in Bello: Key Issues, op.cit., p.93.

تعطيل شبكة الكهرباء في مدينة ما والتي قد يمتد أثرها لآلاف الأميال ويستفيد منها ملايين السكان لا تعد كذلك.

أما الاتجاه الثاني،[١] فيذهب إلى أن الهجمات السيبرانية هي هجمات بمفهوم البروتوكول الإضافي الأول، وإن لم تؤد إلى أضرار مادية ملموسة؛ استنادًا إلى المادة ٢/٥٢ من البرتوكول الأول المتعلقة بالهجمات الموجهة ضد الأهداف العسكرية؛ إذ تنص على أن "تقصر الهجمات على الأهداف العسكرية فحسب، وتنحصر الأهداف العسكرية فيما يتعلق بالأعيان على تلك التي تسهم مساهمة فعالة في العمل العسكري سواء كان ذلك بطبيعتها أم بموقعها أم بغايتها أم باستخدامها، والتي يحقق تدميرها التام أو الجزئي أو الاستيلاء عليها أو تعطيلها في الظروف السائدة حينذاك ميزة عسكرية أكيدة".[٢] فالمعنى العادي لعبارة "تعطيلها في الظروف السائدة" يتضمن تعطيلها من خلال إحداث خلل في النظم المشغلة، دون أن يؤدي هذا التعطيل بالضرورة إلى تدميرها، والذي قد يتأتى من خلال الهجمات السيبرانية.

---

[١] Knut Dörmann, Applicability of the Additional Protocols to Computer Network Attacks, available at: https://www.icrc.org/en/doc/assets/files/other/applicabilityofihltocna.pdf

[٢] المادة ٢/٥٢ من البروتوكول الإضافي الأول.

ولكن هذا الاتجاه يُفسر مصطلح "الهجوم" بشكل واسع وشديد العمومية، ويخلط بين مفهوم الهجوم وبين العمليات النفسية المشروعة التي تستهدف السكان المدنيين. فيجدر التفريق في هذا المقام بين أعمال الهجوم وما تعرف بأعمال المجهود الحربي، ففي حين أن الهجوم يشمل الأعمال التي تؤدى للإضرار بالخصم أو يحتمل أن ينتج عنها أضرار للخصم أو تدميره، ويجب أن يصل هذا الضرر إلى حد معين؛[١] فإنَّ أعمال المجهود الحربى تشمل – بوجه عام – جميع الأنشطة التي تساهم بشكل غير مباشر في إلحاق الهزيمة العسكرية بالخصم كإنتاج الأسلحة والمعدات العسكرية، وبناء الطرق، والمطارات، والجسور وغيرها من أعمال البنى التحتية خارج سياق العمليات العسكرية الملموسة.[٢] وفي حين يعتبر القانون الدولي الإنساني النوع الأول

[١] يعرف Verri الهجوم بأنه أعمال عنف يرتكبها المقاتل ضد عدو من أجل وضع حد لمقاومته وفرض التسليم بسلطته، ويعرفه Salmon بأنه مجموعة من الأعمال الهجومية أو الدفاعية والعمليات العسكرية التي ينفذها المقاتل في إطار نزاع مسلح.

See, Verri, Dictionary of International Law of Armed Conflicts, Geneva, ICRC, 1992; Salmon, Dictionnaire de droit international public, Bruxelles: Bruylant, 2001, P.550

[٢] إن توسيع مفهوم الأعمال العدائية ليشمل كل أعمال المجهود الحربى سيكون واسعاً جداً، حيث يشارك كل السكان تقريباً في الحروب الحديثة في أعمال المجهود الحربى ولو بصورة غير مباشرة ولا يمكن على أساسه اعتبار كل السكان مقاتلين.

من الأعمال "أعمال هجومية" لأنها تؤدي لتبعات عنيفة، لا يعتبر النوع الثاني من الأعمال كذلك.

من ناحية أخرى، يرى البعض أن الأسلحة السيبرانية مُصممة أساسًا للحصول على تبعات غير مباشرة وغير عنيفة في طبيعتها،[١] ومع ذلك، فقد تكون هذه التبعات خطيرة، كأن تؤدي إلى تعطيل البنية التحتية الحيوية للدول ومنها القطاع المالي، والطبي، والتجاري.[٢] ويرى البعض الآخر أن استخدام السلاح السيبراني يوفر للقادة

Prosecutor V. Strugar, Case No. IT-01-42-A, Judgment of 17 July 2008, ss 175-176

[١] Arimatsu, L., 'A treaty for governing cyberweapons: potential benefits and practical limitations', eds C. Czossesk, R. Ottis and K. Ziolkowski, 2012 4th International Conference on Cyber Conflict, Proceedings (NATO Cooperative Cyber Defence Centre of Excellence Publications: Tallinn, 2012), p. 97

[٢] D. Blake and J. S. Imburgia, '"Bloodless weapons"? The need to conduct legal reviews of certain capabilities and the implications of defining them as "weapons"', Air Force Law Review (2011), p. 161.

ميزة اختيار استخدام سلاح ليس له أثر حركي، في حالة إحساسهم بالضغط للتصرف في ظل أزمة معينة لكنهم قلقون من استخدام القوة.[١]

يرى Schmitt أن كلا الاتجاهين له وجاهته، فالاتجاه الأول يراعي الفهم التقليدي للقانون الدولي الإنساني ويطبقه كما هو موجود على حالة الهجمات السيبرانية، في حين أنَّ الثاني يحاول وضع فهم شامل لمفهوم الهجمات يتدارك عيوب الفهم التقليدي. فببساطة، فإن الاتجاه الأول *lex lata* (القانون كما هو موجود)، والثاني *lex ferenda* (القانون المستقبلي).[٢] ونؤيده، إلا أننا نُرجح الاتجاه الأول؛ إذ إنه ما يجري عليه العمل في الوقت الحالي، فمثلاً الهجوم السيبراني على إستونيا عام ٢٠٠٧، لم يرتفع لمستوى النزاع المسلح؛ وبالتالي لم يخضع للقانون الدولي الإنساني. وعلى العكس، فإن الهجمات السيبرانية التي حدثت عام ٢٠٠٨، على جورجيا والنزاع الجاري بين روسيا وأوكرانيا ينطبق عليهما القانون الدولي الإنساني؛ لأن الهجوم كان جزءًا من

[١] "Cyber operations may provide a non-kinetic option for leaders who feel pressure to act in a crisis, but who are wary of using force." Josh Rovner, Cyber War as an Intelligence Contest, WAR ON THE ROCKS (Sep. 16, 2019), https://warontherocks.com/2019/09/cyber-war-as-an-intelligence-contest/.

[٢] Michael N. Schmitt, Cyber Operations and the Jus in Bello: Key Issues, op.cit., p.99.

تأجيج النزاع، وكانت الهجمات السيبرانية معززة بأعمال عدائية على أرض الواقع ترقى إلى وصف نزاع مسلح.

المطلب الثاني

الهجمات السيبرانية في إطار النزاع المسلح غير الدولي

يركز البروتوكول الإضافي الثاني[١] على النزاعات المسلحة غير الدولية، وهي تلك النزاعات التي تكون أحد أطرافها دولة والطرف الآخر جماعة مسلحة،[٢] كما يدخل في مفهوم النزاعات المسلحة غير الدولية – بحسب نص المادة الثالثة المشتركة – أيضًا

[١] البروتوكول الإضافي الثاني هو بروتوكول عام ١٩٧٧ الإضافي الثاني الملحق باتفاقيات جنيف لعام ١٩٨٩ والخاص بحماية ضحايا المنازعات المسلحة غير الدولية (ويُشار إليه فيما بعد بالبروتوكول الإضافي الثاني). انظر لنصوص البروتوكول كاملة:
https://www.icrc.org/ar/doc/resources/documents/misc/5ntce2.htm

[٢] في دليل صادر عن الأمم المتحدة عام ٢٠٠٦ عُرِّفت الجماعات المسلحة بأنها: "الجماعات التي لديها القدرة على توظيف السلاح في استخدام القوة لتحقيق أهداف سياسية أو أيدولوجية أو اقتصادية، وينبغي ألا تخضع تلك الجماعات لسيطرة الدول التي تنشط فيها أو أن تكون في إطار هياكل عسكرية رسمية لدول أو تحالفات دول أو منظمات غير حكومية."
Guidelines on Humanitarian Negotiations with Armed Groups, UN publications, January 2006, available at: https://www.unicef.org/emerg/files/guidelines_negotiations_armed_groups.pdf

النزاعات التي يكون كافة أطرافها جماعات مسلحة. وحيث إن الهجمات السيبرانية غير مكلفة، فقد تكون هي السلاح الأمثل في الاستخدام من قبل الجماعات المسلحة، خاصة في النزاعات غير المتكافئة، والتي يكون أحد أطرافها دولة تملك تكنولوجيا متقدمة، والطرف الآخر جماعة مسلحة محدودة الإمكانات؛ فحينها يلجأ الطرف الضعيف إلى استخدام وسائل وأساليب غير تقليدية في قتاله ضد الطرف الأقوى لتعويض ضعفه.[١] وبالتالي، فإن الهجمات السيبرانية متصورة الحدوث بشكل أكبر في سياق النزاعات المسلحة غير الدولية.

كما سبق، فإن النزاع المسلح يبدأ حينما يكون هناك تبادل في الأعمال العدائية المسلحة بين أطراف النزاع، بغض النظر عن حجم الأعمال العدائية وآثارها.[٢] عند

---

[١] A. Al Aridi, How Hybrid Is Modern Warfare? (April 27, 2017). International Network of Doctoral Studies, 2017 – 5th International Conference of PhD Students and Young Researchers, How Deep Is Your Law? Brexit. Available at SSRN: https://ssrn.com/abstract=3064737, p.9

[٢] "The International Group of Experts agreed that a conflict is international if two or more States are involved as parties on opposing sides. It also agreed that a conflict is international when an organized armed group that is under the 'overall control' of one State engages in hostilities against another State (see discussion below). As a practical matter, it may be

تطبيق ذلك على الهجمات السيبرانية في إطار النزاعات المسلحة غير الدولية، فإنه ينبغي التفريق بين نوعين من الهجمات السيبرانية، الأول: الهجمات السيبرانية التي تؤدي إلى تبعات عنيفة، والثاني: الهجمات السيبرانية التي لا تؤدي إلى تبعات عنيفة.

أولاً: الهجمات السيبرانية التي تؤدي إلى تبعات عنيفة:

بالنسبة للهجمات السيبرانية من قبل جهات من غير الدول والتي تؤدي إلى تبعات عنيفة، أو تتم في سياق نزاع مسلح، أو كجزء من أعمال العنف، ففي هذه الحالات يُطبق عليها قواعد القانون الدولي الإنساني المتعلقة بالنزاعات المسلحة غير الدولية.

وتضحى الصعوبة في بعض الحالات التي تكون فيها الدولة متخفية وراء أحد الجماعات المسلحة، وقد تعرضت محكمة العدل الدولية في قضية نيكاراغوا لهذه الإشكالية، ووضعت معيارًا تقليديًّا وهو معيار "السيطرة الفعالة"،[١] وقد أعادت المحكمة

---

difficult to ascertain whether a State is controlling a non-State actor's cyber activities" Tallinn Manual, op.cit., p. 30. ٨٠.

[١] The Court decided that: "United States participation, even if preponderant or decisive, in the financing, organizing, training, supplying and equipping of the contras [Nicaraguan guerrillas], the selection of its military or paramilitary targets, and the planning of the whole of its operation, is still insufficient . . . for the purpose of attributing to the United States the acts

في قضية الكونغو وقضايا الإبادة الجماعية تأكيد هذا المعيار.[١] وتعني السيطرة الفعالة أن يكون للدول التي تتخفى وراء الجماعات المسلحة سيطرة شاملة من الدولة على الجماعات المسلحة، أو الميليشيا المسلحة، أو الوحدات شبه العسكرية التي تتصرف بالنيابة عنها، وأن تتضمن أكثر من مجرد تقديم المساعدة المالية، أو العسكرية، أو المعدات، أو التدريب، ومع ذلك، فليس بالضرورة أن تتضمن السيطرة إصدار أوامر محددة من قبل الدولة، أو متابعة كل عملية فردية. وعليه، فإن العلاقة

committed by the contras . . . . All the forms of United States participation above, and even the general control by the respondent State mentioned over a force with a high degree of dependency on it, would not in that the United States directed themselves mean, without further evidence, to human rights and or enforced the perpetration of the acts contrary well be humanitarian law alleged by the applicant State. Such acts could committed by members of the contras without the control of the United For this conduct to give rise to legal responsibility of the United States. principle have to be proved that that State had effective States, it would in operations in the course of which the control of the military or paramilitary alleged violations were committed".

[١] Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), 2005 I.C.J. 116, ¶ 160 (Dec. 19); Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb. & Mont.), 2007 I.C.J. 91, ¶¶ 391–92 (Feb. 26).

بين الدولة والجماعات المسلحة يجب أن تتجاوز مجرد الدعم اللوجستي، مع الوضع في الاعتبار أن يكون هذا الدعم موجهًا للجماعات المسلحة؛ بغرض تقويتها ضد الدولة التي تقاتلها. [١]

وبالتالي، فإذا كانت هناك سيطرة فعالة من الدولة على جماعة مسلحة ما تُقاتل ضد دولة أخرى، فحينها يُصبح النزاع نزاعًا مسلحًا دوليًّا، وقد أكدت المحكمة الجنائية الدولية ليوغسلافيا السابقة ذلك، فقررت أن النزاع المسلح بين الجماعات المسلحة ودولة يُصبح نزاعًا مسلحًا دوليًّا، في حالتين: "إذا تدخلت دولة في نزاع داخلي بقواتها المسلحة، أو كان أحد المشاركين في النزاع الداخلي يتصرف بالنيابة عن تلك الدولة". [٢] لذلك، عندما توجه دولة ما هجمات سيبرانية معينة ضد دولة أخرى، ولكن بواسطة جماعات مسلحة تقاتل ضد الدولة، أو تشارك، أو تُخطط لهذه الهجمات باستخدام

---

[١] S. Vite, Typology of armed conflicts in international humanitarian law: legal concepts and actual situations, IRRC, Volume 91 Number 873 March ٣2009, p.7. Available at: https://www.icrc.org/en/doc/assets/files/other/irrc-873-vite.pdf

[٢] A. Paulus and M. Vashakmadze, Asymmetrical War and the Notion of Armed Conflict – a tentative conceptualization, IRRC, Volume 91 Number 873 March 2009, p. ١٠١

الجماعات المسلحة، فإن النزاع يتحول إلى نزاع مسلح دولي، وتُطبق عليه القواعد التي تعرضنا إليها سالفًا.

ثانيًا: الهجمات السيبرانية التي لا تؤدي إلى تبعات عنيفة:

في حالة أنَّ الهجمات السيبرانية لا تؤدي إلى تبعات عنيفة، أو غير مرتكبة في سياق عمليات عدائية حركية، وذلك من قبل إحدى الجماعات المسلحة ضد دولة، فهل تُصنف على أنها تبدأ نزاعًا مسلحًا غير دولي؟

بدايةً، لا يبدأ أي نزاع مسلح عندما تتسامح الدولة أو تتعاطف مع الهجمات السيبرانية المنبثقة من أراضيها، أما إذا كانت الدولة لا تتسامح مع هذه الهجمات، فإن ذلك يثير صعوبة تحديد حالة النزاع المسلح غير الدولي خاصةً في غياب عمليات حركية على أرض الواقع.

يتناول البروتوكول الإضافي الثاني والمادة الثالثة المشتركة بالتنظيم حالة النزاع المسلح غير الدولي. بالنسبة للبروتوكول الإضافي الثاني، فيُشترط لتطبيقه أن تكون الجماعة المسلحة على قدر عال من التنظيم، وتمارس سيطرتها على جزء من إقليم الدولة بما

يمكنها من القيام بعمليات عسكرية مستمرة ومتضافرة العمليات.[١] وبالتالي فإن البروتوكول الإضافي الثاني ينطبق على الجماعات المسلحة التي لها نشاط حركي على أرض الواقع، وقد تكون العمليات السيبرانية التي تقوم بها جزء من أنشطتها العدائية.

أما المادة الثالثة المشتركة لاتفاقيات جنيف فهي أوسع في نطاقها من البروتوكول الإضافي الثاني، فتُطبق في حالات النزاعات المسلحة شديدة الحدة بصرف النظر عن تصنيفها القانوني كنزاعات مسلحة دولية أو غير دولية. وعليه، فالمادة الثالثة المشتركة تُطبق دائمًا مع البروتوكول الإضافي الثاني، كما تُطبق في حالات أخرى لا يشملها البروتوكول الإضافي الثاني. وبالتالي فمجال انطباقها أوسع من البروتوكول الإضافي الثاني من حيث شموليتها لعدد أكبر من الجماعات المسلحة. وقد وضعت المادة الثالثة المشتركة معيارين لانطباقها، وهما: أن تتمتع الجماعات المسلحة بقدر من التنظيم، وأن يصل النزاع لقدر من الحدة.

[١] البروتوكول الإضافي الثاني المادة ١/١.

أولاً: أن تتمتع الجماعات المسلحة بقدر من التنظيم:

يعرف دليل اللجنة الدولية للصليب الأحمر مستوى التنظيم المقصود في المادة الثالثة المشتركة بأنه: "أن يكون التعرف إلى هوية أطراف النزاع ممكنًا، أي أن تتمتع بحد أدنى من التنظيم والهيكلية وبتسلسل في القيادة".[١] كما وضحت المحكمة الجنائية الدولية ليوغسلافيا السابقة المقصود بـ "التنظيم" وفقًا للمادة الثالثة المشتركة بأنه يعني: "إمكانية التعرف على هوية أطراف النزاع، ومن العناصر التي يجب أخذها في الاعتبار وجود هيكل تنظيمي لتلك الجماعة، ووجود سلطة لاتخاذ القرارات، وتخطيط العمليات بين وحدات مختلفة، والقدرة على تجنيد وتدريب وحدات جديدة".[٢]

وبالتالي، يستبعد من هذه الفئة، أي هجمات سيبرانية يشنها "قراصنة" hackers، أفراد أو مجموعات قراصنة الذين يفتقرون إلى الدرجة اللازمة من التنظيم لاعتبار أفعالهم خاضعة للقانون الدولي الإنساني المتعلق بالنزاع المسلح غير الدولي؛ إذ تخضع

---

[١] تعزيز احترام القانون الدولي الإنساني في النزاعات المسلحة غير الدولية، منشورات اللجنة الدولية للصليب الأحمر، ١ كانون الأول/ديسمبر ٢٠١٥، ص.٤. متاح على الرابط التالي:
https://shop.icrc.org/icrc/pdf/view/id/567?_ga=2.167669758.1968292653.1583061162-2027439923.1566121970

[٢] ICTY, Prosecutor v. Boskoski, Case No. IT04-82, Judgment (Trial Chamber), 10 July 2008, para 175

أفعالهم للتجريم وفقًا للقانون الجنائي الداخلي، وليس للقانون الدولي الإنساني. أما إذا كانت الجماعة التي تشن الهجوم السيبراني منظمة فعليًا على النحو المنصوص عليه في المادة الثالثة المشتركة، فحينها تخضع أفعالها للقانون الدولي الإنساني فيما يتعلق بالنزاع المسلح غير الدولي.[١]

وحيث إن المهاجمين السيبرانيين قد يتواجدون في أماكن مختلفة، ويصعب التعرف على هويتهم، بل أنهم قد لا يعرفون هوية بعضهم البعض، ناهيك عن أن يكون عملهم وفقًا لهيكل تنظيمي؛ فيوضح دليل تالين أن التنظيم المطلوب في الجماعة التي تقوم بالهجمات السيبرانية وفقًا للمادة الثالثة المشتركة يعني أن يكون هناك تقسيم للمهام فيما بينهم وصولاً لأهداف سيبرانية محددة يسعون لتحقيقها، وأن يجروا معًا تقييمًا للضرر السيبراني، ويقدرون ما إذا كانت هناك حاجة لإعادة تثبيت الهجوم وغيرها من المسائل الفنية، أي أن الجماعة يجب أن تعمل "بشكل تعاوني" فيما بينها.

[١] Michael N. Schmitt, Cyber Operations and the Jus in Bello: Key Issues, op.cit., p.93.

وأكد الدليل على أن عدم تمكن أعضاء المجموعة من اللقاء جسديًّا لا يمنع – وحده – من توافر الدرجة المطلوبة من التنظيم وفقًا للمادة الثالثة المشتركة.[١]

ثانيًا: حدة النزاع:

تبدأ المادة الثالثة المشتركة بالنص على أن نطاق تطبيقها هو النزاعات المسلحة التي "ليس لها طابع دولي"، وبالتالي، فهي تنطبق على طائفة واسعة من الجماعات المسلحة المنخرطة في أية نزاعات مسلحة "ليس لها طابع دولي". وبالرغم من أن المادة الثالثة المشتركة لم تعرَّف المقصود بالنزاع المسلح الذي "ليس له طابع دولي"، إلا أنه يوجد اتفاق في الفقه على أن المقصود به النزاعات شديدة الحدة، فمستوى حدتها أعلى من حالات الاضطرابات والتوترات الداخلية، أو الأفعال العنيفة المعزولة والمتفرقة، والتي لا تسري عليها المادة الثالثة المشتركة، ولا البروتوكول الإضافي الثاني. [٢]

[١] Tallinn Manual, op.cit., p.452.

[٢] ووفقًا للمحكمة الجنائية الدولية ليوغوسلافيا السابقة في قضية Tadic فإنَّ النزاعات المسلحة غير الدولية تنطوي على عنف مسلح ممتد بين السلطات الحكومية والجماعات المسلحة المنظمة أو بين هذه المجموعات داخل دولة، وهو نفس المفهوم الذي تبنته المحكمة الجنائية الدولية لرواندا والنظام الأساسي للمحكمة الجنائية الدولية.

ويرى البعض أن حدة النزاعات المقصودة بالمادة الثالثة المشتركة قد تصل إلى مستوى أعلى من مستوى حدة النزاعات المسلحة الدولية، دون أن يُصنف النزاع قانونًا كنزاع مسلح دولي.[١] وقد وصف تقرير للجنة الدولية للصليب الأحمر "حدة النزاع" بأنها تعني أن يصل النزاع إلى مستوى معين من الحدة، بحيث لا تكفي قوات الشرطة لتداركه وتكون الدولة مجبرة على اللجوء لاستخدام قواتها المسلحة أو الوسائل العسكرية.[٢] وقد فسرت المحكمة الجنائية الدولية ليوغسلافيا السابقة معيار حدة النزاع المطلوب لانطباق المادة الثالثة المشتركة، فقضت بأنه يشمل عدة عوامل إرشادية، وهي: " عدد ومدة وشدة المواجهات الفردية، نوع الأسلحة والمعدات العسكرية الأخرى المستخدمة، عدد الذخائر التي أطلقت، عدد الأشخاص ونوع القوات المشاركة في القتال، عدد الضحايا، مدى الدمار المادي، وعدد المدنيين الفارين من مناطق القتال، كذلك فإن

Prosecutor v. Tadic, Case No. IT-94-1-A, Appeals Chamber Decision on Motion for Interlocutory Appeal on Jurisdiction, ¶ 70 (Int'l the Defence Oct. 2, 1995); Prosecutor v. Crim. Trib. for the Former Yugoslavia Akeyesu, Case No. ICTR-96-4-T, Judgment, ¶ 619 (Sept. 2, 1998); Statute, art. 8(2)(f). Rome

[١] H.P. Gasser, International Humanitarian Law: An Introduction, in: Humanity for All: The International Red Cross and Red Crescent Movement, H. Haug (ed.), Paul Haupt Publishers, Berne, 1993, p. 555.

[٢] تعزيز احترام القانون الدولي الإنساني في النزاعات المسلحة غير الدولية، المرجع السابق، ص.٤

مشاركة مجلس الأمن التابع للأمم المتحدة قد تكون مؤشرًا على شدة النزاع".[١] وينبغي ملاحظة أن العوامل الإرشادية تلك هي للتدليل على حدة النزاع، وليست شروطًا يجب توافرها مجتمعة.

وبتطبيق هذا المتطلب على الهجمات السيبرانية، فيلاحظ أن تلك الهجمات يجب أن تؤدي إلى نتائج أو آثار حركية عنيفة، حتى يُطبق عليها المادة الثالثة المشتركة. أما الهجمات السيبرانية التي لا تؤدي لنتائج حركية عنيفة، فإنها تستبعد من تصنيفها على أنها نزاع مسلح غير دولي. كذلك، فالهجمات السيبرانية الفردية أو المتفرقة من الأفراد،

[١] "Trial Chambers have relied on indicative factors relevant for assessing the "intensity" criterion, none of which are, in themselves, essential to establish that the criterion is satisfied. These indicative factors include the number, duration and intensity of individual confrontations; the type of weapons and other military equipment used; the number and calibre of munitions fired; the number of persons and type of forces partaking in the fighting; the number of casualties; the extent of material destruction; and the number of civilians fleeing combat zones. The involvement of the UN Security Council may also be a reflection of the intensity of a conflict". Prosecutor v Haradinaj, Case No. IT-04-84-84-T, 3 April 2008, para. 49

بغض النظر عما إذا كان لها نتائج تدميرية من عدمه، لا تنطبق عليها المادة الثالثة المشتركة؛ لعدم استيفاء متطلب التنظيم، حتى وإن طال أمدها.

والخلاصة، أنه سواء في إطار النزاعات المسلحة الدولية أو النزاعات المسلحة غير الدولية، فالمستقر عليه -إلى الآن - والمعمول به **هو أنَّ الهجمات السيبرانية التي تؤدي إلى تبعات عنيفة هي وحدها التي تخضع لقواعد القانون الدولي الإنساني.** وبالتالي، فإن الهجمات السيبرانية غير المدمرة، أو التي لا تؤدي إلى نتائج حركية، من غير المرجح حتى وصفها بأنها نزاع مسلح على الإطلاق. ومع ذلك، فهناك اتجاه في الفقه يدعو إلى اعتبار الهجمات السيبرانية خاضعة للقانون الدولي الإنساني حتى ولو لم تؤد إلى تبعات عنيفة، باعتبارها توفر مزايا مثل تقليل الأضرار العرضية الناتجة من ضرب الأهداف العسكرية (المشروعة) مثل الخسائر البشرية في المدنيين، وتدمير الأعيان المدنية، ويدعون بالتالي إلى تطبيق أكثر مرونة لأحكام القانون الدولي الإنساني.

الفصل الثاني

الأسلحة السيبرانية كوسيلة للقتال

تمهيد:

بما أن السلاح السيبراني من الأسلحة الجديدة التي أفرزها التطور التكنولوجي الحديث؛ فيجب على الدول – قبل استخدام هذا السلاح – أن تقوم بمراجعته؛ لتتأكد من مشروعيته قبل أن تضمه لأسلحتها، وذلك وفقًا للمادة ٣٦ من البروتوكول الإضافي الأول آلية لاستعراض ومراجعة الأسلحة، التي تُلزم الدول بالتأكد من مشروعية أي سلاح قبل استخدامه. وبالإضافة إلى آلية استعراض الأسلحة، توجد قواعد أخرى في القانون الدولي الإنساني، وهي ما اصطلح على تسميتها بـ "قانون السلاح" تحدد مدى مشروعية السلاح في حد ذاته، وذلك بالنظر للآثار العادية التي يخلفها استخدامه.

ولذلك، سنقوم بالتعرض لمدى مشروعية استخدام الأسلحة السيبرانية كوسيلة لتنفيذ الهجوم السيبراني من زاويتين، الأولى: من حيث مدى مشروعية استخدامها كأسلحة جديدة، وذلك وفقًا لآلية استعراض الأسلحة الجديدة المبينة في المادة ٣٦ من

البروتوكول الإضافي الأول، والثانية: من حيث مدى مشروعية الأسلحة السيبرانية في حد ذاتها باعتبار ما تؤدي إليه من تبعات تعد نتائج طبيعية لاستخدامها العادي.

وعلى ذلك سنتعرض فيما يلي لبحث هذه المسائل، من خلال التعرض للمقصود بالأسلحة السيبرانية وأنواعها واستعراضها كأسلحة جديدة في مبحث أول، ثم للضوابط التي تحدد مدى مشروعية استخدام الأسلحة ومدى انطباق هذه الضوابط على الأسلحة السيبرانية بوجه خاص وذلك في مبحث ثانٍ.

تقسيم:

ستقسم الدراسة في هذا الفصل إلى مبحثين على النحو التالي:

المبحث الأول: المقصود بالأسلحة السيبرانية واستعراضها كأسلحة جديدة.

المبحث الثاني: مدى مشروعية الأسلحة السيبرانية في حد ذاتها.

المبحث الأول

المقصود بالأسلحة السيبرانية واستعراضها كأسلحة جديدة

إذا كان الهجوم السيبراني هو "عملية سيبرانية، هجومية أو دفاعية من المتوقع – بشكل معقول – أن تتسبب في إصابة، أو وفاة الأشخاص، أو تلف، أو تدمير الأشياء"،[١] فيبرز التساؤل في هذا المقام حول ماهية السلاح الذي قد يتسبب في هذه التبعات، كذلك يبرز التساؤل حول مدى إمكانية استعراضه كسلاح جديد وفقًا للمادة ٣٦ من البروتوكول الإضافي الأول الخاصة بآلية استعراض ومراجعة الأسلحة الجديدة. وفيما يلي سنتعرض لكل منهما في مطلب مستقل.

المطلب الأول

المقصود بالأسلحة السيبرانية وأنواعها

لم يضع البروتوكول الإضافي الأول تعريفًا للمقصود بكل من الأسلحة، أو أدوات الحرب، أو أسلوبها. ومع ذلك ففي تعليق اللجنة الدولية للصليب الأحمر على المادة ٣٦ من البروتوكول الإضافي الأول ذكرت أن "أدوات الحرب هي الأسلحة أو نظم

[١] Tallinn Manual, op.cit., p.415.

الأسلحة، أما أسلوب الحرب فهو التكتيكات والتقنيات المتبعة لإجراء العمليات العدائية، وتغطي نطاقًا كبيرًا من المجالات لا تتعلق كلها باستخدام الأسلحة، أو وسائل وأساليب الحرب"،[١] ويشير مصطلح "سلاح" إلى القدرة الهجومية التي يمكن أن توجه ضد هدف عسكري، وتشمل المعدات التي قد لا تشكل سلاحًا بالمعنى التقليدي، ولكن لها أثر مباشر على القدرة الهجومية للقوات التي تملكها.

وقد عرف دليل تالين "وسائل الحرب السيبرانية" بأنها: "الأسلحة السيبرانية وما يرتبط بها من نظم أسلحة سيبرانية".[٢] كما وضح أن الأسلحة السيبرانية تشمل: "الوسائل السيبرانية للحرب، التي تُستخدم، أو تُصمم، أو يُقصد استخدامها لإحداث إصابة، أو موت الأشخاص، أو إتلاف، أو تدمير الأشياء، والتي ينتج عنها العواقب المطلوبة لاعتبار العملية السيبرانية "هجومًا".[٣] ويشمل ذلك كلًّا من الأسلحة السيبرانية ونظم

---

[١] Yves Sandoz, Christophe Swinarski, & Bruno Zimmermann, eds, ICRC, Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949 (Geneva: Martinus Nijhoff, 1987), at 1410–1439. available at: https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul .

[٢] "Means of cyber warfare are cyber weapons and their associated cyber systems". Tallinn Manual, op.cit., p.452.

[٣] Tallinn Manual, op.cit., p.452.

الأسلحة السيبرانية، التي تكون تحت سيطرة المهاجم، فالمعيار في تصنيف جهاز معين كسلاح، أو نظام سلاح هو وجوده تحت سيطرة المهاجم. وعليه فإن نظم الكومبيوتر التي تستخدم في الهجوم مثلاً تعتبر سلاحًا؛ في حين أن نظم البنية التحتية السيبرانية مثل شبكة الإنترنت لا تعد كذلك؛ لأنها ليست تحت سيطرة الطرف المهاجم.[١]

ويعرف البعض الأسلحة السيبرانية بأنها: "شيء مصمم، أو تم تطويره، أو الحصول عليه؛ من أجل تحقيق غرض أساسي وهو قتل، أو تشويه، أو إصابة الأشخاص، أو تدمير، أو إتلاف الأعيان".[٢] وفي تعريف القوات الجوية الأمريكية، فإن الأسلحة السيبرانية هي: "أي جهاز أو برنامج حاسوبي يهدف إلى تعطيل، أو رفض، أو

---

[١] Tallinn Manual, op.cit., p.456

[٢] "An object designed for, and developed or obtained for, the primary purpose of killing, maiming, injuring, damaging, or destroying". Brown, G. D. and Metcalf, A. O., 'Easier said than done: legal reviews of cyber weapons', Journal of National Security Law and Policy, vol. 7, no.1 (2014).

إضعاف، أو إبطال، أو تدمير أنظمة الكمبيوتر، أو البيانات، أو الأنشطة، أو القدرات للخصم".[١]

ووفقًا لتلك المفاهيم، فإن أدوات الهجوم السيبراني مثل الفيروسات والبرامج الضارة وغيرها تندرج تحت وصف أدوات الحرب، باعتبارها أسلحة. والسؤال هنا: ما أدوات الهجوم السيبراني، أو ما أسلحته؟

تُقسم Afroditi [٢] الأسلحة السيبرانية إلى ثلاث فئات رئيسة: **الأولى:** البرمجيات الخبيثة Malware، **والثانية:** هجمات منصات الخوادم Client-Server Platform Attacks، **والثالثة:** هجمات رفض الخدمة الموزعة DDOS Distributed Denial of Service. وفي حين أن الفئة الأولى تندرج تحت وصف أدوات الحرب، فإن الفئة

[١] "Any device or software payload intended to disrupt, deny, degrade, negate, impair or destroy adversarial computer systems, data, activities or capabilities". US Department of the Air Force, Secretary of the Air Force, Air Force Instruction 51-402, Legal Reviews of Weapons and Cyber Capabilities, 27 July 2011. Available at: https://nsarchive.gwu.edu/document/21449-document-53

[٢] Papanastasiou Afroditi, Application of International Law in Cyber Warfare Operations, op.cit., p.10.

الثانية والثالثة تندرجان تحت وصف أسلوب الحرب، أو الكيفية التي يتم بها استخدام أسلحة الحرب.

الفئة الأولى: البرمجيات الخبيثة Malware:

تحتوي هذه الفئة على البرامج الضارة مثل الفيروسات وأكواد معينة مصممة لإفساد أو تدمير البيانات، والديدان worms، وبرامج النسخ الذاتي، والبرامج المصممة؛ ليتم تشغيلها عند استيفاء ظروف معينة، والجذور الخفية rootkits وهذه البرمجيات تحتوي على trojan horses فتبدو غير ضارة، إلا أنها تحتوي على برمجيات ضارة يتم تفعيلها في وقت معين.

١- الفيروسات Computer Viruses:

تعد الفيروسات من أكثر الوسائل انتشارًا وشهرة، ويعرفها المركز القومي للحاسب الآلي في الولايات المتحدة الأمريكية بأنها: "برنامج مهاجم يصيب أنظمة الحاسبات، بأسلوب يماثل إلى حد كبير أسلوب الفيروسات الحيوية التي تصيب الإنسان، حيث يقوم هذا البرنامج بالتجول في الحاسب الآلي باحثًا عن برنامج غير مصاب، وعندما يجد أحدها ينتج نسخة من نفسه لتدخل فيه، حيث يقوم البرنامج المصاب فيما بعد

بتنفيذ أوامر الفيروس، ومن أهم خصائصه قدرته الفائقة على الاختفاء والانتشار، وقدرته على تدمير نظام الحاسب الآلي بأكمله".[١]

وتتميز الفيروسات بعدة خصائص وهي: **الأولى:** أنها قادرة على نسخ نفسها في أماكن مُختلفة من جهاز الحاسب المنتقلة إليه The Replication Mechanism، **الثانية:** أنها متخفية بطبيعتها، فلا يمكن اكتشافها عندما تُصيب أجهزة الكمبيوتر، ولكن في العادة تُكتشف بعد أن تُحدث أثرها التخريبي The Protection Mechanism، **الثالثة:** أنها قادرة على تفعيل نفسها بشكل تلقائي عندما يحين وقت معين The trigger Mechanism، **والرابعة:** أنه عند تفعيلها فإنها تقوم بتنفيذ الأوامر المصممة على تنفيذها بدلاً من تنفيذ أوامر الجهاز الموجودة فيه The Payload Mechanism.[2]

---

[١] نور أمير الموصلي، الهجمات السيبرانية في ضوء القانون الدولي الإنساني، الجامعة الافتراضية السورية ٢٠٢١، رسالة ماجستير

[2] للمزيد حول فيروسات الحاسب الآلي، راجع الرابط التالي:
https://mawdoo3.com/%D8%A8%D8%AD%D8%AB_%D8%B9%D9%86_%D9%81%D9%8A%D8%B1%D9%88%D8%B3%D8%A7%D8%AA_%D8%A7%D9%84%D8%AD%D8%A7%D8%B3%D8%A8
والرابط التالي:

٢- برامج الدودة Worm Software

تُشبه برامج الدودة الفيروسات بشكل كبير من حيث قدرتها على الانتشار ونسخ نفسها، لكنها تستخدم آلية وصول مختلفة، فهي تنتقل فقط عبر الإنترنت ومن خلال البريد الإلكتروني، وتستخدم الديدان نقاط الضعف في الشبكة للانتقال من جهاز مضيف إلى آخر. وهذا يعني أن الديدان لا تتطلب من المستخدم فتح أي شيء أو تفعيلها على أي حال، فهي تخترق شبكة المستخدم من خلال ثغرة في نظام أمانها. وفور دخولها إلى الشبكة، تبدأ الدودة بالبحث عن مكان آخر لتنتشر. ويمكن لبرامج الدودة التسبب بنفس أنواع الضرر الناتج عن الفيروس. ومع ذلك، يمكن للديدان الخالية من الحمولة، والتي تبدو غير ضارة أن تتسبب بحمل زائد على الشبكة، أو تطلق "هجمات رفض الخدمة.denial-of-service attack "[١].

٣- حصان طروادة Trojan Horse:

https://mafhome.com/%D9%85%D9%81%D9%87%D9%88%D9%85-%D9%81%D9%8A%D8%B1%D9%88%D8%B3%D8%A7%D8%AA-%D8%A7%D9%84%D9%83%D9%88%D9%85%D8%A8%D9%8A%D9%88%D8%AA%D8%B1/

[١] للمزيد حول هجمات رفض الخدمة، راجع الرابط التالي:
https://nasainarabic.net/main/articles/view/malicious-software-worms-trojans-and-bots-oh-my

هي نوع من أنواع البرامج فيروسية، ولكن تختلف عنها في أن "حصان طروادة" لا يتكاثر ولا يلتصق بالملفات وإنما هو برنامج مستقل بذاته يحمل في طياته توقيت تفعيله، وقد يؤدي إلى تعديل البرامج، أو تعديل المعلومات على النظام، أو إلى تدمير النظام كله. وهذه البرامج هي في الأساس من الناحية التقنية هي برمجيات اختراق وتجسس، وسميت بهذا الاسم؛ لأنها في ظاهرها لا تبدو أنها برامج فيروسات أو برامج ضارة، إلا أنه عند حلول وقت معين أو أمر معين تبدأ بالتفعيل.[١]

٤- برامج القنابل المعلوماتية Bomb:

تعرف القنبلة المعلوماتية باسم الشفرة الموقوتة Disabling Code، وهي نوع من أنواع البرامج الخبيثة صغيرة الحجم، يتم إدخالها بطرق خفية مع برامج أخرى، وهي ليست ملفًا كاملاً، وإنما شفرة تتضمن عددًا من الملفات، والتي تتفكك عندما تصل لجهاز الكمبيوتر؛ حتى لا يمكن كشفها وتبقى ساكنة لمدة قد تصل لأشهر أو أعوام إلى حين حلول توقيت معين فتقوم بالتفعيل. وتُستخدم هذه البرامج لتدمير المعلومات

[١] انظر: جريمة إتلاف وتدمير المعطيات والبيانات بواسطة الإنترنت، أبريل ٢٠٠٩، متاح على الرابط التالي:
https://www.startimes.com/?t=16193884

والبيانات،[١] ويوجد منها نوعان، وهما: القنبلة المنطقية Logic Bomb وهذا النوع ينشط بمجرد حدوث واقعة معينة مثل بدء تشغيل الكومبيوتر أو بدء تشغيل برنامج معين داخله، والقنبلة الزمنية Time Bomb وهذا النوع ينشط بحلول وقت معين في تاريخ معين.[٢]

الفئة الثانية: هجمات منصات الخوادم Client–Server Platform Attacks

وهي هجمات مصممة لاستغلال ثغرات نظام تشغيل Windows، أو التلاعب في أنظمة الأمان، بواسطة وسائل اختراق برامج أمن الكمبيوتر الشخصي، ولا يؤدي مثل هذا الهجوم دائمًا إلى تدمير شبكة الكمبيوتر أو ملف البنية التحتية التي يسيطر عليها. وتتم هذه الهجمات عادة باستخدام برامج التسلل، فبمجرد أن يتسلل المهاجم إلى شبكة كمبيوتر آمنة، يمكنه تنفيذ مجموعة متنوعة من الإجراءات، قد تتضمن تعطيل العمل. فعلى سبيل المثال، هجوم Stuxnet استهدف شبكات الكمبيوتر الآمنة في إيران؛ لغرض تعطيل عمل المنشأة النووية. وقد يتضمن برنامج التسلل إرسال

[١] نور أمير الموصلي، الهجمات السيبرانية في ضوء القانون الدولي الإنساني، الجامعة الافتراضية السورية ٢٠٢١، رسالة ماجستير.

[٢] انظر: جريمة إتلاف وتدمير المعطيات والبيانات بواسطة الإنترنت، أبريل ٢٠٠٩، متاح على الرابط التالي:
https://www.startimes.com/?t=16193884

معلومات كاذبة بغرض تحقيق نتائج عسكرية معينة، ففي عام ٢٠٠٣، قبل غزو العراق، اخترقت الولايات المتحدة نظام البريد الإلكتروني لوزارة الدفاع العراقية للاتصال بضباط عراقيون وإعطائهم تعليمات باستسلام سلمي، وقد نجحت هذه الرسالة في توجيه الجيش العراقي للاستسلام. وقد تم هذا الهجوم باستخدام ملف "هجوم القيادة والسيطرة" وهو ملف يُقصد به التدخل في قدرة العدو على قيادة قواته والسيطرة عليها.

تثبت هذه الأمثلة أن الهجمات لا تتم بالضرورة عبر الإنترنت، ولكنها قد تتضمن بدلاً من ذلك من خلال التسلل إلى شبكات منفصلة وآمنة. هذه الشبكات لا تضم فقط أجهزة الكمبيوتر المكتبية والمحمولة، بل تشمل كل شبكة تتضمن أنظمة الحوسبة، مثل أنظمة التحكم الصناعية.

الفئة الثالثة: هجمات رفض الخدمة الموزعة DDOS Distributed Denial of Service

وهي الأكثر استخدامًا في الآونة الأخيرة للتسلل إلى البنية التحتية لشبكة العدو، حيث يتم فيها استخدام أدوات مؤتمتة لتحويل أجهزة الكمبيوتر إلى "زومبي" أو "روبوتات"، والتي بدورها "تلوث" دون علم أجهزة الكمبيوتر الأخرى المتصلة بها. في هذه

الهجمات المنسقة يتم السيطرة على مجموعات من آلاف أجهزة الكمبيوترات بفيروسات ترهق الخوادم عن طريق زيارة مواقع ويب المعينة بشكل متكرر، مما يؤدي في النهاية إلى تعطيل النظام المستهدف وإغلاقه في النهاية.[١]

ومثال هذه الهجمات، الهجوم السيبراني على إستونيا في أبريل ٢٠٠٧، حيث تم باستخدام هجوم DDOS، من قبل مجموعة من المتسللين، وقد أصابت الهجمات الاقتصاد، والحكومة، وخدمات الطوارئ الإستونية بالشلل لفترة من الزمن، لكنها لم تسبب أي آثار جسدية مباشرة.[٢] ولم يُنسب الهجوم رسميًّا إلى أي دولة، بالرغم من الإشارة إلى تورط روسيا؛ بسبب تعقيد وحجم الهجوم.[٣] وبالرغم من أن آثار هذه

[١] طلال ياسين العيسى، وعدي محمد عناب، المسئولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر، مجلة الزرقاء للبحوث والدراسات الإنسانية – المجلد التاسع عشر – العدد الأول، ٢٠١٩، ص٨٦.

[٢] Ido Kilovaty, Cyber Conflict and The Thresholds Of War, (June 22, 2021). Forthcoming, Is the International Legal Order Unraveling? (David Sloss, ed.) Oxford University Press (2022), p. ٩. Available at: https://ssrn.com/abstract=3871931 or http://dx.doi.org/10.2139/ssrn.3871931

[٣] Jeffrey T. G. Kelsey, Note, Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare, op.cit., p.1429.

الهجمات غالبًا ما تسبب مجرد إزعاج، إلا أن هذا الهجوم كان مهددًا للحياة تقريبًا، حيث كان خط الطوارئ لاستدعاء سيارة إسعاف أو سيارة إطفاء خارج الخدمة لمدة ساعة.[١] كذلك، في يوليو ٢٠٠٩، تم إغلاق عدد من المواقع الحكومية والتجارية في الولايات المتحدة وفي كوريا الجنوبية بهجوم DDOS، وبالرغم من أن كوريا الجنوبية ألقت باللوم على كوريا الشمالية، إلا أن الولايات المتحدة لم تتهم أي دولة.[٢] وفي ديسمبر ٢٠١٥، عانت المناطق الغربية والعاصمة في أوكرانيا من انقطاع التيار الكهربائي بسبب عملية سيبرانية يُزعم أنها مرتبطة بروسيا.[٣] وفي عام ٢٠١٩، ذكرت

---

[١] Newly Nasty: Defences Against Cyberwarfare Are Still Rudimentary. That's Scary, ECONOMIST (May 24, 2007), available at: http://www.economist.com/node/9228757?story_id=9228757

[٢] Officials anonymously leaked qualified reports of U.S. suspicions that the attack emerged in North Korea. U.S. Eyes N. Korea for 'Massive' Cyber Attacks, MSNBC.COM (July 9, 2009, 3:31 AM), available at: http://www.msnbc.msn.com/id/31789294/ns/technology_and_science-security

[٣] Ellen Nakashima, Russian Hackers Suspected in Attack That Blacked Out Parts of Ukraine, WASH. POST, Jan. 5, 2016. Available at: https://www.washingtonpost.com/world/national-security/russian-hackers-suspected-in-attack-that-blacked-out-parts-of-ukraine/2016/01/05/4056a4dc-b3de-11e5-a842-0feb51d1d124_story.html

صحيفة واشنطن بوست أن عملية سيبرانية تسببت في تعطيل عمليات الشبكة الكهربائية في غرب الولايات المتحدة، مما أدى إلى إغراق الشبكة بهجوم رفض الخدمة.[١] وقد تم التصدي لهذا الهجوم، إلا أن الخبراء يعتقدون أنه في حالة نجاح العملية السيبرانية ضد الشبكة الكهربائية يمكن أن تتسبب في "خسائر في الطاقة في أجزاء كبيرة من الولايات المتحدة يمكن أن تستمر أيامًا في معظم الأماكن، وحتى عدة أسابيع في أماكن أخرى.[٢]

وهذا يوضح أمرًا وثيق الارتباط بالهجمات السيبرانية، وبهجمات DDOS بشكل خاص، وهو أنه من الصعب معرفة الفاعل أو إسناد الفعل لدولة معينة، حيث يتم

[١] Robert Knake, A Cyberattack on the U.S. Power Grid, COUNCIL ON FOR. REL. (Apr. 3, 2017), available at: https://www.cfr.org/report/cyberattack-us-power-grid

[٢] ويقدر تأثير مثل هذه العملية على الاقتصاد الأمريكي بما يتراوح بين ٢٥٠ مليار دولار وتريليون دولار ، وفقًا لتقرير صادر عن جامعة كامبريدج.

Lloyd's & University of Cambridge Centre For Risk Studies, Business Blackout: The Insurance Implications of A Cyber Attack on The Us Power Grid, (2015). Available at: https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/crs-lloyds-business-blackout-scenario.pdf

خلال هجمات DDOS تجنيد أجهزة كمبيوتر آمنة من جميع أنحاء العالم، مما يجعل معرفة الفاعل أمرًا صعبًا جدًّا.

وهناك نوع آخر من الهجمات يُعرف باسم "زرع المعلومات غير الدقيقة"، وهو وسيلة أكثر تعقيدًا من هجوم DDOS، وفي هذا الهجوم يقوم المهاجم بإدخال معلومات غير دقيقة – خلسة – إلى نظام الكمبيوتر. بعد إتمام الهجوم، لا يبدو على الكمبيوتر المصاب أي شيء، بل يبدو أنه يعمل بشكل طبيعي، حتى عندما يفشل في أداء أي مهام يبدو طبيعيًّا أيضًا. في عام ١٩٩٩، على سبيل المثال، وضعت الولايات المتحدة خطة لوضع بيانات كاذبة في شبكة قيادة الدفاع الجوي الصربية، مما يعيق قدرة صربيا على استهداف طائرات الناتو، إلا أنه لم يتم تنفيذها في النهاية.[١] كذلك، استخدم سلاح الجو الإسرائيلي استراتيجية مماثلة في ٦ سبتمبر ٢٠٠٧، خلال

[١] كان من الممكن أن تستغل هذه الخطة بسبب زيادة الاعتماد على شبكات الكمبيوتر التي تميز الحروب الحديثة؛ إلا أنه في النهاية تخلت قوات الناتو عن الخطة بسبب مخاوف قانونية حولها الأضرار الجانبية.

Officials anonymously leaked qualified reports of U.S. suspicions that the attack emerged in North Korea. U.S. Eyes N. Korea for 'Massive' Cyber Attacks, MSNBC.COM (July 9, 2009, 3:31 AM), http://www.msnbc.msn.com/id/31789294/ns/technology_and_science-security .

القصف الجوي لمنشأة نووية في سوريا؛ وأدى ذلك إلى عدم اكتشاف الرادارات للطائرات الإسرائيلية؛ بسبب هجوم سيبراني سابق تعرض له نظام الدفاع الجوي السوري، ولا تزال الطريقة الدقيقة للهجوم غير معروفة، ولكن من الواضح أن إسرائيل أرسلت رسائل كاذبة إلى الرادارات، جعلتها لا ترى الطائرات ليلة الضربة، وتظهر أن السماء صافية.[١]

قد تكون هذه الهجمات أسهل في معرفة فاعلها أو إسنادها لفاعلها من هجمات DDOS، بسبب أن هذا النوع من الهجمات السيبرانية عادة ما يصاحبه أو يلحقه هجمات تقليدية. وبالتالي فإن إشكالية الإسناد هنا أقل صعوبة.[٢]

---

[١] Oona A. Hathaway, et al. "The Law of Cyber-Attack", op.cit., pp. 817–85.

[٢] لفهم طريقة عمل الأسلحة السيبرانية، يوضح Herr أنَّ جميع البرامج الضارة تشترك في ثلاثة عناصر أساسية، وهي: طريقة الانتشار Propagation Method، برمجيات إكسبلويت Exploits، والحمولة Payload. طريقة الانتشار، هي الوسيلة لنقل التعليمات البرمجية الضارة من المصدر إلى الهدف، برمجيات إكسبلويت تعمل على تمكين البرمجيات الضارة من الانتشار وتشغيل الحمولة من خلال الاستفادة من نقاط الضعف في النظام المستهدف أثناء التشغيل، أما الحمولة فهي رمز مكتوب لتحقيق بعض النهايات الخبيثة المرغوبة مثل حذف البيانات أو التلاعب بنظام التحكم الصناعي.

Herr, Trey, PrEP: A Framework for Malware & Cyber Weapons (December 20, 2013). The Journal of Information Warfare, Vol.13, No.1, February

وبصفة عامة يمكن تحديد مجموعة من الخصائص التي تتسم بها الأسلحة السيبرانية بأنواعها، وهي:

أولاً: أنها أسلحة في تطور وتحديث مستمر، مما يزيد من قدرتها التدميرية وفاعليتها، لإحداث إصابة، أو موت الأشخاص، أو إتلاف، أو تدمير الأعيان.

ثانيًا: سهولة الاستخدام، وذلك على عكس أسلحة الحرب التقليدية التي تحتاج إلى خبرة فنية وقدرات وتدريب لاستخدامها بشكل فعال.

ثالثًا: عادة ما يكون الهدف من الهجمات السيبرانية هو استهداف البنى التحتية للعدو، مثل: حجب الخطوط الأرضية الوطنية أو شبكة الهاتف، وإغلاق أو اعتراض إشارة شبكة الهواتف المحمولة، أو استهداف وسائل النقل، على سبيل المثال تعطيل حركة المطار عن طريق قطع الطاقة عن أبراج التحكم في الحركة الجوية، أو تعطيل إشارات الوقت من نظام تحديد المواقع العالمي GPS، أو استهداف البنى التحتية

2014, Available at: https://ssrn.com/abstract=2343798 or http://dx.doi.org/10.2139/ssrn.2343798

الحيوية كإمدادات المياه وسدود المياه والغذاء وأنظمة التوزيع وشبكات الطاقة الكهربائية ومحطات الطاقة والوقود وحتى الطاقة النووية وأنظمة سلامة المصنع. [١]

المطلب الثاني

استعراض السلاح السيبراني وفقًا للمادة ٣٦ من البروتوكول الإضافي الأول لعام ١٩٧٧

تنص المادة ٣٦ من البروتوكول الإضافي الأول، الذي يعد ضمن القانون الدولي العرفي، على أن "يلتزم أي طرف سام متعاقد، عند دراسة أو تطوير أو اقتناء سلاح جديد، أو أداة للحرب، أو اتباع أسلوب للحرب، بأن يتحقق مما إذا كان ذلك محظوراً في جميع الأحوال أو في بعضها بمقتضى هذا الملحق "البروتوكول" أو أية قاعدة أخرى من قواعد القانون الدولي التي يلتزم بها الطرف السامي المتعاقد".

[١] Papanastasiou Afroditi, Application of International Law in Cyber Warfare Operations, op.cit., p.19.

١٢- مدى انطباق القانون الدولي الإنساني على الهجمات السيبرانية

وقد كانت مسألة مراقبة استحداث الأسلحة الجديدة وفقًا لمبادئ القانون الدولي الإنساني ضمن الأولويات عند وضع البروتوكول الإضافي الأول، فشُكلت لجنة مخصصة آنذاك لاستكشاف مجال قانون الأسلحة والمبادئ المنطبقة فيه بموجب أحكام القانون الدولي الإنساني، والتي توجت بإدراج المادة ٣٦ ضمن البروتوكول الإضافي الأول.[١] وتُقيد هذه المادة في اختيارها للأسلحة وكيفية استخدامها، وتشمل هذه القيود حظر استخدام الأسلحة المحظورة بموجب القانون الدولي، ومنها الأسلحة غير المشروعة في ذاتها، وكذلك الأسلحة المحظورة بموجب اتفاقيات دولية مثل اتفاقية حظر الأسلحة البيولوجية والكيمائية، وبروتوكول حظر أسلحة الليزر المسببة للعمى[2].

[١] جاستن ماك كليلاند، استعراض الأسلحة وفقا للمادة ٣٦ من البروتوكول الإضافي الأول، مقال، المجلة الدولية للصليب الأحمر، العدد ٨٥٠ (٢٠٠٣)، ص.٨، متاح على:
https://www.icrc.org/ar/doc/assets/files/other/previewoftheweaponsinarticle36.pdf

[2] استعراض الأسلحة الجديدة: نظرة عامة، مقال على الموقع الالكتروني للجنة الدولية للصليب الأحمر.
https://www.icrc.org/ar/doc/war-and-law/weapons/new-weapons/overview-review-of-new-weapons.htm

ويحظى إجراء "استعراض الأسلحة" الجديدة بأهمية كبيرة، خاصة في ضوء التطور السريع الذي تشهده تكنولوجيا الأسلحة. وفي المؤتمر الدولي الثامن والعشرين للصليب الأحمر والهلال الأحمر، أعلنت الدول الأطراف في اتفاقيات جنيف أنه "على ضوء التطور السريع لتكنولوجيا الأسلحة، وسعيًا إلى حماية المدنيين من الآثار العشوائية للأسلحة، والمقاتلين من المعاناة التي لا مبرر لها ومن الأسلحة المحظورة، يتعين أن تخضع جميع الأسلحة الجديدة ووسائل الحرب وأساليبها الجديدة لاستعراض صارم ومتعدد التخصصات".[١] وفي عام ٢٠٠٦، وضعت اللجنة الدولية للصليب الأحمر دليلاً لاستعراض مشروعية الأسلحة الجديدة ووسائل الحرب وأساليبها، تضمن تفسيرًا للمتطلبات القانونية ذات الصلة، ويعرض لتجارب وممارسات الدول التي وضعت إجراءات لاستعراض الأسلحة.[2]

[١] المرجع السابق

[2] A Guide to the Legal Review of New Weapons, Means and Methods of Warfare. Available at: http://e-brief.icrc.org/wp-content/uploads/2016/09/12-A-Guide-to-the-Legal-Review-of-New-Weapons.pdf

ووفقًا للمادة ٣٦ من البروتوكول الإضافي الأول، فعلى الدول التأكد من أن السلاح غير محظور بموجب القانون الدولي عند القيام بالمراجعة القانونية لأي سلاح جديد، وذلك قبل تقييم السلاح.

أولاً: التأكد من أن السلاح غير محظور بموجب القانون الدولي:

وفقًا للمادة ٣٦ من البروتوكول الإضافي الأول، يتعين على الدول عند القيام باستعراض الأسلحة الجديدة أن تتحقق مما إذا كان هذا السلاح محظورًا في جميع الأحوال أو في بعضها "بمقتضى هذا البروتوكول أو أية قاعدة أخرى من قواعد القانون الدولي". وتشمل الأسلحة المحظورة بموجب البروتوكول الإضافي الأول: الأسلحة والمقذوفات والمواد وأساليب الحرب التي تسبب بطبيعتها إصابات زائدة أو معاناة غير ضرورية (المادة ٣٥ (٢))، وأساليب ووسائل الحرب التي من المتوقع أن تتسبب في أضرار واسعة النطاق، وطويلة الأجل وشديدة في الطبيعية البيئية (المادتان ٣٥ (٣) و ٥٥)، الأسلحة التي لا يمكن توجيهها إلى هدف محدد أو غير التمييزية (المادة٥١ (٤) (ب))، وكذلك الأسلحة التي لا يمكن التحكم بآثارها (المادة ٥١ (٤) (ج))، والأساليب التي تستهدف ضرب تمركزات المدنيين أو الأعيان المدنية (المادة ٥١ (٥) (أ))، والهجمات على المدنيين التي لا تتناسب مع المزايا العسكرية المأمولة

(مبدأ التناسب) (المادة ٥١ (٥) (ب)). وذلك بالإضافة إلى الأسلحة المحظورة بموجب المعاهدات الدولية،[١] أو بموجب القانون الدولي العرفي.[٢]

ثانيًا: تقييم السلاح الجديد:

توجد ثلاث حالات تعتبر فيها الأسلحة جديدة، وبالتالي تحتاج لإخضاعها لآلية استعراض الأسلحة، وهي: **الحالة الأولى:** جدة السلاح بالنسبة للدولة التي تنوي

[١] ومن أمثلة هذه الاتفاقيات: اتفاقية حظر تطوير وإنتاج وتخزين الأسلحة البيولوجية والسامة وتدمير تلك الأسلحة لعام ١٩٧٢، واتفاقية حظر الاستخدام العدائي للبيئة لعام ١٩٧٦، واتفاقية حظر استخدام أسلحة معينة لعام ١٩٨٠ وبروتوكولاتها الخمس الملحقة، كذلك اتفاقية حظر تطوير وإنتاج وتخزين الأسلحة الكيميائية لعام ١٩٩٣، وحظر استخدام وتخزين وإنتاج ونقل الألغام المضادة للأفراد وتدمير تلك الألغام لعام ١٩٩٧، ونظام روما الأساسي للمحكمة الجنائية الدولية لعام ١٩٩٨، الذي تضمن النص على أن استخدام أسلحة معينة يشكل جريمة حرب، ومن ذلك: استخدام السم أو الأسلحة المسمومة؛ استخدام الغازات الخانقة أو السامة أو الغازات الأخرى، استخدام الرصاص الذي يتسع أو يسطح بسهولة في جسم الإنسان، استخدام الأسلحة والمقذوفات والمواد وأساليب الحرب التي تسبب إصابات زائدة أو معاناة غير ضرورية.

[٢] وفقًا لدراسة اللجنة الدولية للصليب الأحمر عن العرف الدولي الإنساني، تشمل الأسلحة المحظورة بموجب قواعد القانون الدولي العرفي: استخدام السموم أو الأسلحة المسممة (القاعدة ٧٢)، استخدام الأسلحة البيولوجية (القاعدة ٧٣)، استخدام الأسلحة الكيميائية (القاعدة ٧٤)، حظر استخدام مبيدات الأعشاب كوسيلة من وسائل الحرب (القاعدة ٧٦)، استخدام الرصاصات التي تتسع أو تتسطح بسهولة في جسم الإنسان (القاعدة ٧٧)، الأسلحة تنتج شظايا لا يمكن الكشف عنها بالأشعة السينية (القاعدة ٧٩)

J.-M. Henckaerts and L. Doswald-Beck (eds.), Customary International Humanitarian Law, Cambridge: Cambridge University Press, 2005.

استخدامه، فإذا كان السلاح موجودًا بالفعل في الخدمة لدى دولة معينة وباعته لدولة أخرى، فإن الدولة التي اشترته ينبغي أن تقوم باستعراض للسلاح بموجب المادة ٣٦؛ لأنه يعد جديدًا بالنسبة لها. **الحالة الثانية:** تاريخ دخول السلاح في الخدمة بالنسبة للدولة، فالسلاح الموجود في الخدمة بالفعل وقت تصديق الدولة على البروتوكول لا يعد جديدًا، ومع ذلك فيرى البعض أنه من الاحتياط أن تقوم الدول باستعراض الأسلحة التي لديها حتى تستطيع الدفاع عن امتلاكها لها بشكل أقوى، وحتى تكون لها حجة قانونية قوية عند استخدامها، وإن كانت المادة ٣٦ لا تستوجب ذلك. **الحالة الثالثة:** عند القيام بتطوير سلاح موجود بالفعل بشكل يؤثر على سماته الخاصة، ففي هذه الحالة تجب مراجعته كسلاح جديد، أما إذا كان التطوير لا يؤثر على سمات السلاح الخاصة، وإنما يجعله على سبيل المثال أخف وزنًا دون أن يؤثر على قدرته، فلا يعد سلاحًا جديدًا في هذه الحالة.[١]

وبالتالي، فيتعين على الدول التي تنوي استخدام السلاح السيبراني، أو اتباع أسلوب الهجمات السيبرانية في حروبها، أن تقوم بعملية استعراض لهذا السلاح لبحث مدى

[١] جاستن ماك كليلاند، استعراض الأسلحة وفقًا للمادة ٣٦ من البروتوكول الإضافي الأول، المرجع السابق، ص٩.

مشروعيته، وذلك قبل أن تقوم بالفعل بإنشاء قسم أو وحدة لاستخدام هذا السلاح داخل جيوشها النظامية.

يوضح كليلاند أن عملية "دراسة أو تطوير أو اقتناء الأسلحة" عملية معقدة قد تستغرق سنواتٍ أو شهورًا على حسب طبيعة السلاح، ومن الضروري أن تتم المراجعة القانونية لكل مرحلة من مراحل هذه العملية. ويضيف بأن تلك العملية تمر بست مراحل وهي: التصور، والتقييم، الاختبار، والتصنيع، والخدمة الداخلية، ثم التخلص من السلاح. وبالرغم من أن تلك المراحل فنية بطبيعتها، إلا أنه لابد من التأكد من وجود مشورة قانونية لكافة المراحل، والتي تتم إما من خلال لجنة مشكلة من عدد من الخبراء؛ لتقييم السلاح وتتبع وزارة الدفاع النرويجية هذا الأسلوب، أو عن طريق مراجع فردي (قانوني) وتتبع هذا الأسلوب الولايات المتحدة الأمريكية، أو أن تكون السلطة التنفيذية هي المراجع، أو المراقب على تلك العملية.[١]

استعراض الأسلحة السيبرانية:

[١] جاستن ماك كليلاند، استعراض الأسلحة وفقا للمادة ٣٦ من البروتوكول الإضافي الأول، المرجع السابق، ص ٧،٨.

لا توجد معاهدات تقيد أو تحظر على وجه التحديد حيازة أو استخدام الأسلحة السيبرانية، أو الأساليب السيبرانية في القتال؛ ولذلك فعلى الدول التي ترغب في اقتناء واستخدام السلاح السيبراني أن تبدأ في تقييم هذا السلاح.[١]

لم يحدد البروتوكول الإضافي الأول، الإجراءات التي ينبغي على الدول الأطراف اتباعها للتحقق من مشروعية استخدام الأسلحة الجديدة، أو أدوات الحرب أو وسائلها، تاركًا الباب مفتوحًا أمام كل دولة لإنشاء آلية استعراض خاصة بها. وبرغم اتفاق الدول على التزامها بأن "تخضع جميع الأسلحة الجديدة ووسائل الحرب وأساليبها الجديدة لاستعراض صارم ومتعدد التخصصات"،[٢] إلا أنه لا توجد اليوم سوى بضع دول التي وضعت آليات استعراض رسمية للأسلحة الجديدة، ومنها الولايات المتحدة،

[١] Vincent Boulanin And Maaike Verbruggen, Article 36 Reviews Dealing with The Challenges Posed by Emerging Technologies, Stockholm International Peace Research Institute, 2017, P.25. Available At: https://www.sipri.org/sites/default/files/2017-12/article_36_report_1712.pdf

[٢] وفي المؤتمر الدولي الثامن والعشرين للصليب الأحمر والهلال الأحمر، أعلنت الدول الأطراف في اتفاقيات جنيف أنه "على ضوء التطور السريع لتكنولوجيا الأسلحة، وسعياً إلى حماية المدنيين من الآثار العشوائية للأسلحة، والمقاتلين من المعاناة التي لا مبرر لها ومن الأسلحة المحظورة، يتعين أن تخضع جميع الأسلحة الجديدة ووسائل الحرب وأساليبها الجديدة لاستعراض صارم ومتعدد التخصصات".

بالرغم من أنها ليست عضوًا في البروتوكول الإضافي الأول، ووفقًا لسياسة الاستعراض لديها، تقوم بنوعين من المراجعة القانونية للأسلحة الجديدة، أحدهما قبل اتخاذ قرار تصنيع السلاح، والآخر قبل استخدام السلاح في ساحة القتال.[١] وحتى عام ٢٠٢٢، فقد قامت ست دول بالبدء بالفعل في إجراء استعراض للأسلحة السيبرانية، وهي: الولايات المتحدة (بدأت في الإجراء عام ٢٠١٢)، سويسرا، وألمانيا، والبرازيل، وأستراليا (بدأوا في الإجراء عام ٢٠٢١)، وكندا (بدأت في الإجراء عام ٢٠٢٢).[٢]

ويرى البعض[٣] أنه من الأمور التي يجب وضعها في الحسبان عند استعراض الأسلحة السيبرانية أن هذه الأسلحة هي "برمجيات خبيثة"، وبالتالي فهي خاضعة للتحديث بشكل مستمر، فعلى سبيل المثال، إذا قام الخصم بتحديث دفاعاته بجدار حماية جديد، أو برنامج مكافحة فيروسات، أو تصحيح الثغرة الأمنية التي تستغلها البرمجيات

[١] DOD Directive 3000.09. Available at: https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodd/300009p.pdf

[٢] Legal review of cyber weapons, means and methods of warfare, available at: https://cyberlaw.ccdcoe.org/wiki/Legal_review_of_cyber_weapons,_means_and_methods_of_warfare

[٣] Vincent Boulanin And Maaike Verbruggen, Article 36 Reviews Dealing with The Challenges Posed by Emerging Technologies, op.cit., p. ١٦.

الخبيثة؛ فإنَّ ذلك سيتطلب تحديث كود هذه البرمجيات بالتبعية؛ حتى يمكنها اختراق هذه الأنظمة ذات الحماية المحدَّثة. ونؤيد ذلك، ونرى أنه وفقًا المادة ٣٦ من البروتوكول الإضافي الأول، فإن أي تحديث يؤثر على السمات الخاصة لهذه البرمجيات الخبيثة، سيجعل منها سلاحًا جديدًا، وبالتالي يجب أن تخضع لآلية استعراض الأسلحة مرة أخرى. ولذلك، يجب أن يوضع في الاعتبار كذلك عند استعراض الأسلحة نسخة الكود التي تمت مراجعتها وأنواع التعديل التي يمكن أن تؤدي إلى مراجعة جديدة.

المبحث الثاني

مدى مشروعية الأسلحة السيبرانية في حد ذاتها

لخصت محكمة العدل الدولية في رأيها الاستشاري حول مشروعية استخدام الأسلحة النووية شروط مشروعية السلاح، حين قررت أن السلاح النووي عاجز بطبيعته عن الالتزام بمبدأ التمييز ومبدأ التناسب (أي عشوائي)، كما أنه يسبب بطبيعته آلاما غير ضرورية في جميع الأحوال، وبالتالي فهو غير مشروع في ذاته.[١] ويرى البعض أن هناك ثلاث قواعد أساسية تحدد مدى مشروعية السلاح، أو نظم السلاح في حد ذاتها، وهي: ألا يكون السلاح عشوائيًّا بطبيعته، وألا يسبب السلاح بطبيعته آلامًا أو أضرارًا لا مبرر لها، وألا تكون الآثار التي يخلفها استخدام السلاح لا يمكن التحكم بها.[٢]

---

[١] Nuclear Weapons Advisory Opinion. Also, Meredith Hagger & Tim McCormack, “Regulating the Use of Unmanned Combat Vehicles: AreGeneral Principles of IHL Sufficient?” (2011) 21 JL Inf & Sci 74 at 81-84.

[٢] William Boothby, Weapons and the Law of Armed Conflict, (New York: Oxford University Press 2009) at ch 5.

وعليه، سنتعرض في هذا المبحث للمقصود بهذه القواعد بوجه عام في مطلب أول، ثم لتطبيق هذه القواعد على السلاح السيبراني في مطلب ثانٍ.

المطلب الأول

القواعد التي تحدد مدى مشروعية السلاح

إن السلاح العشوائي هو سلاح غير تمييزي؛ يستهدف كل ما يقع أمامه بدون تمييز بين الهدف المشروع والهدف غير المشروع، وفي نفس الوقت هو سلاح لا يمكن التحكم في الآثار التي يخلفها؛ ولذلك فهو غير مشروع. كذلك الحال بالنسبة للأسلحة التي تسبب آلامًا أو أضرارًا لا مبرر لها. وكلاهما غير مشروع؛ لأن الغاية من وراء قواعد القانون الدولي الإنساني هي تخفيف آثار الحرب على المدنيين، وكذلك أن تكون الحرب أكثر إنسانية؛ وبالتالي، فإن السلاح الذي لا يميز بين العسكري والمدني، أو ذلك الذي يسبب آلامًا لا مبرر لها للأهداف المشروعة (العسكريين) يخالف هذه الغاية. ومن هذا المنطلق، فإن تحديد مشروعية السلاح في حد ذاته تحكمها قاعدتان، وهما: ألا يكون السلاح عشوائيًا، وألا يسبب السلاح بطبيعته آلامًا أو أضرارًا لا مبرر لها.

القاعدة الأولى: ألا يكون السلاح عشوائيًّا:

يعرف البعض الأسلحة العشوائية بأنها تلك التي لا يمكن توجيهها إلى هدف محدد أو التحكم في آثارها.[١] ويعني ذلك، أن يكون السلاح أو نظم السلاح لا يمكن توجيهها ضد هدف عسكري محدد،[٢] أو لا يمكن التحكم في نطاق أثرها، فبمجرد إطلاقها لا يمكن احتواء أضرارها.

وهذه القاعدة موجودة بالمادة ٥١ (٤) من البروتوكول الإضافي الأول لاتفاقيات جنيف، تحت بند حماية السكان المدنيين من الهجمات العشوائية، فينص البروتوكول الإضافي الأول على أن الهجمات العشوائية هي: "أ- تلك التي لا توجه إلى هدف عسكري محدد، ب- أو تلك التي تستخدم طريقة أو وسيلة للقتال لا يمكن أن توجه إلى هدف عسكري محدد، ج- أو تلك التي تستخدم طريقة أو وسيلة للقتال لا يمكن

[١] Rebecca Crootof, The Killer Robots Are Here: Legal and Policy Implications, Cardozo Law Review, vol.36, p.1885

[٢] Anderson K, Reisner D, and Waxman M, 'Adapting the Law of Armed Conflict to Autonomous Weapon Systems' (2014) 90 International Legal Studies.

حصر آثارها ... ومن ثم فإن من شأنها أن تصيب، في كل حالة كهذه، الأهداف العسكرية، والأشخاص المدنيين، أو الأعيان المدنية دون تمييز".[١]

وقد اعتبر قضاة محكمة العدل الدولية في بعض آرائهم المنفردة أن قاعدة "ألا يكون السلاح عشوائيًا" من القواعد الآمرة والمطلقة،[٢] كما تعد من قواعد القانون الدولي العرفي، فكافة الدول ملزمة بعدم شن أي هجوم غير محدد الأهداف أو عشوائي. ويرى Schmitt أن السلاح العشوائي قد يُستخدم بشكل مشروع، فعلى سبيل المثال، فإنَّ استخدام سلاح غير تمييزي بطبيعته في بيئة منعزلة كالصحراء مثلاً أو أعالي

[١] توضح المادة ٥١ (٥) من البروتوكول الإضافي الأول أمثلة على الهجمات العشوائية، ومنها: "أ- الهجوم قصفاً بالقنابل، أياً كانت الطرق والوسائل، الذي يعالج عدداً من الأهداف العسكرية الواضحة التباعد والتميز بعضها عن البعض الآخر والواقعة في مدينة أو بلدة أو قرية أو منطقة أخرى تضم تركزاً من المدنيين أو الأعيان المدنية، على أنها هدف عسكري واحد، ب- والهجوم الذي يمكن أن يتوقع منه أن يسبب خسارة في أرواح المدنيين أو إصابة بهم أو أضراراً بالأعيان المدنية، أو أن يحدث خلطاً من هذه الخسائر والأضرار، يفرط في تجاوز ما ينتظر أن يسفر عنه ذلك الهجوم من ميزة عسكرية ملموسة ومباشرة".

[٢] See Declaration of Judge Bedjaoui, and the Separate Opinion of Judge Guillaume.

مشار إليه في إصدار اللجنة الدولية للصليب الأحمر بعنوان: "القانون الدولي الإنساني وفتوى محكمة العدل الدولية بشأن مشروعية التهديد بالأسلحة النووية أو استخدامها"، متاح على الموقع الإلكتروني:

https://www.icrc.org/ar/publication/lhl-advisory-opinion-icj-legality-threat-or-use-nuclear-weapons#

البحار يعدُّ مشروعًا، وعلى العكس فإن استخدام السلاح المشروع بشكل غير تمييزي يجعل منه سلاحًا غير مشروع، كفتح النار من مدفع رشاش على منطقة مأهولة بالمدنيين والمقاتلين بدون تمييز، وبالتالي فعدم مشروعية نظم السلاح في حد ذاتها لا تبرر حظرها التام، بل يجب النظر أيضًا في مشروعية استخدامها.[١]

ومن ناحية أخرى، فبعض الأسلحة العشوائية بطبيعتها، يمكن أن يتم تطويرها بحيث يمكن أن توجه لهدف محدد، وبالتالي تنتفي العلة من وراء حظرها. ومثال ذلك الألغام المضادة للأفراد،[٢] فبالرغم من أنها سلاح عشوائي بطبيعته، إلا أنَّ الولايات المتحدة قد قامت بتطوير نوع من الألغام "الذكية"، والتي يمكن أن تُدمر أو تُعطل تلقائيًّا بعد فترة زمنية معينة، أو في نهاية الأعمال العدائية، وبالتالي خلعت عنها صفة العشوائية.[٣]

---

[١] Michael N. Schmitt, Autonomous Weapon Systems and International Humanitarian Law, op.cit, p.10

[٢] See, e.g., Why the Ban, INT'L CAMPAIGN TO BAN LANDMINES, http://www.icbl.org/en-gb/problem/why-the-ban.aspx.

[٣] Emily Alpert, Why Hasn't the U.S. Signed an International Ban on Landmines?, L.A. TIMES BLOG, http://latimesblogs.latimes.com/world_now/2012/04/mine-treaty-us-ottawa-convention.html .

والخلاصة، أن السلاح العشوائي محظور في حد ذاته؛ وذلك بسبب أنه سلاح غير تمييزي بطبيعته، ويعرض حياة المدنيين والمقاتلين أيضًا للخطر، ومع ذلك فإن تلك الصفة لا تبرر حظره تمامًا؛ إذ يمكن استخدامه بطريق تمييزي، أو يمكن تطويره بحيث يتلاءم مع قواعد القانون الدولي الإنساني، وبالتالي يُصبح مشروعًا.

القاعدة الثانية: ألا يُسبب السلاح آلامًا أو أضرارًا غير ضرورية:

بدأ أول تقنين لحظر الأسلحة التي تسبب آلامًا أو أضرارًا غير ضرورية أو لا لزوم لها في إعلان سان بطرسبرغ لعام ١٨٦٨، حيث نص على أن الحرب ستتجاوز هدفها إذا تم "استخدام الأسلحة التي تؤدي إلى تفاقم معاناة الرجال المعوقين، أو تجعل موتهم لا مفر منه"، وأن استخدام هذه الأسلحة "يتعارض مع قوانين الإنسانية".[١]

ظهر هذا الحظر مرة أخرى في لوائح لاهاي الثانية لعام ١٨٩٩، وفي المادة ٣٥ (٢) من البروتوكول الإضافي الأول لعام ١٩٧٧، والذي نص على أن "يحظر استخدام

[١] " would be exceeded by the employment of arms which uselessly aggravate the sufferings of disabled men, or render their death inevitable" Declaration Renouncing the Use, in Time of War, of Certain Explosive Projectiles, Nov. 29–Dec. 11, 1868. Available at: https://ihl-databases.icrc.org/ihl/WebART/130-60001?OpenDocument

الأسلحة والقذائف والمواد ووسائل القتال التي من شأنها إحداث إصابات أو آلام لا مبرر لها". كما أن القاعدة (٧٠) من قواعد القانون الدولي الإنساني العرفي التي وضعتها اللجنة الدولية للصليب الأحمر حظرت استخدام "أسلحة وقذائف ومعدات وأساليب حربية يكون من طبيعتها أن تسبب أضراراً مفرطة أو آلاماً لا داعي لها".[١]

وفي عام ١٩٩٦، أوصت الندوة التي عقدتها اللجنة الدولية للصليب الأحمر بشأن "المهن الطبية وآثار الأسلحة" بأهمية إيجاد تعريف موضوعي للأسلحة التي تسبب أذى مفرطًا، أو معاناة لا مبرر لها، والذي عرف فيما بعد بمشروع "سايروس".[٢] وقد

---

[١] Rule 70. Weapons of a Nature to Cause Superfluous Injury or Unnecessary Suffering, INT'L COMMITTEE RED CROSS, http://www.icrc.org/customary-ihl/eng/docs/v1_rul_rule70 .

كذلك انظر: اتفاقية لاهاي (الرابعة) فيما يتعلق قوانين وأعراف الحرب البرية والملحق التابع لها: اللوائح المتعلقة بقوانين وأعراف الحرب البرية، ١٨ أكتوبر/تشرين الأول ١٩٠٧ ،المادة ٢٣/ هـ؛ والبروتوكول الإضافي الأول، المادة ٣٥؛ واتفاقية حظر أو تقييد استخدام أسلحة تقليدية معينة يمكن اعتبارها مفرطة الضرر أو عشوائية الأثر، ١٠ أكتوبر/تشرين الأول ١٩٨٠ ،الديباجة، الفقرة ٣.

[٢] اسم سايروس مشتق من الحظر المفروض على "استخدام الأسلحة والقذائف ومواد وأساليب الحرب التي من شأنها أن تسبب أذى مفرط أو معاناه لا مبرر لها". واقترح المشروع من خلال تحليل البيانات من المستشفيات أربعة معايير لتحديد ذلك، وهي عندما يتسبب السلاح في واحد مما يلي:

أ- مرض محدد أو حالة فسيولوجية غير طبيعية محددة، أو حالة نفسية غير طبيعية محددة أو إعاقة دائمة محددة أو تشوه محدد؛ أو

ب- نسبة وفاه في الميدان تتجاوز نسبة ٢٥٪، أو نسبة وفاه بالمستشفى تتجاوز ٥٪؛ أو

١٢- مدى انطباق القانون الدولي الإنساني على الهجمات السيبرانية

تعرضت بداية عمل المشروع إلى العديد من الانتقادات، أبرزها أنه لم يأخذ مبدأ الضرورة العسكرية في الاعتبار.

ومن أمثلة الأسلحة التي تسبب آلامًا لا مبرر لها: أسلحة الليزر المسببة للعمى،[١] وكذلك القنابل المعبأة بشظايا الزجاج التي لا يمكن رؤيتها بأشعة إكس إذا ما دخلت جسم الإنسان؛ وبالتالي تعقيد العلاج الطبي بدون داع. وتحمي هذه القاعدة المقاتلين على وجه الخصوص من التسبب لهم بآلام أو أضرار لا داعي لها. وبالرغم من أن معظم الأسلحة المستخدمة اليوم لا ينطبق عليها وصف الأسلحة التي تسبب آلامًا أو أضرارًا زائدة أو لا مبرر لها في حد ذاتها،[٢] إلا أن أي سلاح قد يُساء استخدامه بحيث يسبب هذه الآلام أو تلك الأضرار.

ت- جروح من الدرجة الثالثة وفقًا لتصنيف الصليب الأحمر؛ أو

ث- الآثار التي ليس لها علاج مثبت معترف به.

[١] انظر: البروتوكول الرابع الملحق باتفاقية حظر أو تقييد استعمال أسلحة تقليدية معينة يمكن اعتبارها مفرطة الضرر أو عشوائية الأثر 13تشرين الأول/أكتوبر ١٩٩٥ والخاص بأسلحة الليزر المسببة للعمى.

[٢] "إنَّ الألغام المضادة للأفراد المدفونة أو " ذات رأس صاعق " هي الأسلحة الوحيدة التي ينتشر استخدامها وتؤدي إلى إحداث إصابات جسيمة وتنتج عنها إعاقة محددة ودائمة. ويتطلب علاج الإصابات في المتوسط إجراء ضعف عدد العمليات ونقل أربعة أضعاف كميات الدم التي تتطلبها الإصابات الناجمة عن الأسلحة الأخرى." انظر: روبن م. كوبلاند، زميل كلية الجراحين الملكية،

المطلب الثاني

مدى استيفاء الأسلحة السيبرانية لقواعد مشروعية السلاح

لتحديد مدى مشروعية السلاح السيبراني، فإن ذلك يفترض الإجابة على تساؤلين، **الأول،** هل السلاح السيبراني سلاح عشوائي بطبيعته أو بأثره؟ **والثاني،** هل من الممكن أن يُسبب استخدام السلاح السيبراني آلامًا أو أضرارًا لا لزوم لها؟ وسنحاول الإجابة على كل منهما فيما يلي.

أولاً: هل السلاح السيبراني سلاح عشوائي؟

لتحديد ما إذا كان السلاح السيبراني عشوائيًّا بطبيعته أم لا؛ ينبغي في البداية معرفة طبيعة البيئة التي يعمل بها وكيفية عمله.

بالنسبة لطبيعة البيئة التي يعمل بها؛ فإن الفضاء السيبراني – كما سبق تعريفه – هو "كل شبكات الكمبيوتر في العالم، وكل شيء يتصل بها ويتحكم فيها، فهو ليس الإنترنت فحسب..... الفضاء السيبراني يشمل الإنترنت بالإضافة إلى الكثير من

مقال استعراض لمشروعية الأسلحة: مدخل جديد لمشروع "الإصابات المفرطة أو الآلام التي لا مبرر لها" المجلة الدولية للصليب الأحمر، العدد٨٣٥
https://www.icrc.org/ar/doc/resources/documents/misc/5yqfyf.htm

شبكات الكمبيوتر الأخرى التي لا يُفترض أن تكون متاحة للوصول إليها من خلال الإنترنت".[١] وأغلب الفضاء السيبراني ذو استخدام مزدوج، بمعنى أنه من الصعب فصل البنية التحتية المدنية فيه عن البنية التحتية العسكرية؛ إذ أن كليهما يستخدم نفس الفضاء السيبراني. ويرى البعض[٢] أنه حتى في الحالات التي يمكن فيها تمييز البنية التحتية العسكرية عن البنية التحتية المدنية، فإن آثار الهجمة على البنية التحتية العسكرية قد تمتد لنظيرتها المدنية بسبب ترابط الفضاء السيبراني. فعلى سبيل المثال، فإنَّ الفيروسات والديدان إذا أطلقت ضد هدف عسكري، فأسلوب عملها يعتمد على أنها تنسخ نفسها لتصيب عددًا أكبر من الكمبيوترات، وبالتالي فلا يمكن التحكم في آثارها، ولعله من المستحيل أن يضمن صانعوها أو مشغلوها أن أثرها لن يمتد للبنية التحتية المدنية، مما يشكل انتهاكًا لقاعدة ألا يكون السلاح عشوائيًّا. أما إذا فُرض

---

[١] 'Cyberspace is all of the computer networks in the world and everything they connect and control. It's not just the Internet. Let's be clear about the difference. The Internet is an open network of networks. From any network you should be able to communicate with any computer on the Internet, Internet's networks. Cyberspace includes the computers that are not supposed to be accessible from the Internet'.

R Clarke, Cyber War, op.cit., chapter 3.

[٢] كوردولا دوريجي ، لا تقترب من حدود فضائي الإلكتروني، المرجع السابق ، ص ٥٤٠

وأمكن تصميم السلاح السيبراني بحيث يوجه لهدف محدد فقط سيكون حينها مشروعًا؛ لأن آثاره ستقتصر على الكمبيوتر أو الشبكة أو النظام الذي يُعد هدفًا عسكريًّا فقط ولن تمتد لغيره.

ولكن هذا الاتجاه منتقد على أساس أن فيه تضييقًا لتفسير معنى السلاح العشوائي، كما أنه غير متصور في الواقع العملي، حيث إنَّ أغلب العمليات السيبرانية تفقد فاعليتها إذا كانت موجهة بشكل شديد التخصيص نحو هدف معين، بل إن من أبرز خصائص الأسلحة السيبرانية الانتشار، بمعنى أنها تعتمد في التدمير على أن تنتشر في أكبر عدد من أجهزة الكمبيوتر أو الأنظمة الحوسبية. [١]

وفي ذلك، يوضح دليل تالين أنه لكي يعتبر السلاح السيبراني سلاحًا عشوائيًّا يجب أن تكون الآثار الضارة التي من المحتمل أن تنتشر بشكل خارج عن السيطرة من جراء استخدامه، ترقى إلى مستوى معين من الضرر؛ فالانتشار الواسع الذي لا يمكن

[١] William Boothby, 'How will weapons reviews address the challenges posed by new technologies?', Military Law and the Law of War Review, vol. 52, no. 1 (2013)

السيطرة عليه للآثار غير الضارة، أو الآثار التي تكون فقط غير ملائمة أو مزعجة، هي آثار ليست ذات صلة عند تقييم مدى مشروعية السلاح السيبراني.[١]

ومثال ذلك فيروس Stuxnet الذي تم تصميمه ليستهدف المنشآت النووية الإيرانية، فقد أشارت التقارير إلى أن هذا الفيروس لم يكن مقصودًا به إصابة أجهزة الكمبيوتر خارج النظم المستهدفة في المنشآت النووية، ومع ذلك فقد نسخ نفسه خارج إيران، وهذا يوضح صعوبة التحكم في شكل انتشار الفيروس، ولكن من ناحية أخرى فإن انتشاره إلى خارج نطاق الهدف المحدد له لم يسبب أي أضرار للبنية التحتية المدنية، في حين اقتصر الضرر الكبير على المعدات التقنية للعدو؛ وبالتالي فلا يعد هذا السلاح عشوائيًّا.[٢]

ومن ثم، فإنه يجب على الدول عند القيام بعملية استعراض السلاح السيبراني أن تختبر أمرين، **الأول**: أنه يجب حظر استخدام الأسلحة السيبرانية التي تقوم بمهاجمة البنية التحتية المدنية والعسكرية، وتنتشر بها بدون تمييز، وتكون آثارها على البنية التحتية المدنية كبيرة وملموسة؛ إذ إنه في هذه الحالة سينطبق عليها وصف الأسلحة

---

[١] Tallinn Manual, op.cit., p.452.

[٢] كوردولا دوريجي ، لا تقترب من حدود فضائي الإلكتروني، المرجع السابق، ص ٥٥٠

العشوائية، **الثاني:** يجب على كل طرف أن يجري تقييمًا لكل حالة على حدة وبحسب ظروفها، والنظر فيما إذا كان من الممكن توجيه السلاح السيبراني إلى هدف عسكري محدد، بدون أضرار ملموسة على البنية التحتية المدنية، وما إذا كان تأثيره يمكن السيطرة عليه.[١]

ثانيًا: هل من الممكن أن يُسبب استخدام السلاح السيبراني آلامًا أو أضرارًا لا مبرر لها؟

في حين أنَّ آثار الغالبية العظمى من العمليات السيبرانية غير حركية non–kinetic، إلا أنه قد تكون لها آثار حركية kinetic أيضًا، قد تؤدي إلى إحداث الوفاة، أو إصابة الأشخاص من خلال استغلال نقاط الضعف في أنظمة الكمبيوتر والشبكات المرتبطة بالعمليات الفيزيائية وتوجيهها. ومثال ذلك، مصفاة النفط التي تُدار من خلال أجهزة الكمبيوتر، فإنَّ أي تغير ولو طفيف في درجة حرارة غليان السائل، سيؤدي إلى التسخين الشديد للسائل داخل المصفاة، مما يتسبب في وقوع انفجار يودي بحياة مئات الأشخاص من جهة، وشلل الاقتصاد في المنطقة المعنية من جهة أخرى. لذلك، يذهب البعض إلى أنَّ السلاح السيبراني أخطر من أي سلاح آخر؛ إذ إن

[١] Vincent Boulanin And Maaike Verbruggen, Article 36 Reviews Dealing with The Challenges Posed by Emerging Technologies, op.cit., p.25.

مجرد الضغط على زر قد يلحق أضرارًا مادية وخسائر بشرية، أكبر من ضربات صاروخية أو نووية.[1]

وفي الواقع الفعلي، فبالرغم من أن دودة الكمبيوتر Stuxnet التي أصابت نظام التحكم الإشرافي والحصول على البيانات (SCADA) Supervisory Control and Data Acquisition في المنشأة النووية الإيرانية لم تخلف خسائر بشرية أو بيئية، إلا أنها تسببت في خروج أجهزة الطرد المركزي عن السيطرة، مما تسبب في دمار مادي لا إصلاح له، وتدمير ألف جهاز طرد مركزي.[٢] وتوجد أمثلة واقعية على عمليات سيبرانية أدت إلى خسائر مادية وبشرية عن طريق استهداف أجهزة طبية غير

[1] عالم روسي: السلاح السيبراني أخطر سلاح في العالم، RT online، ٢٦ يونيو ٢٠١٩.
https://arabic.rt.com/it/1028347-%D8%A7%D9%84%D8%B9%D8%A7%D9%84%D9%85-%D8%A7%D9%84%D8%B3%D9%84%D8%A7%D8%AD-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A-%D8%A7%D9%84%D8%B9%D8%A7%D9%84%D9%85/

[٢] Ido Kilovaty, Cyber Conflict and The Thresholds of War, op.cit., p.6.

محصنة؛ مما تسبب في إصابات جسدية ووفاة للمرضى، أيضًا أدت العمليات السيبرانية إلى اختطاف مركبات، والتحكم فيها عن بعد مما نتج عنه خسائر بشرية.[١]

ويُلاحظ أنه حتى الآن، لم تتسبب الهجمات السيبرانية في إحداث آلام أو إصابات خطيرة لا مبرر لها أو غير ضرورية. فينبغي العلم أن المعيار هنا في انتهاك قاعدة ألا يسبب السلاح آلامًا أو أضرارًا لا مبرر لها، لا يمنع من أن يتسبب السلاح في إحداث وفيات، أو إصابات، وإنما يعني ببساطة ألا تكون الإصابات لا مبرر لها، أو تتسبب في معاناه غير ضرورية.

ويؤكد دليل تالين على أن وسائل وأساليب الحرب السيبرانية لن تنتهك – إلا في حالات نادرة – هذه القاعدة. ومثال ذلك، إذا كان القائد المستهدف من الهجوم يستخدم جهاز تنظيم ضربات القلب، فمن المشروع – وفقًا للقانون الدولي الإنساني – أن يتم استهدافه بالقتل؛ لأنه هدف عسكري، وسيان أن يتم ذلك عن طريق طلقة رصاص، أو عن طريق السيطرة على جهاز تنظيم ضربات القلب لقتل ذلك الشخص، أو جعله عاجزًا عن القتال. ولكن من غير المشروع – وفقًا لقاعدة ألا يسبب السلاح

[١] Scott Applegate, The Dawn of Kinetic Cyber, in 2013 5TH INTERNATIONAL CONFERENCE ON CYBER CONFLICT 163, 164 (K. Podins, J. Stinissen, M. Maybaum eds., 2013).

آلامًا أو أضرارًا لا لزوم لها - استخدام السيطرة على جهاز تنظيم ضربات القلب بطريقة تهدف إلى إحداث المزيد الألم والمعاناة، مثل وقف قلب الهدف، ثم إحيائه عدة مرات قبل قتله في النهاية؛ لأن القيام بذلك من شأنه أن يتسبب في معاناة لا تخدم أي غرض عسكري.[١]

ومن ثم، يجب على الدول عند القيام بعملية استعراض السلاح السيبراني أن تأخذ في الحسبان في تقييمها الآثار غير المباشرة المحتملة لاستخدام السلاح، ومنها تأثير السلاح على الأشخاص المتأثرين بشكل مباشر بفقدان الاستخدام ووظيفة الأنظمة، هذا التقييم للتأثيرات الجانبية ضروري لتحديد ما إذا كان من المتوقع أن يتسبب استخدام السلاح أو وسائل أو طريقة الحرب الجديدة في إصابات لا داعي لها أو معاناة لا داعي لها.[٢]

وبالتالي، نخلص مما سبق إلى أن السلاح السيبراني - بحسب وضعه الحالي - لا يخالف القواعد التي تحدد مدى مشروعية السلاح، فهو ليس سلاحًا عشوائيًّا، ولا يتسبب استخدامه العادي في آلام غير ضرورية. وإن كان ذلك لا يمنع من إمكانية

---

[١] Tallinn Manual, op.cit., p.452.

[٢] Vincent Boulanin And Maaike Verbruggen, Article 36 Reviews Dealing with The Challenges Posed by Emerging Technologies, op.cit., p.25.

تصميمه أو استخدامه بشكل ينتهك تلك القواعد. وفي كل الأحوال، فإن مراجعة الأسلحة السيبرانية وفقًا للمادة ٣٦ الخاصة باستعراض الأسلحة الجديدة يثير عدة تحديات خاصة وأن البرمجيات في تطور مستمر، وكذلك حماية نظم الكمبيوتر في تطور مستمر، مما يفرض إجراء تطويرات وتحديثات بشكل مستمر على الفيروسات، والبرمجيات التي تستخدم في الهجوم، وما يستتبعه من إجراء استعراض جديد للأسلحة السيبرانية مع كل تعديل جوهري على السلاح المستخدم.

الفصل الثالث

الهجمات السيبرانية كأسلوب للقتال

تمهيد:

يعرف دليل تالين أساليب الحرب السيبرانية بأنها: "التكتيكات والتقنيات السيبرانية والإجراءات التي تتم بها الأعمال العدائية".[١] ووفقًا لذلك، فإن أدوات الهجوم السيبراني مثل الفيروسات والبرامج الضارة وغيرها تندرج تحت وصف أدوات الحرب أو (الأسلحة)، أما توظيفها بشكل تكتيكي معين لإحداث نتيجة معينة فهو "أسلوب الحرب".

ويتفق أغلب الفقه – **ونؤيده** – على أن قواعد القانون الدولي الإنساني هي المطبقة على كافة العمليات السيبرانية التي تؤدي إلى إحداث نتائج عنيفة كالخسائر أو الإصابات البشرية، أو تدمير الأعيان، في حين يرى جانب من الفقه أن القانون

[١] "Methods of cyber warfare are the cyber tactics, techniques, and procedures by which hostilities are conducted". Tallinn Manual, op.cit., p.452.

الدولي الإنساني مطبق حتى على العمليات السيبرانية التي لا تؤدي إلى نتائج عنيفة.[١] ومع ذلك، لا يوجد إجماع في الفقه حول مدى انطباق مبادئ القانون الدولي الإنساني على العمليات السيبرانية.

وبالتالي، يتناول هذا الفصل الهجمات السيبرانية كأسلوب للقتال، ومدى امتثالها بهذه الكيفية – أي كأسلوب للقتال – لمبادئ القانون الدولي الإنساني الثلاثة، وهي: مبدأ التمييز، ومبدأ التناسب، ومبدأ الاحتياط في الهجوم.

تقسيم:

وبناء على ما تقدم، سيتم تقسيم الدراسة في هذا الفصل إلى مبحثين على النحو التالي:

المبحث الأول: مبدأ التمييز في الهجوم.

المبحث الثاني: مبدأ التناسب والاحتياط في الهجوم.

[١] Papanastasiou Afroditi, Application of International Law in Cyber Warfare Operations, op.cit., p.28.

المبحث الأول

مبدأ التمييز في الهجوم

ورد مبدأ التمييز في الهجوم في المادة ٤٨ من البروتوكول الإضافي الأول، التي نصت على: "أن تعمل أطراف النزاع على التمييز بين السكان المدنيين والمقاتلين وبين الأعيان المدنية، والأهداف العسكرية ومن ثم توجه عملياتها ضد الأهداف العسكرية دون غيرها". كما يعد هذا المبدأ من مبادئ القانون الدولي العرفي، وذلك بحسب ما أقرته اللجنة الدولية للصليب الأحمر،[١] وما انتهت إليه محكمة العدل الدولية.[٢]

وفقًا للمادة ٤٨ من البروتوكول الإضافي الأول، فإن مبدأ التمييز يتضمن شقين، **الأول:** التمييز بين المقاتلين والمدنيين، **والثاني:** التمييز بين الأهداف العسكرية والأعيان المدنية. وبناءً عليه، سنتعرض لكل شق منهما في مطلب مستقل، وذلك لتحديد ما إذا كانت الهجمات السيبرانية تفي بمتطلبات مبدأ التمييز.

---

[١] Yves Sandoz and others, Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949, op.cit, at 598.

[٢] Nuclear Weapons Advisory Opinion.

المطلب الأول

التمييز بين المقاتلين والمدنيين

نصت المادة ٤٣ من البروتوكول الإضافي الأول على أن يعد أفراد القوات المسلحة لطرف النزاع "مقاتلين بمعنى أن لهم حقَّ المساهمة المباشرة في الأعمال العدائية".[١] وتنص المادة ٤٤ من نفس البروتوكول على أن "يعد كل مقاتل ممن وصفتهم المادة ٤٣ أسير حرب إذا ما وقع في قبضة الخصم"، وعلى أن "يلتزم المقاتلون، دفعًا لحماية المدنيين ضد آثار الأعمال العدائية، أن يميزوا أنفسهم عن السكان المدنيين أثناء اشتباكهم في هجوم أو في عملية عسكرية تجهز للهجوم. أما وأنَّ هناك من مواقف المنازعات المسلحة ما لا يملك فيها المقاتل المسلح أن يميز نفسه على النحو المرغوب، فإنه يبقى عندئذ محتفظاً بوضعه كمقاتل شريطة أن يحمل سلاحه علناً في مثل هذه المواقف: أ(أثناء أي اشتباك عسكري، ب(طوال ذلك الوقت الذي يبقى

[١] المادة ٢/٤٣ من البروتوكول الإضافي الأول الإضافي إلى اتفاقيات جنيف المعقودة في ١٢ آب / أغسطس ١٩٤٩ والمتعلق بحماية ضحايا المنازعات الدولية المسلحة، متاح على https://www.icrc.org/ar/doc/resources/documents/misc/5ntccf.htm ويشار إليه فيما بعد بـ "البروتوكول الإضافي الأول".

خلاله مرئيّاً للخصم على مدى البصر أثناء انشغاله بتوزيع القوات في مواقعها استعداداً للقتال قبيل شن هجوم عليه أن يشارك فيه".

وبتطبيق هذه القواعد العامة على الهجمات السيبرانية، فإن "المدنيين" هم الفئة المحمية، أي أنه لا يجوز استهدافهم. أما "المقاتلين" فهم الفئة المشروع استهدافهم بالهجمات السيبرانية ويشملون: (أ) أفراد القوات المسلحة، (ب) أعضاء الجماعات المسلحة المنظمة، (ج) المدنيين إذا شاركوا بشكل مباشر أو مستمر في الأعمال العدائية، (د) المشاركين في الانتفاضة الجماعية أو الهبة الشعبية levée en Masse في نزاع مسلح دولي.[١] وسنتناول كل فئة منهم على النحو التالي.

أولاً: المدنيون:

تكمن الحكمة من حماية المدنيين من الاستهداف أثناء المنازعات المسلحة، أن الغرض من الاستهداف هو حرمان الخصم من مقاتليه، وإضعاف قوته القتالية، وبالتالي فطالما أن المدنيين لا يُشاركون في الأعمال العدائية فتنتفي الحكمة من استهدافهم. ويُقصد بـ "الاستهداف" أن تكون الهجمة موجهة ضد المدنيين وعن عمد، أما الهجمات الموجهة ضد أهداف عسكرية مشروعة، وينتج عنها خسائر بشرية بين

[١] Tallinn Manual, op.cit., p. ٤٢٥

المدنيين، أو إهلاك، أو تدمير البنية التحتية المدنية بشكل عرضي، فلا تعد من قبيل استهداف المدنيين. وفي إطار العمليات السيبرانية، فإن الهجوم المحظور ضد المدنيين هو ذلك الذي يؤدي إلى تدمير البنية التحتية، أو إلحاق خسائر بشرية مقصودة بهم، أما ذلك الهجوم الذي يؤدي لإصابة عرضية للمدنيين فلا يُعد هجومًا موجهًا ضد المدنيين. ومثال ذلك، استهداف نظم إلكترونية لإسقاط طائرات عن طريق هجمات سيبرانية، فإذا أدى هذا الاستهداف إلى سقوط طائرات بالإضافة إلى خسائر في أرواح المدنيين، وإصابات وإهلاك أعيان مدنية، فإنَّ ذلك لا يعد هجومًا موجهًا ضد المدنيين.[١]

نظرًا إلى أنَّ الفضاء السيبراني يستخدم من قبل المدنيين والعسكريين على السواء، فقد يصعب تحديد ما إذا كان الهدف، أو الشخص المقصود مدنيًا أم عسكريًا. فعلى سبيل المثال، إذا ثار الشك حول وجود عسكريين (هدف مشروع) داخل مستشفى (هدف غير مشروع)، فهل يجوز توجيه هجمات ضد المستشفى؟ وفقًا للمادة ١/٥٠ من البروتوكول الإضافي الأول، والقاعدة (٦) من قواعد القانون الدولي العرفي التي وضعتها اللجنة الدولية للصليب الأحمر، فإنه في حالة الشك في وضع الشخص – ما

[١] Tallinn Manual, op.cit., p. ٤٢٣

إذا كان مدنيًّا أم مقاتلًا – فيجب اعتبار الشخص حينها مدنيًّا.[١] ولكن المقصود بـ "الشك" كان محل خلاف، ففي أثناء تصديق المملكة المتحدة على البروتوكول الإضافي الأول، لاحظت أن المقصود بـ "الشك" هو "الشك الجوهري" بعد "تقييم المعلومات من جميع المصادر المتاحة بشكل معقول".[٢] في حين أن القانون الدولي الجنائي يأخذ بمعيار "الشك المعقول" لأغراض تحديد المسؤولية بموجب القانون الجنائي الدولي.[٣] ووفقًا لدليل تالين، أيًّا كانت درجة الشك فمن المتفق عليه أن "مجرد الشك" لا يكفي لتطبيق هذه القاعدة.[٤] وبالتالي، فإذا ثار "الشك" حول وجود عسكريين داخل مستشفى، فلا يجوز استهداف تلك المستشفى بهجمات سيبرانية، ولكن ينبغي أن يكون لهذا الشك مبررات كافية ومعقولة.

وتثير Afroditi مسألة استخدام الدول للمدنيين لتنفيذ الهجمات السيبرانية، وترى أنَّ هذا الأمر وارد جدًّا لعدة أسباب، وهي: أن المدنيين يمتلكون الخبرة التقنية في المجال

---

١ IHL Study commentary accompanying Rule 6. ICRC Customary

٢ "substantial doubt still remaining after the assessment of information from all sources which is reasonably available to them from all sources". UK Additional Protocol Ratification Statement, para. (h)

٣ Galić Trial Chamber judgment, para. 55.

٤ Tallinn Manual, op.cit., p. ٤٢٤

السيبراني التي لا تمتلكها الحكومات، وكذلك – والأهم – أن الدول تستطيع – باستخدام المدنيين – أن تُخفي مشاركتها في مثل هذه العمليات، وبالتالي تتنصل من أي مسئولية. وبالفعل، فقد تحملت ناشي Nashi، وهي مجموعة شبابية موالية للكرملين أسسها فلاديمير بوتين، المسؤولية عن الهجمات السيبرانية ضد إستونيا عام ٢٠٠٧، وقد زُعم أن رجال الأعمال الروس يمولون ناشي لتنفيذ هجمات سيبرانية لصالح الحكومة الروسية، في نفس الوقت أنكرت روسيا تمامًا صلتها بهذه الهجمات.[١]

ونرى أن تنفيذ الهجوم السيبراني بواسطة جهات من غير الدول تشبه فكرة "الحروب بالوكالة"، والتي تتم من خلال قيام دولة بدعم جماعات مسلحة لتأجيج نزاعات مسلحة غير دولية، أو لإدامة نزاع مسلح قائم بالأصل، لأجل التأثير على الواقع الداخلي لتلك الدولة، وجني مصالح بعيدة المدى دون أن تظهر هذه الدولة بمظهر المتدخل المباشر في النزاع.[٢]

---

[١] Oona A. Hathaway, et al. "The Law of Cyber-Attack", op.cit., pp. 817–85.

[٢] ومثال لذلك النزاع المسلح الدولي بسوريا، حيث دعمت تركيا تأسيس جماعة "الجيش السوري الحر" للإطاحة بنظام الأسد وإقامة دولة إسلامية في سوريا، وتورط إيران في تسليح الحوثيين في اليمن.
م.د. بشير سبهان أحمد، موقف القانون الدولي من الحرب بالوكالة أو الإنابة (حروب الجيل الرابع)، مجلة جامعة تكريت للحقوق، السنة ٣، المجلد ٣، العدد ٢، الجزء ١، ٢٠١٩، ص. ٧٥.

ثانيًا: المقاتلون:

تشمل فئة المقاتلين – كما هو مبين في دليل تالين – : (أ) أفراد القوات المسلحة، (ب) أعضاء الجماعات المسلحة المنظمة، (ج) المدنيين إذا شاركوا بشكل مباشر أو مستمر في الأعمال العدائية، (د) المشاركين في الانتفاضة الجماعية أو الهبة الشعبية levée en Masse في نزاع مسلح دولي.[١]

وبالتالي، فإن أفراد الوحدات المتخصصة للدفاع السيبراني التابعة للجيوش النظامية يندرجون بوضوح تحت هذه الفئة. كذلك القوات شبه العسكرية، والشرطة المسلحة، ومقاتلي الحروب ممن لا يرتدون زيًّا عسكريًّا موحدًا أو يحملون شارةً أو علامةً، والجماعات المسلحة في إطار النزاعات المسلحة غير الدولية.[٢]

وتبرز إشكالية بشأن اشتراك هذه الفئة في العمليات السيبرانية، وهي اشتراط أن تميز تلك الوحدات نفسها عن السكان المدنيين (المادة ٤٣ من البروتوكول الإضافي الأول)، وكذلك أن يميز المقاتل نفسه عن طريق "حمل السلاح علانية" (المادة ٣/٤٤ من البروتوكول الإضافي الأول)؛ إذ إن ذلك غير ممكن بالنظر لطبيعة الهجمات

---

[١] Tallinn Manual, op.cit., p. ٤٢٥

[٢] المادة ٣/٤٣ من البروتوكول الإضافي الأول.

السيبرانية التي تقوم أساسًا على قدرة المهاجم على اختراق جهاز الكمبيوتر، وإدخال البرمجيات الخبيثة بشكل خفي أو غير مكتشف. ولذلك، فالسهولة النسبية التي يستطيع بها أي شخص (سواء مدنيًا أو عسكريًا) أن يظل غير مكتشف في أثناء قيامه بالهجمات السيبرانية، تثير مسائل عديدة بخصوص مشروعية الهجمات السيبرانية، ومن بينها الامتثال للمادتين ٤٣ و٤٤ من البروتوكول الإضافي الأول.[١]

يرى Gervais أنه يمكن معالجة هذه المشكلة جزئيًا عن طريق نقل المسئولية للحكومات لحظر، أو منع، أو وقف الهجمات السيبرانية على مواقع البنية التحتية للإنترنت. وتتحمل الدول التي لا تمتثل للوائح الأساسية المسئولية الدولية عن عدم الامتثال لتطبيق هذا الحظر.[٢] وبالتالي، يكون أي شخص ينفذ هجمات سيبرانية ضد أي دولة هو بحسب الأصل مقاتلًا، إلا إذا ثبت أنه يقوم بعمليات سيبرانية إجرامية من باب التخريب، فحينها يخضع فعله للقانون الداخلي.

أما بالنسبة لفئة المدنيين المشتركين بشكل مباشر أو مستمر في الأعمال العدائية، فوفقًا للمادة ٣/٥١ من البروتوكول الإضافي الأول، يفقد المدنيون حقهم في عدم

---

[١] Papanastasiou Afroditi, Application of International Law in Cyber Warfare Operations, op.cit., p.31.

[٢] Michael Gervais, Cyber Attacks and the Laws of War, op.cit., p.33.

استهدافهم إذا شاركوا بشكل مباشر أو بشكل مستمر في الأعمال العدائية.[١] ولتفسير ذلك، فقد نظمت اللجنة الدولية للصليب الأحمر ومعهد TMC Asser في الأعوام ٢٠٠٣ و ٢٠٠٤ و ٢٠٠٥ مؤتمرات خبراء لتحديد مفهوم الاشتراك المباشر في الأعمال العدائية لإلقاء بعض الضوء على تفسير دقيق للمادة ٣/٥١ من البروتوكول الإضافي الأول، وبالتحديد الإجابة على سؤال "من يعتبر مدنيًا لغرض تطبيق مبدأ التمييز؟ "، وكانت إحدى النتائج الرئيسة لهذه العملية تبلور ثلاثة معايير تراكمية لتصنيف أعمال المدنيين حتى تصل إلى مستوى اشتراك مباشر في الأعمال العدائية، وبالتالي تخلع عنهم الحماية وتبرر استهدافهم، وهي: عتبة الضرر، علاقة سببية مباشرة بين الفعل والضرر، والارتباط بالعمل الحربي.

[١] تنص المادة ٣/٥١ من البروتوكول الإضافي الأول على أن: "يتمتع الأشخاص المدنيون بالحماية التي يوفرها هذا القسم ما لم يقوموا بدور مباشر في الأعمال العدائية، وعلى مدى الوقت الذي يقومون خلاله بهذا الدور". وقد أكدت اللجنة الدولية للصليب الأحمر أنه وفقًا للقانون الدولي العرفي، فإن المدنيين الذين يشتركون في القتال بشكل مستمر يفقدون الحماية المقررة لهم باعتبارهم مدنيين.

INT'L COMM. OF THE RED CROSS, Interpretive Guidance on The Notion of Direct Participation in Hostilities Under International Humanitarian Law 16 (2009), available at http://www.icrc.org/eng/assets/files/other/icrc_002_0990.pdf

عتبة "الضرر"

إنَّ هدف أي عمل عدائي هو إلحاق ضرر ذي طبيعة عسكرية بالخصم، ويشمل الإضرار بالخصم إلحاق الموت، أو الإصابة أو الدمار بالأهداف العسكرية، وكذلك أي أفعال من شأنها التأثير سلبًا في القدرة العسكرية للخصم مثل الأنشطة السيبرانية التي تؤدى لإعاقة انتشار القوات، أو قطع الاتصالات، أو القبض على أفراد الجيش.[١]

كذلك، يجب أن يكون العمل الضار مصممًا خصيصًا لدعم أحد أطراف النزاع ضد طرف آخر، فإن لم يكن كذلك فلا يمكن اعتبار هذا العمل عملاً عدائيًّا. ومثال ذلك، الهجمات السيبرانية ضد المواقع الإلكترونية الحكومية؛ بهدف سرقة البيانات والتكسب من بيعها، فتلك الأفعال – وإن كانت قد تخدم أحد أطراف النزاع على حساب الطرف الآخر – إلا أن ذلك ليس الغرض من ارتكاب هذه الجرائم، وبالتالي لا يمكن اعتبارها اشتراكًا في الأعمال العدائية، بل تعد جرائم تخضع للقانون الداخلي.

[١] ذكر التقرير أن الوصول إلى حد حصول الضرر يتحقق بوضوح إذا كان من المعقول التوقع بأن يسبب عمل معين أضرارًا مادية معينة للأشخاص أو للأعيان بالموت أو بالإصابة أو بالتدمير.
Report of DPH 2005, ICRC, P.30

علاقة السببية:

يميز تقرير اللجنة الدولية للصليب الأحمر بين الاشتراك المباشر وغير المباشر في الأعمال العدائية على أساس مدى توفر علاقة السببية بين "نشاط الاشتراك" و"الإضرار بممتلكات العدو"؛ فإذا تسبب النشاط العدائي بشكل مباشر في إحداث أضرار بممتلكات العدو، يعد هذا النشاط حينها "اشتراك مباشر"، وإذا تسبب النشاط بشكل غير مباشر في إحداث أضرار بالعدو؛ عُد النشاط حينها "اشتراك غير مباشر".[١] وبالتالي، فالاشتراك المباشر في الأعمال العدائية هو ذلك النشاط الذي يؤدي للإضرار بالقدرة العسكرية للخصم في خطوة مسببة واحدة بعلاقة مباشرة، أما الاشتراك غير المباشر فهو نشاط أو أنشطة تكتفى ببناء القدرات الكفيلة بإلحاق الضرر بالخصم فلا تتسبب بإضراره إلا بشكل غير مباشر.[٢]

---

[١] في عام ٢٠٠٣، قامت اللجنة الدولية للصليب الأحمر بالتعاون مع مؤسسة Asser لعمل مشروع كبير يهدف لتحديد مفهوم المشاركة المباشرة للمدنيين في الأعمال العدائية DPH Project، في صورة تقارير سنوية (٢٠٠٣ –٢٠٠٨)، وتم الانتهاء من هذا المشروع في ٢٠٠٨، وفى مايو ٢٠٠٩ قامت اللجنة الدولية للصليب الأحمر بتجميع خلاصة تلك التقارير في دليل تفسيري واحد.
ICRC, Overview of the ICRC's expert process 2003 –2008, http://www.icrc.org/web/eng/siteeng.nef/html

[٢] Report of DPH 2003, ICRC, P.2, Report of DPH 2004, ICRC, P.6, Report of DPH 2005, ICRC, P.15

ومع ذلك، فإن الأمر ليس بهذه البساطة في التطبيق على الهجمات السيبرانية. فالهجمات السيبرانية عملية معقدة، تعتمد على أنشطة مختلفة يساهم فيها أكثر من شخص؛ مما يجعل تمييز الفاصل بين الاشتراك المباشر والاشتراك المستمر أمرًا يعتمد على ظروف كل حالة على حدة. فعلى سبيل المثال يقوم مصمم البرنامج بتصميم البرمجيات الخبيثة، وبعدها تأتي مرحلة تعديل كود هذا البرنامج وتوظيفه لاستهداف نظم معينة، والتي يقوم بها المبرمج، وبعدها مرحلة التنفيذ الفعلي للهجمة، والتي يقوم بها المُنفذ، وقد يشارك معهم طواقم لجمع البيانات، فضلاً عن القائد المسئول عن تلك العملية. وعليه، فكيف يمكن تحديد أي نشاط منهم يعد اشتراكًا مباشرًا، وأيهم يعد اشتراكًا غير مباشر؛ إذ يصعب في هذه الحالة تحديد مدى تسبب كل نشاط منهم – إذا كان بمعزل عن الأنشطة الأخرى– في إحداث الضرر؛ بمعنى آخر فإن كل نشاط منهم – في حد ذاته – مثل دور المبرمج مثلاً – يساهم بشكل غير مباشر في إحداث الضرر، أما مجموع هذه الأنشطة، كلها فهي تساهم بشكل مباشر في إحداث الضرر بالعدو.

ولذلك فقد استقر الرأي على أنه إذا لم يسبب عملًا محددًا بنفسه وبصورة مباشرة – بمعزل عن الأنشطة الأخرى – الضرر، فإن شرط السببية المباشرة قد يتحقق مع ذلك

١٢- مدى انطباق القانون الدولي الإنساني على الهجمات السيبرانية

إذا كان هذا النشاط جزءًا لا يتجزأ من عملية تكتيكية ملموسة، ومنسقة تسبب هذا الضرر.[١] وبناءً عليه، فإن الاشتراك المباشر في الأعمال العدائية يشمل أيضًا الأنشطة التي لا تسبب الضرر بشكل مباشر – في ذاتها – وإنما باقترانها بأعمال أخرى. كذلك فإنَّ الاشتراك المستمر في الأعمال العدائية، يُفقد المدني الحماية المكفولة له ويجعل منه هدفًا مشروعًا. ومثال ذلك، إذا اعتاد المصمم المدني أن يصمم البرمجيات الخبيثة للمبرمج، ففي هذه الحالة ينطبق عليه وضع أنه يقوم بـ "وظيفة مستمرة تتضمن التحضير، أو التنفيذ، أو قيادة الأعمال، أو العمليات التي ترقى إلى الاشتراك المباشر فيها".[٢] وبالتالي، فتحديد دور المدني في الهجمة، وتكييف اشتراكه في الأعمال العدائية يتطلب النظر بدقة لدور كل مدني متورط في الهجمات السيبرانية على حدة، وبناءً عليه قد يتغير وضعهم، مما يجعلهم أهدافًا مشروعة.

---

[١] Report of DPH 2005, ICRC, P.35

[٢] "Although the principle that a civilian who directly participates in hostilities or who adopts a continuous combat function may be lawfully attacked is not in dispute, the status of a civilian who provides indispensable, contemporaneous assistance in cyber-attacks remains unresolved". Geoffrey S. Corn, Unarmed but How Dangerous? Civilian Augmentees, the Law of Armed Conflict, and the Search for a More Effective Test for Permissible Civilian Battlefield Functions, 2 J. NAT'L SEC. L. & POL'Y 257, 286-87 (2008).

الارتباط بالعمل الحربى

يساعد ارتباط العمل العدائي بزمان ومكان العمليات الحربية في بعض الأحيان على تصنيف الاشتراك في الأعمال العدائية كاشتراك مباشر أو غير مباشر، فعلى سبيل المثال، فإن قيادة شاحنة ذخيرة إلى موقع إطلاق النار في الخطوط الأمامية يعد جزءًا لا يتجزأ من المعركة الجارية، وبالتالي يُصنف كاشتراك مباشر لارتباطه زمنيًّا ومكانيًّا بالعمل العدائي. في حين أن قيادة نفس الشاحنة من مصنع إلى مرفأ لا يؤدى مباشرة لإحداث أضرار عسكرية؛ وبالتالي يمكن تصنيف هذا النشاط كاشتراك غير مباشر في الأعمال العدائية.[١]

ومع ذلك، ففي إطار الهجمات السيبرانية، لا يمكن الاعتماد على الارتباط الزمنى والمكاني وحده لتصنيف الاشتراك في الأعمال العدائية – كاشتراك مباشر أو غير مباشر–، إذ قد يشترك الأشخاص بشكل مباشر في الأعمال العدائية برغم انتفاء الارتباط الزمنى والمكاني بالعمليات العدائية، فالبرمجيات الخبيثة قد يتم ضبطها على التفعيل بعد عدة أشهر أو حتى سنوات، وقد يقوم بها أشخاص بعيدون مكانيًّا عن

[١] Report of DPH 2005, ICRC, P.35

موقع العمليات العدائية. ففي الحالتين، تكون علاقة السببية بين العمل العدائي وحدوث الضرر علاقة مباشرة برغم انتفاء الارتباط الزمني والمكاني بالضرر.

بناءً على ما سبق، يتحقق الاشتراك المباشر في الأعمال العدائية عندما تكون العلاقة مباشرة بين العمل العدائي وحدوث الضرر، أو إذا كان العمل جزءًا من عملية عسكرية واحدة تكتيكية، أما الاشتراك غير المباشر فيتحقق من خلال أي عمل يؤدى إلى حدوث أضرار للخصم بشكل غير مباشر، أو بمعنى آخر، يتحقق من خلال الأنشطة التحضيرية التي تسعى لبناء القدرات الكفيلة بإلحاق الضرر بالخصم.[١]

[١] ومع ذلك، يرى الجنرال كولونيل جيفري إس كورن Geoffrey S. Corn، أن معيار الاشتراك المباشر – بوضعه الحالي – لا يصلح لتحديد الاشتراك في الهجمات السيبرانية، ويقترح معيارًا آخر وهو ما إذا كانت "ممارسة السلطة التقديرية المرتبطة بالنشاط السيبراني ستؤثر على الامتثال لقانون الحرب"، ويُضيف بأن من يحمل صفة المقاتل هم أفراد القوات المسلحة الذين يخضعون لقيادة مسؤولة، ويعملون ضمن التسلسل الهرمي العسكري التي تنطوي على التدريب والانضباط والولاء، هؤلاء فقط هم القادرين على ممارسة السلطة التقديرية التي قد تؤدي إلى انتهاك قانون الحرب، لأنَّ أفعالهم تتم ضمن هيكل قيادة وانضباط يستطيع منع الانتهاكات والمعاقبة عليها. ولذلك فإن الدول لا توظف مدنيين عادة؛ لأنهم لا يملكون سلطة عليهم تمكنهم من التأكد من أنهم يمارسون الأنشطة وفقًا لقانون النزاعات المسلحة.

Geoffrey S. Corn, Unarmed but How Dangerous? Civilian Augmentees, the Law of Armed Conflict, and the Search for a More Effective Test for Permissible Civilian Battlefield Functions, 2 J. NAT'L SEC. L. & POL'Y 257, 286-87 (2008).

المطلب الثاني

التمييز بين الأهداف العسكرية والأعيان المدنية

تنص المادة ٢/٥٢ من البرتوكول الأول على أن "تقتصر الهجمات على الأهداف العسكرية فحسب، وتنحصر الأهداف العسكرية فيما يتعلق بالأعيان، على تلك التي تسهم مساهمة فعالة في العمل العسكري سواء كان ذلك بطبيعتها، أم بموقعها، أم بغايتها، أم باستخدامها، والتي يحقق تدميرها التام أو الجزئي، أو الاستيلاء عليها، أو تعطيلها في الظروف السائدة حينذاك ميزة عسكرية أكيدة".[١] وبالتالي فالهجمات المشروعة ضد الأهداف العسكرية يحكمها شرطان، **الأول:** أن تكون موجهة ضد أهداف عسكرية، **والثاني:** أن يوفر الهجوم ميزة عسكرية أكيدة.

أولاً: أن يكون الهجوم موجهًا ضد أهداف عسكرية:

تعرف الأهداف العسكرية بأنها تلك التي تساهم في العمل العسكري للعدو بشكل فعال؛ بسبب الطبيعة، أو الموقع، أو الغاية، أو الاستخدام، فالأهداف العسكرية بطبيعتها تشمل: المنشآت، والقواعد العسكرية، ومنصات الأسلحة، وغيرها من

[١] المادة ٢/٥٢ من البروتوكول الإضافي الأول.

المنشآت التي تعتبر عسكرية بحكم طبيعتها. ويعرف البروتوكول الإضافي الأول الأعيان المدنية، بأنها "كافة الأعيان التي ليست أهدافاً عسكرية".[١] وبالتالي، فإذا كانت الأعيان المدنية تستخدم من قبل قوات العدو أو موظفة "لأغراض عسكرية"، فلن تتمتع بالحماية، ويمكن أن تكون محلاً لهجوم مشروع.[٢]

بالنسبة للأهداف العسكرية بالنظر للغرض منها، فيرى البعض أنَّ الأهداف العسكرية "بطبيعتها "غالبًا ما تكون أيضًا أهدافًا عسكريةً "من حيث الغرض منها". أمَّا بالنسبة للأهداف العسكرية بحكم موقعها، فهي مثل المنشآت العسكرية، ومنصات الأسلحة وغيرها، وبمفهوم المخالفة، هناك مناطق جغرافية ثابتة أيضًا محظور مهاجمتها، مثل: المستشفيات، أو المدارس، والمتاحف، ودور العبادة وغيرها،[٣] حيث يحظر البروتوكول الإضافي الأول ضرب المرافق الصحية، والمستشفيات، وأماكن علاج الجرحى

[١] المادة ٥٢/١ من البروتوكول الإضافي الأول.

[٢] ICRC, Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949, para. 2022. Available at: www.icrc.org/ihl.nsf/WebList?ReadForm&id=470&t=com

[٣] المواد ٥٤، و٥٦ من البروتوكول الإضافي الأول.

والمصابين، أو التي تقدم خدمات إغاثية.[١] كذلك ينص البروتوكول الإضافي الأول على أنه في حالة ما إذا ثار "أي شك"، فيما يتعلق بوضع الأشخاص، أو الأعيان المدنية، أو الأهداف العسكرية ينبغي أن يفسر لصالح "المدنيين".[٢]

وهذا يعني أنَّ الأهداف السيبرانية المشروعة هي فقط الأهداف العسكرية، ومن بينها: الحواسيب، أو نظم الحواسيب المُستخدمة لدعم البنية التحتية العسكرية، أو البنية التحتية المستخدمة على وجه خاص لأغراض عسكرية. وبالتالي، فإنَّ الهجوم السيبراني الذي يستهدف نظام التحكم بالحركة الجوية العسكرية، ويسبب تحطمًا الطائرات العسكرية فقط، هو هجوم مشروع. أما الهجوم السيبراني على القطاع المصرفي المدني، أو على المستشفيات، والمتاحف، ودور العبادة، فهو هجوم على أعيان مدنية محمية، وبالتالي فهو غير مشروع.[٣]

[١] المواد ٦، ١٠، ١٦، ١٧ ، ٢٠ من اتفاقية حماية الأعيان الثقافية في أوقات النزاعات المسلحة، ١٤ مايو ١٩٥٤، دخلت حيز النفاذ في ٧ أغسطس ١٩٥٤. كذلك المادة ٧/٥٦ من البروتوكول الإضافي الأول.

[٢] المادة ١/٥٠ والمادة ٣/٥٢ من البروتوكول الإضافي الأول.

[٣] مثل أغلب المصانع الكيميائية، تعتمد على شبكة كمبيوتر مغلقة، فيجب أن يُفترض أن هذه الشبكة مدنية.

Hathaway, et al. “The Law of Cyber-Attack”, op.cit., pp. 817– Oona A. 85.

ولكن تكمن الصعوبة في حالة مهاجمة الأهداف التي لا تعد عسكرية بحتة، كالأهداف التي تخدم أغراضًا مدنية وعسكرية، مثل محطات توليد الطاقة، والاتصالات، والجسور، والبنية التحتية المدنية الأخرى التي تستخدم لأغراض عسكرية بالإضافة؛ لاستخدامها العادي لأغراض مدنية. وكما سبق البيان، فإنَّ الفضاءَ السيبرانيَّ مشترك، فمعظم البنية التحتية للإنترنت ذات استخدام مزدوج، حيث تتداخل الأنظمة العسكرية مع البنية التحتية المدنية.[١]

ويوضح البعض أن الفضاء السيبراني يتكون من عدد لا يُحصى من نظم الحواسيب المتصلة ببعضها البعض في أرجاء العالم، وغالباً ما تتصل نظم الحواسيب العسكرية بالنظم التجارية والمدنية، وتعتمد عليها كليّاً أو جزئيّاً. وبالتالي، قد يكون من المستحيل شنّ هجوم سيبراني على بنية تحتية عسكرية، وجعل الآثار المترتبة عليه تقتصر على هدف عسكري فحسب. وتُشير التقديرات إلى أن أكثر من ٩٥٪ من

[١] ففي الولايات المتحدة، على سبيل المثال، تتكون البنية التحتية للاتصالات العسكرية من ١٥٠٠٠ شبكة إلكترونية، وسبعة ملايين جهاز كمبيوتر موزعة في مئات المنشآت في عشرات المدن.
William J. Lynn III, Defending a New Domain: The Pentagon's Cyber Strategy, Foreign Affairs (Sept./Oct.2010), available at: http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain

الاتصالات العسكرية تستخدم شبكات مدنية في مرحلة ما، لذا فمن الممكن أن تكون الشبكات المدنية ذاتها أهدافًا عسكرية؛ نظرًا إلى أنَّ الكثير من الفضاء السيبراني عبارة عن استخدام مزدوج – يستخدمه كلٌّ من المدنيين والعسكريين.[١] ولذلك يرى البعض أن هناك حاجة لتفسير أوسع للأهداف العسكرية وفقًا لمفهوم البروتوكول الإضافي الأول.[٢]

ونرى أنه قد لا تكون هناك حاجة لتبني تفسير أوسع للأهداف العسكرية؛ أي استخدام عسكري للأعيان المدنية يحولها إلى أهداف مشروعة شريطة أن يتم الالتزام بالمبادئ العامة الثلاثة (مبدأ التمييز، ومبدأ التناسب، ومبدأ الاحتياط). فعلى سبيل المثال، إذا كانت هناك محطة تزود الوقود المستخدم في العمليات العسكرية، فهي تتحول إلى

---

[١] Oona A. Hathaway, et al. "The Law of Cyber-Attack", op.cit., pp. 817–85.

[٢] "sustaining capabilities heed to war narrowly on definite military advantage and paying too little focus[sing] to" . Charlotte Lülf, Modern Technologies and Targeting Under International Humanitarian Law, a revised version of the author`s master thesis originally submitted at the LL.M. (reg.) in Public International Law Programme at the University of Leiden (Netherlands). Available at: http://www.ruhr-uni-bochum.de/ifhv/documents/workingpapers/wp3_3.pdf

هدف عسكري حتى لو لم يكن هذا هو غرضها الأساسي، ولكن مع الأخذ في الاعتبار مبدأ التناسب والاحتياط في الهجوم.

ثانيًا: أن يوفر الهجوم ميزة عسكرية أكيدة:

يعد معيار تحقق "ميزة عسكرية أكيدة" definite military advantage عملية تقديرية معقدة، ويعني بها أنه لا ينبغي أن يكون هناك بديل عملي متاح للحصول على ميزة عسكرية مماثلة غير استهداف الأعيان المدنية المحمية. هذا يعني أنه قبل توجيه الهجوم على أي أعيان مدنية، يجب إجراء تقييم للبدائل الأخرى، فالثابت في القانون الدولي الإنساني أن الهجمات المشروعة هي التي تهدف فقط إلى إضعاف القوات العسكرية للعدو؛[1] لذلك، فمن الواضح أن أي هجوم يتجاوز ذلك الهدف هو هجوم غير مشروع.[2] وقد أقرت بذلك أيضًا دائرة الاستئناف التابعة للمحكمة الجنائية

[1] جاء في إعلان سان بطرسبورغ لعام ١٨٦٨ "يجب أن يكون الغرض الشرعي الوحيد الذي تستهدفه الدول أثناء الحرب هو إضعاف قوات العدو العسكرية، ويكفي لهذا الغرض عزل أكبر عدد ممكن من الرجال عن القتال إعلان سان بطرسبورغ؛ بغية حظر استعمال قذائف معينة في زمن الحرب، ١٨٦٨.

[2] As emphasized in the Declaration of Saint- Petersberg: “That the only legitimate object which States should endeavour to accomplish during war is to weaken the military forces of the enemy; That for this purpose it is sufficient to disable the greatest possible number of men; That this object

الدولية ليوغوسلافيا السابقة في قضية Brđanin، إذ قررت أنه "لا يوجد ما يشير إلى أن التدمير قدم أي نوع من المزايا في إضعاف القوات العسكرية المعارضة لصرب البوسنة، أو لصالح موقف صرب البوسنة، أو تم تبريره بطريقة أخرى من خلال ضرورة عسكرية"، وبالتالي فهو تدمير غير مشروع.[1]

ويرى البعض أن معيار تحقق "الميزة العسكرية الأكيدة" له أهمية كبيرة عند تقدير مدى مشروعية استهداف الأعيان ذات الاستخدام المزدوج مثل الفضاء السيبراني. فاستهدافُ الفضاءِ السيبراني ذي الاستخدام المزدوج يكون مشروعًا عندما يحقق ذلك

would be exceeded by the employment of arms which uselessly aggravate the sufferings of disabled men, or render their death inevitable; That the employment of such arms would, therefore, be contrary to the laws of humanity". The 1868 Declaration of Saint Petersburg, available at: https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Treaty.xsp?action=openDocument&documentId=3C02BAF088A50F61C12563CD002D663B

[1] The Appeals Chamber held that "the total or partial destruction of the cultural property in question did not offer a definite military advantage to the Bosnian Serb forces". Brđanin, Appeals Chamber Judgment, IT-99-36-A, 3 April 2007, para.337.

"ميزة عسكرية أكيدة"، أما إذا كان الاستهداف لا يحقق هذه الميزة العسكرية كأن يكون غرضه إضعاف الروح المعنوية للمدنيين، فلا يكون حينها هجومًا مشروعًا.[١]

المبحث الثاني

مبدأ التناسب ومبدأ الاحتياط

يعد مبدأ التناسب، ومبدأ الاحتياط في الهجوم من المبادئ المكملة لمبدأ التمييز، فيرتبط تطبيق هذين المبدأين بتطبيق مبدأ التمييز. إذ يعني مبدأ التناسب الموازنة بين المزايا العسكرية المتوقعة من الضربة، والأضرار المتوقعة ضد المدنيين أو الأعيان المدنية؛ لتحديد ما إذا كانت هناك ضرورة لتوجيه الضربة من عدمها. ويوفر هذا المبدأ حماية إضافية للمدنيين والأعيان المدنية غير المستهدفين مباشرة من الهجوم، ولكنهم عُرضة للتضرر من آثار الهجوم المشروع.

كذلك، يعد مبدأ الاحتياط من المبادئ العامة في القانون الدولي الإنساني، ويتداخل مع مبدئي التمييز والتناسب، إذ إنه يعد معيارًا إضافيًّا يساعد في حسن تطبيق

[١] Michael Gervais, Cyber Attacks and the Laws of War, op.cit., p.37.

المبدأين، ويضع حماية إضافية للمدنيين والأعيان المدنية. وفيما يلي سنتعرض لكل مبدأ منهما.

المطلب الأول

الامتثال لمبدأ التناسب

أشار البروتوكول الإضافي الأول إلى مبدأ التناسب ضمن الأحكام المتعلقة بحظر الهجمات العشوائية، فنصت المادة ٥١/٥/ب منه على أنه يعتبر من ضمن الهجمات العشوائية المحظورة "الهجوم الذي يمكن أن يتوقع منه أن يسبب خسارة في أرواح المدنيين، أو إصابتهم، أو يسبب أضراراً بالأعيان المدنية، يتجاوز ما يُنتظر أن يسفر عن ذلك من ميزة عسكرية ملموسة ومباشرة".[١] كذلك نص المادة ٣/٥٧ تحت عنوان: "الاحتياط أثناء الهجوم"، نصت على أنه "ينبغي أن يكون الهدف الواجب اختياره حين يكون الخيار ممكناً بين عدة أهداف عسكرية للحصول على ميزة عسكرية مماثلة، هو

[١]تمت إعادة الصياغة، النص الأصلي مكتوب كالتالي: " ب (والهجوم الذي يمكن أن يتوقع منه أن يسبب خسارة في أرواح المدنيين أو إصابة بهم أو أضراراً بالأعيان المدنية، أو أن يحدث خلطاً من هذه الخسائر والأضرار، يفرط في تجاوز ما ينتظر أن يسفر عنه ذلك الهجوم من ميزة عسكرية ملموسة ومباشرة". متاح على:
https://www.icrc.org/ar/doc/resources/documents/misc/5ntccf.htm

ذلك الهدف الذي يتوقع أن يسفر الهجوم عليه عن إحداث أقل قدر من الأخطار على أرواح المدنيين والأعيان المدنية."

كذلك أشار نظام روما الأساسي للمحكمة الجنائية الدولية إلى مبدأ التناسب ضمن معرض تعداد الجرائم التي تندرج تحت فئة جرائم الحرب، فنصت المادة ٨/٢/أ/٤ على "تدمير واسع النطاق. . . ليس له ما يبرره بحكم الضرورة العسكرية"، ونصت المادة ٨/٢/ب/٤ على "تعمد شن هجوم مع العلم بأن هذا الهجوم سيسفر عن خسائر تبعية في الأرواح، أو عن إصابات بين المدنيين، أو عن إلحاق أضرار مدنية، أو إحداث ضرر واسع النطاق وطويل الأجل، وشديد للبيئة الطبيعية يكون إفراطه واضحًا بالقياس إلى مجمل المكاسب العسكرية المتوقعة الملموسة المباشرة". [١]

كما يعد مبدأ التناسب من المبادئ العرفية التي يجب مراعاتها قبل توجيه الضربات أو قبل الهجوم، ويعني ببساطة الموازنة بين المزايا العسكرية المتوقعة من الضربة، والأضرار المتوقعة ضد المدنيين أو الأعيان المدنية؛ لتحديد ما إذا كانت هناك ضرورة لتوجيهها من عدمه، وما إذا كانت الأضرار الواقعة على المدنيين أو الأعيان

[١] انظر نظام روما الأساسي للمحكمة الجنائية الدولية، متاح على الرابط التالي:
https://legal.un.org/icc/statute/arabic/rome_statute(a).pdf

المدنية من جراء الهجوم "تتناسب" مع المزايا العسكرية المأمولة.[١] وعلى ذلك، فإن الهجوم الذي يؤدي إلى مقتل مدنيين، أو تدمير ممتلكات مدنية ليس هجومًا غير مشروع في حد ذاته، ولكن ما يجعله غير مشروع هو عدم احترام مبدأ التناسب؛ فالهجوم المتهور، أو الهجوم الذي يودي عن قصد بأرواح المدنيين، أو يدمر ممتلكات مدنية تزيد عما هو ضروري لتحقيق هدف عسكري هو هجوم غير مشروع.

من ناحية أخرى، هناك أعيان مدنية محظورٌ استهدافُها تمامًا في جميع الأحوال، فقد نصت المادة ٥٦ من البروتوكول الإضافي الأول "لا تكون الأشغال الهندسية، أو المنشآت التي تحوي قوى خطرة ألا وهي السدود، والجسور، والمحطات النووية لتوليد الطاقة الكهربية محلاً للهجوم، حتى ولو كانت أهدافاً عسكرية، إذا كان من شأن مثل هذا الهجوم أن يتسبب في انطلاق قوى خطرة يترتب عليها خسائر فادحة بين السكان المدنيين. كما لا يجوز تعريض الأهداف العسكرية الأخرى الواقعة عند هذه الأشغال الهندسية، أو المنشآت، أو على مقربة منها للهجوم إذا كان من شأن مثل هذا الهجوم

[١] Remarks by Dill, J, Interpretive Complexity and the IHL Principle of Proportionality, Proceedings of the Annual Meeting (American Society of International Law), vol. 108, (2014), p. 83.

أن يتسبب في انطلاق قوى خطرة من الأشغال الهندسية، أو المنشآت يترتب عليها خسائر فادحة بين السكان المدنيين".

وبتطبيق ذلك على الهجمات السيبرانية، فإنه يجب دائمًا النظر في تحليل التناسب للهجوم السيبراني في كل حالة على حدة، ولا تكفي المعادلة القائمة على مقارنة عدد القتلى من المدنيين بعدد القتلى من المقاتلين، أو مجرد مقارنة أثر تدمير البنية التحتية المدنية بالبنية التحتية العسكرية.

ومع ذلك، يرى البعض أنَّ الهجمات السيبرانية قد تكون أفضل من الهجمات التقليدية من حيث إمكانية الامتثال لمبدأ التناسب، وذلك من زاويتين: **الأولى:** أن الأسلحة السيبرانية – البرمجيات الخبيثة – يمكن تطويعها بحيث يتم الحد من آثارها بقدر الإمكان لتستهدف بشكل أساسي الأهداف العسكرية، ولا يكون لها آثار على الأعيان المدنية إلا بقدر محدود. على سبيل المثال، فإنَّ الهجوم السيبراني على البرنامج النووي الإيراني، تم باستخدام دودة Stuxnet بعد تعديلها بإضافة خصائص فيها للحد من آثارها. وبالتالي، فإن تأثيرها على الأجهزة الأخرى – غير العسكرية – كان محدودًا، مقارنة بتأثيرها المدمر على الأهداف العسكرية، علاوة على ذلك، تم إرفاق آلية التدمير الذاتي للهجوم، بحيث يتوقف أثر دودة Stuxnet الضار بحلول وقت

معين. هذه الخصائص تضمن أن تأثير الهجوم السيبراني محدودٌ ومتناسبٌ مع الميزة العسكرية المأمولة.[١]

الثانية: أنَّ آثار الهجمات السيبرانية عادة ما تكون غير حركية non-kinetic وغير عنيفة ومؤقتة، هذا بالإضافة إلى أن الهجوم السيبراني يمكن التصدي لآثاره وعكسها قبل أن تؤدي إلى خسائر بشرية أو مادية كبيرة. وبالتالي فقد يكون الهجوم السيبراني أفضل من الهجوم التقليدي في الامتثال لمبدأ التناسب؛ إذ يؤدي الهجوم السيبراني إلى تطبيق مستوى متناسب من القوة، ولكن بدون عدد غير متناسب من الضحايا المدنيين.[٢]

وعلى النقيض، يرى البعض الآخر أنه وفقًا للتفسير التقليدي لمبدأ التناسب، فإن الهجمات السيبرانية لا يمكن أن تمتثل لهذا المبدأ بسبب ازدواجية استخدام الفضاء السيبراني بين المدنيين والعسكريين، وبالتالي فأي هجمة على البنية التحتية العسكرية ستكون لها آثار على المدنيين والأعيان المدنية من الصعب تقييمها، وتقدير ما إذا

---

[١] Michael Gervais, Cyber Attacks and the Laws of War, op.cit., p.35.

[٢] هربرت لين، النزاع السيبراني والقانون الدولي الإنساني، مختارات من المجلة الدولية للصليب الأحمر، مجلد ٩٤، صيف ٢٠١٢، ص٥٢٦. متاح على الرابط التالي:
https://international-review.icrc.org/sites/default/files/12825_-cyber_conflict_and_international_humanitarian_law_-_opt_05.pdf

كانت متناسبة مع الخطر. ومثال ذلك، الهجمات على الشبكة الكهربائية العراقية خلال حرب الخليج ١٩٩٠-١٩٩١، فقد عطلت تلك الهجمات في البداية القيادة والسيطرة العسكرية العراقية (أثر مباشر) ولكن أيضًا أدت إلى حرمان المدنيين من الحصول على الكهرباء، وبالتالي أثر ذلك على المستشفيات، وعلى إمكانية الاستجابة لحالات الطوارئ وما إلى ذلك (تأثير غير مباشر). هذا التأثير كان محدودًا وغير مباشر على المدنيين، أما الهجوم السيبراني فقد لا يكون بهذه البساطة؛ نظرًا للترابط بين أنظمة الكمبيوتر، وتعقيد الهجمات السيبرانية، واحتمالية عالية للتأثير على الأنظمة المدنية، وانخفاض نسبي في فهم طبيعة الهجمات وتقدير أثرها، مما يصعب من عملية التقييم.[١]

ويرى البعض، أنه صحيح أن الهجمات السيبرانية تؤدي إلى إلحاق ضرر جسدي مباشر أقل من الهجمات التقليدية؛ إلا أن مداها أوسع بكثير من الهجمات التقليدية، فقد تُلحق أضرارًا بكل الأصول المدنية التي تشمل جميع البنية التحتية التي تنظمها أجهزة الكمبيوتر تقريبًا، مما يجعلها تنحرف تمامًا عن فرضية الامتثال لمبادئ القانون الدولي الإنساني. ولذلك، لا ينبغي أن يتم تخفيف القواعد الموجودة في القانون الدولي

[١] Charlotte Lülf, Modern Technologies and Targeting Under International Humanitarian Law, op.cit, p.43-44

الإنساني، بل يجب أن تُفسر بشكل ضيق حتى توفر حماية أكثر للمدنيين. كذلك فحتى مبدأ التناسب في تطبيقه التقليدي يحظر الاستهداف الواسع للبنية التحتية المدنية.

الخلاصة أنه إذا طبقت مبادئ القانون الدولي الإنساني بصرامة فإن ذلك سيؤدي إلى استخدام الأساليب السيبرانية بشكل مقيد بشدة.[١]

المطلب الثاني

الامتثال لمبدأ الاحتياط

تضمنت المادتان ٥٧ و٥٨ من البروتوكول الإضافي الأول أحكامًا بخصوص مبدأ الاحتياط، يمكن تقسيمها إلى نوعين: **الأول:** الاحتياط قبل الهجوم، حيث نصتا على أن يبذل صاحب قرار الهجوم أو المخطط له "ما في طاقته عمليًّا" للتأكد من أن الأهداف التي يخطط لضربها هي أهدافٌ مشروعة – أي أهداف غير محمية بموجب القانون الدولي–، وأن "يتخذ جميع الاحتياطات الممكنة" عند اختيار أساليب، ووسائل الهجوم لتجنب إحداث خسائر وأضرار لا مبرر لها بين المدنيين، **والثاني:** الاحتياط

[١] هربرت لين، النزاع السيبراني والقانون الدولي الإنساني، المرجع السابق، ص٥٢٦.

أثناء الهجوم، أو الاحتياط لمواجهة آثار الهجوم،[١] فنصت على أن تتخذ أطراف النزاع "كافة الاحتياطات المعقولة"؛ لتجنب إحداث الخسائر في أرواح المدنيين وفي الممتلكات المدنية، وأن تُبذل "رعاية متواصلة" في إدارة العمليات العسكرية، من أجل تفادي السكان المدنيين والأشخاص والأعيان المدنية.[٢] ويعد مبدأ الاحتياط من المبادئ العامة في القانون الدولي الإنساني، ويتداخل مع مبدأي التمييز والتناسب؛ إذ إنه يعد معيارًا إضافيًّا يضمن حسن تطبيق المبدأين.

أولاً: الاحتياط قبل الهجوم:

ألزمت المادة ٥٧ من البروتوكول الإضافي الأول "من يخطط لهجوم، أو يتخذ قرار بشأنه" أن "يبذل ما في طاقته عملياً للتحقق من أن الأهداف المقرر مهاجمتها ليست أشخاصاً مدنيين أو أعياناً مدنية ..."، وأن "يتخذ جميع الاحتياطات المستطاعة عند تخير وسائل وأساليب الهجوم؛ من أجل تجنب إحداث خسائر في أرواح المدنيين، أو

[١] تُقسم دوريجي الامتثال لمبدأ الاحتياط إلى قسمين: الاحتياط في الهجوم، والاحتياط لمواجهة آثار الهجوم.
كوردولا دوريجي ، لا تقترب من حدود فضائي الإلكتروني، المرجع السابق، ص ٥٥٠

[٢] انظر: المواد ٥٧، و٥٨ من البروتوكول الإضافي الأول.

إلحاق الإصابة بهم أو الأضرار بالأعيان المدنية ...".[1] أما بالنسبة لأطراف النزاع، فقد نصت المادة ٥٨ من البرتوكول الإضافي الأول بشكل خاص على بذل أقصى جهد ممكن من الأطراف المسيطرة لنقل المدنيين أو الأعيان المدنية بعيدًا عن المناطق المجاورة للأهداف العسكرية، وتجنب تمركز القوات أو القواعد العسكرية بقرب الأماكن المكتظة بالسكان.[٢]

يعتمد تقدير "ما هو في طاقة شخص ما عمليًّا" على عدة عوامل، منها: أن يكون القائد أو صاحب الضربة ملمًّا بكافة المعلومات والحقائق التي تؤكد مشروعية الهجوم، وتشمل هذه المعلومات تحديد الهدف، وما إذا كان عسكريًّا (هدف مشروع)، أو مدنيًّا (هدف غير مشروع). كذلك يجب أن يكون على علم تام بعدد المدنيين، وما إذا كان هناك ما من شأنه أن يؤثر على صحتهم مثل: محطات الصرف الصحي، أو محطات تحلية مياه، كذلك لابد أن تتوفر لديه معلومات حول طبيعة المكان المستهدف من حيث البنية التحتية، وكذلك البدائل المتاحة. ومن ضمن معايير الاحتياط قبل الهجوم أنه في حالة الشك، أو عدم التأكد من دقة هدف معين، ولتجنب

[1] انظر المادة ٥٧ الفقرة ٢/أ من البروتوكول الإضافي الأول.
[٢] انظر المادة ٥٨ من البروتوكول الإضافي الأول.

الأضرار الزائدة للمدنيين، فيجب الرجوع للقائد.[١] وبعد تقدير كل هذه العوامل وأخذها في الاعتبار، ينبغي على صاحب قرار الهجوم أن يلغيه إذا تبين أنه قد يتسبب في أضرار عرضية مفرطة للمدنيين.[٢]

وبالتطبيق على الهجمات السيبرانية، فقد يتصور أن تتضمن الاحتياطات قبل الهجوم، جمع كافة المعلومات المتاحة؛ من أجل التحقق من الهدف، وتأثير الهجوم عليه، وقد يشمل ذلك تصميم خريطة لشبكة كمبيوتر الخصم - إذا كان الهجوم على نظام حاسوبي مستهدف بعينه - ودراسة كافة الآثار المحتملة للهجوم.[٣] وفي هذا السياق يوضح دليل تالين أن العمليات السيبرانية بطبيعتها عمليات معقدة، ترتفع فيها احتمالية

---

[١] ينص دليل وزارة الدفاع الأمريكية على أنه إذا كان لدى المخطط للهجوم قلق تجاه التدمير المتوقع نتيجة الهجوم، فإن الاستشارة "ستتيح تقييم أفضل للمزايا العسكرية المتوقعة من الهجمة (فمن المتوقع أن يكون لدى القادة الأعلى فهم أكثر شمولية للسياق الاستراتيجي والعملياتي)"

" allow for a better evaluation of the expected military advantage from the attack (as it is likely that more senior commanders have a more comprehensive understanding of the strategic and operational context)."

DOD Directive 2012, at 248.

[٢] ما من فراغ قانوني في الفضاء السيبراني، مقابلة مع كوردولا دورغيه المستشار القانوني في اللجنة الدولية للصليب الأحمر، متاح على:

https://www.icrc.org/ar/doc/resources/documents/interview/2011/cyber-warfare-interview-2011-08-16.htm

[٣] كوردولا دوريجي ، لا تقترب من حدود فضائي الإلكتروني، المرجع السابق، ص ٥٧٠.

الإضرار بالبنية التحتية المدنية، وقد يكون لدى منفذي الهجوم السيبراني فهم محدود بطبيعة الهجمات، وما يمكن أن تؤدي إليه؛ وبالتالي فلابد من الاستعانة بالخبرة التقنية لدى القيادات لمساعدتهم في اتخاذ القرارات مع اتخاذ التدابير الاحتياطية المناسبة.[١]

كذلك، يجب أن يؤخذ في الاعتبار حالة استخدام الهجمات السيبرانية المضادة لأغراض الدفاع، فقد يتم برمجة أجهزة الكمبيوتر لتتصدى من تلقاء نفسها لأي هجوم سيبراني محتمل، وتوجه إليه هجومًا مضادًا. هذه الهجمات المضادة تكون آلية أو تلقائية ضد أجهزة الكومبيوتر التي أصدرت الهجمة، بغض النظر عن كون مصدر الهجمة أجهزة كمبيوتر عسكرية أم مدنية. وفي ذلك، ترى دوريجي أنه ينبغي على الدول في هذه الحالات أن تتوخى الحذر في تقييم مشروعية الهجمات المضادة في ضوء مبدأ الاحتياط.[٢]

ثانيًا: الاحتياط أثناء الهجوم (أو لمواجهة آثار الهجوم):

جاءت المادة ٥٧ من البروتوكول الإضافي الأول تحت عنوان الاحتياطات أثناء الهجوم، وتضمنت بعض التدابير الوقائية الواجب مراعاتها قبل الهجوم، وبعض

[١] Tallinn Manual, op.cit., p.

[٢] كوردولا دوريجي ، لا تقترب من حدود فضائي الإلكتروني، المرجع السابق، ص ٥٧٤.

التدابير الأخرى الواجب على إدارة العمليات العسكرية مراعاتها أثناء الهجوم. فنصت الفقرة الأولى منها على أن " تُبذل رعاية متواصلة في إدارة العمليات العسكرية، من أجل تفادي السكان المدنيين، والأشخاص، والأعيان المدنية"، كما تنص الفقرة الرابعة منها على أن "يتخذ كل طرف في النزاع كافة الاحتياطات المعقولة عند إدارة العمليات العسكرية ... لتجنب إحداث الخسائر في أرواح المدنيين، وإلحاق الخسائر بالممتلكات المدنية".

وقد فسر تعليق اللجنة الدولية للصليب الأحمر عبارة "كافة الاحتياطات المعقولة"، بأنها تعني "كل إجراء عملي أو ممكن عمليًّا"،[١] ويوضح Schmitt أنَّ العديد من معاهدات الأسلحة وممارسات الدول قد فسرت كلمة "المعقولة" على أنها تعني: "تلك الاحتياطات العملية أو الممكنة عمليًّا مع الوضع في الاعتبار كافة الظروف السائدة في هذا الوقت بما في ذلك الاعتبارات الإنسانية والعسكرية"؛[٢] مما يفترض القيام

---

١. ICRC, Commentary on AP I, para. 2198.

٢. "practicable or practically possible, taking into account all the humanitarian and military circumstances ruling at the time, including considerations". Schmitt M and Thurnher J, Out of the Loop: Autonomous Weapon Systems and the Law of Armed Conflict, (2013), 4 Harvard National Security Journal, p. 264. Available at:

بعملية تقييم لكافة النتائج المحتملة للضربة، وبناءً عليه يتم اتخاذ احتياطات لتجنب الأضرار والخسائر غير المبررة بصرف النظر عن النتيجة أو المحصلة النهائية.

ويرى Schmitt إنَّ تقدير مدى الامتثال لمبدأ الاحتياط أثناء الهجوم – كما يتضح من الفقه والقضاء – يعتمد على قدر التطور التكنولوجي وقدر التدريب والمهارة لدى أطراف النزاع، فعلى سبيل المثال فإن سقف "الاحتياطات المعقولة" بالنسبة لطرف تتوفر لدية التكنولوجيا المتطورة في جمع المعلومات، وتحليلها، وتحديد دقة الضربة أعلى من نظيره ممن لا تتوافر لديه هذه الإمكانية، فالدول المتقدمة عسكريًّا لديها إمكانية الدخول لقدر هائل من أدق المعلومات عن الهدف المراد ضربه، ويمكنها تقييم تغيير الظروف كنتيجة لأعمال المراقبة المستمرة للأهداف بواسطة التصوير بالقمر الصناعي، والمركبات الجوية بدون تدخل العنصر البشري، كما أن لديها تكنولوجيا متطورة للإرسال تمكنها من نقل تلك المعلومات بسرعة كبيرة للأشخاص المعنية

http://harvardnsj.org/2013/05/out- of- the- loop- autonomous-weapon-systems-and-the-law-of-armedconflict/

باتخاذ القرار. وبالتالي يتعين أن يكون سقف الاحتياطات المعقولة لديها أعلى من ذاك المتصور بالنسبة لدولة لديها إمكانات محدودة.[١]

ويوضح دليل تالين أن التزام الدول باتخاذ الاحتياطات المعقولة قد يشمل فصل البنية التحتية العسكرية عن المدنية،[٢] وفصل النظم الحاسوبية التي تعتمد عليها البنية التحتية المدنية الحيوية عن شبكة الإنترنت، ووضع التدابير اللازمة لضمان الإصلاح الفوري للنظم الحاسوبية المهمة، ومكافحة الفيروسات لحماية النظم المدنية التي قد تتأثر بالأضرار أو التدمير أثناء الهجوم.[٣]

ويرى البعض أن تمييز أو فصل البنية التحتية العسكرية عن البنية التحتية المدنية أمر في غاية الصعوبة، وقد يكون غير متصور عمليًا. لكن إجراءات الاحتياط أثناء الهجوم قد تتضمن أيضًا – بالإضافة إلى ما سبق – إجهاض الهجمات إذا اتضح أن الهدف قد تم تصنيفه – كهدف عسكري مشروع – بشكل خاطئ؛ وهذا يستلزم أن يكون لدى

---

[١] Ibid.

[٢] كما يوصي التقييم القانوني الذي أجرته وزارة الدفاع الأمريكية بأنه حيثما يكون هناك اختيار، ينبغي إبقاء النظم العسكرية منفصلة عن البنى الأساسية المدنية المستخدمة.
Department of Defense Office of General Counsel, an assessment of International Legal Issues in Information Operations, May 1999, available at: https://irp.fas.org/eprint/io-legal.pdf

[٣] Tallinn Manual, op.cit., p. ٤٥٠

صاحب قرار الهجوم القدرة على السيطرة على السلاح السيبراني، ووقف الهجمات في أي وقت.[١]

الخلاصة، أن الامتثال لمبادئ القانون الدولي الإنساني الثلاثة (مبدأ التمييز، ومبدأ التناسب، ومبدأ الاحتياط في الهجوم)، عند استخدام الهجمات السيبرانية كأسلوب للقتال تواجهه عقبة رئيسة وهي أن الفضاء السيبراني مزدوج الاستخدام، أي أنه مستخدم للأغراض المدنية والأغراض العسكرية، أو بشكل أكثر دقة فهو مُستخدم بشكل أساسي ورئيس لأغراض مدنية، والاستخدام العسكري لهذا الفضاء هو استخدام عارض. وتثير ازدواجية الاستخدام تلك إشكاليات في تقدير مدى إمكانية الامتثال لمبادئ القانون الدولي الإنساني الثلاثة، إذ تطمس الفارق بين المدنيين والعسكريين، وبين الأهداف العسكرية، والأعيان المدنية، وتجعل من الصعب إسناد الهجمة إلى فاعل معين (الامتثال لمبدأ التمييز). كذلك تجعل الموازنة صعبة بين الميزة العسكرية، والضرر الذي سيلحق بالأعيان المدنية، أو الضرر الذي سيلحق بالمدنيين كخسائر بشرية مثلاً (الامتثال لمبدأ التناسب). أما بالنسبة للامتثال لمبدأ الاحتياط، فذلك يعتمد على مدى فهم المهاجم لطبيعة الهجمات، وما يمكن أن تؤدي إليه، وذلك أيضًا يصعب تقديره.

[١] Charlotte Lülf, Modern Technologies and Targeting Under International Humanitarian Law, op.cit., p.45

خاتمة

طرحنا في المقدمة الإشكالية الرئيسة لهذه الدراسة وهي: هل القانون الدولي الإنساني – بوضعه الحالي – صالح للتطبيق على الهجمات السيبرانية، أم أنَّ هناك حاجة لتطويع بعض قواعده لتلاحق التطورات التكنولوجية الحديثة؟

ووضحنا أن مفهوم "الهجمات السيبرانية" واسع ويشمل العديد من الأفعال التي قد ينطبق عليها القانون الدولي الإنساني، وقد تنطبق عليها قوانين أخرى. ولذلك، تعرضت الدراسة في البداية إلى المقصود بالهجمات السيبرانية التي ينطبق عليها القانون الدولي الإنساني على وجه التحديد، ثم انتقلت من ذلك إلى بحث مدى انطباق القانون الدولي الإنساني على الهجمات السيبرانية من زاويتين، الأولى: من حيث استخدام الأسلحة السيبرانية كوسيلة للهجوم السيبراني، وذلك من خلال التعرض لمدى الامتثال للقواعد التي تنظم اقتناء الأسلحة الجديدة، والثانية: من حيث استخدام الهجمات السيبرانية كأسلوب للقتال، وذلك من خلال بحث مدى انطباق القواعد التي تنظم مشروعية الهجمات.

وقد توصلت الدراسة في تحديد "الهجمات السيبرانية" التي ينطبق عليها القانون الدولي الإنساني إلى التمييز بين حالتين: الحالة الأولى: إذا كان هناك نزاعٌ مسلحٌ قائمٌ بالفعل، وفي هذه الحالة فإن الهجمات السيبرانية تعد مكونًا أو جانبًا من العمليات العدائية المستمرة داخل هذا النزاع المستمر، وبالتالي فهي خاضعة لقواعد القانون الدولي الإنساني. والحالة الثانية: إذا لم يكن هناك نزاعٌ مسلحٌ قائمٌ بالفعل، فهل تفي الهجمات السيبرانية بـ "عتبة" النزاع المسلح، وبالتالي ينطبق عليها القانون الدولي الإنساني؟

لم يُعرِّف القانون الدولي الإنساني "النزاع المسلح"، ولكنه ميز بين حالتين: النزاع المسلح الدولي والنزاع المسلح غير الدولي، وقد تتبعنا خلال الدراسة هذين الفرضين لتحديد "الهجمات السيبرانية" التي ينطبق عليها القانون الدولي الإنساني.

بالنسبة للنزاع المسلح الدولي، فقد توصلنا إلى التمييز بين فرضين: إذا كانت الهجمات السيبرانية تؤدي إلى تبعات عنيفة؛ فإنها تخضع في هذا الفرض إلى قواعد القانون الدولي الإنساني، أما إذا كانت لا تؤدي إلى تبعات عنيفة، فقد انقسم الفقه في ذلك إلى اتجاهين، أحدهما يرى أن القانون الدولي الإنساني لا ينطبق إلا على الهجوم الذي يؤدي لتبعات عنيفة فقط، والآخر يرى أن التبعات العنيفة ليست شرطًا، وبالتالي

١٢- مدى انطباق القانون الدولي الإنساني على الهجمات السيبرانية

ينطبق القانون الدولي الإنساني عليها في الحالتين. أما بالنسبة للنزاع المسلح غير الدولي، فلابد أن تؤدي الهجمات السيبرانية إلى تبعات عنيفة حتى يُطبق عليه القانون الدولي الإنساني.

وقد أيدنا الاتجاه الأول، حيث إننا نرى أن الهجمات السيبرانية التي ينطبق عليها القانون الدولي الإنساني هي تلك التي تؤدي إلى تبعات عنيفة فقط، ورجحنا تعريف الهجمات السيبرانية الوارد في دليل تالين بناءً على ذلك، وهو أنها: "عملية سيبرانية، هجومية أو دفاعية من المتوقع – بشكل معقول – أن تتسبب في إصابة أو وفاة الأشخاص أو تلف أو تدمير الأشياء". وبالتالي فالهجمات السيبرانية التي لا تؤدي إلى إحداث إصابة أو وفاة الأشخاص أو تلف أو تدمير الأشياء لا ينطبق عليها القانون الدولي الإنساني.

وانطلقنا من هذا المفهوم لتحديد مدى انطباق القانون الدولي الإنساني على الأسلحة السيبرانية كوسيلة للقتال، وعلى الهجمات السيبرانية كأسلوب للقتال.

وبالنسبة لاستخدام السلاح السيبراني – بحسب وضعه الحالي – فقد خلصنا إلى أنه لا يخالف القواعد التي تحدد مدى مشروعية السلاح، فهو ليس سلاحًا عشوائيًّا، ولا يتسبب استخدامه العادي في آلام غير ضرورية. وإن كان ذلك لا يمنع من إمكانية

تصميمه أو استخدامه بشكل ينتهك تلك القواعد؛ ولذلك تضحى آلية مراجعة الأسلحة الجديدة وفقًا للمادة ٣٦ من البروتوكول الإضافي الأول لعام ١٩٧٧ ضرورية في هذا السياق، لضمان مشروعية السلاح السيبراني.

وفي كل الأحوال، فإن مراجعة الأسلحة السيبرانية وفقًا للمادة ٣٦ الخاصة باستعراض الأسلحة الجديدة تثير عدة تحديات، خاصة وأن البرمجيات في تطور مستمر وكذلك حماية نظم الكمبيوتر في تطور مستمر، مما يفرض إجراء تطويرات وتحديثات بشكل مستمر على الفيروسات والبرمجيات التي تستخدم في الهجوم، وما يستتبعه من إجراء استعراض جديد للأسلحة السيبرانية.

أما بالنسبة لاستخدام الهجمات السيبرانية كأسلوب للقتال، فإن مسألة انطباق مبادئ القانون الدولي الإنساني الثلاثة عليها (مبدأ التمييز ومبدأ التناسب ومبدأ الاحتياط في الهجوم) تواجهه عدة تحديات:

الأول: أن الفضاء السيبراني مزدوج الاستخدام، أي أنه مستخدم للأغراض المدنية والأغراض العسكرية، أو لنكن أكثر دقة فهو مُستخدم بشكل أساسي ورئيسي لأغراض مدنية، والاستخدام العسكري لهذا الفضاء هو استخدام عارض؛ مما يؤدي لاستحالة التمييز بين الأهداف العسكرية والأعيان المدنية والتمييز بين المدنيين والعسكريين.

الثاني: أن الهجمات السيبرانية تعتمد على الخفاء والتستر، وبالتالي فمن الصعب إسناد الهجمة إلى فاعل معين، ناهيك عن صعوبة تحديد ما إذا كان الرد على هذه الهجمات سيكون متناسبًا مع الهجمة أم لا وسيستهدف الأهداف العسكرية فقط، أم سيمتد للإضرار بالبنية التحتية السيبرانية المدنية.

الثالث: أن الهجمات السيبرانية لا تتطلب تدريبًا عسكريًّا أو خبرة فنية كبيرة؛ فأي مدني يستطيع القيام بهذه الهجمات، ومن هنا تُفضل الدول الاعتماد على المدنيين في شن الهجمات السيبرانية لسببين: الأول: حتى لا يُنسب لها الهجوم، والثاني: لتستفيد من قدرات المدنيين على شن الهجوم السيبراني. ومع شيوع الاعتماد على المدنيين، والتسليم بقدرتهم على شن الهجمات السيبرانية أكثر من العسكريين، فإن ذلك سيثير تساؤلات حول مدى معرفة هؤلاء المدنيين بأثر الضربة، وتقييم المزايا العسكرية أمام الخسائر والأضرار المدنية، وبالتالي الامتثال لمبدأ التناسب، ومبدأ الاحتياط في الهجوم، بل ومبدأ التمييز أيضًا.

وبالتالي، وفي رأينا، فلا تزال هذه الأمور الثلاثة التي عرضناها مطروحة، وغير واضح فيها مدى إمكانية استخدام الهجمات السيبرانية – أي تلك التي تؤدي إلى

إحداث إصابة، أو وفاة، أو تدمير الأعيان المدنية – بالامتثال لمبادئ القانون الدولي الإنساني الثلاثة.

وفي رأينا أن الحل يكمن في أحد خيارين، إما أن يتم تطويع الأسلحة السيبرانية وطريقة الهجمات لتمتثل للقواعد الحالية للقانون الدولي الإنساني، وإما أن يتم تطوير القانون الدولي الإنساني ليواكب هذا التطور، وذلك من خلال تبني تفسير أكثر مرونة، أو أوسع لقواعد القانون الدولي الإنساني الحالية، أو بتبني قواعد جديدة تناسب التطورات الحديثة.

وقد لاحظنا اتجاهين للكتابات القانونية في هذا السياق:

الأول: يؤيد تبني تعريف واسع للهجمات السيبرانية بحيث تشمل تلك التي لا تؤدي إلى تبعات عنيفة، ويُشجع التوسع في استخدامها عوضًا عن الهجمات التقليدية، لتقليل الأضرار العرضية لاستهداف الأهداف العسكرية (المشروعة) مثل الخسائر البشرية في المدنيين وتدمير الأعيان المدنية، ويدعون بالتالي إلى تطبيق أكثر مرونة

لأحكام القانون الدولي الإنساني، فيما يؤيد البعض تبني معاهدة جديدة مصممة لتنظيم الهجمات السيبرانية.[١]

الثاني: يرى أن القانون الدولي الإنساني يوفر إطارًا قانونيًّا شاملاً قادر على التكيف مع الابتكارات التكنولوجية الجديدة. ويبدو أن هذا هو اتجاه الدول أيضًا، إذ تعاونت الدول على مدى العقود الماضية لوضع معاهدة لتقييد استخدام الأسلحة السيبرانية، إلا

[١] قد تكون الاتفاقية التقليدية مشابهة لهيكل البروتوكول الإضافي الأول، فتشمل في البداية تعريف للمصطلحات، وتأكيد أهمية مبادئ القانون الدولي الإنساني، ثم وضع قواعد محددة بشأن الهجمات السيبرانية التي قد تتسبب في معاناة لا داعي لها، وأن يستهدف المحظورات على وجه التحديد المواقع المحمية وكذلك اللوائح المتعلقة بمسألة الحياد. ويضيف شولمان أن إدراج آليات الإنفاذ مهم في هذا الصدد، والتي تشير إلى المجرمين الفرديين المسؤولية وكذلك مسؤولية الدولة. يقترح تضمين بند منح محاكمة جرائم الحرب السيبرانية إلى اختصاص المحكمة الجنائية الدولية. وكذلك آلية إنفاذ أخرى هي شرط تسوية إلى محكمة العدل الدولية ، بموجب المادة ٣٦ من النظام الأساسي لمحكمة العدل الدولية ، التي تمنح المحكمة سلطة الفصل في الأسئلة المتعلقة بتفسير وتطبيق المعاهدات الدولية، وكذلك دعاوى الأضرار التي لحقت بالدول. مؤيدين هذا الاتجاه:
Discrimination in the Laws of Information Warfare, Mark R. Shulman, (1999), at 965. D. Hollis, Why Columbia Journal of Transnational Law 37 and States Need an International Law for Information Operations, Lewis Clark Law Review 11 (2007); K. Geers, Cyber Weapons Convention, 5 Security Law Review 26 (2010); D. Elliot, Weighting Computer Law and Cyberwarfare, Arms Control Association the Case of a Convention to Limit (2009);

أنه لم يتم إلى الآن وضع مشروع لها، مما يبين أنه لا نية حالية لدى الدول لوضع معاهدة دولية جديدة تنظم الهجمات السيبرانية.[١]

وإننا نؤيد الاتجاه الثاني، ونرى أن القانون الدولي الإنساني – بوضعه الحالي – كافٍ؛ لأنه –ببساطة – يضع مبادئ إنسانية للحرب، من أجل المحافظة على الأرواح والأعيان، ولم تكن المشكلة أبدًا في وجود نقص في هذا الفرع من القانون، ولكن المشكلة كانت دائمًا في عدم الامتثال لهذه المبادئ.

[١] A. Schaap, Cyberwarfare Operations: Development and Use under International Law, Air Force Law Review 64 (2009), at 124.

قائمة بأهم المراجع

أولاً: الكتب والرسائل العلمية:

(١) باللغة العربية:

- خالد وليد محمود، الهجمات عبر الإنترنت: ساحة الصراع الإلكترونيّ الجديدة، سلسلة: دراسات ٢٠١٣، المركز العربي للأبحاث ودراسة السياسات.
- نور أمير الموصلي، الهجمات السيبرانية في ضوء القانون الدولي الإنساني، الجامعة الافتراضية السورية ٢٠٢١، رسالة ماجستير.
- وليد غسان سعيد جلعود، دور الحرب الإلكترونية في الصراع العربي الإسرائيلي، رسالة ماجستير – جامعة النجاح الوطنية، ٢٠١٣.

(٢) باللغة الإنجليزية:

- Tallinn Manual 2.0 on the International Law Applicable to Cyber Operation, edited by Michael N. Schmitt, United States Naval War College, Newport, Rhode Island, Cambridge University Press, February 2017.
- J. Pictet, Commentary on the Geneva Conventions of 12 August 1849. Available at: https://www.loc.gov/rr/frd/Military_Law/pdf/GC_1949-I.pdf

- H. Haug (ed.), Humanity for All: The International Red Cross and Red Crescent Movement, Paul Haupt Publishers, Berne, 1993.
- Yves Sandoz, Christophe Swinarski, & Bruno Zimmermann, eds, ICRC, Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949 (Geneva: Martinus Nijhoff, 1987).
- J.-M. Henckaerts and L. Doswald-Beck (eds.), Customary International Humanitarian Law, Cambridge: Cambridge University Press, 2005.
- K. Podins, J. Stinissen, M. Maybaum eds., 5th International Conference on Cyber Conflict (2013). Available at:

  https://ccdcoe.org/library/publications/5th-international-conference-in-cyber-conflict-proceedings-2013/
- Verri, Dictionary of International Law of Armed Conflicts, Geneva, ICRC, 1992.
- William Boothby, Weapons and the Law of Armed Conflict, (New York: Oxford University Press 2009)
- C. Czossesk, R. Ottis and K. Ziolkowski eds, 4th International Conference on Cyber Conflict,

Proceedings (NATO Cooperative Cyber Defence Centre of Excellence Publications: Tallinn, 2012).

- Julie E. Mehan, CyberWar, CyberTerror, CyberCrime (Ely: IT Governance Publishing, 2008).
- SJ Lukasik, SE Goodman & DW Longhurst, 'Protecting Critical Infrastructures Against Cyber-Attack', OUP New York, 2003.
- Michael N. Schmitt & Brian T. O'Donnell eds., Computer Network Attack and International Law, 2002, (Vol. 76, US Naval War College International Law Studies).

ثانيًا: الأبحاث:

(١) باللغة العربية:

- أ.م.د. كرار عباس متعب فرج، الحرب السيبرانية: دراسة في استراتيجية الهجمات السيبرانية بين الولايات المتحدة الأمريكية وإيران، مجلة حمورابي للدراسات، العدد ٤٠ – السنة العاشرة شتاء ٢
- طلال ياسين العيسى، وعدي محمد عناب، المسئولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر، مجلة الزرقاء للبحوث والدراسات الإنسانية – المجلد التاسع عشر – العدد الأول، ٢٠١٩.

- جاستن ماك كليلاند، استعراض الأسلحة وفقا للمادة ٣٦ من البروتوكول الإضافي الأول، مقال، المجلة الدولية للصليب الأحمر، العدد ٨٥٠ (٢٠٠٣)

- روبن م. كوبلاند، زميل كلية الجراحين الملكية، مقال استعراض لمشروعية الأسلحة: مدخل جديد لمشروع "الإصابات المفرطة أو الآلام التي لا مبرر لها" المجلة الدولية للصليب الأحمر، العدد٨٣٥

- عمر محمود أعمر، الحرب الإلكترونية في القانون الدولي الإنساني، دراسات علوم الشريعة والقانون، المجلد ٤٦، عدد ٣، ٢٠١٩.

- سهيلة هادي، الحروب الإلكترونية في ظل عصر المعلومات، مجلة رؤى استراتيجية، يوليو ٢٠١٧.

- كوردولا دوريجي، " لا تقترب من حدود فضائي الإلكتروني: الحرب الإلكترونية والقانون الدولي الإنساني وحماية المدنيين"، المجلة الدولية للصليب الأحمر، مجلد ٩٤ العدد ٨٨٦، صيف ٢٠١٢.

- هربرت لين، النزاع السيبراني والقانون الدولي الإنساني، مختارات من المجلة الدولية للصليب الأحمر، مجلد ٩٤، صيف ٢٠١٢.

(٢) باللغة الإنجليزية:

- Oona A. Hathaway, et al. “The Law of Cyber-Attack”, California Law Review, vol. 100, no. 4, 2012,

JSTOR, available at: http://www.jstor.org/stable/23249823 .

- Ido Kilovaty, Cyber Conflict and The Thresholds of War, (June 22, 2021). Forthcoming, Is the International Legal Order Unraveling? (David Sloss, ed.) Oxford University Press (2022).
- Cf. J. Kelsey, Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare, Michigan Law Review 106 (2008).
- Thomas C. Wingfield, The Law of Information Conflict: National Security Law in Cyberspace, Aegis Research Corp., 2000.
- Fred Schreier, On Cyberwarfare, Working Paper No. 7, DCAF Horizon, Geneva,2015. Available at: https://www.dcaf.ch/sites/default/files/publications/documents/OnCyberwarfare-Schreier.pdf
- Michael Gervais, Cyber Attacks and the Laws of War (October 1, 2011). Available at: https://ssrn.com/abstract=1939615
- Michael N. Schmitt, Computer Network Attack and The Use of Force in International Law: Thoughts on a normative framework, Columbia journal of transnational law, 1998– 1999, Vol. 37.

- Papanastasiou Afroditi, 'Application of International Law in Cyber Warfare Operations', Electronic copy, available at: https://ssrn.com/abstract=1673785
- Tom Gjelten, Extending the Law of War to Cyberspace, NAT'L PUB. RADIO (Sept. 22, 2010), available at: http://www.npr.org/templates/story/story.php?storyId=130023318
- Cameran Ashraf, Defining cyberwar: towards a definitional framework, Defense & Security Analysis, (2021).
- Richard A. Clarke & Robert K. Knake, Cyber War: The Next Threat to National Security and What to Do About It, (2010).
- Craig B. Greathouse, Cyber War and strategic thought: Do the Classic theorists Still Matter? in J. F Kremer and B. Muller Eds Cyberspace And international Relations (Verlog Berlin Heidelberg Spriner 2014).
- James A. Lewis & Katrina Timlin, Cybersecurity and Cyberwarfare 2011, Washington D.C., CSIS, UNIDIR. Available at: https://unidir.org/sites/default/files/publication/pdfs/

/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf

- Michael N. Schmitt, Cyber Operations and the Jus in Bello: Key Issues, International Law Studies, Vol. 87, 2011.
- Kenneth Anderson & Matthew C. Waxman, Debating Autonomous Weapon Systems, Their Ethics, And Their Regulation Under International Law, American University Washington College of Law, Washington College of Law Research Paper No. 2017-21
- Charles J Dunlap JR, Perspectives for cyber strategies on Law for Cyberwar", Strategic Studies Quarterly, Spring 2011.
- Knut Dörmann, Applicability of the Additional Protocols to Computer Network Attacks, available at: https://www.icrc.org/en/doc/assets/files/other/applicabilityofihltocna.pdf
- A. Paulus and M. Vashakmadze, Asymmetrical War and the Notion of Armed Conflict – a tentative conceptualization, IRRC, Volume 91 Number 873 March 2009.

- S. Vite, Typology of armed conflicts in international humanitarian law: legal concepts and actual situations, IRRC, Volume 91 Number 873 March 2009, p.٧٣. Available at: https://www.icrc.org/en/doc/assets/files/other/irrc-873-vite.pdfH.P.
- D. Blake and J. S. Imburgia, '"Bloodless weapons"? The need to conduct legal reviews of certain capabilities and the implications of defining them as "weapons"', Air Force Law Review (2011).
- Josh Rovner, Cyber War as an Intelligence Contest, WAR ON THE ROCKS (Sep. 16, 2019), https://warontherocks.com/2019/09/cyber-war-as-an-intelligence-contest/ .
- Robert Knake, A Cyberattack on the U.S. Power Grid, COUNCIL ON FOR. REL. (Apr. 3, 2017), available at: https://www.cfr.org/report/cyberattack-us-power-grid
- Lloyd's & University of Cambridge Centre For Risk Studies, Business Blackout: The Insurance Implications of a Cyber Attack on The Us Power Grid, (2015). Available at: https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/crs-lloyds-business-blackout-scenario.pdf

- Herr, Trey, PrEP: A Framework for Malware & Cyber Weapons (December 20, 2013). The Journal of Information Warfare, Vol.13, No.1, February 2014, Available at: https://ssrn.com/abstract=2343798
- Brown, G. D. and Metcalf, A. O., 'Easier said than done: legal reviews of cyber weapons', Journal of National Security Law and Policy, vol. 7, no.1 (2014).
- Meredith Hagger & Tim McCormack, "Regulating the Use of Unmanned Combat Vehicles: Are General Principles of IHL Sufficient?" (2011) 21 JL Inf & Sci 74.
- Rebecca Crootof, The Killer Robots Are Here: Legal and Policy Implications, Cardozo Law Review, vol.36.
- Anderson K, Reisner D, and Waxman M, 'Adapting the Law of Armed Conflict to Autonomous Weapon Systems' (2014) 90 International Legal Studies.
- Vincent Boulanin And Maaike Verbruggen, Article 36 Reviews Dealing with The Challenges Posed by Emerging Technologies, Stockholm International Peace Research Institute, 2017. Available At: https://www.sipri.org/sites/default/files/2017-12/article_36_report_1712.pdf
- William Boothby, 'How will weapons reviews address the challenges posed by new technologies?',

Military Law and the Law of War Review, vol. 52, no. 1 (2013).

- Geoffrey S. Corn, Unarmed but How Dangerous? Civilian Augmentees, the Law of Armed Conflict, and the Search for a More Effective Test for Permissible Civilian Battlefield Functions, 2 J. NAT'L SEC. L. & POL'Y (2008).

- Charlotte Lülf, Modern Technologies and Targeting Under International Humanitarian Law, a revised version of the author`s master thesis originally submitted at the LL.M. (reg.) in Public International Law Programme at the University of Leiden (Netherlands). Available at: http://www.ruhr-uni-bochum.de/ifhv/documents/workingpapers/wp3_3.pdf

- Ralph Crawshaw, Human rights and the theory and practice of policing, The International Journal of Human Rights, (1997), published online in 2007.
- Schmitt M and Thurnher J, Out of the Loop: Autonomous Weapon Systems and the Law of Armed Conflict, (2013), 4 Harvard National Security Journal. Available at: http://harvardnsj.org/2013/05/out- of- the- loop-

autonomous-weapon-systems-and-the-law-of-armedconflict/

- A. Schaap, Cyberwarfare Operations: Development and Use under International Law, Air Force Law Review 64 (2009).
- Mark R. Shulman, Discrimination in the Laws of Information Warfare, Columbia Journal of Transnational Law 37, (1999).
- D. Hollis, Why States Need an International Law for Information Operations, Lewis and Clark Law Review 11 (2007).
- Charles J Dunlap JR, Perspectives for cyber strategies on Law for Cyberwar", Strategic Studies Quarterly, Spring 2011.
- William J. Lynn III, Defending a New Domain: The Pentagon's Cyber Strategy, Foreign Affairs (Sept./Oct.2010), available at: http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain
- Remarks by Dill, J, Interpretive Complexity and the IHL Principle of Proportionality, Proceedings of the Annual Meeting (American Society of International Law), vol. 108, (2014)

ثالثًا: أحكام المحاكم الدولية:

- Prosecutor V. Strugar, Case No. IT-01-42-A, 17 July 2008.
- Prosecutor v Haradinaj, Case No. IT-04-84-84-T, 3 April 2008.
- Prosecutor v. Tadic, Case No. IT-94-1-A, Appeals Chamber Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, (Oct. 2, 1995).
- ICTY, Prosecutor v. Boskoski, Case No. IT04-82, Judgment (Trial Chamber), 10 July 2008.
- Prosecutor v. Tadic, Case No. IT-94-1-A, Appeals Chamber Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction.
- Prosecutor v. Akeyesu, Case No. ICTR-96-4-T, Judgment, (Sept. 2, 1998).
- Brđanin, Appeals Chamber Judgment, IT-99–36-A, 3 April 2007.

رابعًا: معاهدات دولية:

- إعلان سان بطرسبرج ١٨٦٨.

- اتفاقية لاهاي (الرابعة) فيما يتعلق قوانين وأعراف الحرب البرية والملحق التابع لها: اللوائح المتعلقة بقوانين ٣٢ وأعراف الحرب البرية، ١٨ أكتوبر/تشرين الأول ١٩٠٧.
- اتفاقيات جنيف الأربع لعام ١٩٤٩.
- البروتوكول الأول الإضافي إلى اتفاقيات جنيف المعقودة في ١٢ آب / أغسطس ١٩٤٩ والمتعلق بحماية ضحايا المنازعات المسلحة الدولية لعام ١٩٧٧.
- البروتوكول الثاني الإضافي إلى اتفاقيات جنيف المعقودة في ١٢ آب / أغسطس ١٩٤٩ والمتعلق بحماية ضحايا المنازعات المسلحة غير الدولية لعام ١٩٧٧.
- اتفاقية حظر أو تقييد استعمال أسلحة تقليدية معينة يمكن اعتبارها مفرطة الضرر أو عشوائية الأثر لعام ١٩٨٠، بصيغتها المعدلة في ٢١ ديسمبر ٢٠٠١ (اتفاقية الأسلحة التقليدية) دخلت حيز النفاذ في ٢ ديسمبر ١٩٨٣.
- البروتوكولات الملحقة بالاتفاقية:

البروتوكول الأول بشأن الشظايا التي لا يمكن كشفها لعام ١٩٨٠ (دخل حيز النفاذ في ٢ ديسمبر ١٩٨٣).

البروتوكول الثاني بشأن حظر أو تقييد استخدام الألغام والشراك الخداعية والنبائط الأخرى لعام ١٩٨٠ (دخل حيز النفاذ في ٣ ديسمبر ١٩٩٨).

البروتوكول الثالث بشأن حظر أو تقييد استخدام الأسلحة الحارقة لعام ١٩٨٠ (دخل حيز النفاذ في ٢ ديسمبر ١٩٨٣).

البرتوكول الرابع بشأن أسلحة الليزر المسببة للعمى لعام ١٩٩٥ (دخل حيز النفاذ في ٣٠ يوليو ١٩٩٨).

البروتوكول الخامس بشأن المتفجرات من مخلفات الحرب لعام ٢٠٠٣ (دخل حيز النفاذ في ١٢ نوفمبر ٢٠٠٦).

نظام روما الأساسي للمحكمة الجنائية الدولية ١٩٩٨.

خامسًا: تقارير وأدلة عمل:

- US Department of the Air Force, Secretary of the Air Force, Air Force Instruction 51-402, Legal Reviews of Weapons and Cyber Capabilities, 27 July 2011. Available at: https://nsarchive.gwu.edu/document/21449-document-53

- U.S. Army Training & Doctrine Command, Handbook No. 1.02, Critical Infrastructure Threats and Terrorism, At Vii-2 (2006).

- Losing Humanity: The Case Against Killer Robots, Human Rights Watch (2012), available at: https://www.hrw.org/report/2012/11/19/losing-humanity/case-against-killer-robots

- United Kingdom Ministry of Defense, 2017, Unmanned Aircraft Systems, Joint Doctrine Publication 0-30.2, p. III, available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/640299/20170706_JDP_0-30.2_final_CM_web.pdf

- Department of Defense Cyberspace Policy Report A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934 November 2011. Available at: https://irp.fas.org/eprint/dod-cyber.pdf

- DOD Directive 3000.09. Available at:
- https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodd/300009p.pdf
- A Guide to the Legal Review of New Weapons, Means and Methods of Warfare. Available at:
- http://e-brief.icrc.org/wp-content/uploads/2016/09/12-A-Guide-to-the-Legal-Review-of-New-Weapons.pdf
- ICRC, Review of New Weapons (29 October 2010), http://www.icrc.org/eng/war-andlaw/weapons/new-weapons/overview-review-of-new-weapons.html

- Legal review of cyber weapons, means and methods of warfare, available at:

- https://cyberlaw.ccdcoe.org/wiki/Legal_review_of_cyber_weapons,_means_and_methods_of_warfare
- INT'L COMM. OF THE RED CROSS, Interpretive Guidance on The Notion Of Direct Participation In Hostilities Under International Humanitarian Law 16 (2009), available at http://www.icrc.org/eng/assets/files/other/icrc_002_0990.pdf
- ICRC, Overview of the ICRC's expert process 2003 - 2008, http://www.icrc.org/web/eng/siteeng.nef/html
- ICRC, Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949. Available at: www.icrc.org/ihl.nsf/WebList?ReadForm&id=470&t=com
- Department of Defense Office of General Counsel, an assessment of International Legal Issues in Information Operations, May 1999, available at: https://irp.fas.org/eprint/io-legal.pdf

سادسًا: مواقع إلكترونية:

(١)باللغة العربية:

- حول هجمات رفض الخدمة:

https://nasainarabic.net/main/articles/view/malicious-software-worms-trojans-and-bots-oh-my

- جريمة إتلاف وتدمير المعطيات والبيانات بواسطة الإنترنت، أبريل ٢٠٠٩، متاح على الرابط التالي:

https://www.startimes.com/?t=16193884

- استعراض الأسلحة الجديدة: نظرة عامة، مقال على الموقع الإلكتروني للجنة الدولية للصليب الأحمر.

https://www.icrc.org/ar/doc/war-and-law/weapons/new-weapons/overview-review-of-new-weapons.htm

- المقصود من مصطلح "إلكتروني" بالمعنى اللغوي والفني:

https://www.vocabulary.com/dictionary/electronic
https://scholar.najah.edu/sites/default/files/%D9%88%D9%84%D9%8A%D8%AF%20%D8%AC%D9%84%D8%B9%D9%88%D8%AF.pdf

- حول فيروسات الحاسب الآلي:

https://mawdoo3.com/%D8%A8%D8%AD%D8%AB_%D8%B9%D9%86_%D9%81%D9%8A%D8%B1%D9%

88%D8%B3%D8%A7%D8%AA_%D8%A7%D9%84%D8%AD%D8%A7%D8%B3%D8%A8

- ما من فراغ قانوني في الفضاء السيبراني، مقابلة مع كوردولا دورغيه المستشار القانوني في اللجنة الدولية للصليب الأحمر، متاح على:

https://www.icrc.org/ar/doc/resources/documents/interview/2011/cyber-warfare-interview-2011-08-16.htm

- موسكو تلوّح في استخدامه.. سلاح تفادت روسيا استخدامه في العملية العسكرية في أوكرانيا!، جريدة الوطن، ٨ مارس ٢٠٢٢. متاح على:

https://alwatannews.net/Life-Style/article/994774/

- خالد وليد محمود، كيف يمكن استخدام السلاح السيبراني في الأزمة الروسية الأوكرانية؟، الجزيرة، 21/2/2022. متاح على: https://1-a1072.azureedge.net/opinions/2022/2/21/

- منشأة نطنز النووية الإيرانية: ما هي وما سر الحوادث المتكررة فيها؟، بي بي سي بالعربي، ٢٢ أبريل/ نيسان ٢٠٢١. متاح على: https://www.bbc.com/arabic/middleeast-56721332

- خير الدين الجابري، أكبر هجوم سيبراني في تاريخ إسرائيل".. ماذا وراء عمليات الاختراق التي شلت وزارات حكومة تل أبيب؟، عربي بوست ١٥/٠٣/٢٠٢٢. متاح على الرابط التالي: https://arabicpost.net/

- هجوم سيبراني على أكثر من ١٠٠ موقع إلكتروني لمؤسسات إيرانية عامة وخاصة، موقع ايران انترناشيونال 04/25/2022 . متاح على الرابط التالي:

https://www.iranintl.com/ar/202204255536

- ما هي الحرب السيبرانية وما مدى خطورتها، مقال منشور على CyberOne، متاح على:

https://cyberone.co/%D9%85%D8%A7-%D9%87%D9%8A-%D8%A7%D9%84%D8%AD%D8%B1%D8%A8-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9/

- عالم روسي: السلاح السيبراني أخطر سلاح في العالم، RT online، ٢٦ يونيو ٢٠١٩.

https://arabic.rt.com/it/1028347-%D8%A7%D9%84%D8%B9%D8%A7%D9%84%D9%85-%D8%A7%D9%84%D8%B3%D9%84%D8%A7%D8%AD-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A-%D8%A7%D9%84%D8%B9%D8%A7%D9%84%D9%85/

- الحرب الإلكترونية العسكرية... سلاح "غير مرئي" يصيب الجيوش بـ"شلل تام"، متاح على الرابط التالي:

https://sputnikarabic.ae/20191001/%D8%A7%D9%84%D8%AD%D8%B1%D8%A8-

%D8%A7%D9%84%D8%A5%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A%D8%A9-%D8%A7%D9%84%D8%B9%D8%B3%D9%83%D8%B1%D9%8A%D8%A9-%D8%B3%D9%84%D8%A7%D8%AD-%D8%BA%D9%8A%D8%B1-%D9%85%D8%B1%D8%A6%D9%8A-%D9%8A%D8%B5%D9%8A%D8%A8-%D8%A7%D9%84%D8%AC%D9%8A%D9%88%D8%B4-%D8%A8%D9%80%D8%B4%D9%84%D9%84-%D8%AA%D8%A7%D9%85-1043031829.html

(٢)باللغة الإنجليزية:

- 'War in the Fifth Domain', The Economist, July 1st of 2010. Available at: https://www.economist.com/briefing/2010/07/01/war-in-the-fifth-domain

- Newly Nasty: Defences Against Cyberwarfare Are Still Rudimentary. That's Scary, ECONOMIST (May 24, 2007), available at: http://www.economist.com/node/9228757?story_id=9228757

- Officials anonymously leaked qualified reports of U.S. suspicions that the attack emerged in North Korea. U.S. Eyes N. Korea for 'Massive' Cyber Attacks, MSNBC.COM (July 9, 2009), available at:

http://www.msnbc.msn.com/id/31789294/ns/technology_and_science-security

- Russia's war on Ukraine: Timeline of cyber-attacks, Think Tank, European Parliament, 21-06-2022. Available at:

  https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)733549

- Cf. B. Graham, Bush Orders Guidelines for Cyber-Warfare, Washington Post, 7 February 2003, available at: http://www.stanford.edu/class/msande91si/www-spr04/readings/week5/bush_guidelines.html

- Ellen Nakashima, Russian Hackers Suspected in Attack That Blacked Out Parts of Ukraine, WASH. POST, Jan. 5, 2016. Available at: https://www.washingtonpost.com/world/national-security/russian-hackers-suspected-in-attack-that-blacked-out-parts-of-ukraine/2016/01/05/4056a4dc-b3de-11e5-a842-0feb51d1d124_story.html

- Emily Alpert, Why Hasn't the U.S. Signed an International Ban on Landmines?, L.A. TIMES BLOG, http://latimesblogs.latimes.com/world_now/2012/04/mine-treaty-us-ottawa-convention.html

- Cf. B. Graham, Bush Orders Guidelines for Cyber-Warfare, Washington Post, 7 February 2003, http://www.stanford.edu/class/msande91si/www-spr04/readings/week5/bush_guidelines.html .

K. Ban, Secretary-General's remarks to the Advisory Board on Disarmament Matter (2009), http://www.un.org/apps/sg/sgstats.asp?nid=3717