IRRC
المجلة الدولية للصليب الأحمر (2020)، **102** (913)، 287–334.
التقنيات الإلكترونية والحرب
معرّف الوثيقة الرقمي: 10.1017/S1816383120000387

بعد عشرين عامًا: القانون الدولي الإنساني وحماية المدنيين من آثار العمليات السيبرانية أثناء النزاعات المسلحة

لوران جيزل وتيلمان رودنهاوسر وكنوت دورمان*
لوران جيزل رئيس وحدة الأسلحة وسير الأعمال العدائية في الشعبة القانونية باللجنة الدولية للصليب الأحمر (اللجنة الدولية) في جنيف. وفي الفترة بين عامي 2013 و 2020، شغل باللجنة الدولية منصب كبير المستشارين القانونيين ورئيس الفريق السيبراني والمسؤول عن ملف القواعد التي تحكم سير الأعمال العدائية في إطار القانون الدولي الإنساني، ويشمل ذلك تطبيقها أثناء حروب المدن والعمليات السيبرانية وعمليات الفضاء الخارجي.

الدكتور تيلمان رودنهاوسر مستشار قانوني باللجنة الدولية يعمل في مجالات العمليات السيبرانية أثناء النزاع المسلح والجماعات المسلحة من غير الدول ونقل المحتجزين.

* نشر نفس المؤلفين نسخة سابقة من هذا المقال تحت عنوان "انطباق القانون الدولي الإنساني وتطبيقه على الحرب السيبرانية" في المجلة الصينية للقانون الدولي، المجلد 32، العدد 4، 2019. ثم تم تحديثه وتوسيع نطاقه إلى حد كبير تمهيدًا لنشره في هذا العدد من المجلة. وهذا المقال مكتوب بصفحة شخصية ولا يعبر بالضرورة عن آراء اللجنة الدولية.

الدكتور كنوت دورمان رئيس بعثة اللجنة الدولية لدى الاتحاد الأوروبي وحلف شمال الأطلسي ومملكة بلجيكا (بروكسل) وسبق له شغل منصب كبير المسؤولين القانونيين ورئيس الشعبة القانونية (2007-2019). وقبل ذلك، شغل منصب نائب رئيس الشعبة القانونية باللجنة الدولية (2004-2007) وعمل مستشارًا قانونيًا باللجنة الدولية (1999-2004) في مجالات منها العمليات السيبرانية.

مُلخَّص

شهد العقدان الماضيان تطورًا ملحوظًا في اللجوء إلى العمليات السيبرانية أثناء النزاعات المسلحة، وامتد هذا التطور إلى مسألة كيفية تطبيق القانون الدولي الإنساني على هذه العمليات. وتابع مؤلفو المقال هذه التطورات عن كثب وشاركوا في مناقشات الخبراء الحكوميين وغير الحكوميين بشأن هذا الموضوع، وذلك في إطار أدوارهم المختلفة التي اضطلعوا بها في الشعبة القانونية باللجنة الدولية. ونحلل في هذا المقال المسائل الإنسانية والقانونية والسياساتية ذات الصلة بهذا الموضوع. فنعمد أولًا إلى بيان أن استخدام العمليات السيبرانية أثناء النزاع المسلح قد أضحى سمة واقعية من سمات النزاعات المسلحة ومن المرجح أن يسلط عليها مزيد من الضوء في المستقبل. ويثير هذا التطور عددًا من الشواغل في مجتمعات اليوم التي تعتمد اعتمادًا متزايدًا على الفضاء السيبراني الذي تتسبب فيه العمليات السيبرانية الضارة في احتمال تعطيل البشر وإلحاق الأضرار الجسيمة بهم. ثانيًا، نقدم لمحة عامة موجزة للمناقشات المتعددة الأطراف المتعلقة بالإطار القانوني والمعياري الذي ينظم العمليات السيبرانية أثناء النزاعات المسلحة، وننظر تحديدًا في الحجج المختلفة المتعلقة بانطباق القانون الدولي الإنساني على العمليات السيبرانية أثناء النزاع المسلح، والعلاقة القائمة بين القانون الدولي الإنساني وميثاق الأمم المتحدة. ونؤكد ونحن نعرض وجهة نظرنا أنه ليس ثمة شك في أن القانون الدولي الإنساني ينظم العمليات السيبرانية أثناء النزاعات المسلحة أو الحرب السيبرانية- شأن أي سلاح أو أسلوب أو وسيلة للقتال يلجأ إليها أي طرف من الأطراف المتحاربة في النزاع، قديمة كانت أو حديثة. ثالثًا، نركز في الجزء الرئيسي من هذا المقال على كيفية تطبيق القانون الدولي الإنساني على العمليات السيبرانية. ومن خلال تحليل أحدث المواقف القانونية للدول والخبراء، نعيد النظر في بعض المناقشات الأبرز التي أجريت في العقد الماضي، مثل تحديد العمليات السيبرانية التي تصل إلى حد "الهجوم" على النحو المحدد في القانون الدولي الإنساني وما إذا كانت البيانات المدنية تتمتع بحماية مماثلة للحماية التي تحظى بها "الأعيان المدنية". ونتناول بالدراسة أيضًا قواعد القانون الدولي الإنساني المنطبقة على العمليات السيبرانية بخلاف الهجمات ونظم الحماية الخاصة لبعض الجهات الفاعلة والبنى التحتية، مثل المرافق الطبية والمنظمات الإنسانية.

الكلمات الرئيسية: االعمليات السيبرانية، النزاع المسلح، الحرب السيبرانية، التكلفة البشرية، القانون الدولي الإنساني.

: : : : : : :

شهد العقدان الماضيان تطورًا ملحوظًا في اللجوء إلى العمليات السيبرانية أثناء النزاعات المسلحة، وامتد هذا التطور إلى مسألة كيفية تطبيق القانون الدولي الإنساني على هذه العمليات. وهذه النتيجة صحيحة على المستويات العملياتية والقانونية والسياسية. فعلى المستوى العملياتي، أضحى استخدام العمليات السيبرانية أثناء النزاع المسلح واقعًا يميز النزاعات المسلحة ومن المرجح أن يسلط عليه مزيد من الضوء في المستقبل. ويثير هذا التطور عددًا من الشواغل في مجتمعات اليوم التي تعتمد اعتمادًا غير مسبوق على الفضاء السيبراني، الذي تتسبب فيه العمليات السيبرانية الضارة في احتمال تعطيل البشر وإلحاق الأضرار الجسيمة بهم. وعلى المستويين السياسي والقانوني، توصلت الدول من خلال عمليات متعددة الأطراف إلى توافق بشأن بعض جوانب الإطار القانوني والمعياري الذي ينظم العمليات السيبرانية؛ ومع ذلك، يظل تطبيق القانون الدولي الإنساني على العمليات السيبرانية أثناء النزاع المسلح موضوع نقاش مكثف. ونشرت بضع دول مواقف حول كيفية تطبيق القانون الدولي الإنساني على العمليات السيبرانية أثناء النزاعات المسلحة، وهناك ثروة من الدراسات الأكاديمية حول هذه المسألة، ومع ذلك تظل المسائل الرئيسية محل خلاف وتفتقر إلى اتفاق بين الدول والخبراء الآخرين أو تتطلب مزيدًا من التحليل. وهي تشمل مفهوم "الهجوم"، والمسألة المتعلقة بكيفية حماية البيانات المدنية من العمليات السيبرانية الضارة، وكيفية تطبيق قواعد القانون الدولي الإنساني على العمليات السيبرانية بخلاف الهجمات. وتابع مؤلفو المقال هذه التطورات والمناقشات عن كثب وشاركوا في مناقشات الخبراء الحكوميين وغير الحكوميين حول انطباق القانون الدولي الإنساني وتطبيقها على العمليات السيبرانية أثناء النزاعات المسلحة منذ انطلاق شرارتها الأولى، وذلك في إطار أدوارهم المختلفة التي اضطلعوا بها في الشعبة القانونية باللجنة الدولية.

ونشرت اللجنة الدولية مؤخرًا موقفًا مؤسسيًا شاملًا بشأن القانون الدولي الإنساني والعمليات السيبرانية أثناء النزاعات المسلحة، قُدم إلى فريق الخبراء الحكوميين والفريق العامل المفتوح العضوية التابعين للأمم المتحدة.[1] وفي هذا المقال، نتوسع في بيان هذا الموقف ونوضح في البداية السبب في اعتبار التكلفة البشرية المحتملة للعمليات السيبرانية مصدرًا للقلق على الصعيد الإنساني. ونؤكد بعد ذلك أن القانون الدولي الإنساني ينطبق على العمليات السيبرانية أثناء النزاعات المسلحة -ومن ثم يقيدها- ونتدارس وجهات نظر الدول المختلفة حول هذا الموضوع. ثالثًا، نحلل الحالات التي قد تؤدي العمليات السيبرانية فيها إلى نزاع مسلح، وكيف يرتبط هذا الحد بحظر استخدام القوة والحق في الدفاع عن النفس بموجب ميثاق الأمم المتحدة والقانون الدولي العرفي. وفي الجزء الأخير والأشمل من المقال، نتعمق في دراسة بعض الأسئلة التي طال أمدها حول كيفية تطبيق القانون الدولي الإنساني على العمليات السيبرانية أثناء النزاعات المسلحة، والمواقف التي اتخذتها الدول بشأن بعض المسائل الرئيسية.

فعلى المستوى العملياتي، أضحى استخدام العمليات السيبرانية أثناء النزاع المسلح سمة واقعية من سمات النزاعات المسلحة ومن المرجح أن يسلط عليه مزيد من الضوء في

1 اللجنة الدولية، القانون الدولي الإنساني والعمليات السيبرانية خلال النزاعات المسلحة، ورقة موقف مقدمة إلى فريق العمل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، وإلى فريق الخبراء الحكوميين المعني بالارتقاء بسلوك الدول المسؤول في ميدان الفضاء السيبراني في سياق الأمن الدولي، 2019، متاح من خلال الرابط التالي:
www.icrc.org/ara/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts
(جرى الاطلاع على جميع مراجع الإنترنت في آب/أغسطس 2020). وهي متاحة أيضًا في قسم "التقارير والوثائق" في هذا العدد من المجلة.

المستقبل. وأقرت بعض الدول علنًا بأنها أجرت عمليات سيبرانية في نزاعات مسلحة جارية. فقد كشفت الولايات المتحدة والمملكة المتحدة وأستراليا على وجه الخصوص أنها لجأت إلى العمليات السيبرانية في نزاعها ضد تنظيم الدولة الإسلامية.[2] نشرت أيضًا تقارير عامة تشير إلى أن إسرائيل استخدمت عمليات سيبرانية ضد حماس - ومزاعم بأن حماس استخدمت عمليات سيبرانية ضد إسرائيل.[3] وعلاوة على ذلك، أثرت العمليات السيبرانية على بلدان أخرى مشاركة في نزاعات مسلحة، مثل جورجيا في عام 2008،[4] وأوكرانيا في الفترة 2015-2017،[5] والمملكة السعودية العربية في عام 2017،[6] وإن كان منفذو هذه الهجمات لا يزالون مجهولي الهوية وثمة تنازع على عزو المسؤولية. لذلك، ليس من الواضح ما إذا كانت هذه العمليات لها علاقة بالنزاعات المسلحة ذات الصلة، ومن ثم ما إذا كان القانون الدولي الإنساني ينطبق أم لا. وبالإضافة إلى ذلك، وردت تقارير عن عمليات سيبرانية نفذتها دول في حالات أخرى قد لا يكون فيها التصنيف القانوني واضحًا، ومنها الحالات التي يشار إليها أحيانًا باسم "المنطقة الرمادية".[7] وتبين هذه الأمثلة وجود زيادة في العمليات السيبرانية العسكرية على مدى العقد الماضي- وهو ما يمثل تغيرًا قد يستمر في الحروب. والواقع أن هناك عددًا متزايدًا من الدول يقال إنها

2 انظر على وجه الخصوص:
Mike Burgess, Australian Signals Directorate, "Offensive Cyber and the People Who Do It", speech given to the Lowy Institute, 27 March 2019, available at: www.asd.gov.au/speeches/20190327-lowy-institute-offensive-cyber-operations.html; Paul M. Nakasone, "Statement of General Paul M. Nakasone, Commander, United States Cyber Command, before the Senate Committee on Armed Services", 14 February 2019, available at: www.armed-services.senate.gov/imo/media/doc/Nakasone_0219-14-.pdf; Jeremy Fleming, GCHQ, "Director's Speech at CyberUK18", 12 April 2018, available at: www.gchq.gov.uk/pdfs/speech/director-cyber-uk-speech-2018.pdf.

3 "Hackers Interrupt Israeli Eurovision WebCast with Faked Explosions", BBC News, 15 May 2019, available at: www.bbc.co.uk/news/technology-48280902; Zak Doffman, "Israel Responds to Cyber Attack with an Air Strike on Cyber Attackers in World First", Forbes, 6 May 2019, available at: www.forbes.com/sites/zakdoffman/2019/05/06/israeli-military-strikes-and-destroys-hamas-cyber-hq-in-world-first/#1c692f73afb5.

في حين أن الهدف المزعوم للعملية السيبرانية التي يُزعم أن حماس ارتكبتها لم يُعلن بعد، فقد قيل إن استهداف مبنى حماس بالوسائل الحركية يستند إلى معلومات استخبارية تم الحصول عليها في إطار جهود الدفاع السيبراني لقوات الدفاع الإسرائيلية.

4 David Hollis, "Cyberwar Case Study: Georgia 2008", Small War Journal, 2010, available at: https://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf.

5 Andy Greenberg, "How an Entire Nation Became Russia's Test Lab for Cyberwar", Wired, 20 June 2017, available at: www.wired.com/story/russian-hackers-attack-ukraine/; Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History", Wired, 22 August 2018, available at: www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

6 Blake Johnson et al., "Attackers Deploy New ICS Attack Framework 'TRITON' and Cause Operational Disruption to Critical Infrastructure", Fireeye Blogs, 14 December 2017, available at www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html.

7 على سبيل المثال، أفادت تقارير إعلامية مختلفة - تستند إلى مصادر رسمية لم تكشف عن هويتها- بأن الولايات المتحدة نفذت عمليات سيبرانية ضد أهداف في روسيا وإيران، وأن إسرائيل نفذت عملية سيبرانية ضد ميناء في إيران. انظر:
Ellen Nakashima, "U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms", *Washington Post*, 27 February 2019, available at: https://tinyurl.com/yxs8twyv; David E. Sanger and Nicole Perlroth, "U.S. Escalates Online Attacks on Russia's Power Grid", *New York Times,* 15 June 2019, available at: www.nytimes.com/201915/06//us/politics/trump-cyber-russia-grid.html; Julian E. Varnes and Thomas Gibbons-Neff, "U.S. Carried out Cyberattacks on Iran", *New York Times*, 22 June 2019, available at: www.nytimes.com/201922/06//us/politics/us-iran-cyber-attacks.html; Joby Warrick and Ellen Nakashima, "Officials: Israel Linked to a Disruptive Cyberattack on Iranian Port Facility", *Washington Post*, 18 May 2020, available at: https://tinyurl.com/y4onsrt9.

وبشأن ما يسمى "المناطق الرمادية" والتكنولوجيا السيبرانية، انظر:
Camille Faure, "Utilisation contemporaine et future des technologies cyber/numériques dans les conflits armés", in Gabriella Venturini and Gian Luca Beruto (eds), *Whither the Human in Armed Conflict? IHL Implications of New Technology in Warfare*, 42nd Round Table on Current Issues of International Humanitarian Law, International Institute of Humanitarian Law, Sanremo, 2020 (forthcoming); Gary Corn, "Punching on the Edges of the Grey Zone: Iranian Cyber Threats and State Cyber Responses", *Just Security*, 11 February 2020, available at: www.justsecurity.org/68622/punching-on-the-edges-of-the-grey-zone-iranian-cyber-threats-and-state-cyber-responses/.

وبشأن حد تطبيق القانون الدولي الإنساني، انظر: القسم أدناه المعنون "العمليات السيبرانية التي تخضع للقانون الدولي الإنساني".

لديها قدرات عسكرية سيبرانية أو بصدد تطوير هذه القدرات، ومنها الدول الخمس الدائمة العضوية في مجلس الأمن التابع للأمم المتحدة.[8] ومن أمثلة استخدام العمليات السيبرانية أثناء النزاعات التجسس؛ وتحديد الأهداف؛ والعمليات المعلوماتية الرامية إلى التأثير على معنويات العدو وإرادته إزاء القتال؛ وقطع نظم اتصالات العدو أو تضليلها أو التشويش عليها ابتغاء إعاقة تنسيق القوات؛ والعمليات السيبرانية الرامية إلى دعم العمليات الحركية.[9] ومن أمثلة الفئة الأخيرة تعطيل محطات الرادار العسكرية للعدو لدعم الضربات الجوية.[10] وبالإضافة إلى ذلك، وكما تبين لنا في طائفة من العمليات السيبرانية على مدى العقد الماضي- التي ربما لم تقع بالضرورة في سياق نزاعات مسلحة- تشكل العمليات السيبرانية التي تستهدف شبكات الكهرباء أو نظم الرعاية الصحية أو المنشآت النووية أو غيرها من الهياكل الأساسية الحيوية خطرَ إلحاق أضرار جسيمة بالبشر.[11] وعلى المستوى القانوني، انطلقت قبل أكثر من عقدين مناقشات حول ما إذا كان القانون الدولي الإنساني ينطبق على العمليات السيبرانية ويقيدها أثناء النزاعات المسلحة وكيفية ذلك.[12] وأظهرت عمليات صياغة دليلَي تالين بشأن أحكام القانون الدولي

8 بالإضافة إلى الولايات المتحدة والمملكة المتحدة، حددت فرنسا الهدف من "الحصول على قدرة دفاع سيبرانية" بالدفاع عن نفسها ضد "الدول الأجنبية أو الجماعات الإرهابية [التي] قد تهاجم الهياكل الأساسية الحيوية". فرنسا، وكالة أمن نظم المعلومات الوطنية، دفاع وأمن نظم المعلومات: استراتيجية فرنسا، 2011، متاحة من خلال الرابط التالي:
www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf.
وينص الكتاب الأبيض لعام 2015 حول الاستراتيجية العسكرية للصين على أنه "استجابة للتطور المتزايد للقدرات العسكرية السيبرانية لدى الدول الأخرى، ستطور الصين قدرة عسكرية سيبرانية دفاعية". انظر: حكومة الصين، الكتاب الأبيض بشأن الاستراتيجية العسكرية للصين، 2015، متاح من خلال الرابط التالي: www.gov.cn/zhengce/2015-05/26/content_2868988.html.
كانت روسيا أقل وضوحًا بشأن هذا الموضوع، إلا أن مبدأ أمن المعلومات في الاتحاد الروسي ينص على أن "تحديث نظام أمن المعلومات للقوات المسلحة والقوات والتشكيلات والهيئات العسكرية الأخرى التابعة للاتحاد الروسي، بما في ذلك قوات ووسائل المواجهة المعلوماتية" هو "مجال رئيسي لضمان أمن المعلومات في ميدان الدفاع الوطني". انظر: وزارة خارجية الاتحاد الروسي، مبادئ أمن المعلومات في الاتحاد الروسي، 5 كانون الأول/ديسمبر 2016، متاحة من خلال الرابط التالي: https://tinyurl.com/y6yhp7pv. انظر أيضًا:
Ministry of Defence of the Russian Federation, "Western MD Operators Repelled Cyberattack of the Simulated Enemy in the Course of the Union Shield - 2015", 2015, available at:
https://eng.mil.ru/en/news_page/country/more.htm?id=12056193@egNews.
للاطلاع على تقديرات عامة حول انتشار الأدوات السيبرانية، انظر:
Anthony Craig, "Understanding the Proliferation of Cyber Capabilities", Council on Foreign Relations, 2018, available at: www.cfr.org/blog/understanding-proliferation-cyber-capabilities.
ويفيد المؤشر السيبراني لمعهد الأمم المتحدة لبحوث نزع السلاح بأن سبعًا وأربعين دولة كان لديها في عام 2012 برامج للأمن السيبراني أسندت بعض الأدوار لقواتها المسلحة (UNIDIR, *The Cyber Index: International Security Trends and Realities,* UN Doc. UNIDIR/2013/ 3, Geneva, 2013, p. 1)، في حين سجل مرصد المراقبة الرقمية في عام 2020 ما عدده ثلاث وعشرون دولة وثلاثون دولة لديها على الترتيب أدلة أو مؤشرات على وجود قدرات سيبرانية هجومية
(Digital Watch Observatory, "UN GGE and OEWG", available at: https://dig.watch/processes/un-gge).

9 ICRC, *Avoiding Civilian Harm from Military Cyber Operations during Armed Conflicts*, forthcoming.

10 Sharon Weinberger, "How Israel Spoofed Syria's Air Defense System", *Wired*, 4 October 2007, available at: www.wired.com/2007/10/how-israel-spoo/; Lewis Page, "Israeli Sky-Hack Switched Off Syrian Radars Countrywide", *The Register*, 22 November 2007, available at: www.theregister.co.uk/2007/11/22/israel_air_raid_syria_hack_network_vuln_intrusion/.

11 في تشرين الثاني/نوفمبر 2018، عقدت اللجنة الدولية اجتماعًا للخبراء لإجراء تقييم واقعي للقدرات السيبرانية وتبعاتها الإنسانية المحتملة في ضوء الخصائص التقنية. انظر:
Laurent Gisel and Lukasz Olejnik (eds), ICRC *Expert Meeting: The Potential Human Cost of Cyber Operations*, ICRC, Geneva, 2019, available at: www.icrc.org/en/download/file/96008/the-potential-human-cost-of-cyber-operations.pdf.
انظر أيضًا:
Sergio Caltagirone, "Industrial Cyber Attacks: A Humanitarian Crisis in the Making", *Humanitarian Law and Policy Blog*, 3 December 2019, available at: https://blogs.icrc.org/law-and-policy/201903/12//industrial-cyber-attacks-crisis/. The World Economic Forum (WEF) *Global Risks Report 2020* ranks cyber attacks among the top ten risks in terms of both likelihood and impact; see WEF, *The Global Risks Report 2020*, 2020, p. 3, available at: www.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf.

12 انظر: مكتب المستشار العام بوزارة الدفاع الأمريكية، تقييم المسائل القانونية الدولية في عمليات المعلومات، 1999، متاح من خلال الرابط التالي:

المنطبقة على العمليات السيبرانية (دليلا تالين) أن هناك إجماعًا كبيرًا بين الخبراء على أن القانون الدولي الإنساني ينطبق في الفضاء السيبراني وأن قواعده ومبادئه الأساسية يمكن بل ويجب تطبيقها عند تنفيذ العمليات السيبرانية أثناء النزاع المسلح.[13] ومن ناحية أخرى، كما يتبين من الآراء المتباينة المسجلة في دليلَي تالين وكذلك في عدد متزايد من مواقف الدول والمجموعة الثرية من المنشورات الأكاديمية حول المسائل المتعلقة بالفضاء السيبراني، تظل شتى الجوانب المتعلقة بكيفية تطبيق قواعد معينة من القانون الدولي الإنساني في هذا المجال تعاني من قلة الدراسة، ويوجد خلاف بشأن مسائل أخرى، منها بعض المسائل التي قُتلت بحثًا (انظر القسم أدناه حول "القيود التي يفرضها القانون الدولي الإنساني على استخدام القدرات السيبرانية أثناء النزاعات المسلحة"). وعلى المستوى السياسي، بينت المناقشات الأخيرة والجارية في الأمم المتحدة أن التوصل إلى اتفاق بشأن انطباق القانون الدولي الإنساني على العمليات السيبرانية وتعزيز الدارسة المتعلقة بكيفية تفسير قواعده هما من المسائل التي لا تزال تنطوي على تحديات.[14] وبدأت المناقشات حول المسائل المتعلقة بـ "أمن المعلومات" عندما قدم الاتحاد الروسي أول قرار بشأن هذا الموضوع في الجمعية العامة للأمم المتحدة في عام 1998. وشهدت السنوات القليلة الماضية تكثيف هذه المناقشات. فمنذ عام 2004، يجتمع خبراء حكوميون في إطار ستة أفرقة متتالية من الخبراء الحكوميين بشأن مسائل تتصل بالمعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي. وفي عام 2018، أنشأت الجمعية العامة للأمم المتحدة أيضًا الفريق العامل المفتوح العضوية، الذي يمارس مهامه جنبًا إلى جنب مع فريق الخبراء الحكوميين. وكلا الفريقين مكلف بمهام منها دراسة "كيفية انطباق القانون الدولي على استخدام الدول لتكنولوجيات المعلومات والاتصالات".[15] وينبغي أن تستفيد هذه المناقشات من الاستنتاجات المهمة التي خلص إليها فريق الخبراء الحكوميين السابق. وفي عامي 2013 و 2015، أكدت الدول الأعضاء في فريق الخبراء الحكوميين أن "أحكام القانون الدولي، ولا سيما ميثاق الأمم المتحدة، قابلة للتطبيق" في بيئة تكنولوجيا المعلومات والاتصالات وأشارت إلى "المبادئ القانونية الدولية المعمول بها، بما في ذلك، حسب الاقتضاء، مبادئ الإنسانية والضرورة والتناسب والتمييز".[16] ومع ذلك، يبدو من المناقشات الأخيرة في عمليات الأمم المتحدة المذكورة، وعلى النحو المبين بمزيد

https://fas.org/irp/eprint/io-legal.pdf:

وللاطلاع على واحدة من الدراسات الأكاديمية المبكرة التي تناولت هذه المسائل، انظر:
Knut Dörmann, "Computer Network Attack and International Humanitarian Law", 2001, available at: www.icrc.org/en/doc/resources/documents/article/other/5p2alj.html.

13 انظر:
Michael N. Schmitt (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, Cambridge, 2013 (Tallinn Manual) [دليل تالين]:

وانظر:
Michael N. Schmitt and Liis Vihul (eds), *Tallinn Manual 2.0 on International Law Applicable to Cyber Operations*, 2nd ed., Cambridge University Press, Cambridge, 2017 (Tallinn Manual 2.0) [دليل تالين 2].

14 انظر، على وجه الخصوص:
OEWG, "Initial 'Pre-draft' of the Report of the OEWG on Developments in the Field of Information and Telecommunications in the Context of International Security", 11 March 2020, available at: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020200311-/03/Pre-Draft-OEWG-ICT.pdf.

15 قرار الجمعية العامة للأمم المتحدة73/27 ، "التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي"، وثيقة الأمم المتحدة A/RES/73/27، 11 كانون الأول/ديسمبر 2018، الفقرة 5؛ وقرار الجمعية العامة للأمم المتحدة 73/266، "الارتقاء بسلوك الدول المسؤول في الفضاء الإلكتروني في سياق الأمن الدولي"، وثيقة الأمم المتحدة A/RES/73/266، 2 كانون الثاني/يناير 2019، الفقرة 3.

16 الجمعية العامة للأمم المتحدة، "فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي: مذكرة من الأمين العام"، وثيقة الأمم المتحدة A/70/174، 22 تموز/يوليو 2015، الفقرتان 24 و28 (د).

من التفصيل أدناه، أن التوصل إلى اتفاق بشأن انطباق القانون الدولي الإنساني على العمليات السيبرانية وتعزيز الدارسة المتعلقة بكيفية تفسير قواعده لا تزال تمثل تحديًا.

وعلى الصعيد الإقليمي، سبق للدول الأعضاء في منظمة شنغهاي للتعاون أن قررت في عام 2009 أن "تطوير واستخدام أسلحة المعلومات" و "التحضير لحرب المعلومات وتنفيذها" يشكلان تهديدًا رئيسيًا في مجال أمن المعلومات الدولي، إلا أنها التزمت الصمت بشأن الإطار القانوني المنطبق.[17] وأجريت مناقشات بشأن تطبيق القانون الدولي، بما في ذلك القانون الدولي الإنساني، في المنظمة الاستشارية القانونية الآسيوية الأفريقية (آلكو) (التي أنشأت فريقًا عاملًا مفتوح العضوية بشأن القانون الدولي في الفضاء السيبراني في عام 2015)،[18] والكومنولث،[19] والاتحاد الأوروبي،[20] ومنظمة حلف شمال الأطلسي (الناتو)،[21] ومنظمة الدول الأمريكية،[22] بالإضافة إلى جهات أخرى.

التكلفة البشرية المحتملة للعمليات السيبرانية

يوفر تطوير تكنولوجيا المعلومات والاتصالات، بما في ذلك الاتصال عبر شبكات الكمبيوتر (الفضاء السيبراني)، فوائد وفرصًا هائلة للدول والمجتمعات والأفراد في المجالات الاجتماعية والاقتصادية والتنموية والمعلوماتية ومجالات الاتصال، بالإضافة إلى مجالات أخرى. ويعتمد المجتمع الدولي والمجتمعات وكل فرد منا بشكل متزايد على الأدوات الرقمية. وهذا الاتجاه - الذي ربما تسارعت وتيرته بفعل انتشار جائحة كوفيد-19 في وقت كتابة هذا المقال - يزيد من اعتمادنا على استمرار تشغيل هذه التقنيات، وبالتالي يزيد من تعرضنا للعمليات السيبرانية. ولذلك، فإن الطبيعة السريعة التطور التي يتسم بها الفضاء السيبراني والتكنولوجيا السيبرانية، والتكلفة البشرية المحتملة للعمليات السيبرانية، تتطلبان رصدًا وتقييما مستمرين.

واستخدام الأدوات السيبرانية باعتبارها من وسائل أو أساليب القتال يتيح للجيوش إمكانية تحقيق أهدافها دون التسبب بالضرورة في إلحاق ضرر مباشر بالمدنيين أو إلحاق أضرار مادية بالبنية التحتية المدنية. وحسب الظروف، قد تتيح العمليات السيبرانية استهداف هدف عسكري مع تقليل الأضرار العرضية المتوقع أن تلحق بالأعيان المدنية مقارنة باستخدام وسائل الحرب الأخرى. وفي المناقشات الحكومية الدولية الأخيرة، شددت بعض الدول على أن تكنولوجيا

17 اتفاقية التعاون في مجال ضمان أمن المعلومات الدولي بين الدول الأعضاء في منظمة شنغهاي للتعاون، يكاترينبورغ، 16 حزيران/يونيو 2009 (اتفاقية منظمة شنغهاي للتعاون)؛ ترجمة غير رسمية في وزارة الدفاع في الاتحاد الروسي،
"The State and the Prospects of Russian Military Cooperation on International Information Security (A Collection of Papers)", 2014, pp. 77 ff.

انظر أيضًا على سبيل المثال: J.Fleming، الحاشية 2 أعلاه، الصفحة 5.

18 انظر:
AALCO, *International Law in Cyberspace*, Doc. No. AALCO/58/DAR ES SALAAM/2019/SD/17, available at: www.aalco.int/Final%20Cyberspace%202019.pdf.

19 انظر: إعلان الكومنولث بشأن العمليات السيبرانية الصادر في اجتماع رؤساء حكومات الكومنولث، لندن، 16-20 نيسان/أبريل 2018، متاح من خلال الرابط التالي: https://thecommonwealth.org/commonwealth-cyber-declaration.

20 انظر على سبيل المثال: استنتاجات مجلس الاتحاد الأوروبي، اجتماع مجلس الشؤون العامة، الوثيقة رقم 13/11357، 25 حزيران/يونيو 2013.

21 انظر على سبيل المثال: إعلان قمة ويلز الصادر عن رؤساء الدول والحكومات المشاركين في اجتماع الناتو في ويلز، 5 أيلول/سبتمبر 2014، الفقرة. 72، متاح من خلال الرابط التالي: www.nato.int/cps/en/natohq/official_texts_112964.html.

22 انظر:
OAS, Improving Transparency: *International Law and State Cyber Operations: Fourth Report*, OAS Doc. CJI/doc. 603/20 rev.1 corr.1, 5 March 2020, available at: www.oas.org/en/sla/iajc/docs/CJI_doc_60320-_rev1_corr1_eng.pdf.

المعلومات والاتصالات إذا وُظفت بطريقة مسؤولة ووفقًا للقانون الدولي، "فإن استخدامها في السياقات العسكرية قد تكون له الأفضلية عن استخدام الأسلحة الحركية ويمكن أن يؤدي إلى التهدئة".[23] في المقابل، وكما أشرنا آنفًا، حذرت الدول الأعضاء في منظمة شنغهاي للتعاون من "تطوير واستخدام أسلحة المعلومات" و "التحضير لحرب المعلومات وشنها".[24]

قد ينطوي تنفيذ عمليات سيبرانية شديدة التمييز تتوافق مع القانون الدولي الإنساني وتتفادي إصابة السكان المدنيين على تحديات تقنية. والترابط الذي يميز الفضاء السيبراني يعني أن أي شيء له واجهة بينية تتصل بالإنترنت يمكن أن يتأثر بالعمليات السيبرانية التي تُنفذ في أي مكان في العالم. وقد يخلف الهجوم السيبراني الذي يستهدف نظامًا معينًا تداعيات على نظم أخرى مختلفة، بغض النظر عن مكانٍ وجود تلك النظم. وثمة خطر حقيقي من أن تؤدي الأدوات السيبرانية - سواء عمدًا أو خطأً - إلى آثار واسعة النطاق ومتنوعة على البنية التحتية المدنية الحيوية. وترابط الفضاء السيبراني يعني أيضًا أن جميع الدول ينبغي أن تهتم بالرقابة الفعالة عليه: "الهجمات التي تُشن ضد دولة واحدة يمكن أن تؤثر على العديد من الدول الأخرى - بغض النظر عن مكان وجودها وعن مشاركتها في النزاع".[25] وأظهرت العمليات السيبرانية التي نُفذت على مدى السنوات الأخيرة - أساسًا خارج نطاق النزاعات المسلحة - أن البرامج الضارة سرعان ما تنتشر في جميع أنحاء العالم وتؤثر على البنية التحتية المدنية وتوفير الخدمات الأساسية.[26] نتيجة لذلك، يحذر المعلقون من أن الهجمات الإلكترونية الصناعية تمثل "أزمة إنسانية في طور التكوين".[27]

وقطاع الرعاية الصحية على ما يبدو مُعرّض للغاية للهجمات السيبرانية.[28] فالقطاع يتجه نحو زيادة الرقمنة والاتصال، الأمر الذي يؤدي إلى زيادة اعتماده على الأدوات الرقمية واتساع الرقعة المعرضة للهجوم - وهو تطور من المرجح أن يستمر في السنوات المقبلة. وفي كثير من الأحيان، لم يقابل هذه التطورات تحسنٌ في الأمن السيبراني.[29] وباتت نقطة الضعف المذكورة أبرز خلال جائحة كوفيد-19، حيث تعطلت المستشفيات وغيرها من مرافق الرعاية الصحية

23 UK Response to Chair's Initial 'Pre-draft' of the Report of the OEWG on Developments in the Field of Information and Telecommunications in the Context of International Security", available at: https://front.un-arm.org/wp-content/uploads/2020/04/20200415-oewg-predraft-uk.pdf.

وانظر أيضًا: اللجنة الدولية، الحاشية 9 أعلاه؛ وانظر:
Gary Corn, "The Potential Human Costs of Eschewing Cyber Operations", Humanitarian Law and Policy Blog, 31 May 2019, available at: https://blogs.icrc.org/law-and-policy/201931/05//potential-human-costs-eschewing-cyber-operations/.

24 اتفاقية منظمة شنغهاي للتعاون، الحاشية 17 أعلاه، المادة 2.

25 Helen Durham, "Cyber Operations during Armed Conflict: 7 Essential Law and Policy Questions", Humanitarian Law and Policy Blog, 26 March 2020, available at: https://blogs.icrc.org/law-and-policy/2020/03/26/cyber-armed-conflict-7-law-policy-questions/.

26 تشمل الأمثلة برنامج CrashOverride الضار، وبرنامج الفدية WannaCry، وبرنامج NotPetya المعروف باسم "الممسحة"، وبرنامج Triton الضار. وأثّر برنامج CrashOverride على إمداد الكهرباء في أوكرانيا؛ وأثر برنامج WannaCry على المستشفيات في عدة بلدان؛ وأثر برنامج NotPetya على عدد كبير للغاية من الشركات؛ وكان برنامج Triton يستهدف تعطيل نظم التحكم الصناعية وتشير تقارير إلى استخدامه في توجيه هجمات إلى المنشآت البتروكيميائية السعودية. للاطلاع على بعض المناقشات في هذا الصدد، انظر:
Laurent Gisel and Lukasz Olejnik, "The Potential Human Cost of Cyber Operations: Starting the Conversation", *Humanitarian Law and Policy Blog*, 14 November 2018, available at: https://blogs.icrc.org/law-and-policy/201814/11//potential-human-cost-cyber-operations/.

27 انظر: S. Caltagirone، الحاشية 11 أعلاه.

28 انظر: L. Gisel and L. Olejnik (eds)، الحاشية 11 أعلاه، الصفحات 18-22.

29 انظر:
Aaron F. Brantly, "The Cybersecurity of Health", *Council on Foreign Relations Blog*, 8 April 2020, available at: https://tinyurl.com/yxc4oc9j.

في دول مختلفة بسبب العمليات السيبرانية العدائية. وفي ضوء الأهمية الخاصة لقطاع الرعاية الصحية في تخفيف المعاناة في جميع الأوقات، وخاصة أثناء النزاعات المسلحة والأزمات الصحية، دعت اللجنة الدولية جميع الدول إلى احترام الخدمات الطبية والمرافق الطبية وحمايتها من الهجمات السيبرانية من أي نوع، سواء في وقت السلم أو في وقت النزاع، وإعادة تأكيد القواعد الدولية التي تحظر هذه الأعمال وإعادة الالتزام بها.[30] وبينما تجسد هذه الدعوة الالتزامات القائمة بموجب أحكام القانون الدولي الإنساني المنطبقة على العمليات السيبرانية أثناء النزاع المسلح،[31] فهي تعيد التأكيد، أو تعزز كما يرى البعض، على المحظورات القائمة بموجب القانون الدولي العام التي تنطبق في جميع الأوقات.[32]

قد تتسبب العمليات السيبرانية التي تستهدف البنية التحتية المدنية الحيوية، مثل الكهرباء والمياه والصرف الصحي، في إحداث أضرار جسيمة بالبشر.[33] وغالبًا ما يتم تشغيل هذه البنية التحتية عن طريق نظم التحكم الصناعية. ويحتاج الهجوم السيبراني الذي يستهدف نظام التحكم الصناعي قدرًا معينًا من الخبرة والتطور، وفي كثير من الأحيان برامج ضارة مخصصة. ولئن كانت الهجمات التي تستهدف نظم التحكم الصناعية أقل تواترًا في حدوثها مقارنة بسائر أنواع العمليات السيبرانية، تشير التقارير إلى أن وتيرتها آخذة في الزيادة، وقد تطورت خطورة التهديد بسرعة أكبر مما كان متوقعًا قبل بضع سنوات فقط.[34] وأشار متخصصون في الأمن السيبراني إلى أنه "لما كان من المحتمل أن تؤدي الهجمات السيبرانية المادية إلى إحداث تأثير حركي وإصابات، فمن الملح والأهم بالنسبة للأوساط الدولية للمتخصصين في أمن تكنولوجيا المعلومات، والحكومات، والخبراء القانونيين المتخصصين في مجال العمل الإنساني التحاور بشأن كيفية تنظيم تنفيذ الهجمات السيبرانية المادية".[35]

30 انظر:
"Call by Global Leaders: Work Together Now to Stop Cyberattacks on the Healthcare Sector", *Humanitarian Law and Policy Blog*, 26 May 2020, available at: https://blogs.icrc.org/law-and-policy/202026/05//call-global-leaders-stop-cyberattacks-healthcare/.

في الإطار المحدد للفريق العامل المفتوح العضوية المذكور أعلاه، اقترحت اللجنة الدولية أن تعتمد الدول قاعدة تلتزم بموجبها "بعدم إجراء أو دعم عمليات سيبرانية عن قصد من شأنها الإضرار بالخدمات الطبية أو المرافق الطبية، واتخاذ تدابير لحماية الخدمات الطبية من الضرر". ويتضمن هذا الاقتراح عنصرًا "سلبيًا"، ألا وهو أن الدول لا ينبغي لها أن تجري أو تدعم عن قصد نشاطًا سيبرانيًا من شأنه الإضرار بالخدمات أو المرافق الطبية، وعنصرًا "إيجابيًا" يعني أن الدول ينبغي لها اتخاذ تدابير لحماية الخدمات الطبية من الضرر. انظر:
ICRC, "Norms for Responsible State Behavior on Cyber Operations Should Build on International Law", 11 February 2020, available at: www.icrc.org/en/document/norms-responsible-state-behavior-cyber-operations-should-build-international-law.

31 انظر أدناه: القسم المعنون "قواعد القانون الدولي التي تحمي الأعيان التي لا غنى عنها لبقاء السكان المدنيين والخدمات الطبية وعمليات الإغاثة الإنسانية".

32 للاطلاع على المزيد من التفاصيل حول كيفية تطبيق القانون الدولي على هذه العمليات، انظر:
Kubo Mačák, Laurent Gisel and Tilman Rodenhäuser, "Cyber Attacks against Hospitals and the COVID-19 Pandemic: How Strong are International Law Protections?", *Just Security*, 27 March 2020, available at: www.justsecurity.org/69407/cyber-attacks-against-hospitals-and-the-covid-19-pandemic-how-strong-are-international-law-protections/.

انظر أيضًا: [بيان أكسفورد]
the Oxford Statement on the International Law Protections against Cyber Operations Targeting the Health Care Sector, May 2020 (Oxford Statement), available at: www.elac.ox.ac.uk/the-oxford-statement-on-the-international-law-protections-against-cyber-operations-targeting-the-hea.

33 L. Gisel and L. Olejnik (eds)، الحاشية 11 أعلاه، الصفحات 23-28. انظر أيضًا:
Aron Heller, "Israeli Cyber Chief: Major Attack on Water Systems Thwarted", *ABC News*, 28 May 2020, available at: https://abcnews.go.com/International/wireStory/israeli-cyber-chief-major-attack-water-systems-thwarted-70920855.

34 المرجع نفسه، الصفحة 25.

35 Marina Krotofil, "Casualties Caused through Computer Network Attacks: The Potential Human Costs of Cyber Warfare", 42nd Round Table on Current Issues of International Humanitarian Law, 2019, available at: http://iihl.org/wp-content/uploads/2019/11/Krotofil1.pdf.

وكما سيتبين لاحقًا في هذا المقال، يوفر القانون الدولي الإنساني حماية شاملة لقطاع الرعاية الصحية في النزاع المسلح، ويحظر الهجمات على البنية التحتية المدنية، ما لم تتحول هذه البنية التحتية إلى هدف عسكري.

بالنظر إلى ما هو أبعد من تأثير العمليات السيبرانية على بنية تحتية محددة، هناك ثلاث خصائص على الأقل للعمليات السيبرانية تثير المزيد من القلق.[36]

أولًا، ثبت أن عزو المسؤولية عن الهجمات السيبرانية إلى دولة أو جهة فاعلة من غير الدول أمر صعب إن لم يكن مستحيلًا.[37] ويعرقل هذا إمكانية تحديد الجهات الفاعلة التي تنتهك القانون الدولي الإنساني في الفضاء السيبراني وتحميلها المسؤولية، وهي إحدى سبل كفالة الامتثال للقانون الدولي الإنساني. وقد تؤدي سياسة إنكار الهجمات السيبرانية، والأمل في عدم الكشف عنها أيضًا إلى تغيير الحسابات السياسية المستخدمة في تنفيذ هذه الهجمات السيبرانية - وفي تنفيذها على نحو ينتهك القانون الدولي.

ثانيًا، كما أشارت الصين، على سبيل المثال، "فإن انتشار الأدوات والتكنولوجيا السيبرانية الضارة آخذ في الزيادة".[38] وقد تنتشر الأدوات والأساليب السيبرانية في الواقع بطريقة فريدة يصعب السيطرة عليها. واليوم، لا تُنفذ الهجمات السيبرانية المتطورة إلا من قبل الجهات الفاعلة الأكثر تقدمًا والتي تتمتع بأفضل الموارد. وبمجرد استخدام البرامج الضارة أو سرقتها أو تسريبها أو إتاحتها بأي طريقة أخرى، قد تتمكن جهات فاعلة، بخلاف من طوروا البرامج الضارة، من العثور على هذه البرامج على شبكة الإنترنت وإعادة تصميمها واستخدامها لأغراضها الخاصة.

ثالثًا، تنطوي العمليات السيبرانية على خطر المبالغة في رد الفعل من جانب الدول المستهدفة وتصعيد العنف لاحقًا. ويصعب على هدف الهجوم السيبراني عادةً معرفة ما إذا كان المهاجم يهدف إلى التجسس أم التسبب في أضرار مادية أخرى محتملة. ولا يمكن تحديد هدف العملية السيبرانية على وجه اليقين إلا بمجرد تحقيق التأثير أو الهدف النهائي. ومن ثم، هناك خطر يتمثل في أن هدف العملية سيتوقع إحداث أسوأ تأثير وسيرد بطريقة أقوى مما لو كان يعلم أن قصد المهاجم كان يقتصر على التجسس.

وفي وقت كتابة هذا التقرير، لم تكن العمليات السيبرانية قد تسببت في إلحاق أضرار كبيرة بالبشر. إلا أنها أحدثت أضرارًا اقتصادية كبيرة.[39] وبالإشارة إلى التكلفة البشرية المحتملة

36 انظر أيضًا: اللجنة الدولية، القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة، جنيف (تقرير التحديات الصادر عن اللجنة الدولية لعام 2019)، الصفحة 27، متاح من خلال الرابط التالي:
https://shop.icrc.org/international-humanitarian-law-and-the-challenges-of-contemporary-armed-conflicts-recommitting-to-protection-in-armed-conflict-on-the-70th-anniversary-of-the-geneva-conventions-pdf-ar؛

وانظر: Gisel and L. Olejnik (eds)، الحاشية 11 أعلاه، الصفحة 7.

37 للاطلاع على مناقشة أوسع عن عزو المسؤولية، بما في ذلك قواعد القانون الدولي ذات الصلة، انظر: القسم أدناه المعنون "مسألة عزو المسؤولية".

38 Statement by Counsellor Sun Lei of the Chinese Delegation at the Thematic Discussion on Information and Cyber Security at the First Committee of the 72nd Session of the UN General Assembly, 23 October 2017, available at: www.china-un.org/eng/chinaandun/disarmament_armscontrol/unga/t1505683.html.

39 تُقاس التكلفة الإجمالية للجرائم السيبرانية وحدها بتريليونات الدولارات: فقد قُدرت بنحو 3 تريليونات دولار في عام 2015 في جميع أنحاء العالم، ومن المتوقع أن يتضاعف هذا الرقم بحلول عام 2021
(Steve Morgan, "Hackerpocalypse: A Cybercrime Revelation", Herjavec Group, 17 August 2016, available at: www.herjavecgroup.com/hackerpocalypse-cybercrime-report/).

قُدر تأثير برنامج NotPetya بأكثر من مليار دولار، وتصل بعض التقديرات إلى 10 مليارات دولار
(Fred O'Connor, "NotPetya Still Roils Company's Finances, Costing Organizations $1.2 Billion in Revenue", *Cybereason*, 9 November 2017, available at: www.cybereason.com/blog/notpetya-costs-companies-1.2-billion-in-revenue; A. Greenberg,

الحاشية 5 أعلاه). ويتأثر النظام المالي أيضًا في أغلب الأحوال بالهجمات السيبرانية: انظر على سبيل المثال:

للعمليات السيبرانية، نجهل الكثير عن التطور التكنولوجي والقدرات والأدوات التي طورتها الجهات الفاعلة الأكثر تطورًا - ومنها الجهات العسكرية - وقد يختلف مدى إمكانية استخدام العمليات السيبرانية أثناء النزاعات المسلحة عن الاتجاهات التي لوحظت حتى الآن. بمعنى آخر، في حين أن مخاطر التكلفة البشرية لا تبدو مرتفعة للغاية بناءً على الملاحظات الحالية، لا سيما بالنظر إلى الدمار والمعاناة اللذين تسببهما النزاعات دائمًا، فإن تطور العمليات السيبرانية يتطلب اهتمامًا وثيقًا بسبب أوجه عدم اليقين الحالية والوتيرة السريعة للتغيير.

انطباق القانون الدولي الإنساني على العمليات السيبرانية أثناء النزاعات المسلحة

من وجهة نظر قانونية، يعتبر القانون الدولي الإنساني الإطار الأساسي الذي يفرض قيودًا على اللجوء إلى العمليات السيبرانية أثناء النزاع المسلح ويحمي السكان المدنيين من الأضرار المحتملة.

ولا يحتوي القانون الدولي الإنساني ولا مجالات القانون الدولي الأخرى على تعريف للعمليات السيبرانية أو الحرب السيبرانية أو القتال السيبراني. واستخدمت دول معينة تعريفات مختلفة للعمليات السيبرانية في وثائق عسكرية أو غيرها.[40] وتشير دول أخرى بدلًا من ذلك إلى قتال المعلومات أو حرب المعلومات، وتعرف هذا المفهوم بطريقة تشمل على الأقل بعض جوانب ما يُفهم غالبًا على أنه الحرب السيبرانية.[41] وبصرف النظر عن كيفية تعريف الدول والجهات الأخرى للعمليات السيبرانية أو الحرب السيبرانية أو حرب المعلومات، فإن تحديد انطباق أو عدم انطباق القانون الدولي الإنساني على هذه العمليات يجب أن يتم بناءً على طبيعة هذه العمليات وآثارها وظروفها.

وتفهم اللجنة الدولية "العمليات السيبرانية أثناء النزاع المسلح" على أنها تعني العمليات التي تستهدف نظم أو شبكات الكمبيوتر أو جهازًا آخر متصلًا، من خلال تدفق البيانات، عند استخدامها كوسيلة أو أسلوب للحرب في سياق نزاع مسلح.[42]

وبينما يستمر الجدل حول مسألة ما إذا كان القانون الدولي الإنساني ينطبق على العمليات السيبرانية أثناء النزاع المسلح، وبالتالي يقيدها، اتخذت اللجنة الدولية منذ البداية موقفًا واضحًا وإيجابيًا.[43] وترى اللجنة الدولية أنه ليس ثمة شك في أن القانون الدولي الإنساني ينظم العمليات السيبرانية أثناء النزاعات المسلحة أو الحرب السيبرانية- شأن أي سلاح أو

Choe Sang-Hun, "Computer Networks in South Korea Are Paralyzed in Cyberattacks", *New York Times*, 20 March 2013, available at: www.nytimes.com/201321/03//world/asia/south-korea-computer-network-crashes.html.

40 انظر على سبيل المثال: US Department of Defense, DOD *Dictionary of Military and Associated Terms*.

41 تعرف اتفاقية منظمة شنغهاي للتعاون، الحاشية 17 أعلاه، "حرب المعلومات" على أنها "مواجهة بين دولتين أو أكثر في فضاء المعلومات بهدف الإضرار بنظم المعلومات والعمليات والموارد، والهياكل الحيوية وغيرها، وتقويض النظم السياسية والاقتصادية والاجتماعية، والتلاعب النفسي بجموع السكان من أجل زعزعة استقرار المجتمع والدولة وكذلك إجبار الدولة على اتخاذ قرارات لصالح الطرف المعادي". وتُعرّف القوات المسلحة للاتحاد الروسي حرب المعلومات بالطريقة نفسها، مشيرة إلى أن "القوات المسلحة للاتحاد الروسي تتبع ... القانون الإنساني الدولي" أثناء الأنشطة العسكرية في فضاء المعلومات العالمي (وزارة دفاع الاتحاد الروسي، مفهوم أنشطة القوات المسلحة التابعة للاتحاد الروسي في فضاء المعلومات، 2011، القسم 1-2، متاح من خلال الرابط التالي: https://eng.mil.ru/en/science/publications/more.htm?id=10845074@cmsArticle).

42 انظر: اللجنة الدولية، الحاشية 1 أعلاه.

43 انظر: اللجنة الدولية، القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة، جنيف، 2011 (تقرير التحديات لعام 2011 الصادر عن اللجنة الدولية)، الصفحات 36-39، متاح من خلال الرابط التالي:
https://www.icrc.org/ar/document/international-humanitarian-law-and-challenges-contemporary-armed-conflicts

وانظر: K. Dörmann، الحاشية 12 أعلاه.

أساليب ووسائل القتال التي يلجأ إليها أي طرف من الأطراف المتحاربة في النزاع، سواء كانت قديمة أو حديثة. واعتماد العمليات السيبرانية على تقنية جديدة ومتطورة باستمرار لا يحول دون تطبيق القانون الدولي الإنساني على استخدام هذه التقنيات باعتبارها من وسائل أو أساليب القتال. ويصح ذلك سواء كان الفضاء السيبراني يعتبر ميدانًا جديدًا للحرب على غرار الجو والأرض والبحر والفضاء الخارجي، أو يعتبر نوعًا مختلفًا من الميادين لأنه من صنع الإنسان في حين أن الأول طبيعي؛ أو لا يعتبر ميدانًا على هذا النحو.

ونرى أن هناك تأييدًا قويًا لهذا الرأي في معاهدات القانون الدولي الإنساني، وفي الاجتهاد القضائي لمحكمة العدل الدولية، وفي الآراء التي أعرب عنها عدد من الدول والمنظمات الدولية.

والهدف والغرض من القانون الدولي الإنساني هو تنظيم النزاعات المقبلة، أي التي تقع بعد اعتماد معاهدة من معاهدات القانون الدولي الإنساني. وأدرجت الدول، لدى اعتماد معاهدات القانون الدولي الإنساني، القواعد التي تستشرف تطوير وسائل وأساليب جديدة للحرب وافترضت أن القانون الدولي الإنساني سينطبق عليها. ففي عام 1868، كان إعلان سان بيترسبرغ يهدف إلى الحفاظ على المبادئ التي وضعها بشأن "التحسينات المقبلة التي قد يدخلها العلم علي تسليح الجيوش".[44] ويمكن الاطلاع على قاعدة مهمة وحديثة من قواعد القانون الدولي الإنساني في هذا الصدد في المادة 36 من البروتوكول الإضافي الأول لعام 1977 (البروتوكول الإضافي الأول)،[45] التي تنص على ما يلي:

> 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 محظورًا في جميع الأحوال أو في بعضها بمقتضى هذا البروتوكول أو أية قاعدة أخرى من قواعد القانون الدولي التي يلتزم بها الطرف السامي المتعاقد.

ولا شك في أن هذا الالتزام يستند إلى افتراض مفاده أن القانون الدولي الإنساني ينطبق على هذه الأسلحة والوسائل والأساليب الجديدة، وإلا فلن يكون من الضروري استعراض مشروعيتها بموجب أحكام القانون الحالية. وهذا يشمل الأسلحة ووسائل وأساليب القتال التي تعتمد على التكنولوجيا السيبرانية.

والاستنتاج القائل بأن القانون الدولي الإنساني ينطبق على العمليات السيبرانية أثناء النزاع المسلح يلقى مزيدًا من التأييد في الآراء التي أعربت عنها محكمة العدل الدولية. فقد ذكرت المحكمة، في فتواها بشأن مشروعية التهديد بالأسلحة النووية أو استخدامها، أن مبادئ القانون الدولي الإنساني وقواعده المستقرة المنطبقة في النزاع المسلح "تنطبق على كافة أشكال الحروب وعلى كافة أنواع الأسلحة، بما فيها "ما سيكون في المستقبل".[46] ونشير مرة أخرى إلى أن هذا يشمل العمليات السيبرانية. وهذا الرأي معترف به أيضًا على نطاق واسع بين الخبراء.[47]

44 إعلان سان بيترسبرغ بغية حظر استعمال قذائف معينة، في زمن الحرب، سان بيترسبرغ، 29 تشرين الثاني/نوفمبر/ 11 كانون الأول/ديسمبر 1868.

45 البروتوكول الإضافي (الأول) لاتفاقيات جنيف المؤرخة 12 آب/أغسطس 1949، والمتعلق بحماية ضحايا المنازعات الدولية المسلحة، 3 UNTS 1125، 8 حزيران/يونيو 1977 (دخل حيز النفاذ في 7 كانون الأول/ديسمبر 1978).

46 محكمة العدل الدولية، مشروعية التهديد بالأسلحة النووية أو استخدامها، فتوى، 8 تموز/يوليو 1996، الفقرة 86.

47 انظر: دليل تالين 2، الحاشية 13 أعلاه، القاعدة 80؛ وبيان أكسفورد، الحاشية 32 أعلاه، النقطة 5. انظر أيضًا: مقال Zhixiong Huang و Yaohui

وهناك إقرار متزايد بين الدول بأن القانون الدولي الإنساني ينطبق على العمليات السيبرانية أثناء النزاعات المسلحة ومن ثم يقيدها. وكما ذكرنا آنفًا، خلص الخبراء في تقريري عامي 2013 و 2015 لفريق الخبراء الحكوميين التابع للأمم المتحدة، إلى أن "أحكام القانون الدولي، ولا سيما ميثاق الأمم المتحدة، قابلة للتطبيق" في بيئة تكنولوجيا المعلومات والاتصالات،[48] وهو استنتاج رحبت به الجمعية العامة للأمم المتحدة في بداية الأمر[49] ثم أكدته.[50] وأشار تقرير عام 2015 أيضًا إلى "المبادئ القانونية الدولية المعمول بها، بما في ذلك، حسب الاقتضاء، مبادئ الإنسانية والضرورة والتناسب والتمييز".[51] وإن كانت هذه القائمة من المبادئ لا تذكر القانون الدولي الإنساني صراحة، فقد أشار الخبراء إلى أن هذه المبادئ هي "المبادئ الأساسية للقانون الدولي الإنساني".[52]

ووفقًا لهذا الاستنتاج، أكد عدد متزايد من الدول والمنظمات الدولية علانية أن القانون الدولي الإنساني ينطبق على العمليات السيبرانية أثناء النزاع المسلح. ويشمل هذا على سبيل المثال الاتحاد الأوروبي[53] والناتو.[54] علاوة على ذلك، أعاد نداء باريس للثقة والأمن في الفضاء السيبراني (أيدته 78 دولة في نيسان/أبريل 2020) التأكيد على انطباق القانون الدولي الإنساني على العمليات السيبرانية أثناء النزاعات المسلحة؛[55] وأعلن رؤساء حكومات دول الكومنولث البالغ عددها 54 دولة "الالتزام بالمضي قدمًا في المناقشات حول كيف ... يطبق في الفضاء السيبراني القانون الدولي الإنساني المنطبق من جميع جوانبه"؛[56] وقد كشفت ردود الدول على دراسة أجرتها اللجنة القانونية التابعة لمنظمة الدول الأمريكية "تأييد انطباق القانون الدولي الإنساني "في الفضاء السيبراني.[57]

Ying في هذا العدد من المجلة؛ وانظر ما شينمين، نائب المدير العام لإدارة المعاهدات والقانون بوزارة الخارجية في جمهورية الصين الشعبية آنذاك، حيث كتب بصفته الشخصية ما يلي: "اتسع نطاق انطباق قواعد القانون الدولي الإنساني ... واتسع مداه أيضًا ليشمل الفضاء السيبراني. أكد فريق الخبراء الحكوميين التابع للأمم المتحدة المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي في تقريريه لعامي 2013 و2015 أن أحكام القانون الدولي، ولا سيما ميثاق الأمم المتحدة، قابلة للتطبيق في الفضاء السيبراني. لذلك، يُفترض أن يكون القانون الدولي الإنساني قابلًا للتطبيق من حيث المبدأ على الهجمات السيبرانية، لكن كيفية تطبيقه لا تزال مفتوحة للنقاش "(ترجمة غير رسمية).
Ma Xinmin, "International Humanitarian Law in Flux: Development and New Agendas - In Commemoration of the 40th Anniversary of the 1977 Adoption Protocols to the Geneva Conventions", *Chinese Review of International Law*, Vol. 30, No. 4, 2017, p. 8.

48 الجمعية العامة للأمم المتحدة، "فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي: مذكرة من الأمين العام"، وثيقة الأمم المتحدة A/68/98، 24 حزيران/يونيو 2013، الفقرة 19، ووثيقة الأمم المتحدة A/70/174، 22 تموز/يوليو 2015، الفقرة 24.

49 قرار الجمعية العامة للأمم المتحدة 237/70، "التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي"، وثيقة الأمم المتحدة A/RES/70/237، 03 كانون الأول/ديسمبر 2015، الفقرة 16 من الديباجة.

50 قرار الجمعية العامة للأمم المتحدة 73/27، الحاشية 15 أعلاه، الفقرة 17 من الديباجة؛ وقرار الجمعية العامة للأمم المتحدة 266/73، الحاشية 15 أعلاه، الفقرة 12 من الديباجة.

51 وثيقة الأمم المتحدةA/70/174 ، الحاشية 48 أعلاه، الفقرة 28 (د).

52 Michael N. Schmitt, "France Speaks Out on IHL and Cyber Operations: Part I", *EJIL: Talk!*, 30 September 2019, available at: www.ejiltalk.org/france-speaks-out-on-ihl-and-cyber-operations-part-i/.

53 استنتاجات مجلس الاتحاد الأوروبي، الحاشية 20 أعلاه.

54 إعلان قمة ويلز، الحاشية 21 أعلاه، الفقرة 72.

55 انظر:
"Cybersecurity: Paris Call of 12 November 2018 for Trust and Security in Cyberspace", *France Diplomacy*, available at: www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in.

56 إعلان الكومنولث بشأن العمليات السيبرانية، الحاشية 19 أعلاه، الصفحة 4، الفقرة 4.

57 انظر: منظمة الدول الأمريكية، الحاشية 22 أعلاه، الفقرة 43 (التي تشير إلى بوليفيا، وبيرو، وشيلي، وغيانا، والولايات المتحدة)؛ وتضمنت استجابة الإكوادور على ما يبدو مثل هذا الدعم (انظر أيضًا: الفقرات 19-21، و25). وأعربت دول أعضاء أخرى في منظمة الدول الأمريكية عن هذا الموقف في سياق الفريق العامل المفتوح العضوية. انظر: التعليقات التي قدمتها أوروغواي، والبرازيل، وكولومبيا على المسودة الأولية لتقرير الفريق العامل المفتوح

في الوقت نفسه، وفي سياق المناقشات حول انطباق القانون الدولي الإنساني على العمليات السيبرانية أثناء النزاع المسلح، أعرب عدد من الدول عن معارضتها لعسكرة الفضاء السيبراني أو سباق التسلح السيبراني. كذلك أعربت الدول عن مخاوفها بشأن إمكانية شرعنة استخدام العمليات العسكرية السيبرانية،[58] ودعت إلى توخي الحيطة في مناقشة انطباق القانون الدولي الإنساني،[59] وأشارت إلى أن القانون الدولي الإنساني "يجب أن يُطبق مع مراعاة خصوصيات الحرب السيبرانية".[60] وهذه اعتبارات مهمة، لكن لا ينبغي أن تُفهم على أنها متعارضة مع تطبيق القانون الدولي الإنساني على العمليات السيبرانية أثناء النزاع المسلح.

نرى من ناحية أخرى أن التأكيد على أن القانون الدولي الإنساني ينطبق على العمليات السيبرانية أثناء النزاع المسلح لا يشجع على عسكرة الفضاء السيبراني ولا ينبغي، بأي حال من الأحوال، أن يُفهم على أنه يضفي الشرعية على الحرب السيبرانية.[61] أي لجوء من جانب الدول إلى القوة، سواء كان ذو طابع سيبراني أو حركي، يظل دائمًا خاضعًا لميثاق الأمم المتحدة والقانون الدولي العرفي، ولا سيما حظر استخدام القوة.[62] يجب تسوية المنازعات الدولية بالطرق السلمية. وينطبق هذا المبدأ في الفضاء السيبراني كما ينطبق في جميع المجالات الأخرى. وبالإضافة إلى

العضوية، متاحة من خلال الرابط التالي: www.un.org/disarmament/open-ended-working-group/.

انظر من ناحية أخرى: وجهات نظر فنزويلا وكوبا ونيكاراغوا، التي أشارت إلى أمور منها عدم وجود توافق في الآراء حتى الآن بشأن انطباق القانون الدولي الإنساني في الفضاء السيبراني وأن الإشارة المباشرة إلى القانون الدولي الإنساني في التقرير قد تضفي الشرعية على عسكرة الفضاء السيبراني.

58 انظر: التعليقات التي قدمتها مؤخرًا إيران، والصين، وكوبا، ونيكاراغوا وغيرها في المسودة الأولية لتقرير الفريق العامل المفتوح العضوية، متاحة من خلال الرابط التالي: www.un.org/disarmament/open-ended-working-group/.

انظر أيضًا، على سبيل المثال:

People's Republic of China, *Position Paper of the People's Republic of China for the 73rd Session of the United Nations General Assembly*, 2018, p. 10, available at: https://tinyurl.com/y4qquywp; "Declaration by Miguel Rodríguez, Representative of Cuba, at the Final Session of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", 23 June 2017, p. 2; Ministry of Foreign Affairs of the Russian Federation, "Response of the Special Representative of the President of the Russian Federation for International Cooperation on Information Security Andrey Krutskikh to TASS' Question Concerning the State of International Dialogue in This Sphere", 29 June 2017.

59 "يجب توخي الحيطة في التعامل مع انطباق قانون النزاعات المسلحة وقانون مسوغات الحرب. ولا ينبغي الاعتراف بشرعية الحرب السيبرانية تحت أي ظرف من الظروف. ولا ينبغي للدول أن تحول الفضاء السيبراني إلى ساحة قتال جديدة":

"China's Submissions to the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security", September 2019, p. 6, available at: https://s3.amazonaws.com/unoda-web/wp-content/uploads/201909//china-submissions-oewg-en.pdf.

"ينبغي أن نتوخى الحذر الشديد إزاء أي محاولة لإدخال استخدام القوة بأي شكل من الأشكال في الفضاء السيبراني، وإجراء تقييم دقيق للنزاعات والمواجهات المحتملة الناتجة عن التطبيق العشوائي لقانون النزاعات المسلحة في الفضاء السيبراني والامتناع عن توجيه رسائل خاطئة إلى العالم":

"China's Contribution to the Initial Pre-Draft of OEWG Report", April 2020, p. 5, available at: https://front.un-arm.org/wp-content/uploads/202004//china-contribution-to-oewg-pre-draft-report-final.pdf.

"في ظل غياب ممارسة الدول، ينبغي لنا أن نتوخى الحذر الشديد بشأن مناقشة تطبيق القانون الإنساني على ما يسمى 'الحروب السيبرانية'. والسبب بسيط للغاية ولكنه أساسي: أولًا، لا ينبغي السماح بأي حروب سيبرانية؛ وثانيًا، ستكون الحرب السيبرانية شكلًا جديدًا تمامًا من أشكال حرب التكنولوجيا المتقدمة":

China statement at AALCO 58th Annual Session, in AALCO, *Verbatim Record of Discussions: Fifty-Eighth Annual Session*, Doc No. AALCO/58/ DAR ES SALAAM/2019/VR, 2019, p. 176, available at: www.aalco.int/Verbatim%20(FINAL)%2020200311.pdf.

60 أفادت الصين في اجتماع للفريق العامل التابع للمنظمة الاستشارية القانونية الآسيوية الأفريقية المعني بالقانون الدولي في الفضاء السيبراني أن "نظامي قانون الحرب وقانون مسوغات الحرب يجب أن يُطبقا مع مراعاة خصوصيات الحرب السيبرانية".

AALCO, *Summary Report of the Fourth Meeting of the Open-Ended Working Group on International Law in Cyberspace*, 3 September 2019, available at: www.aalco.int/Summary%20Report%20as%20Adopted.pdf.

61 أُعرب عن هذا الرأي في مجموعة من الوثائق ومنها الإفادات المقدمة من أستراليا، والبرازيل، والدانمرك، وشيلي، والمملكة المتحدة في المسودة الأولية لتقرير الفريق العامل المفتوح العضوية، متاحة من خلال الرابط التالي: www.un.org/disarmament/open-ended-working-group/.

62 ميثاق الأمم المتحدة، المادة 2 (4).

مقتضيات ميثاق الأمم المتحدة- وكذلك بمعزل عنها - يوفر القانون الدولي الإنساني قيودًا على سير الأعمال العدائية متى قررت الدول أو الأطراف من غير الدول اللجوء إلى العمليات السيبرانية أثناء النزاع المسلح. وعلى وجه الخصوص، يحمي القانون الدولي الإنساني المدنيين والأعيان المدنية من آثار الأعمال العدائية من خلال تقييد اختيار المتحاربين لوسائل وأساليب القتال، بغض النظر عن مشروعيةٍ أو عدم مشروعية استخدام القوة. وهذا يعني أن القانون الدولي الإنساني-قانون الحرب- بدلًا من إضفاء الشرعية على العمليات السيبرانية (أو أي عملية عسكرية أخرى) أثناء النزاع المسلح، فإنه يفرض قيودًا بالإضافة إلى القيود المنصوص عليها في ميثاق الأمم المتحدة والقانون الدولي العرفي - قانون مسوغات الحرب. علاوة على ذلك، يفرض القانون الدولي الإنساني في الواقع بعض القيود على عسكرة الفضاء السيبراني. فهو يحظر على سبيل المثال تطوير قدرات سيبرانية يمكن اعتبارها أسلحة وتكون عشوائية بطبيعتها أو من شأنها أن تسبب إصابات غير مبررة أو معاناة غير ضرورية.[63]

إذا قبلنا فكرة أن القانون الدولي الإنساني ينطبق على العمليات السيبرانية أثناء النزاعات المسلحة عمومًا، فإن السؤال التالي هو هل تنطبق جميع قواعد القانون الدولي الإنساني أم بعضها فقط. وفي هذا الصدد، يمكن تقسيم نطاق تطبيق قواعد القانون الدولي الإنساني التي تنظم وسائل وأساليب القتال إلى قواعد تنطبق على جميع الأسلحة ووسائل وأساليب القتال، أينما استخدمت (مثل مبادئ التمييز والتناسب والاحتياط)، والقواعد الخاصة بأسلحة معينة (مثل معاهدات الأسلحة)، أو مجالات معينة (مثل القواعد التي تنظم الحرب البحرية تحديدًا). وتنتمي جميع المبادئ والقواعد العرفية الرئيسية التي تنظم سير الأعمال العدائية إلى الفئة الأولى وتنطبق بالفعل على العمليات السيبرانية أثناء النزاع المسلح.[64] ومن ناحية أخرى، يلزم إجراء تحليل أكثر تفصيلًا بشأن انطباق قواعد القانون الدولي الإنساني المتعلقة تحديدًا بأسلحة معينة أو مجالات معينة.

وانطباق القانون الدولي الإنساني لا يمنع الدول من مواصلة تطوير القانون الدولي، أو الاتفاق على قواعد طوعية، أو العمل على وضع تفسيرات مشتركة للقواعد الحالية. فعلى سبيل المثال، عندما أنشئ الفريق العامل المفتوح العضوية التابع للأمم المتحدة في عام 2018، فإن معظم الدول في الجمعية العامة للأمم المتحدة "رحبت بمجموعة القواعد والمعايير والمبادئ الدولية للسلوك المسؤول للدول" التي تستند إلى المعايير التي وضعتها على مر السنين أفرقة الخبراء الحكوميين التابعة للأمم المتحدة.[65] وثمة مثال آخر على قواعد جديدة محتملة في ميدان أمن المعلومات ورد في مدونة قواعد السلوك الدولية لأمن المعلومات التي قدمتها الدول الأعضاء في منظمة شنغهاي للتعاون في عام 2011 إلى الأمم المتحدة. وبموجب المدونة، تتعهد الدول، بجملة أمور منها، "عدم نشر أسلحة المعلومات والتكنولوجيات ذات الصلة".[66] وهناك

63 انظر: جون-ماري هنكرتس ولويز دوزوالد-بك، القانون الدولي الإنساني العرفي، المجلد الأول: القواعد، القاهرة، 2007 (دراسة اللجنة الدولية للقانون العرفي)، القاعدتان 70 و 71، متاح من خلال الرابط التالي: https://ihl-databases.icrc.org/customary-ihl/ara/docs/v1_rul.

64 يُسلط مزيد من الضوء أدناه على المبادئ والقواعد التي تنظم سير الأعمال العدائية، تحت القسم المعنون "القيود التي يفرضها القانون الدولي الإنساني على استخدام القدرات السيبرانية أثناء النزاعات المسلحة".

65 قرار الجمعية العامة للأمم المتحدة 27/73، الحاشية 15 أعلاه.

66 المدونة المقترحة لقواعد السلوك الدولية لأمن المعلومات متاحة من خلال الرابط التالي:
http://nz.chineseembassy.org/eng/zgyw/t858978.html.
وقد قدمته أوزبكستان، وروسيا، والصين، وطاجيكستان في عام 2011 وانضم إلى قائمة مقدميه كل من كازاخستان وقيرغيزستان في عام 2013 (انظر:

أيضًا اقتراحات أكاديمية، منها ما يتعلق بزيادة القيود القانونية أو السياساتية على العمليات السيبرانية أثناء النزاعات المسلحة.[67]

وخلاصة القول، رغم وجود أسباب قانونية مقنعة وتزايد التأييد الدولي للاستنتاج الذي يذهب إلى أن القانون الدولي الإنساني ينطبق على العمليات السيبرانية أثناء النزاع المسلح، فإن المسألة لا تحظى باتفاق عالمي بعد. ومن ناحية أخرى، كما تبين في هذا القسم، فإن الفحص الدقيق لمختلف الحجج التي أثيرت في المناقشات المتعددة الأطراف يُظهر أن تأكيد انطباق القانون الدولي الإنساني لا يضفي الشرعية على عسكرة الفضاء السيبراني أو اللجوء إلى العمليات السيبرانية الضارة. وهو، علاوة على ذلك، لا يحول دون وضع قواعد جديدة محتملة، بل يوفر إطارًا قانونيًا أساسيًا يمكن للقواعد الجديدة المحتملة الاستناد إليه - بل وينبغي لها ذلك.

هل يمكن للعمليات السيبرانية أن تتجاوز وحدها "الحد"؟ توضيح الفرق بين الحدود ذات الصلة بموجب القانون الدولي الإنساني وميثاق الأمم المتحدة

في ضوء العمليات السيبرانية المتعددة التي يتم الإبلاغ عنها يوميًا، من المهم أن نتذكر أن القانون الدولي الإنساني ينطبق فقط على العمليات السيبرانية التي تشكل جزءًا من نزاع مسلح يُشن باستخدام أسلحة تقليدية أو، على الأرجح، العمليات السيبرانية التي تصل في حد ذاتها إلى مستوى النزاع المسلح في ظل غياب العمليات الحركية. وكما أكد القسم السابق، يجب تحليل مسألة انطباق أو عدم انطباق القانون الدولي الإنساني على العمليات السيبرانية أثناء النزاعات المسلحة بعيدًا عن مسألة وجود أو عدم وجود انتهاك للقواعد التي تحكم استخدام القوة بموجب ميثاق الأمم المتحدة. وفي سياق تطبيق القانون الدولي الإنساني وميثاق الأمم المتحدة، تتمثل المسألة الرئيسية في عزو المسؤولية عن العمليات السيبرانية إلى الدول. ويتناول هذا القسم النقاط الثلاث المذكورة وهي تحديد العمليات السيبرانية التي تخضع للقانون الدولي الإنساني،[68] والعلاقة بين القانون الدولي الإنساني وميثاق الأمم المتحدة، والمسائل المتعلقة بعزو المسؤولية.

وثيقة الأمم المتحدة A/68/98، الحاشية 48 أعلاه، الصفحة 9، الفقرة 18). وكذلك، قدمت وزارة خارجية الاتحاد الروسي في عام 2011 مشروع اتفاقية بشأن أمن المعلومات الدولي (22 أيلول/سبتمبر 2011، متاح من خلال الرابط التالي:
www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666)

يدرج من بين "التدابير الرئيسية لتجنب النزاع العسكري في فضاء المعلومات" أن تقوم الدول "باتخاذ إجراءات تهدف إلى الحد من انتشار 'أسلحة المعلومات' والتكنولوجيا اللازمة لإنشائها" (المادة 6 (10)). وتنص المادة 7 (2) أيضًا على أنه "في أي نزاع دولي، فإن حق الدول الأطراف المشاركة في النزاع في اختيار وسائل 'حرب المعلومات' مقيد بمعايير القانون الإنساني الدولي المنطبقة".

67 أشار العديد من الكتّاب ومنهم باسكوتشي (Pascucci)، على سبيل المثال، إلى أن التفاوض بشأن بروتوكول رابع إضافي قد يُمكّن من معالجة بعض المسائل التي يثيرها تطبيق مبدأ التمييز ومبدأ التناسب في الفضاء السيبراني:
Peter Pascucci, "Distinction and Proportionality in Cyberwar: Virtual Problems with a Real Solution", *Minnesota Journal of International Law*, Vol. 26, No. 2, 2017.

وقدم شميت (Schmitt)، في الوقت نفسه، مقترحات بشأن سياسات قد تعتمدها الدول:
Michael N. Schmitt, "Wired Warfare 3.0: Protecting the Civilian Population during Cyber Operations", *International Review of the Red Cross*, Vol. 101, No. 910, 2019, pp 333-355.

68 للاطلاع على توضيح لهذه المناقشات، انظر:
"Scenario 13: Cyber Operations as a Trigger of the Law of Armed Conflict", in Kubo Mačák, Tomáš Minárik and Taťána Jančárková (eds), *Cyber Law Toolkit*, available at: https://cyberlaw.ccdcoe.org/.

العمليات السيبرانية التي تخضع للقانون الدولي الإنساني

عندما تنفذ العمليات السيبرانية في سياق نزاع مسلح دولي أو غير دولي قائم يُنفذ من خلال وسائل حركية وتكون العمليات متصلة بهذا النزاع، فإن قواعد القانون الدولي الإنساني ذات الصلة تنطبق على جميع أطراف النزاع وتنظم سلوكهم.[69] والعمليات السيبرانية التي تُنفذ إلى جانب العمليات الحركية وتدعمها أثناء النزاعات المسلحة هي النوع الوحيد من العمليات التي اعترفت به الدول واعتبرتها خاضعة للقانون الدولي الإنساني.[70]

ثمة سؤال منفصل يتعلق بما إذا كانت العمليات السيبرانية وحدها - في ظل غياب العمليات الحركية - يمكن أن تخضع للقانون الدولي الإنساني. بعبارة أخرى، هل يمكن أن تكون العملية السيبرانية هي الطلقة الأولى، وربما الوحيدة، في نزاع مسلح على النحو المحدد في القانون الدولي الإنساني؟ تُقيم هذه المسألة حسب المادتين 2 و3 المشتركتين بين اتفاقيات جنيف الأربع لعام 1949 [71] الخاصتين بالنزاعات المسلحة الدولية وغير الدولية على الترتيب.[72] يختلف هذان النوعان من النزاعات المسلحة في طبيعة الأطراف المشاركة فيها، وشدة العنف الذي يؤدي إلى انطباق القانون الدولي الإنساني، وبعض قواعد القانون الدولي الإنساني التي تنطبق.

بالإشارة إلى النزاعات المسلحة الدولية، تنص المادة 2 على ما يلي: "تنطبق هذه الاتفاقية في حالة الحرب المعلنة أو أي اشتباك مسلح آخر ينشب بين طرفين أو أكثر من الأطراف السامية المتعاقدة، حتى لو لم يعترف أحدها بحالة الحرب". ومن المتفق عليه اليوم أنه "يقوم نزاع مسلح كلما تم اللجوء إلى القوة المسلحة بين الدول".[73] وفيما يتعلق بمسألة وجود أو عدم وجود حد للشدة في سياق النزاعات المسلحة الدولية، تشير بعض ممارسات الدول، وبعض الحجج الإنسانية والنظرية القوية إلى أن القانون الدولي الإنساني ينطبق بمجرد اللجوء إلى القوة المسلحة بين الدول، بغض النظر عن شدة العنف. يُعنى القانون الدولي الإنساني في المقام الأول بحماية الأشخاص المتضررين من النزاعات المسلحة. وهكذا، يتعين على الدول، بمجرد اللجوء إلى القوة المسلحة، أن توجه هجماتها نحو الأهداف العسكرية وليس إلى المدنيين أو الأعيان المدنية، ويجب أن تتوخى الحذر باستمرار لتجنب إصابة الفئة الأخيرة. ولا يهم ما إذا كان هناك مدني واحد أو أكثر يحتاجون إلى الحماية من الهجوم.[74] وينطبق القانون الدولي الإنساني على الأقل في

69 انظر: التعليق على اتفاقية جنيف الأولى: الاتفاقية الأولى لتحسين حال الجرحى والمرضى بالقوات المسلحة في الميدان، الطبعة الثانية، جنيف، 2016 (تعليق اللجنة الدولية على اتفاقية جنيف الأولى)، الفقرة 254؛ وانظر: دليل تالين 2، الحاشية 13 أعلاه، القاعدة 80.

70 انظر: المراجع الواردة في الحاشية 2 أعلاه.

71 اتفاقية جنيف الأولى لتحسين حال الجرحى والمرضى بالقوات المسلحة في الميدان، المؤرخة 12 آب/أغسطس 1949، 75 UNTS 31 (دخلت حيز النفاذ في 21 تشرين الأول/أكتوبر 1950) (اتفاقية جنيف الأولى)؛ واتفاقية جنيف الثانية لتحسين حال جرحى ومرضى وغرقى القوات المسلحة في البحار، المؤرخة 12 آب/أغسطس 1949، 75 UNTS 85 (دخلت حيز النفاذ في 21 تشرين الأول/أكتوبر 1950) (اتفاقية جنيف الثانية)؛ واتفاقية جنيف الثالثة بشأن معاملة أسرى الحرب، المؤرخة 12 آب/أغسطس 1949، 75 UNTS 135 (دخلت حيز النفاذ في 21 تشرين الأول/أكتوبر 1950) (اتفاقية جنيف الثالثة)؛ واتفاقية جنيف الرابعة بشأن حماية الأشخاص المدنيين في وقت الحرب، المؤرخة 12 آب/أغسطس 1949، 75 UNTS 287 (دخلت حيز النفاذ في 21 تشرين الأول/أكتوبر 1950) (اتفاقية جنيف الرابعة).

72 المادة 2 (1) المشتركة: "تنطبق هذه الاتفاقية في حالة الحرب المعلنة أو أي اشتباك مسلح آخر ينشب بين طرفين أو أكثر من الأطراف السامية المتعاقدة، حتى لو لم يعترف أحدها بحالة الحرب". المادة 3 (1) المشتركة: "في حالة قيام نزاع مسلح ليس له طابع دولي في أراضي أحد الأطراف السامية المتعاقدة..."

73 International Criminal Tribunal for the former Yugoslavia (ICTY), *The Prosecutor v. Duško Tadić*, Case No. IT-94-1, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, 2 October 1995, para. 70;

وتعليق اللجنة الدولية على اتفاقية جنيف الأولى، الحاشية 69 أعلاه، الفقرة 218.

74 بالمثل، إذا أدى اللجوء إلى القوة المسلحة، على سبيل المثال، إلى وقوع إصابات أو أسر أحد أفراد القوات المسلحة التابعة لدولة أخرى، فإن قواعد القانون الدولي الإنساني المتعلقة بحماية الجرحى والمرضى أو وضع أسرى الحرب ومعاملتهم يعتد بها سواء كان هناك أسير واحد أو العديد من الأسرى

الحالات التي يؤدي فيها استخدام العمليات السيبرانية بين الدول إلى تأثيرات مشابهة للتأثيرات التي تخلفها وسائل وأساليب الحرب التقليدية.

يتفق الخبراء عمومًا على أن العمليات السيبرانية، في حد ذاتها، لها القدرة على تجاوز حد النزاع المسلح الدولي بموجب القانون الدولي الإنساني.[75] وتوافق اللجنة الدولية على هذا الرأي.[76] وفي تعبير نادرٍ عن موقف دولة بشأن هذه المسألة، ذكرت فرنسا أن "العمليات السيبرانية التي تشكل أعمالًا عدائية بين دولتين أو أكثر قد تكون من السمات المميزة لوجود نزاع مسلح دولي".[77]

والمسألة المتعلقة بمكان وجود هذا الحد على وجه التحديد لا تزال غير محسومة.[78] وترى اللجنة الدولية أنه لا يوجد سبب للتعامل مع عملية سيبرانية واحدة أو أكثر تؤدي إلى تدمير الأصول المدنية أو العسكرية، أو إلى وفاة أو إصابة جنود أو مدنيين، معاملة مختلفة عن الهجمات المماثلة التي تُشن من خلال وسائل وأساليب القتال التقليدية. فالعمليات السيبرانية قد تؤدي أيضًا على أية حال إلى تعطيل الأعيان دون إتلافها فعليًا. ويبقى لنا أن نرى ما إذا كانت الدول وتحت أي ظروف قد تعتبر هذه العمليات بمثابة لجوء إلى القوة المسلحة كما هو مفهوم في القانون الدولي الإنساني، ومن ثم يجب أن تخضع لهذا الفرع من فروع القانون.[79]

وبالإشارة إلى النزاعات المسلحة غير الدولية، قد تصل حالات العنف الداخلي إلى حد النزاع المسلح غير الدولي إذا كان هناك "عنف مسلح طويل الأمد بين سلطات حكومية وجماعات مسلحة منظمة أو بين هذه الجماعات المسلحة داخل الدولة".[80] ويطرح المعياران المستمدان من هذا التعريف - تنظيم أطراف النزاع وشدة العنف - أسئلة مختلفة تتعلق بالعمليات السيبرانية. أولًا، بينما تستوفي القوات المسلحة التابعة للدولة معيار التنظيم، فإن تحديد درجة تنظيم جماعة مسلحة هو تقييم أعقد وأكثر ارتباطًا بالحقائق؛ ويزداد الأمر صعوبة - وإن كان البعض يرى أنه ليس مستحيلًا - عندما تكون هذه المجموعة منظمة عن طريق شبكة الإنترنت فقط.[81] ثانيًا، بخلاف أحكام القانون الدولي الإنساني المنطبقة على النزاعات المسلحة الدولية، والتي تحكم أي لجوء إلى القوة المسلحة بين الدول بغض النظر عن شدتها،[82] لن يقوم نزاع مسلح غير دولي إلا إذا كان العنف القائم بين طرفين منظمين أو أكثر شديدًا بالقدر الكافي. مرة

أو كان هناك جريح واحد أو العديد من الجرحى الذين يجب الاعتناء بهم. انظر: تعليق اللجنة الدولية على اتفاقية جنيف الأولى، الحاشية 69 أعلاه، الفقرات 236-244.

75 دليل تالين 2، الحاشية 13 أعلاه، القاعدة 82، الفقرة 16.

76 تعليق اللجنة الدولية على اتفاقية جنيف الأولى، الحاشية 69 أعلاه، الفقرات 253-256.

77 وزارة الجيوش الفرنسية، أحكام القانون الدولي المطبقة على العمليات في الفضاء السيبراني، 2019، الصفحة 12، متاحة من خلال الرابط التالي: www.defense.gouv.fr/content/download/567648977052 7//file/international+law+applied+to+operations+in+cyberspace.pdf.

تنص هذه الوثيقة على أنه "بينما لا يمكن من حيث المبدأ استبعاد النزاع المسلح الذي لا يتكون إلا من أنشطة رقمية، فهو يعتمد على قدرة العمليات السيبرانية الذاتية التشغيل على الوصول إلى حد العنف المطلوب لكي تُصنف على هذا النحو".

78 دليل تالين 2، الحاشية 13 أعلاه، القاعدة 82، الفقرات 11-16؛ وكما يتبين من الفقرتين 12-13، فإن المسألة لم تحسم بعد بالنسبة للعمليات الحركية أيضًا، وهذا الشك سيتخلل النقاش بشأن ما إذا كانت العمليات السيبرانية وحدها يمكن أن تتجاوز حد النزاع المسلح الدولي بخلاف المسائل المحددة المتعلقة بالعمليات السيبرانية.

79 تعليق اللجنة الدولية على اتفاقية جنيف الأولى، الحاشية 69 أعلاه، الفقرة 255؛ ودليل تالين 2، الحاشية 13 أعلاه، القاعدة 82، الفقرة 11.

80 ICTY, *Tadić*، الحاشية 73 أعلاه، الفقرة 70.

81 تعليق اللجنة الدولية على اتفاقية جنيف الأولى، الحاشية 69 أعلاه، الفقرة 437؛ ودليل تالين 2، الحاشية 13 أعلاه، القاعدة 83، الفقرات 13-15. للاطلاع على تحليل متعمق لهذه المسألة، انظر:

Tilman Rodenhäuser, Organizing Rebellion: Non-State Armed Groups under International Humanitarian Law, Human Rights Law, and International Criminal Law, Oxford University Press, Oxford, 2018, pp. 104-108.

82 تعليق اللجنة الدولية على اتفاقية جنيف الأولى، الحاشية 69 أعلاه، الفقرات 236-244.

أخرى، لئن كان البعض يرى أن هذا الأمر ليس مستحيلًا في ظروف استثنائية، فمن غير المرجح أن تفي العمليات السيبرانية وحدها بمتطلبات الشدة التي تحدد وجود نزاع مسلح غير دولي.[83] وبينما أعربت فرنسا عن رأي مفاده أن العمليات السيبرانية الطويلة الأمد قد تشكل من حيث المبدأ وحسب الظروف نزاعًا مسلحًا غير دولي، فقد رأت أن حالة التكنولوجيا تستبعد على ما يبدو هذا الاحتمال في الوقت الراهن.[84]

أكد البعض، وكانوا على صواب في ذلك، على أن قانون النزاع المسلح "لا ينظم العمليات السيبرانية التي تقع خارج نطاق حالة النزاع المسلح".[85] ومع ذلك، توجد آراء متباينة حول ما إذا كان ينبغي تطبيق بعض مبادئه أو كلها، من الناحية السياساتية، على العمليات السيبرانية في جميع الظروف.

وذكرت الولايات المتحدة مؤخرًا أنه "حتى إذا كان قانون الحرب لا ينطبق من الناحية التقنية لأن العملية العسكرية السيبرانية المقترحة لن تحدث في سياق نزاع مسلح، فإن [وزارة الدفاع] مع ذلك تطبق مبادئ قانون الحرب"[86] كما تفعل عمومًا إزاء جميع عملياتها.[87] أما روسيا فحذرت من "محاولات قد تكون خطيرة...لفرض الانطباق الكامل والتلقائي للقانون الدولي الإنساني على بيئة تكنولوجيا المعلومات والاتصالات في وقت السلم".[88]

في حين أنه من المرجح أن تستمر المناقشات السياسية حول هذه المسألة، فلا جدال، من وجهة نظر قانونية، في أن القانون الدولي الإنساني لا ينطبق خارج سياق النزاع المسلح. وصحيح أن بعض قواعد القانون الدولي الإنساني، مثل حماية الأشخاص الذين لا يشاركون في الأعمال العدائية أو كفوا عن المشاركة فيها، والمكرسة في المادة 3 المشتركة، أو الحماية القوية لمرافق الرعاية الصحية أو الأعيان التي لا غنى عنها لبقاء السكان المدنيين، يمكن أن تترك آثارًا إيجابية إذا طبقت في جميع الأوقات. وفي المقابل، قد يكون من الصعب تطبيق قواعد القانون الدولي الإنساني الأخرى خارج سياق النزاع المسلح، ولا سيما القواعد المستمدة من مبدأ التمييز ومبدأ التناسب. فهذه القواعد تستند إلى افتراض مفاده أن الهجمات على الأهداف العسكرية مشروعة بموجب القانون الدولي الإنساني أثناء النزاع المسلح. أما خارج نطاق النزاع المسلح، فلا وجود لمفهوم "الأهداف العسكرية" التي يجوز مهاجمتها بشكل قانوني- بل تحظر الهجمات

83 المرجع نفسه، الفقرة 437. للاطلاع على المزيد من المناقشات، انظر: دليل تالين 2، الحاشية 13 أعلاه، القاعدة 83، الفقرات 7-10؛ وكوردولا دروغيه، "لا تقترب من حدود فضائي الإلكتروني: الحرب الإلكترونية والقانون الدولي الإنساني وحماية المدنيين"، المجلة الدولية للصليب الأحمر، المجلد 94، العدد 886، 2012، الصفحة 553؛ وانظر:
Michael N. Schmitt, "Classification of Cyber Conflict", *Journal of Conflict and Security Law*, Vol. 17, No. 2, 2012, p. 260.

84 وزارة الجيوش الفرنسية، الحاشية 77 أعلاه، الصفحة 12.

85 قوة الدفاع النيوزيلندية، دليل قانون القوات المسلحة، المجلد 4: قانون النزاع المسلح، الطبعة الثانية، 2017، DM 69 (الدليل العسكري لنيوزيلندا)، الفقرة 2-5-23، متاح من خلال الرابط التالي: www.nzdf.mil.nz/assets/Publications/DM-69-2ed-vol4.pdf.

86 Paul C. Ney Jr., US Department of Defence General Counsel, Remarks at US Cyber Command Legal Conference, 2 March 2020, available at: www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/.

87 انظر: وزارة الدفاع الأمريكية، التوجيه 2311.01E، "برنامج وزارة الدفاع لقانون الحرب"، 2006 (عُدل في عام 2011)، الفقرات من 4 إلى 4-1: "سياسة وزارة الدفاع هي أن...أعضاء مكونات وزارة الدفاع يمتثلون لقانون الحرب أثناء جميع النزاعات المسلحة، مهما كان تصنيف هذه النزاعات، وفي جميع العمليات العسكرية الأخرى" (التوكيد مضاف). انظر أيضًا: وزارة الدفاع الأمريكية، دليل قانون الحرب، 2015 (دليل وزارة الدفاع لقانون الحرب)، الفقرة 3-1-1-2، متاح من خلال الرابط التالي: https://tinyurl.com/y6f7chxo.

88 Russia, "Commentary of the Russian Federation on the Initial 'Pre-draft' of the Final Report of the United Nations Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security", April 2020, available at: https://front.un-arm.org/wp-content/uploads/2020/04/russian-commentary-on-oweg-zero-draft-report-eng.pdf.

على القوات المسلحة التابعة لدولة أخرى. وفي حين أن مبدأ التناسب قائم أيضًا خارج نطاق النزاع المسلح، فإن له معنى مميزًا في إطار فروع القانون الأخرى، وبالتالي يطبق بطريقة مختلفة أثناء النزاعات المسلحة وخارج نطاقها.[89] فخارج نطاق النزاع المسلح، تُنظم المنازعات بين الدول واللجوء إلى القوة فقط من خلال فروع أخرى من القانون الدولي، مثل ميثاق الأمم المتحدة وقانون حقوق الإنسان، حسب الاقتضاء.

العلاقة بين القانون الدولي الإنساني وميثاق الأمم المتحدة

يجب على الدولة التي تفكر في تنفيذ عملية سيبرانية ضد دولة أخرى أن تحلل شرعية هذه العملية بموجب إطار قانون مسوغات الحرب (كما هو وارد في ميثاق الأمم المتحدة والقانون الدولي العرفي) وإطار قانون الحرب (القانون الدولي الإنساني). وميثاق الأمم المتحدة والقانون الدولي الإنساني مكملان لبعضهما البعض عندما يتعلق الأمر بحماية البشر من الحرب وآثارها، على الرغم من أنهما مجالان مختلفان من مجالات القانون الدولي. وأهدافهما يكمل بعضها بعضا: فبينما تنص ديباجة ميثاق الأمم المتحدة على أنه يهدف إلى "إنقاذ الأجيال المقبلة من ويلات الحرب"، تنص ديباجة البروتوكول الإضافي الأول على أن هدف القانون الدولي الإنساني هو "حماية ضحايا النزاعات المسلحة". ومن الواضح أن ميثاق الأمم المتحدة يحظر استخدام القوة في غير حالة الدفاع عن النفس أو عندما يأذن بها مجلس الأمن. ولا يحل تطبيق القانون الدولي الإنساني محل القواعد الأساسية لميثاق الأمم المتحدة أو يتجاهلها، ولكن في حالة اندلاع نزاع مسلح، يحدد القانون الدولي الإنساني تدابير الحماية لمن لا يشاركون (المدنيون) في الأعمال العدائية أو كفوا عن المشاركة فيها (على سبيل المثال، الجنود الجرحى أو المحتجزون)، ويقيد اختيار الأطراف المتحاربة لوسائل وأساليب القتال. وهكذا، بينما ينص ميثاق الأمم المتحدة - رهنًا باستثناءات محدودة - على حظر استخدام القوة، يفرض القانون الدولي الإنساني قيودًا على كيفية إدارة الأعمال العدائية بمجرد اندلاع النزاع.

في الوقت نفسه، يشكل القانون الدولي الإنساني وميثاق الأمم المتحدة مجالين مختلفين من مجالات القانون الدولي، ولكل منهما مفاهيمه ومصطلحاته الخاصة. ولما كان كلاهما معني بتنظيم اللجوء إلى القوة، فإن بعض المصطلحات التي يستخدمها كل منهما متشابهة ومربكة في بعض الأحيان. وهذا هو الحال، على سبيل المثال، في سياق مفهوم "اللجوء إلى القوة المسلحة بين الدول" لتصنيف النزاع بموجب القانون الدولي الإنساني، وحظر "التهديد بالقوة أو استخدامها" والحق في الدفاع عن النفس ضد "هجوم مسلح" بموجب ميثاق الأمم المتحدة. وفي حين أن معاهدات القانون الدولي لا تُعرّف هذه المفاهيم - لا بشكل عام ولا في سياق الفضاء السيبراني - يمكن استخلاص بعض العناصر الأساسية من الاجتهادات القضائية والشروح.

وكما تبين آنفًا، ينطبق القانون الدولي الإنساني بمجرد اللجوء إلى القوة المسلحة بين الدول، بغض النظر عن شدة العنف.

لا يُعرّف ميثاق الأمم المتحدة مصطلح "استخدام القوة" بموجب المادة 2 (4)، وتبقى مسألة نوع القوة المؤهلة في هذا الصدد موضع نقاش. وإذا تتبعنا تاريخ صياغة الحكم

89 للاطلاع على تقييم موجز، انظر: تقرير التحديات الصادر عن اللجنة الدولية لعام 2019، الحاشية 36 أعلاه، الصفحات 18-22.

وممارسة الدول اللاحقة، يمكن أن نستنتج أن استخدام الإكراه السياسي أو الاقتصادي غير مدرج في هذا المفهوم.[90] بل يرى البعض أن حظر استخدام القوة بموجب ميثاق الأمم المتحدة "يقتصر على القوة المسلحة".[91] ومن المهم الإشارة فيما يتعلق بالعمليات السيبرانية إلى أن محكمة العدل الدولية ذكرت أن المادة 2 (4) تحظر "أي استعمال للقوة بصرف النظر عن الأسلحة المستخدمة".[92] وبناءً على هذ الاستنتاج، أكدت بعض الدول أن "تجاوز حد استخدام القوة لا يتوقف على الوسائل الرقمية المستخدمة ولكن على آثار العملية السيبرانية"، وخلصت بذلك إلى أن "العملية السيبرانية التي تنفذها دولة ضد أخرى تنتهك حظر استخدام القوة إذا كانت آثارها مماثلة للآثار الناجمة عن استخدام الأسلحة التقليدية".[93] ويعكس عدد من الأمثلة التي ساقتها الدول على استخدام القوة في الفضاء السيبراني على ما يبدو هذا الفهم، مثل العمليات السيبرانية التي تتسبب في إصابة الأشخاص أو موتهم أو إلحاق الضرر بالممتلكات أو تدميرها؛[94] والتسبب في انهيار محطة نووية؛ وفتح سد فوق منطقة مأهولة، الأمر الذي يؤدي إلى الدمار؛ وتعطيل خدمات مراقبة الحركة الجوية، الأمر الذي يؤدي إلى حوادث الطائرات؛ وإعاقة الأنظمة اللوجستية للقوات المسلحة.[95] وتفسر بعض الدول على ما يبدو الحظر المفروض على استخدام القوة على نطاق أوسع، مشيرة إلى أنه لا يمكن استبعاد أن "توصف عملية سيبرانية لا تخلف آثارًا مادية أيضًا بأنها استخدام للقوة"،[96] أو أن "عملية سيبرانية لها أثر مالي أو اقتصادي خطير للغاية قد توصف بأنها استخدام للقوة".[97]

بالانتقال إلى الحق في الدفاع عن النفس بموجب ميثاق الأمم المتحدة والقانون الدولي العرفي، لا يجوز ممارسة هذا الحق إلا لصد "هجوم مسلح". وعقب الاستنتاج الذي خلصت

90 انظر:
Oliver Dörr and Albrecht Randelzhofer, "Article 2(4)", in Bruno Simma *et al.* (eds), *The Charter of the United Nations: A Commentary*, Vol. 1, Oxford University Press, Oxford, 2016, paras 17-20 of the commentary on Art. 2(4).

بناءً على ذلك، خلص الخبراء إلى أنه "لا العمليات النفسية السيبرانية غير المدمرة التي تهدف فقط إلى تقويض الثقة في الحكومة، ولا حظر الدولة للتجارة الإلكترونية مع دولة أخرى بهدف إحداث عواقب اقتصادية سلبية، يُصنف على أنه استخدام للقوة": دليل تالين 2، الحاشية 13 أعلاه، الفقرة 3 من شرح القاعدة 69.

91 O. Dörr and A. Randelzhofer، الحاشية 90 أعلاه، الصفحة 208، الفقرة 16.

92 محكمة العدل الدولية، الحاشية 46 أعلاه، الفقرة 39.

93 وزارة الجيوش الفرنسية، الحاشية 77 أعلاه، الصفحة 7. انظر أيضًا: دليل تالين 2، الحاشية 13 أعلاه، الفقرة 1 من شرح القاعدة 69.

94 انظر:
Estonia, "President of the Republic at the Opening of CyCon 2019", 29 May 2019, available at: www.president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019/index.html.

وزارة الشؤون الخارجية والتجارة الأسترالية، "استراتيجية أستراليا الدولية بشأن المشاركة السيبرانية"، 2019، متاحة من خلال الرابط التالي:
www.dfat.gov.au/international-relations/themes/cyber-affairs/Pages/australias-international-cyber-engagement-strategy.

95 دليل وزارة الدفاع لقانون الحرب، الحاشية 87 أعلاه، الفقرة 16-3-1.

96 وزارة الجيوش الفرنسية، الحاشية 77 أعلاه، الصفحة 7. ومن الأمثلة التي تقدمها فرنسا على الإجراءات التي "يمكن اعتبارها استخدامات للقوة" "اختراق النظم العسكرية من أجل تعريض القدرات الدفاعية الفرنسية للخطر، أو تمويل أو حتى تدريب أفراد على تنفيذ هجمات سيبرانية تستهدف فرنسا".

97 وزارة الشؤون الخارجية الهولندية، "رسالة إلى البرلمان بشأن النظام القانوني الدولي في الفضاء السيبراني"، 5 تموز/يوليو 2019، الصفحة 4، متاحة من خلال الرابط التالي:
www.government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentary-documents/201926/09//letter-to-the-parliament-on-the-international-legal-order-in-cyberspace؛

ووزارة الجيوش الفرنسية، الحاشية 77 أعلاه، الصفحة 7. للاطلاع على لمحة عامة حديثة عن مواقف الدول، انظر:
Przemysław Roguski, *Application of International Law to Cyber Operations: A Comparative Analysis of States' Views*, Policy Brief, Hague Program for Cyber Norms, 2020.

للاطلاع على توضيح لهذه المناقشات، انظر، على سبيل المثال:
Kenneth Kraszewski, "Scenario 14: Ransomware Campaign",in K. Mačák, T. Minárik and T. Jančárková (eds),

الحاشية 68 أعلاه، الفقرات L13–L5.

إليه محكمة العدل الدولية ومفاده أن "أخطر أشكال استخدام القوة" هي فقط التي يمكن اعتبارها هجمات مسلحة وأن هذه الهجمات يجب أن تصل إلى "نطاق وتأثيرات" معينة،[98] فقد يُستنتج أن استخدام القوة يجب أن يصل إلى مستوى شدة معينة لكي يوصف بأنه "هجوم مسلح".[99] ومرة أخرى، رأى الخبراء أن "بعض العمليات السيبرانية قد تكون خطيرة بما يكفي لتبرير تصنيفها على أنها 'هجوم مسلح' بالمعنى المقصود في الميثاق"،[100] ولا سيما العمليات التي تخلف آثارًا مماثلة للآثار التي تخلفها الهجمات المسلحة التقليدية. ويرد هذا الرأي أيضًا في المواقف العامة لبعض الدول.[101]

تتطور باستمرار المسائل المتعلقة بكيفية تفسير حدود اللجوء إلى القوة المسلحة التي ينطبق عليها القانون الدولي الإنساني، وحظر استخدام القوة بموجب ميثاق الأمم المتحدة، ومفهوم "الهجمات المسلحة" التي تؤدي إلى نشوء الحق الطبيعي في الدفاع عن النفس في الفضاء السيبراني. وفي حين يمكن تحديد بعض المعالم بناءً على الاجتهاد القضائي لمحكمة العدل الدولية، والسوابق القضائية للمحاكم والهيئات القضائية الجنائية الدولية، وممارسة الدول، وآراء الخبراء، لا تزال العديد من المسائل غامضة في الوقت الحالي.

ومع ذلك، من المهم التأكيد على أن هذه المفاهيم والأفكار الثلاثة تنبع من فروع مختلفة من القانون الدولي وتحتمل معان مختلفة. وعلى النحو المشار إليه أعلاه، ترى اللجنة الدولية أن العملية السيبرانية التي تصل إلى حد اللجوء إلى القوة المسلحة بين الدول بموجب القانون الدولي الإنساني يحكمها ذلك الفرع من القانون حتى في حالة عدم وجود نزاع مسلح سابق. ومن الناحية العملية، قد تصل هذه العملية أيضًا إلى حد الاستخدام المحظور للقوة بموجب ميثاق الأمم المتحدة. ومع ذلك، يتطلب الاستنتاجان تحليلًا قانونيًا منفصلًا: استنتاج أن الحد تم الوصول إليه بموجب فرع واحد من القانون لا يمنع بالضرورة التوصل إلى استنتاج مختلف بموجب الفرع الآخر من القانون. ويكتسي هذا الأمر أهمية خاصة عند التمييز بين انطباق القانون الدولي الإنساني والحق في الدفاع عن النفس بموجب ميثاق الأمم المتحدة. وفي ضوء الرأي الذي يذهب إلى أن أخطر أشكال استخدام القوة - أي التي تصل إلى نطاق وتأثيرات معينة - هي فقط التي يمكن اعتبارها هجمات مسلحة، فمن الواضح أنه ليس كل لجوء إلى القوة المسلحة ينطبق عليه القانون الدولي الإنساني يصل إلى حد هجوم مسلح، بموجب ميثاق الأمم المتحدة، يؤدي إلى الحق في الدفاع عن النفس.[102] وهذه الاختلافات لها تبعات قانونية وعملية كبيرة. لذلك، فإن أي تحليل للحالة التي تستخدم فيها دولة العمليات السيبرانية ضد دولة أخرى يجب أن يميز بين المفاهيم المختلفة وألا يدمجها في "حد" واحد غير محدد.

مسألة عزو المسؤولية

في الحرب عمومًا - وفي الفضاء السيبراني خصوصًا - تستعين الدول أحيانًا بجهات فاعلة من

98 محكمة العدل الدولية، القضية المتعلقة بالأنشطة العسكرية وشبه العسكرية في نيكاراغوا وضدها (نيكاراغوا ضد الولايات المتحدة الأمريكية)، الحكم، 27 حزيران/يونيو 1986، الفقرتان 191 و 195.

99 إلا أن هذا الرأي ليس مقبولًا من جميع الدول. فعلى سبيل المثال، ترى الولايات المتحدة أن أي استخدام للقوة هو هجوم مسلح.

100 دليل تالين 2، الحاشية 13 أعلاه، الفقرة 4 من شرح القاعدة 71.

101 وزارة الشؤون الخارجية الهولندية، الحاشية 97 أعلاه، الصفحة 4؛ ووزارة الجيوش الفرنسية، الحاشية 77 أعلاه، الصفحة 7.

102 H. Durham، الحاشية 25 أعلاه.

غير الدول، مثل الجماعات المسلحة من غير الدول أو الشركات العسكرية والأمنية الخاصة، لتنفيذ أعمال معينة، منها العمليات السيبرانية. والخصائص المحددة للفضاء السيبراني، مثل تنوع احتمالات قيام الجهات الفاعلة بإخفاء أو تزوير هويتها، تؤدي إلى تعقد عزو المسؤولية عن السلوك إلى أفراد معينين، وإلى أطراف في النزاعات المسلحة.[103] ويثير ذلك تحديات مهمة عند البت في انطباق القانون الدولي الإنساني في حالة معينة. فإذا تعذر تحديد مرتكب عملية معينة - وبالتالي تحديد العلاقة بين العملية ونزاع مسلح - فسيكون من الصعب للغاية تحديد ما إذا كان القانون الدولي الإنساني ينطبق حتى على العملية.[104] أولًا، على النحو المبين آنفًا، هناك حدود مختلفة للعنف يُعتد بها لتصنيف الهجمات السيبرانية التي تشنها الدول أو الأطراف من غير الدول على أنها نزاع مسلح. وبالتالي، إذا كانت الدولة أو الطرف من غير الدول الذي تنطلق منه العملية السيبرانية خارج نطاق نزاع مسلح مستمر غير معلومة، فلا يكون من الواضح أي حد ينطبق في هذا الصدد. ثانيًا، حتى في حالة حدوث نزاع مسلح، فإن الهجمات السيبرانية التي ليس لها صلة بالنزاع (مثل الأعمال الإجرامية غير المرتبطة بالنزاع) لا تخضع للقانون الدولي الإنساني، وقد يؤدي العجز عن تحديد هوية مصمم العملية السيبرانية إلى إعاقة تحديد ما إذا كانت هذه الصلة بالنزاع قائمة أم لا. وتُظهر هذه الأمثلة أن هناك عواقب قانونية مهمة تترتب على تحديد مصمم العملية السيبرانية، وما إذا كان يمكن عزو المسؤولية عن العملية إلى دولة أو طرف من غير الدول في النزاع.

كما أن عزو المسؤولية عن العمليات السيبرانية مهم لضمان إمكانية محاسبة الجهات الفاعلة التي تنتهك القانون الدولي، بما في ذلك القانون الدولي الإنساني. والتصور القائل بأنه سيكون من الأسهل إنكار المسؤولية عن الهجمات غير القانونية قد يضعف أيضًا من الحظر المفروض على هذه الاستخدامات - وقد يجعل الجهات الفاعلة أقل حرصًا بشأن إجراء عمليات تنتهك القانون الدولي.[105]

ومع ذلك، فإن عزو المسؤولية لا يمثل مشكلة من منظور الجهات الفاعلة التي تنفذ العمليات السيبرانية أو توجهها أو تتحكم فيها: فهي لديها جميع الحقائق المتاحة لتحديد الإطار القانوني الدولي الذي تعمل بموجبه والالتزامات التي يتعين عليها احترامها.[106]

بموجب القانون الدولي، تتحمل الدولة المسؤولية عن السلوك المنسوب إليها، بما في ذلك الانتهاكات المحتملة للقانون الدولي الإنساني. وهذا يشمل:

(أ) الانتهاكات التي ترتكبها الهيئات التابعة لها، بما فيها قواتها المسلحة؛
(ب) الانتهاكات التي يرتكبها أشخاص أو كيانات مخولة بممارسة اختصاصات السلطة الحكومية؛
(ج) الانتهاكات التي يرتكبها أشخاص أو جماعات تتصرف في الواقع بناءً على تعليماتها أو بتوجيه منها أو تحت سيطرتها؛

103 للاطلاع على دراسة للتحديات التقنية المتعلقة بعزو المسؤولية عن الهجمات السيبرانية إلى جهات فاعلة محددة، انظر:
"Know Your Enemy and Know Yourself: Attribution in the Cyber Domain", *Humanitarian Law and Policy Blog*, 3 June 2019, available at: https://blogs.icrc.org/law-and-policy/201903/06//know-your-enemy-know-yourself-cyber-domain-attribution/.
104 تقرير التحديات الصادر عن اللجنة الدولية لعام 2011، الحاشية 43 أعلاه، الصفحة 36.
105 اللجنة الدولية، الحاشية 1 أعلاه، الصفحة 9.
106 المرجع نفسه.

(د) الانتهاكات التي يرتكبها أفراد عاديون أو مجموعات خاصة تقر بها وتعتمدها باعتبارها سلوكها الخاص.[107]

تنطبق هذه المبادئ سواء ارتكب انتهاك القانون الدولي الإنساني عن طريق وسائل سيبرانية أو غيرها.[108]

القيود التي يفرضها القانون الدولي الإنساني على استخدام القدرات السيبرانية أثناء النزاعات المسلحة

الاعتراف بأن القانون الدولي الإنساني ينطبق على العمليات السيبرانية المرتبطة بنزاع مسلح ليس سوى خطوة أولى. وتثير الخصائص المحددة لهذه التقنية الجديدة العديد من التحديات في إطار تفسير قواعد القانون الدولي الإنساني، بما في ذلك القواعد المتعلقة بسير الأعمال العدائية.

وتشكل الطبيعة غير المادية جزئيًا (أي الرقمية) للفضاء السيبراني والترابط بين الشبكات العسكرية والمدنية تحديات عملية وقانونية في تطبيق قواعد القانون الدولي الإنساني العامة التي تحمي المدنيين والأعيان المدنية من العمليات السيبرانية، ولا سيما التي تصل إلى حد الهجمات بموجب القانون الدولي الإنساني. بل يقال إنه قد يكون من المستحيل أحيانًا تطبيق مبادئ القانون الدولي الإنساني الأساسية في الفضاء السيبراني. وكما سيتضح أدناه، قد تكون هناك مبالغة في التعبير عن هذا التحدي. ومع ذلك، تظهر مشكلات رئيسية تتعلق بحماية البنية التحتية السيبرانية المدنية الأساسية من الهجمات العسكرية. ولما كانت العديد من قواعد القانون الدولي الإنساني التي تحكم سير الأعمال العدائية لا تنطبق إلا على العمليات العسكرية التي تصل إلى حد "الهجمات" على النحو المحدد في القانون الدولي الإنساني، فإن هذا القسم يبحث أولاً في مختلف المسائل المتعلقة بالعمليات السيبرانية التي تصنف على أنها هجمات، ويشمل ذلك السؤال البارز المتعلق بأي العمليات يعتبر هجمات بموجب القانون الدولي الإنساني. ثانيًا، يستطلع هذا القسم التزامات أطراف النزاعات المسلحة في العمليات العسكرية بخلاف العمليات التي تصل إلى حد "الهجمات". ثالثًا، يحلل القسم بعض التحديات المتعلقة بالمراجعة القانونية للقدرات السيبرانية.

العمليات السيبرانية التي تصل إلى حد الهجوم بموجب القانون الدولي الإنساني

يحدد القانون الدولي الإنساني القواعد الأساسية التي تقيد العمليات السيبرانية التي تصل إلى حد "الهجمات" على النحو المحدد في القانون الدولي الإنساني. ويبحث هذا القسم في القواعد والمبادئ التي خضعت لأشد النقاشات حدة. وهو يبحث أولاً فيما إذا كانت الهجمات السيبرانية

107 انظر: دراسة اللجنة الدولية للقانون العرفي، الحاشية 63 أعلاه، القاعدة 149. انظر أيضًا: لجنة القانون الدولي، مسؤولية الدول عن الأفعال غير المشروعة دوليًا، 2001، ولا سيما المواد 4-11.

108 اللجنة الدولية، الحاشية 1 أعلاه، الصفحة 9؛ ودليل تالين 2، الحاشية 13 أعلاه، القواعد 15-17. للاطلاع على وجهة نظر مختلفة، انظر: تعليق الصين على المسودة الأولية لتقرير الفريق العامل المفتوح العضوية والذي يشير إلى أنه فيما يتعلق "بمسؤولية الدولة، والتي، على عكس قانون النزاعات المسلحة أو حقوق الإنسان، لم تحصل بعد على إجماع دولي، لا يوجد أي أساس قانوني على الإطلاق لأي مناقشة حول تطبيقه في الفضاء السيبراني". تعليقات الصين على المسودة الأولية لتقرير الفريق العامل المفتوح العضوية، متاحة من خلال الرابط التالي:
www.un.org/disarmament/open-ended-working-group/.

عبر شبكة الإنترنت، من منظور تقني، يمكن توجيهها إلى أهداف عسكرية محددة على النحو الذي يقتضيه مبدأ التمييز. ويحلل الجزء الثاني كيفية تفسير مفهوم الهجوم بموجب القانون الدولي الإنساني في الفضاء السيبراني. ويناقش الجزء الثالث الجدال الوثيق الصلة بشأن وجوب أو عدم وجوب منح البيانات المدنية نفس الحماية التي تتمتع بها "الأعيان" المدنية في إطار أغراض القانون الدولي الإنساني، ويتناول الجزء الأخير الجدل الدائر حول كيفية تطبيق قواعد القانون الدولي الإنساني المتعلقة بسير الأعمال العدائية على الأعيان المستخدمة في الوقت نفسه لأغراض مدنية وعسكرية (تسمى غالبًا الأعيان ذات الاستخدام المزدوج)، والتي تنتشر بشكل خاص في الفضاء السيبراني.

من وجهة نظر تقنية، يمكن توجيه الهجمات السيبرانية إلى أهداف عسكرية محددة

يقتضي تنفيذ مبدأ التمييز ومبدأ التناسب، وحظر الهجمات العشوائية، أن يكون الهجوم موجهًا نحو هدف عسكري وألا يتسبب في أضرار عرضية مفرطة للمدنيين أو الأعيان المدنية. وعلى عكس الافتراض القائل بأن هذه المبادئ قد تصبح بلا معنى في الفضاء السيبراني بسبب الترابط الذي يميزه، فإن الدراسة الدقيقة للعمليات السيبرانية تظهر أن هذه العمليات ليست عشوائية بطبيعتها. فعلى سبيل المثال، إذا نُفذت عملية سيبرانية من خلال مشغلين يُدخلون هدفًا وينفذون عملية، فإن هؤلاء المشغلين يكونون على دراية بمكانهم وما يقومون به. وبالمثل، تُظهر تحليلات الأدوات السيبرانية أنها ليست بالضرورة عشوائية. ومن ناحية أخرى، فإن برمجة البرامج الضارة التي تميز بين الأعيان المدنية والأهداف العسكرية، وتنفيذ العمليات السيبرانية دون التسبب في وقوع أضرار عرضية مفرطة، تتطلب قدرات واختبارات متطورة.

ويمكن لمن يطورون برامج ضارة أو يخططون لهجمات سيبرانية تصميم أدواتهم دون أن تتضمن وظائف الانتشار الذاتي. وفي تلك الحالة، لا يمكن أن تنتشر البرامج الضارة دون تدخل بشري إضافي. وحتى لو كانت الهجمات ذاتية الانتشار، فقد أظهرت على مر السنين أنه من الممكن تصميم برامج ضارة لمهاجمة أجهزة أو برامج معينة فقط. وهذا يعني أنه حتى في حالة برمجة البرامج الضارة بحيث تنتشر على نطاق واسع، فيمكن تصميمها لإلحاق ضرر يقتصر على هدف معين أو مجموعات محددة من الأهداف. وقد تتطلب الهجمات السيبرانية خاصة التي تهدف إلى إحداث ضرر مادي لنظم التحكم الصناعية أدوات سيبرانية مصممة تحديدًا لهذا الهدف وهذا الغرض. وفي كثير من الحالات، تؤدي الحاجة إلى مثل هذه الأدوات المصممة خصيصًا إلى العرقلة الفعلية - من منظور تقني - للقدرة على تنفيذ هجوم سيبراني على نطاق واسع أو بطريقة عشوائية. وإمكانية توجيه الهجمات السيبرانية بدقة من الناحية التقنية لا تعني بالضرورة أنها قانونية إذا نُفذت في النزاع. ومع ذلك، تبين الخصائص التي تظهر في عدد من العمليات السيبرانية أنه يمكن تصميمها بدقة شديدة لإحداث تأثيرات تقتصر على أهداف محددة، وبالتالي فإن هذه العمليات لها القدرة على الامتثال لمبادئ وقواعد القانون الدولي الإنساني.

وإذا كانت بعض الأدوات السيبرانية المعروفة قد صُممت لتنتشر ذاتيًا وتسببت في آثار ضارة على النظم الحاسوبية المدنية المستخدمة على نطاق واسع، فإن ذلك لا يؤيد الحجة التي تذهب إلى أن الترابط الشديد الذي يتسم به الفضاء السيبراني يجعل من الصعب، إن لم

يكن من المستحيل، تنفيذ قواعد القانون الدولي الإنساني الأساسية. بل على العكس من ذلك، يحظر القانون الدولي استخدام هذه الأدوات السيبرانية أثناء النزاعات المسلحة.[109] ويحظر القانون الدولي الإنساني الهجمات التي تستخدم وسائل وأساليب القتال، بما في ذلك الوسائل والأساليب السيبرانية التي لا يمكن توجيهها إلى هدف عسكري محدد أو قد يُتوقع أن تخرج عن نطاق سيطرة المستخدم،[110] أو يتوقع منها- أثناء توجيهها إلى هدف عسكري- أن تتسبب في أضرار مدنية عرضية مفرطة مقارنة بالميزة العسكرية الملموسة والمباشرة المنتظرة.[111]

مفهوم "الهجوم" في إطار القانون الدولي الإنساني وتطبيقه على العمليات السيبرانية

مسألة وصول أو عدم وصول عملية معينة إلى حد "الهجوم" على النحو المحدد في القانون الدولي الإنساني هي مسألة أساسية لتطبيق العديد من القواعد المستمدة من مبادئ التمييز والتناسب والاحتياط التي توفر حماية مهمة للمدنيين والأعيان المدنية. وعمليًا، فإن قواعد مثل حظر الهجمات على المدنيين والأعيان المدنية،[112] وحظر الهجمات العشوائية[113] وغير المتناسبة،[114] والالتزام باتخاذ جميع الاحتياطات الممكنة لتجنب، أو على الأقل، تقليل الضرر العرضي الذي يلحق بالمدنيين والأضرار التي تلحق بالأعيان المدنية عند تنفيذ هجوم،[115] تنطبق على العمليات التي تعتبر "هجمات" على النحو المحدد في القانون الدولي الإنساني. لذا فإن مسألة مدى اتساع أو ضيق تفسير مفهوم "الهجوم" في سياق العمليات السيبرانية ضرورية لتطبيق القواعد الرئيسية - والحماية التي توفرها للمدنيين والبنية التحتية المدنية - على العمليات السيبرانية.

تُعرّف المادة 49 من البروتوكول الإضافي الأول الهجمات بأنها "أعمال العنف الهجومية والدفاعية ضد الخصم". من المقرر أن مفهوم العنف في هذا التعريف قد يشير إما إلى وسائل القتال أو الآثار المترتبة عليها، وهذا يعني أن العملية التي تسبب آثارًا عنيفة يمكن أن تكون هجومًا، حتى لو لم تكن الوسائل المستخدمة لإحداث هذه الآثار عنيفة في حد ذاتها.[116] وعلى أساس هذا الفهم، يقترح دليل تالين 2 التعريف التالي للهجوم السيبراني: "الهجوم السيبراني هو عملية سيبرانية، سواء كانت هجومية أو دفاعية، يُتوقع استنادًا إلى أسباب معقولة أن تتسبب في إصابة أو وفاة الأشخاص أو إلحاق أضرار بالأعيان أو تدميرها".[117]

109 بالمثل، يخلص [دليل قانون الحرب الصادر عن وزارة الدفاع]، الحاشية 87 أعلاه، الفقرة 16-6 إلى ما يلي: "على سبيل المثال، يُحظر فيروس الكمبيوتر المدمر المبرمج لكي ينتشر ويدمر بشكل لا يمكن السيطرة عليه داخل نظم الإنترنت المدنية بوصفه سلاحًا عشوائيًا بطبيعته".

110 Yves Sandoz, Christophe Swinarski and Bruno Zimmerman (eds.), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*, ICRC, Geneva, 1987 (ICRC Commentary on the APs), para. 1963.

[شرح البروتوكولين الإضافيين].

111 البروتوكول الإضافي (الأول) لاتفاقيات جنيف المؤرخة 12 آب/أغسطس 1949، والمتعلق بحماية ضحايا المنازعات الدولية المسلحة، 3 UNTS 1125، 8 حزيران/يونيو 1977 (دخل حيز النفاذ في 7 كانون الأول/ديسمبر 1978) (البروتوكول الإضافي الأول)، المادة 51 (4)-(5)؛ ودراسة اللجنة الدولية للقانون العرفي، الحاشية 63 أعلاه، القاعدتان 11 و 14.

112 انظر: البروتوكول الإضافي الأول، المادة 52؛ ودراسة اللجنة الدولية للقانون العرفي، الحاشية 63 أعلاه، القواعد 7-10.

113 انظر: البروتوكول الإضافي الأول، المادة 54 (ج)؛ ودراسة اللجنة الدولية للقانون العرفي، الحاشية 63 أعلاه، القاعدة 11.

114 انظر: البروتوكول الإضافي الأول، المادة 51 (5) (ب)؛ ودراسة اللجنة الدولية للقانون العرفي، الحاشية 63 أعلاه، القاعدة 14.

115 انظر: البروتوكول الإضافي الأول، المادة 57 (1)؛ ودراسة اللجنة الدولية للقانون العرفي، الحاشية 63 أعلاه، القاعدة 15.

116 انظر: سي. دروغيه، الحاشية 83 أعلاه، الصفحة 557؛ وانظر:

William H. Boothby, *The Law of Targeting*, Oxford University Press, Oxford, 2012, p. 384.

وتشير دروغيه إلى أنه "لا خلاف على أن استخدام العناصر البيولوجية أو الكيميائية أو الإشعاعية يشكل هجومًا، حتى إذا لم يتضمن الهجوم استخدام القوة المادية".

117 دليل تالين 2، الحاشية 13 أعلاه، القاعدة 92.

ومن المسلم به على نطاق واسع من قبل الدول التي اتخذت موقفًا بشأن هذه المسألة، ومن قبل اللجنة الدولية والخبراء أن العمليات السيبرانية التي تسبب الوفاة أو الإصابة أو الضرر المادي على الأقل تشكل هجمات بموجب القانون الدولي الإنساني.[118] وتُدرج بعض الدول صراحة الضرر الناجم عن الآثار غير المباشرة (أو الارتدادية) المتوقعة للهجمات،[119] وهو رأي تعتمده اللجنة الدولية.[120] وهذا صحيح، على سبيل المثال، إذا قُتل المرضى في وحدة العناية المركزة نتيجة لعملية سيبرانية ضد شبكة كهرباء تسببت في انقطاع التيار الكهربائي عن المستشفى.

بخلاف هذا الإجماع الأساسي، توجد آراء مختلفة حول ما إذا كانت العملية السيبرانية التي تعطل عينًا دون الإضرار بها ماديًا تصل إلى حد الهجوم بموجب القانون الدولي الإنساني.[121] وأجريت مناقشات مستفيضة حول هذه المسألة في إطار عملية صياغة دليل تالين. فقد رأى أغلب الخبراء أن العملية السيبرانية تصل إلى حد الهجوم إذا كان من المتوقع أن تعطل القدرة على العمل وإذا كانت استعادة هذه القدرة تتطلب استبدال المكونات المادية. ويرى بعض الخبراء أن العملية السيبرانية ستصل أيضًا إلى حد الهجوم إذا كانت استعادة القدرة على العمل تتطلب إعادة تثبيت نظام التشغيل أو بيانات معينة.

اتخذت اللجنة الدولية موقفًا مفاده أن العملية المصممة لتعطيل جهاز كمبيوتر أو شبكة كمبيوتر أثناء نزاع مسلح تشكل هجومًا على النحو المحدد في القانون الدولي الإنساني سواء تعطلت العين أو لم تتعطل بفعل التدمير أو أي طريقة أخرى.[122]

هناك سببان رئيسيان يدعمان موقف اللجنة الدولية. الأول ناتج عن تفسير مفهوم الهجوم في سياقه.[123] وبالنظر إلى أن تعريف الأهداف العسكرية الوارد في المادة 52 (2) من البروتوكول الإضافي الأول لا يشير إلى التدمير أو الاستيلاء فحسب، بل يشير أيضًا إلى "التعطيل" كنتيجة محتملة للهجوم، فينبغي إدراك مفهوم "الهجوم" بموجب المادة 49 من البروتوكول الإضافي الأول على أنه يشمل العمليات التي تهدف إلى إعاقة عمل الأعيان (أي تعطيلها) دون التسبب في ضرر مادي أو تدمير. وفي الواقع، تم التأكيد على أن الإشارة الصريحة إلى التعطيل

118 انظر: اللجنة الدولية، القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة، جنيف، 2015 (تقرير التحديات الصادر عن اللجنة الدولية لعام 2015)، الصفحتان 41-42، متاح من خلال الرابط التالي:
https://www.icrc.org/ar/document/international-humanitarian-law-and-challenges-contemporary-armed-conflicts؛
وانظر: دليل تالين 2، الحاشية 13 أعلاه، القاعدة 92. بالنسبة للدول التي اعتمدت رأيًا بشأن كيفية تطبيق مفهوم الهجوم بموجب القانون الدولي الإنساني على العمليات السيبرانية، انظر على وجه الخصوص: وزارة الشؤون الخارجية والتجارة الأسترالية، الحاشية 94 أعلاه، المرفق ألف؛ ووزارة الدفاع الدنماركية، الدليل العسكري للقانون الدولي المتعلق بالقوات المسلحة الدنماركية في العمليات الدولية، 2016 (الدليل العسكري الدنماركي)، الصفحتان 290-291، النسخة الإنجليزية متاحة من خلال الرابط التالي:
www.forsvaret.dk/omos/publikationer/Documents/Military%20Manual%20updated%202020.pdf؛
ووزارة الجيوش الفرنسية، الحاشية 77 أعلاه، الصفحة 13؛ والنرويج، دليل القانون الدولي للحرب، 2013 (الدليل العسكري النرويجي)، الفقرة 9-54، متاحة من خلال الرابط التالي:
https://fhs.brage.unit.no/fhs-xmlui/bitstream/handle/11250194213//manual_krigens_folkerett.pdf?sequence=1&isAllowed=y؛
ودليل نيوزيلندا العسكري، الحاشية 85 أعلاه، الفقرة 8-10-17؛ ودليل وزارة الدفاع لقانون الحرب، الحاشية 87 أعلاه، الفقرة 16-5-1.

119 الدليل العسكري الدنماركي، الحاشية 118 أعلاه، الصفحة 677 (عند مناقشة الهجمات على شبكات الكمبيوتر)؛ ودليل نيوزيلندا العسكري، الحاشية 85 أعلاه، الفقرة 8-10-22؛ والدليل العسكري النرويجي، الحاشية 118 أعلاه، الفقرة 9-54.

120 اللجنة الدولية، الحاشية 1 أعلاه، الصفحة 7.

121 انظر على سبيل المثال: دليل تالين 2، الحاشية 13 أعلاه، شرح القاعدة 92، الفقرات 10-12.

122 انظر: تقرير التحديات الصادر عن اللجنة الدولية لعام 2015، الحاشية 119 أعلاه، الصفحتان 41-42. انظر أيضًا: دليل تالين 2، الحاشية 13 أعلاه، الفقرة 12 من شرح القاعدة 92.

123 اتفاقية فيينا لقانون المعاهدات، المادة 31 (1).

بموجب المادة 52 (2) زائدة عن الحاجة من ناحية أخرى.[124] والسبب الثاني، أن من الصعب التوفيق بين الفهم المقيد للغاية لمفهوم الهجوم والغرض والهدف من القواعد المتعلقة بسير الأعمال العدائية التي تهدف إلى ضمان حماية السكان المدنيين والأعيان المدنية من آثار الأعمال العدائية. وفي الواقع، في ظل الفهم المقيد للغاية، فإن العملية السيبرانية التي تهدف إلى تعطيل شبكة مدنية (شبكات الكهرباء أو الخدمات المصرفية أو الاتصالات أو غيرها) أو يُحتمل أن تتسبب في حدوث ذلك عرضيًا، قد تكون مستبعدة من نطاق قواعد القانون الدولي الإنساني الأساسية التي تحمي السكان المدنيين والأعيان المدنية.[125]

بطريقة مماثلة، يشير الخبراء المعلقون إلى أنه من المهم "تفسير الحكم [المادة 49 من البروتوكول الإضافي الأول] مع مراعاة التطورات التكنولوجية الحديثة وتوسيع مفهوم 'العنف' بحيث لا يشمل الضرر المادي الذي يلحق بالأعيان فحسب، بل يشمل أيضًا تعطيل البنية التحتية دون تدمير".[126]

ونظرًا لأن العمليات السيبرانية يمكن أن تعطل الخدمات الأساسية بشكل كبير دون التسبب بالضرورة في أضرار مادية، فإن هذا يشكل أحد المناقشات الأكثر أهمية لحماية المدنيين من آثار العمليات السيبرانية. لذلك، من الأهمية بمكان أن تعرب الدول عن آرائها بشأن هذه المسألة وأن تعمل على التوصل إلى تفاهم مشترك. وفي الوقت الحالي، تختلف الآراء بين الدول التي اتخذت مواقف علنية.

وتجسد تعاريف مفهوم "الهجوم" المعتمدة في الأدلة العسكرية للنرويج ونيوزيلندا التعريف المعتمد في دليل تالين 2. ومع ذلك، فمن غير الواضح ما إذا كانت هذه الأدلة تهدف إلى التعبير عن موقف بشأن هذه المناقشة، لأن شرح القاعدة 92 من دليل تالين 2 يشير إلى وجهات نظر مختلفة حول كيفية فهم "الضرر" في السياق السيبراني. وذكرت أستراليا أن العمليات السيبرانية تعتبر هجمات إذا وصلت "إلى نفس حد 'الهجوم الحركي بموجب القانون الدولي الإنساني'"،[127] ولكن من غير الواضح ما إذا كان المقصود من ذلك أن يشكل موقفًا في هذه المناقشة.

يركز عدد قليل من الدول على الضرر المادي لكي تصنف عملية سيبرانية على أنها هجوم. ووفقًا لدراسة أجرتها منظمة الدول الأمريكية، رأت بيرو أنه لكي يتم تصنيف عملية معينة على أنها هجوم، يجب "إلحاق الأذى الفعلي بالأشخاص أو الأعيان".[128] وينص الدليل

124 Knut Dörmann, "Applicability of the Additional Protocols to Computer Network Attacks", 2004, p. 4, available at www.icrc.org/en/doc/assets/files/other/applicabilityofihltocna.pdf:

و سي. دروغيه، الحاشية 83 أعلاه، الصفحة 559. وللاطلاع على وجهة نظر مختلفة، انظر:
Michael N. Schmitt, "Cyber Operations and the Jus in Bello: Key Issues", *International Law Studies*, Vol. 87, 2011, pp. 95-96; Heather Harrison Dinniss, *Cyber Warfare and the Laws of War*, Cambridge University Press, Cambridge, 2012, p. 198.

125 بنفس المعنى، انظر أيضًا: M. N. Schmitt، الحاشية 67 أعلاه، الصفحة 339.

126 Marco Roscini, *Cyber Operations and the Use of Force in International Law*, Oxford University Press, Oxford, 2014, p. 181.

انظر أيضًا:
Dieter Fleck, "Searching for International Rules Applicable to Cyber Warfare - A Critical First Assessment of the New *Tallinn Manual*", *Journal of Conflict and Security Law*, Vol. 18, No. 2, 2013, p. 341:

"في الواقع، من غير المقنع الإصرار على أن مصطلح" الهجمات "ينبغي أن يقتصر على الأفعال التي تؤدي مباشرة إلى إصابات أو دمار مادي، في الحالات التي يؤدي فيها نفس الإجراء، على سبيل المثال، إلى تعطيل الإمدادات الأساسية للمستشفيات أو غيرها من البني التحتية المدنية المهمة".

127 وزارة الخارجية والتجارة الأسترالية، الحاشية 94 أعلاه، المرفق ألف.

128 منظمة الدول الأمريكية، الحاشية 22 أعلاه، الفقرة 43.

العسكري الدنماركي على أن مصطلح "الهجوم" "يشمل أي ضرر مادي، بالإشارة إلى الأضرار التي تلحق بالأعيان. ومع ذلك، فإن المصطلح لا يشمل العجز المؤقت عن التشغيل وغيره من أشكال التعطيل التي لا تنطوي على ضرر مادي (على سبيل المثال، "التجميد" الرقمي لنظام التحكم في الاتصال)."[129] وأشارت الولايات المتحدة في تعليقها الذي قدمته في عام 2014 إلى فريق الخبراء الحكوميين التابع للأمم المتحدة إلى ما يلي:

> عند تحديد ما إذا كان نشاط سيبراني يشكل "هجومًا" في إطار أغراض قانون الحرب، يجب على الدول أن تنظر في جملة أمور منها ما إذا كان النشاط السيبراني ينتج عنه تأثيرات حركية وتأثيرات على المدنيين أو الأعيان المدنية أو البنية التحتية السيبرانية المدنية لا يمكن عكس مسارها، أو تأثيرات غير حركية على الفئات نفسها يمكن عكس مسارها.[130]

على نفس المنوال، يسوق دليل قانون الحرب الصادر عن وزارة الدفاع الأمريكية مثالًا على "هجوم سيبراني من شأنه تدمير النظم الحاسوبية المعادية"، ويلاحظ أن "العوامل التي تشير إلى أن العملية السيبرانية ليست 'هجومًا' تشمل ما إذا كانت العملية تسبب تأثيرات يمكن عكس مسارها أم تأثيرات مؤقتة فقط".[131] ولسوء الحظ، لا توضح هذه الوثائق ما تعنيه بالتأثيرات "التي يمكن عكس مسارها" أو "المؤقتة" أو الفرق - إن وجد - بين المفهومين.[132] وهي لا تناقش ما إذا كان التأثير لم يعد يعتبر مؤقتًا- وإذا كان كذلك فبعد كم من الوقت- أو كيفية النظر في العمليات المتكررة التي من شأنها أن تتسبب كل منها في إحداث تأثير مؤقت، وإن كان متراكمًا بشكل متعمد. وهي لا تناقش ما إذا كان مصطلح "يمكن عكس مسارها" يشير فقط إلى العمليات التي قد يقوم فيها مصمم العملية بعكس مسار تأثيرات الهجوم،[133] أم يشير أيضًا إلى العمليات التي يتعين فيها على الهدف اتخاذ إجراءات لاستعادة وظيفة النظام المستهدف أو إنهاء أو عكس مسار آثار الهجوم. وفي هذا الصدد، يجب أن نتذكر أن إمكانية إصلاح الضرر المادي الناجم عن عملية عسكرية (سواء كانت سيبرانية أم حركية) لا تُفهم عمومًا على أنها معيار لعدم اعتبار عملية معينة هجومًا بموجب القانون الدولي الإنساني.[134] وهذا صحيح حتى إذا كان الإصلاح يؤدي إلى عكس مسار التأثير المباشر لتلك العملية واستعادة وظيفة العين محل الدراسة.[135]

129 الدليل العسكري الدنماركي، الحاشية 118 أعلاه، الصفحة 290. ينص الدليل في سياق الهجمات على شبكات الكمبيوتر وعمليات هذه الشبكات أن "هذا يعني على سبيل المثال، أن العمليات التي تعتمد على الشبكات يجب أن تعتبر هجمات بموجب القانون الدولي الإنساني إذا كانت النتيجة أنها تسبب ضررًا ماديًا". المرجع نفسه، الصفحة 291.

130 تعليق الولايات المتحدة المقدم إلى فريق الأمم المتحدة للخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، 2014-2015، الصفحة 5.

131 انظر أيضًا: دليل قانون الحرب الصادر عن وزارة الدفاع، الحاشية 87 أعلاه، الفقرتان 16-5-1 و 16-5-2.

132 Gary Brown and Kurt Sanger, "Cyberspace and the Law of War", *Cyber Defense Review*, 6 November 2015, available at: https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/1136032/cyberspace-and-the-law-of-war/.

133 على سبيل المثال، الهجوم الموزع لتعطيل تقديم الخدمة الذي تعود فيه الشبكة أو النظام المستهدف تلقائيًا إلى العمل بصورة طبيعية عندما ينهي المهاجم الهجوم الموزع ولا يقع أي تأثير غير مباشر آخر خلال الوقت الذي تتأثر فيه الشبكة أو النظام.

134 Laurent Gisel, "The Use of Cyber Technology in Warfare: Which Protection Does IHL afford and Is It Sufficient?", in G. Venturini and G. L. Beruto (eds), الحاشية 7 أعلاه.

135 على سبيل المثال، يناقش مايكل لويس ممارسة شن هجمات على الجسر طوليًا خلال حرب الخليج لعام 1991، ويلاحظ جملة أمور منها أن "الضرر الذي يلحق بالجسر سيكون أقرب إلى منتصف المسافة وبالتالي يسهل إصلاحه"، دون الادعاء بأن هذه السمة ستمنع عملية توصف بأنها هجوم. انظر: Michael Lewis, "The Law of Aerial Bombardment in the 1991 Gulf War", *American Journal of International Law*, Vol. 97, No. 3, 2003, p. 501.

وأعربت فرنسا عن فهم أوضح وأوسع نطاقًا لمفهوم الهجوم السيبراني. فهي ترى أن:

> العملية السيبرانية هي هجوم لم تعد فيه المعدات ولا النظم المستهدفة توفر الخدمة التي تُنفذ من أجلها، سواء بشكل مؤقت أو دائم، أو بشكل يمكن عكس مساره أم لا. وإذا كانت الآثار مؤقتة أو يمكن عكس مسارها، فإن الهجوم يمكن تمييزه عندما تكون الإجراءات التي يتخذها الخصم ضرورية لاستعادة البنية التحتية أو النظام (إصلاح المعدات أو استبدال جزء أو إعادة تثبيت الشبكة وما إلى ذلك).[136]

لاحظ شميت، في تعليقه على هذا الموقف، قائلًا إن "وجهة النظر المذكورة يمكن الدفاع عنها بدرجة كبيرة من الناحية القانونية، لأن المعنى البسيط للضرر يمتد بشكل معقول إلى النظم التي لا تعمل على النحو المنشود وتتطلب بعض أشكال الإصلاح لاستعادة الوظائف".[137] بطريقة مماثلة، وفقًا لدراسة منظمة الدول الأمريكية المذكورة أعلاه، تشير شيلي أنه لكي يتم تصنيف عملية معينة على أنها هجوم، فإن نتيجتها يجب أن تتطلب من الدولة المتضررة "اتخاذ إجراءات لإصلاح أو استعادة البنية التحتية أو نظم الكمبيوتر المتضررة، فعواقب الهجوم في تلك الحالات تكون مماثلة للعواقب المذكورة أعلاه ، ولا سيما الأضرار المادية التي تلحق بالممتلكات".[138] وأشارت الدراسة أيضًا إلى أن غواتيمالا أعربت عن رأي مفاده أن العملية السيبرانية التي "لا تؤدي سوى إلى "فقدان القدرة على التشغيل" تصل إلى حد الهجوم، وهو الرأي الذي ذهبت إليه إكوادور.[139] كما ترى بوليفيا وإكوادور وغيانا أن هذه العمليات السيبرانية قد تشكل هجومًا بموجب القانون الدولي الإنساني لا سيما عندما تعطل البنية التحتية الحيوية أو تقديم الخدمات الأساسية للسكان.[140]

وعلى أي حال، لن تشكل جميع العمليات السيبرانية أثناء النزاعات المسلحة "هجمات" بمعناها المفهوم في القانون الدولي الإنساني. أولًا، لا يشمل مفهوم الهجوم في القانون الدولي الإنساني التجسس. ثانيًا، لا تحظر القواعد المتعلقة بسير الأعمال العدائية جميع العمليات التي تعطل نظم الاتصالات المدنية: فقد درجت العادة على عدم اعتبار التشويش على الاتصالات اللاسلكية أو البث التلفزيوني هجومًا على النحو المحدد في القانون الدولي الإنساني. ومع ذلك، فإن التمييز بين الهجمات وتعطيل الاتصالات الذي لا يصل إلى حد الهجوم ربما يكون أقل وضوحًا في العمليات السيبرانية مقارنة بالعمليات الحركية أو الكهرومغناطيسية التقليدية.[141] ثالثًا، مفهوم "العمليات العسكرية" بموجب القانون الدولي الإنساني، بما فيها العمليات التي تُنفذ باستخدام وسائل سيبرانية، أوسع نطاقًا من مفهوم "الهجمات"، كما سيتبين في الأجزاء التالية.

136 وزارة الجيوش الفرنسية، الحاشية 77 أعلاه، الصفحة 13.

137 M. N. Schmitt، الحاشية 52 أعلاه. وبنفس المعنى، انظر أيضًا: W. H. Boothby، الحاشية 116 أعلاه، الصفحة 386.

138 منظمة الدول الأمريكية، الحاشية 22 أعلاه، الفقرة 43.

139 قررت الإكوادور أن "العملية السيبرانية يمكن أن تعتبر هجومًا إذا أدت إلى تعطيل البنية التحتية الحيوية للدولة أو غير ذلك مما يعرض أمن الدولة للخطر". المرجع نفسه، الفقرة 44.

140 أشارت بوليفيا إلى أن العملية السيبرانية "يمكن اعتبارها هجومًا عندما يكون هدفها تعطيل الخدمات الأساسية للدولة (المياه أو الكهرباء أو الاتصالات أو النظام المالي)"؛ وأشارت غيانا إلى أن "العمليات السيبرانية التي تقوض عمل نظم الكمبيوتر والبنية التحتية اللازمة لتوفير الخدمات والموارد للسكان المدنيين تشكل هجومًا" وأدرجت ضمنها "المحطات النووية والمستشفيات والمصارف ونظم مراقبة الحركة الجوية". المرجع نفسه، الصفحتان 44-45.

141 تقرير التحديات الصادر عن اللجنة الدولية لعام 2015، الحاشية 118 أعلاه، الصفحتان 41-42؛ وسي. دروغيه، الحاشية 83 أعلاه، الصفحة 560.

حماية البيانات بوصفها من "الأعيان المدنية"

بالإضافة إلى السؤال الأساسي المتعلق بأي العمليات السيبرانية يصل إلى حد "الهجمات" بموجب القانون الدولي الإنساني، يدور نقاش كبير حول مسألة ما إذا كانت البيانات المدنية تتمتع بنفس الحماية التي تتمتع بها الأعيان المدنية، ولا تزال مسألة غير محسومة. وتكتسي حماية البيانات المدنية من العمليات السيبرانية الخبيثة أثناء النزاع المسلح أهمية متزايدة لأن البيانات ركن أساسي في المجال الرقمي وحجر زاوية للحياة في العديد من المجتمعات: فالبيانات الطبية الخاصة بالأفراد، وبيانات الضمان الاجتماعي، والسجلات الضريبية، والحسابات المصرفية، وملفات عملاء الشركات، وقوائم وسجلات الانتخابات، كلها عناصر رئيسية لأداء معظم مناحي الحياة المدنية. ولما كان من المتوقع لهذا الاتجاه أن يستمر، إن لم يتصاعد في السنوات المقبلة، فثمة قلق متزايد إزاء حماية هذه البيانات الأساسية المدنية.

وتتسم قواعد الحماية بالشمول في سياق البيانات الخاصة بفئات معينة من الأعيان التي تتمتع بحماية خاصة بموجب القانون الدولي الإنساني. وكما هو مبين أدناه، يجب فهم الالتزامات باحترام وحماية المرافق الطبية وعمليات الغوث الإنساني على أنها تمتد إلى البيانات الطبية الخاصة بتلك المرافق وبيانات المنظمات الإنسانية الضرورية لعملياتها.[142] كما يُحظر حذف البيانات أو العبث بها بطريقة تعطل الأعيان التي لا غنى عنها لبقاء السكان المدنيين، مثل منشآت مياه الشرب وشبكات الري.[143]

ومع ذلك، من المهم توضيح مدى حماية البيانات المدنية من خلال القواعد العامة القائمة بشأن سير الأعمال العدائية. وعلى وجه الخصوص، نشأ الجدل حول ما إذا كانت البيانات تشكل أهدافًا على النحو المفهوم بموجب القانون الدولي الإنساني، وفي هذه الحالة تخضع العمليات السيبرانية على البيانات (مثل حذفها) لمبادئ التمييز والتناسب والاحتياطات والحماية التي توفرها للأعيان المدنية.[144]

ترتبط هذه المسألة ارتباطًا وثيقًا بالمناقشات المبينة آنفًا حول مفهوم "الهجوم". بادئ ذي بدء، إذا حُذفت البيانات أو جرى التلاعب بها بطريقة يُقصد بها أو يُتوقع منها أن تسبب، بشكل مباشر أو غير مباشر، وفاة أو إصابة شخص، أو إلحاق الضرر (بسبل منها، من وجهة نظرنا، التعطيل) بعين مادية، فإن العملية تشكل هجومًا بغض النظر عما إذا كانت البيانات نفسها تشكل أعيانًا في إطار أغراض القانون الدولي الإنساني. وهذا صحيح لأن عواقب أي عملية تستهدف البيانات يمكن أن تصنف تلك العملية على أنها هجوم بموجب القانون الدولي الإنساني وبالتالي تخضع لأحكام القانون الدولي الإنساني ذات الصلة. وبالنسبة لهذه الهجمات، لا يهم ما إذا كانت البيانات تُصنف أو لا تصنف كعين بموجب القانون الدولي الإنساني.

142 انظر: المناقشة في القسم المعنون أعلاه "قواعد القانون الدولي التي تحمي الأعيان التي لا غنى عنها لبقاء السكان المدنيين".

143 البروتوكول الإضافي الأول، المادة 54؛ والبروتوكول الإضافي (الثاني) لاتفاقيات جنيف المؤرخة 12 آب/أغسطس 1949، المتعلق بحماية ضحايا المنازعات المسلحة غير الدولية،609 UNTS 1125، 8 حزيران/يونيو 1977 (دخل حيز النفاذ في 7 كانون الأول/ديسمبر 1978) (البروتوكول الإضافي الثاني)، المادة 14؛ ودراسة اللجنة الدولية للقانون العرفي، الحاشية 63 أعلاه، القاعدة 54.

144 انظر: دليل تالين 2، الحاشية 13 أعلاه، الفقرتان 6-7 من شرح القاعدة 100. للاطلاع على مناقشة أكاديمية، انظر: ***Israel Law Review***, Vol. 48, No. 1, pp. 39-132

وانظر: M. N. Schmitt، الحاشية 67 أعلاه.

ومن ناحية أخرى، فإن المسألة المتعلقة بما إذا كانت البيانات تشكل أعيانًا في إطار أغراض القانون الدولي الإنساني هي مسألة بالغة الأهمية للعمليات التي لا يُقصد بها أو يُتوقع منها أن تسبب نتائج من هذا القبيل. وعمومًا، يمكن النظر في نهجين عامين. بموجب النهج الأول، الذي يعتبر البيانات أعيانًا بموجب القانون الدولي الإنساني، فإن العملية التي يُقصد بها أو يُتوقع منها أن تؤدي إلى حذف البيانات أو التلاعب بها ستشكل هجومًا تحكمه جميع قواعد القانون الدولي الإنساني ذات الصلة لأنها تصل إلى حد أو إتلاف عين (البيانات). ويصح ذلك أيضًا إذا لم يُتوقع أن يتسبب هذا الحذف أو التلاعب في وفاة أو إصابة شخص أو إتلاف أو تعطيل عين مادية. ومن ناحية أخرى، حتى في ظل هذا الرأي، فإن العملية التي يقتصر هدفها على الوصول إلى بيانات (قد تكون سرية) دون حذفها أو التلاعب بها - مثل التجسس - لن تشكل هجومًا.

في المقابل، إذا لم تكن البيانات تعتبر أعيانًا بموجب القانون الدولي الإنساني، فإن العملية التي تهدف إلى حذفها أو التلاعب بها دون التسبب في وفاة أو إصابة شخص أو إلحاق ضرر بعين لن تخضع لقواعد الهجمات، أو بعض القواعد الأخرى العامة التي توفر الحماية للأعيان المدنية (مثل الالتزام بالحرص الدائم على تجنب إصابة المدنيين والأعيان المدنية، على النحو المبين أدناه في القسم المعنون "القواعد التي تحكم العمليات العسكرية بخلاف الهجمات"). فالعمليات يمكن أن تخضع، من ناحية أخرى، لنظم حماية معينة بموجب القانون الدولي الإنساني، سيرد تحليلها في الأجزاء التالية في القسم المعنون "قواعد القانون الدولي التي تحمي الأعيان التي لا غنى عنها لبقاء السكان المدنيين والخدمات الطبية وعمليات الإغاثة الإنسانية". ومع ذلك، ستكون هناك ثغرة في حماية البيانات المدنية الأساسية التي لا تستفيد من نظام حماية محدد، وهذا من شأنه أن يثير القلق.

والخبراء لديهم وجهات نظر مختلفة حول ما إذا كانت البيانات تعتبر أعيانًا في إطار أغراض قواعد القانون الدولي الإنساني بشأن سير الأعمال العدائية.[145] فثمة رأي يذهب إليه أغلب الخبراء المشاركين في عملية صياغة دليل تالين، ومفاده أن المعنى العادي للمصطلح "عين" على النحو المبين في شرح اللجنة الدولية للبروتوكول الإضافي الأول الذي أصدرته في عام 1987، لا يمكن أن يُفسر على أنه يشمل البيانات لأن الأعيان تكون مادية ومرئية وملموسة.[146] ومع ذلك، فإن الشرح المتصل بالموضوع الوارد في شرح اللجنة الدولية يهدف إلى التمييز بين الأعيان ومفاهيم مثل "الهدف" أو "الغرض"، وليس التفريق بين الأعيان الملموسة وغير الملموسة، وبالتالي لا يمكن اعتباره عاملاً حاسمًا للنقاش حول البيانات.[147] في المقابل، دفع آخرون بأنه ينبغي اعتبار كل أنواع البيانات أو بعضها أعيانًا بموجب القانون الدولي الإنساني. وذهب رأي

145 للاطلاع على توضيح لهذه المناقشات، انظر:
"Scenario 12: Cyber Operations against Computer Data", in **K. Mačák, T. Minárik and T. Jančárková (eds)**, الحاشية 68 أعلاه.

146 يعرف قاموس أكسفورد العين بأنها "شيء مادي يمكن رؤيته ولمسه". وبالإشارة إلى المعنى العادي لكلمة "عين"، يصف شرح اللجنة الدولية لعام 1987 للبروتوكولين الإضافيين العين على أنها "شيء مرئي وملموس". شرح اللجنة الدولية للبروتوكولين الإضافيين، الحاشية 110 أعلاه، الفقرة 2008. انظر أيضًا: دليل تالين 2، الحاشية 13 أعلاه، الفقرة 6 من شرح القاعدة 100. ومن المثير للاهتمام أن نلاحظ هنا أن قاموس أكسفورد يتضمن اليوم تعريفًا محددًا للأعيان المستخدمة في الحوسبة: "بناء من البيانات يوفر وصفًا لأي شيء معروف يتصل بجهاز كمبيوتر (مثل المعالج أو جزء من التعليمات البرمجية) ويحدد طريقة تشغيله."

147 انظر أيضًا:
International Law Association (ILA) Study Group on the Conduct of Hostilities in the 21st Century, "The Conduct of Hostilities and International Humanitarian Law: Challenges of 21st Century Warfare", ***International Law Studies***, **Vol. 93, 2017 (ILA Report), pp. 338-339.**

إلى أن "المعنى الحديث" لمفهوم الأعيان في مجتمع اليوم، وتفسير المصطلح في ضوء موضوعه والغرض منه، يجب أن يؤدي إلى استنتاج مفاده أن "البيانات تشكل 'عينًا' في إطار أغراض قواعد القانون الدولي الإنساني بشأن الاستهداف".[148] وهذا التفسير مدعوم بالفهم التقليدي لمفهوم "العين" بموجب القانون الدولي الإنساني، وهو مفهوم أوسع نطاقًا من المعنى العادي للكلمة ويشمل أيضًا المواقع والحيوانات. وثمة اقتراح آخر هو التمييز بين "البيانات على المستوى التشغيلي"، أو "الرمز"، و "البيانات على مستوى المحتوى".[149] ويرى البعض في هذا النموذج أن البيانات على المستوى التشغيلي على وجه الخصوص قد تعتبر هدفًا عسكريًا، وهو ما يعني ضمنًا أن هذا النوع من البيانات يمكن أن يُعتبر أيضًا عينًا مدنية.[150] وأثناء النظر في البيانات التشغيلية باعتبارها أعيانًا تتماشى مع وجهة النظر المبينة أعلاه التي تذهب إلى أن تعطيل الأعيان يشكل هجومًا، يتبين على ما يبدو أنها لا توفر حماية إضافية. وفي هذه المناقشة، رأى البعض أن الاستنتاجات المقترحة ليس فيها أي فكرة مرضية تمامًا، فكل منها إما أنه يفتقر إلى الشمول أو مفرط في الشمول.[151]

شددت اللجنة الدولية، من جانبها، على ضرورة حماية البيانات المدنية الأساسية، مؤكدة أن حذف البيانات أو التلاعب بها في الفضاء السيبراني يمكن أن يؤدي إلى توقف تام للخدمات الحكومية والشركات الخاصة، وبالتالي يمكن أن يتسبب في ضرر للمدنيين أكبر من تدمير الأعيان المادية. وبالتالي، ترى اللجنة الدولية أنه يبدو من الصعب التوفيق بين الاستنتاج القائل بأن هذا النوع من العمليات لا يحظره القانون الدولي الإنساني في عالم اليوم الأكثر اعتمادًا على الفضاء السيبراني، وأهداف وأغراض هذه المجموعة من القواعد.[152] ومن الناحية المنطقية، لا ينبغي أن تؤدي الاستعاضة عن الملفات والمستندات الورقية ببيانات رقمية إلى تقليل الحماية التي يوفرها القانون الدولي الإنساني لها.[153] وقد أكدت اللجنة الدولية أن "استبعاد البيانات المدنية الأساسية من نطاق الحماية التي يوفرها القانون الدولي الإنساني للأعيان المدنية من شأنه أن يؤدي إلى فجوة خطيرة في الحماية".[154]

148 Kubo Mačák, "Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law", *Israel Law Review*, Vol. 48, No. 1, 2015, p. 80; Robert McLaughlin, "Data as a Military Objective", Australian Institute of International Affairs, 20 September 2018, available at: www.internationalaffairs.org.au/australianoutlook/data-as-a-military-objective/.

149 بموجب التمييز المقترح، قد تتضمن البيانات على مستوى المحتوى بيانات "من قبيل نص هذا المقال أو محتويات قواعد البيانات الطبية وفهارس المكتبات وما إلى ذلك"، في حين أن البيانات على المستوى التشغيلي تصف في "الأساس" 'روح الجهاز'"، أي "نوع البيانات التي تمنح الأجهزة وظائفها وقدرتها على أداء المهام التي نطلبها".
Heather Harrison Dinniss, "The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives", *Israel Law Review*, Vol. 48, No. 1, 2015, p. 41.

150 المرجع نفسه، الصفحة 54.

151 لذلك يرى شميت أن الدول، من الناحية السياساتية، ينبغي لها أن "تولي حماية خاصة إلى 'الوظائف أو الخدمات المدنية الأساسية' من خلال الالتزام بالامتناع عن إجراء عمليات سيبرانية تستهدف البنية التحتية المدنية أو البيانات تؤدي إلى تعطيلها". M. N. Schmitt، الحاشية 67 أعلاه، الصفحة 342.

152 تقرير التحديات الصادر عن اللجنة الدولية لعام 2015، الحاشية 118 أعلاه، الصفحة 43.

153 تقرير التحديات الصادر عن اللجنة الدولية لعام 2019، الحاشية 36 أعلاه، الصفحة 21.

154 اللجنة الدولية، الحاشية 1 أعلاه، الصفحة 8. وانظر أيضًا: P. Pascucci، الحاشية 67 أعلاه، الذي يشير إلى أن الموقف الذي اتخذه غالبية الخبراء في دليل تالين فيما يتعلق بالبيانات يوجد "فجوة واسعة على ما يبدو بشأن ما يشكل عينًا" ثم يدفع لاحقًا بأنه "من غير الواقعي في عصر المعلومات أن تقع البيانات خارج نطاق ما يشكل عينًا، الأمر الذي يؤدي من ثم إلى الإخفاق في تلقي الحماية التي يوفرها القانون الدولي الإنساني المرتبطة بمبدأ التمييز ومبدأ التناسب".

أعرب عدد قليل من الدول حتى الآن عن رأيها بشأن ما إذا كان ينبغي فهم مفهوم "العين" على أنه يشمل البيانات وذلك في إطار القواعد التي تحكم سير الأعمال العدائية. فعلى سبيل المثال، يرى الدليل العسكري الدنماركي أن "البيانات (الرقمية) لا تشكل عمومًا عينًا".[155] وفي المقابل يذهب الدليل العسكري النرويجي إلى أن البيانات ينبغي اعتبارها أعيانًا ولا يجوز أن تتعرض للهجوم المباشر إلا إذا كان تصنف على أنها هدف قانوني.[156] وأعربت فرنسا عما يمكن اعتباره وجهة نظر وسطية حيث أشارت إلى أنه "نظرًا للحالة الراهنة للاعتماد على التقنيات الرقمية، فإن بيانات المحتوى (مثل البيانات المدنية أو المصرفية أو الطبية وغيرها) محمية بموجب مبدأ التمييز".[157] ويبدو أن وصف موقف بيرو في تقرير تحسين الشفافية الصادر عن منظمة الدول الأمريكية يعكس موقفًا مشابهًا: بينما لم تتخذ بيرو موقفًا صريحًا بشأن ما إذا كانت البيانات تعتبر أعيانًا، يُفسر موقفها على أنه يقيم العمليات مقابل البيانات بموجب مفهوم "الهدف العسكري"، مشيرة إلى أن بعض نظم البيانات قد لا تتعرض للهجمات لأن هذه الهجمات "لن توجد ميزة عسكرية مشروعة".[158] نظرًا لأن تعريف "الأهداف العسكرية" بموجب المادة 52 (2) من البروتوكول الإضافي الأول ينطبق "بقدر ما يتعلق الأمر بالأعيان"، فإن هذه الفكرة تعني ضمنيًا على ما يبدو أن البيانات تشكل أعيانًا. وتقترح شيلي النظر في الآثار التي يخلفها الهجوم على البيانات وخلصت إلى أنه "يجب من ثم مراعاة مبدأ التمييز في سياق العمليات السيبرانية، وبموجبه ينبغي للدولة أن تمتنع عن مهاجمة البيانات في حالة كان ذلك يؤثر على السكان المدنيين". وتفيد التقارير أن شيلي أكدت أيضًا على أن "الهجوم الموجه حصريًا إلى بيانات الكمبيوتر قد يؤدي إلى عواقب وخيمة تؤثر على السكان المدنيين".[159]

وفي عالم يتزايد اعتماده على البيانات، ستكون مسألة كيفية تفسير الدول لقواعد القانون الدولي الإنساني وتطبيقها لحماية البيانات الأساسية من التدمير أو الحذف أو التلاعب اختبارًا أساسيًا لمدى ملاءمة قواعد القانون الإنساني الحالية.

حماية البنية التحتية السيبرانية التي تخدم الأغراض العسكرية والمدنية في آن واحد

من أجل حماية البنية التحتية المدنية الحيوية التي تعتمد على الفضاء السيبراني، من الضروري أيضًا حماية البنية التحتية للفضاء السيبراني نفسه. لكن التحدي يكمن في الترابط بين الشبكات المدنية والعسكرية. فمعظم الشبكات العسكرية تعتمد على البنية التحتية السيبرانية المدنية، مثل كابلات الألياف الضوئية تحت سطح البحر أو الأقمار الاصطناعية أو أجهزة التوجيه أو العُقد. وتُجهز المركبات المدنية وأنشطة الشحن ومراقبة الحركة الجوية بشكل متزايد بمعدات الملاحة التي تعتمد على الأقمار الاصطناعية لنظام الملاحة عبر الأقمار الاصطناعية (GNSS) مثل بايدو (BeiDou) وغلوناس (GLONASS) والنظام العالمي لتحديد المواقع (GPS) وغاليليو (Galileo)، وهي نظم قد يستخدمها الجيش أيضًا. وتستخدم سلاسل التوريد اللوجستية المدنية (للأغذية والإمدادات الطبية) والشركات الأخرى نفس شبكات الإنترنت والاتصالات التي

155 الدليل العسكري الدنماركي، الحاشية 118 أعلاه، الصفحة 292.
156 الدليل العسكري النرويجي، الحاشية 118 أعلاه، الصفحة 9-58.
157 وزارة الجيوش الفرنسية، الحاشية 77 أعلاه، الصفحة 14.
158 منظمة الدول الأمريكية، الحاشية 22 أعلاه، الفقرة 49، الحاشية 115.
159 المرجع نفسه، الفقرة 48.

تمر عبرها بعض الاتصالات العسكرية. وباستثناء بعض الشبكات المخصصة تحديدًا للاستخدام العسكري، من المستحيل إلى حد كبير التمييز بين البنى التحتية السيبرانية المدنية البحتة والعسكرية البحتة.

بموجب القانون الدولي الإنساني، يجب أن تقتصر الهجمات بشكل صارم على الأهداف العسكرية. وفيما يتعلق بالأعيان، تقتصر الأهداف العسكرية على الأهداف التي تسهم، بحكم طبيعتها أو موقعها أو غايتها أو استخدامها، مساهمة فعالة في العمل العسكري، ويحقق تدميرها التام أو الجزئي أو الاستيلاء عليها أو تعطيلها في الظروف السائدة حينذاك ميزة عسكرية أكيدة. وجميع الأعيان التي ليست أهدافًا عسكرية بموجب هذا التعريف هي أعيان مدنية بموجب القانون الدولي الإنساني ويجب ألا تكون هدفًا لهجوم أو أعمال انتقامية. وإذا ثار الشك حول ما إذا كانت عين ما تكرس عادةً لأغراض مدنية إنما تستخدم في تقديم مساهمة فعالة للعمل العسكري، فإنه يفترض أن تظل محمية بوصفها عينًا مدينة.[160]

ودرج الفهم على أن العين قد تتحول إلى هدف عسكري عندما يفي استخدامها للأغراض العسكرية بتعريف الهدف العسكري، ولو استخدمت في نفس الوقت لأغراض مدنية. وقد يؤدي التفسير الواسع لهذه القاعدة إلى استنتاج مفاده أن العديد من الأعيان التي تشكل جزءًا من البنية التحتية للفضاء السيبراني قد تشكل أهدافًا عسكرية وبالتالي لن تكون محمية من الهجوم، سواء أكان سيبرانيًا أم حركيًا. وقد يكون هذا مصدر قلق بالغ بسبب الاعتماد المدني المتزايد باستمرار على الفضاء السيبراني.

غير أن هذا الاستنتاج سيكون ناقصًا. أولًا، لا يمكن إجراء تحليل للتوقيت الذي تتحول فيه عين مدنية إلى هدف عسكري في سياق الفضاء السيبراني أو شبكة الإنترنت عمومًا. وبدلًا من ذلك، يجب على الأطراف المتحاربة تحديد أجهزة الكمبيوتر أو العقد أو أجهزة التوجيه أو الشبكات التي قد تكون هدفًا عسكريًا. وفي هذا الصدد، يجب أن تُحلل على حدة أجزاء الشبكة أو أجهزة الكمبيوتر المحددة أو الأجهزة الأخرى التي يمكن فصلها عن شبكة أو نظام ككل. يجب أن تتيح الوسائل والأساليب المستخدمة توجيه الهجوم نحو الهدف (الأهداف) العسكرية المحددة التي ربما تم تحديدها، ويجب اتخاذ جميع الاحتياطات الممكنة لتجنب التأثير العرضي على الأعيان المدنية أو أجزاء الشبكة المتبقية أو على الأقل الحد منها إلى أدنى حد.[161] ويرى البعض أيضًا أنه يُحظر التعامل مع عدد من الأهداف العسكرية السيبرانية المنفصلة بوضوح في البنية التحتية السيبرانية المستخدمة في المقام الأول لأغراض مدنية باعتبارها هدفًا واحدًا، إذا كان القيام بذلك سيلحق الضرر بالأشخاص أو الأعيان المشمولين بالحماية.[162] ثانيًا، الفضاء السيبراني مصمم بمستوى عال من التكرار، وهذا يعني أن من خصائصه القدرة على إعادة توجيه حركة البيانات بشكل فوري. ويجب مراعاة هذه المرونة الداخلية عند تقييم ما إذا كان تدمير الهدف أو تعطيله سيوفر ميزة عسكرية أكيدة كما يقتضي ذلك تعريفُ الهدف العسكري. فإذا لم يكن هذا صحيحًا، فستظل العين مدنية ولا يجوز مهاجمتها. وثالثًا، يخضع أي هجوم للحظر

160 انظر: البروتوكول الإضافي الأول، المادة 52. دراسة اللجنة الدولية للقانون العرفي، الحاشية 63 أعلاه، القواعد 7-10.
161 انظر: البروتوكول الإضافي الأول، المادة 51 (4)، و57 (2) ’2‘ (أ)؛ ودراسة اللجنة الدولية للقانون العرفي، الحاشية 63 أعلاه، القواعد 12-17.
162 انظر: دليل تالين 2، الحاشية 13 أعلاه، القاعدة 112 المستمدة من الحظر المفروض على قصف المناطق المنصوص عليه في المادة 51 (5) (أ) من البروتوكول الإضافي الأول والقانون الدولي الإنساني العرفي (انظر: دراسة اللجنة الدولية للقانون العرفي، الحاشية 63 أعلاه، القاعدة 13).

المفروض على الهجمات العشوائية وقاعدتي التناسب والاحتياطات في الهجوم. ومن شأن إيقاف أو تعطيل الاستخدام المدني لعين ما، بما يشكل انتهاكًا لإحدى هذه القواعد، أن يحول الهجوم إلى هجوم غير قانوني رغم أن العين تحولت إلى هدف عسكري.[163]

مقارنة بالعمليات العسكرية الحركية، قد يؤدي استخدام العمليات السيبرانية، حسب الظروف، إلى التمكين من تحقيق تأثير معين مع إحداث دمار أقل (على الهدف أو بشكل عرضي على أعيان أو نظم أخرى) أو إحداث ضرر يمكن إصلاحه أو استعادته بسهولة أكبر. وهذا الاعتبار مهم للغاية في سياق الأعيان ذات الاستخدام المزدوج، كما يتضح من سيناريو طرف محارب يحاول تعطيل مخبأ قيادة تحت الأرض تابع للعدو عن طريق قطع إمداد الكهرباء الذي يوفر في الوقت نفسه الطاقة للبنية التحتية المدنية. وقد تسمح العملية السيبرانية للمشغل بالقيام عن بعد باختيار أجزاء الشبكة التي سيتم إيقاف تشغيلها.[164] وقد يمكن ذلك المهاجم من تحقيق التأثير المطلوب مع تجنب الآثار الضارة التي تلحق بتوصيل الكهرباء إلى المدنيين أو على الأقل التقليل منها إلى أدنى حد. وفي هذه الحالة، وبشرط أن يكون اختيار استخدام عملية سيبرانية بدلًا من عملية حركية أمرًا ممكنًا، يصبح تنفيذ العملية السيبرانية أمرًا مطلوبًا بمقتضى مبدأ الاحتياط. وفي الواقع، فإن الالتزام باتخاذ جميع الاحتياطات الممكنة في تخير وسائل وأساليب الحرب لتجنب الأضرار المدنية العرضية أو على الأقل التقليل منها إلى أدنى حد[165] هو إجراء محايد من الناحية التقنية: فهو ينطبق أيضًا على الوسائل والأساليب التي تعتمد على التقنيات الجديدة، بل وقد يقتضي استخدامها.[166] وتتوقف إمكانية ذلك على الظروف السائدة في ذلك الوقت، ومنها الاعتبارات الإنسانية والعسكرية.[167]

القيود المفروضة على العمليات السيبرانية بخلاف العمليات التي تصل إلى حد "الهجمات"، بما في ذلك الحماية الخاصة لبعض الأشخاص والأعيان

في حين أن العديد من القواعد العامة المتعلقة بسير الأعمال العدائية تقتصر على الأعمال التي تصل إلى حد الهجمات على النحو المحدد في القانون الدولي الإنساني، فإن بعض قواعد القانون الدولي الإنساني التي تحكم سير الأعمال العدائية تنطبق على مجموعة أوسع من العمليات: أولًا، تنطبق بعض القواعد على جميع "العمليات العسكرية" وثانيًا، تتجاوز الحماية الخاصة الممنوحة لفئات معينة من الأشخاص والأعيان نطاق الحماية من الهجمات.

163 مع الإقرار بوجود وجهة نظر أخرى أيضًا، اعتبر فريق الدراسة التابع لرابطة القانون الدولي المعني بسير الأعمال العدائية أن هذا "رأي أفضل" استنادًا إلى ممارسة الدول والوثائق الرسمية والمبادئ: انظر: تقرير رابطة القانون الدولي، الحاشية 147 أعلاه، الصفحتان 336-337. انظر أيضًا:
ICRC, *International Expert Meeting Report: The Principle of Proportionality in the Rules Governing the Conduct of Hostilities under International Humanitarian Law*, Geneva, 2018, p. 39, available at www.icrc.org/en/document/international-expert-meeting-report-principle-proportionality; Helen Durham, Keynote Address, in Edoardo Greppi (ed.), *Conduct of Hostilities: The Practice, the Law and the Future*, 37th Round Table on Current Issues of International Humanitarian Law, International Institute of Humanitarian Law, Sanremo, 2015, p. 31.

164 أشارت بعض التقارير إلى حدوث ذلك في العمليات السيبرانية التي استهدفت شبكة الكهرباء في أوكرانيا في عام 2015. انظر:
Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid", *Wired*, 3 March 2016, available at: www.wired.com/201603//inside-cunning-unprecedented-hack-ukraines-power-grid/.

165 انظر: البروتوكول الإضافي الأول، المادة 57 (2) (أ) ('2')؛ ودراسة اللجنة الدولية للقانون العرفي، الحاشية 63 أعلاه، القاعدة 17.

166 انظر: تقرير رابطة القانون الدولي، الحاشية 147 أعلاه، الصفحة 384.

167 في حين قد تشمل الاعتبارات العسكرية "هشاشة" الوسائل والطرق السيبرانية، فهي ليست العامل الوحيد المناسب الذي يحدد الإمكانية. وليس من الممكن استبعاد أن يكون من الممكن، وبالتالي مطلوبًا، استخدام العمليات السيبرانية لتجنب الأضرار المدنية العرضية أو على الأقل التقليل منها إلى أدنى حد، على أساس وحيد هو أن الوسائل أو الأساليب السيبرانية المستخدمة "هشة"، دون النظر إلى مجمل الحالة بما في ذلك جميع الاعتبارات الإنسانية ذات الصلة.

القواعد التي تحكم العمليات العسكرية بخلاف الهجمات

ثمة مسألة تحتاج إلى المزيد من الاهتمام، ألا وهي تحديد، وربما توضيح، القواعد التي توفر حماية عامة للسكان المدنيين والأعيان المدنية من آثار العمليات السيبرانية التي لا تصل إلى حد الهجمات. وهذا أمر بالغ الأهمية إذا أخذنا بالرأي الذي مفاده أن العمليات التي تسبب ضررًا ماديًا هي فقط التي تعتبر هجمات: وفي هذه الحالة، ستكون هناك فئة واسعة إلى حد ما من العمليات السيبرانية التي لا تنطبق عليها سوى مجموعة محدودة من قواعد القانون الدولي الإنساني. ومن شأن هذا الاستنتاج أن يسبب قلقًا حقيقيًا بشأن حماية المدنيين والبنية التحتية المدنية.

يظهر مفهوم "العملية العسكرية" في عدد من مواد اتفاقيات جنيف لعام 1949 وبروتوكوليّها الإضافيين لعام 1977.[168] الأمر الأهم هنا هو القواعد التي تنظم سير العمليات العسكرية، ومنها العمليات التي تُنفذ باستخدام وسائل سيبرانية. وهي تشمل القاعدة الأساسية التي تنص على أن "أطراف النزاع ... توجه عملياتها ضد الأهداف العسكرية دون غيرها" (البروتوكول الإضافي الأول، المادة 48)، والمبدأ القائل بأن "السكان المدنيون والأشخاص المدنيون يتمتعون بحماية عامة ضد الأخطار الناجمة عن العمليات العسكرية" (البروتوكول الإضافي الأول، المادة 51 (1))،[169] والالتزام بضرورة بذل "رعاية متواصلة من أجل تفادي السكان المدنيين والأشخاص والأعيان المدنية" في إدارة العمليات العسكرية (البروتوكول الإضافي الأول، المادة 57 (1)).[170]

يؤدي المعنى العادي لمصطلح "العملية العسكرية" والتفسير المنهجي لهذه المواد إلى استنتاج مفاده أن هذا المفهوم يختلف عن مفهوم "الهجوم" على النحو المحدد في المادة 49 من البروتوكول الإضافي الأول.[171] ويشير شرح اللجنة الدولية للمادة 48 من البروتوكول الإضافي الأول إلى أن المفهوم يشير إلى العمليات العسكرية التي يستخدم فيها العنف، وليس إلى الحملات الأيديولوجية أو السياسية أو الدينية، إلا أنه يوضح أنه مفهوم أوسع نطاقًا من "الهجمات". ويُعرِّف الشرح "العمليات العسكرية" في إطار أغراض هذه المواد على أنها "أي تحركات ومناورات وأنشطة أخرى أيًا كان نوعها تقوم بها القوات المسلحة بهدف القتال" أو "تتعلق بالأعمال العدائية" - وهو فهم مقبول على نطاق واسع.[172]

168 انظر: اتفاقية جنيف الثالثة، المادة 23؛ واتفاقية جنيف الرابعة، المادة 28؛ والبروتوكول الإضافي الأول، المواد 3 و 39 و 44 و 51 و 56-60؛ والبروتوكول الإضافي الثاني، المادة 13.

169 انظر أيضًا: البروتوكول الإضافي الأول، المادة 58؛ والبروتوكول الإضافي الثاني، المادة 13 (1).

170 انظر: دراسة اللجنة الدولية للقانون العرفي، الحاشية 63 أعلاه، القاعدة 15؛ ودليل تالين 2، الحاشية 13 أعلاه، القاعدة 114.

171 التفسير الذي يستوعب مفهومي "العملية" و "الهجوم" من شأنه أن ينزع عن القواعد المطبقة على "العمليات" المحتوى الهادف وأن يحولها إلى قواعد زائدة عن الحاجة في الأساس. انظر: سي. دروغيه، الحاشية 83 أعلاه، الصفحة 556.

172 شرح اللجنة الدولية للبروتوكولين الإضافيين، الحاشية 110 أعلاه، الفقرات 2191 و 1936 و 1875. وفي السياق نفسه، انظر:
Michael Bothe, Karl Josef Partsch and Waldemar A. Solf, *New Rules for Victims of Armed Conflict: Commentary on the Two 1977 Protocols Additional to the Geneva Conventions of 1949*, Martinus Nijhoff, Leiden, 2013, para. 2.2.3 on Art. 48, para. 2.8.2 on Art. 57;

وانظر: وزارة الدفاع بالمملكة المتحدة، دليل الخدمة المشتركة لقانون النزاع المسلح، منشور الخدمة المشتركة 383، 2004 (الدليل العسكري للمملكة المتحدة)، الفقرة 5-32، الحاشية 187؛ وتقرير رابطة القانون الدولي، الحاشية 147 أعلاه، الصفحة 380. يطبق دليل برنامج السياسة الإنسانية وأبحاث النزاعات بشأن أحكام القانون الدولي المنطبقة على الحرب الجوية والصاروخية (برنامج السياسة الإنسانية وأبحاث النزاعات، جامعة هارفارد 2009) الالتزام ببذل العناية المتواصلة على "العمليات القتالية الجوية أو الصاروخية" (القاعدة 34)، وهو مفهوم أوسع نطاقًا من مفهوم "الهجوم" الذي يشمل جملة أمور منها التزود بالوقود، والتشويش على رادارات العدو، واستخدام أجهزة الإنذار المحمولة جوًا والإبرار الجوي (شرح القاعدة 1 (ج)،

يُناقش المفهوم غالبًا في سياق الالتزام التعاهدي والعرفي بتوخي الحرص الدائم، في إدارة العمليات العسكرية على تفادي إصابة السكان المدنيين، والأشخاص المدنيين، والأعيان المدنية. وذكرت فرنسا صراحة أن هذا الالتزام ينطبق أيضًا في الفضاء السيبراني.[173] يقتضي هذا الالتزام من جميع المشاركين في العمليات العسكرية أن يضعوا في اعتبارهم باستمرار آثار العمليات العسكرية على السكان المدنيين والأشخاص المدنيين والأعيان المدنية، وأن يتخذوا خطوات لتقليل تلك الآثار قدر الإمكان وأن يسعوا إلى تجنب أي آثار غير ضرورية.[174] وقد وُصف بأنه التزام إيجابي ومستمر يهدف إلى التخفيف من حدة المخاطر ومنع الضرر ويفرض متطلبات تزداد بما يتناسب مع المخاطر التي يتعرض لها المدنيون.[175] ويوضح دليل تالين في هذا الصدد أن

> القانون لا يعترف بأي حالة أو وقت يجوز فيه للأفراد المشاركين في عملية التخطيط والتنفيذ أن يتجاهلوا آثار عملياتهم على المدنيين والأعيان المدنية. ويتطلب ذلك في السياق السيبراني دراية بالأحوال في جميع الأوقات، وليس فقط أثناء المرحلة التحضيرية للعملية.[176]

أما المسألة الأصعب فهي تطبيق مبدأ التمييز على العمليات العسكرية بخلاف الهجمات. وكما ذُكر أعلاه، تتطلب المادة 48 من البروتوكول الإضافي الأول توجيه العمليات العسكرية ضد الأهداف العسكرية دون غيرها. وتؤكد الشروح التي قدمتها اللجنة الدولية وبوته وبارتش وسولفي[177] على الطابع الأساسي لهذه المادة، إلا أنها لا تسلط الكثير من الضوء على المعنى الدقيق لهذا الالتزام ونطاقه، الذي لا يزال موضع نقاش.

تُفهم المادة 48 أحيانًا على أنها مبدأ شامل يُنفذ من خلال تطبيق مختلف قواعد القسم الوارد في البروتوكول الإضافي الذي يفتتح به. لذلك، يرى بعض المعلقين أن القواعد المحددة المنبثقة عن مبدأ التمييز لا تنطبق إلا على الهجمات وليس على العمليات العسكرية بخلاف الهجمات.[178] وبناءً على ذلك، تنص بعض الأدلة العسكرية صراحةً على أن العمليات

الفقرة 3). انظر أيضًا:
Noam Neuman, "A Precautionary Tale: The Theory and Practice of Precautions in Attack", *Israel Yearbook on Human Rights,* Vol. 48, 2018, p. 28; Jean-François Quéguiner, "Precautions under the Law Governing the Conduct of Hostilities", International Review of the Red Cross, Vol. 88, No. 864, 2006, p. 797; Chris Jenks and Rain Liivoja, "Machine Autonomy and the Constant Care Obligation", Humanitarian Law and Policy, 11 December 2018, available at: https://blogs.icrc.org/law-and-policy/201811/12//machine-autonomy-constant-care-obligation/.

وتحديدًا في سياق العمليات السيبرانية، انظر دليل تالين 2، الحاشية 13 أعلاه، الفقرة 2 من شرح القاعدة 114 (التي تشير إلى أن مفهوم الأعمال العدائية الذي ينطبق عليه الالتزام ببذل العناية المتواصلة أوسع نطاقًا من مفهوم الهجمات)؛ H. Harrison Dinniss، الحاشية 124 أعلاه، الصفحة 199. للاطلاع على وجهة نظر مختلفة على الأقل في سياق مبدأ التمييز، انظر: M. Roscini، الحاشية 127، الصفحة 178.

173 وزارة الجيوش الفرنسية، الحاشية 77 أعلاه، الصفحة 15.

174 الدليل العسكري للمملكة المتحدة، الحاشية 172 أعلاه، الفقرة 5-32-1؛ ودليل تالين 2، الحاشية 13 أعلاه، الفقرة 4 من شرح القاعدة 114؛ Dieter Fleck, *The Handbook of International Humanitarian Law*, 3rd ed., Oxford University Press, Oxford, 2013, p. 199; N. Neuman, الحاشية 172 أعلاه، الصفحتان 28-29.

175 تقرير رابطة القانون الدولي، الحاشية 147 أعلاه، الصفحة 381.

176 دليل تالين 2، الحاشية 13 أعلاه، الفقرة 4 من شرح القاعدة 114.

177 M. Bothe, K. J. Partsch and W. A. Solf، الحاشية 172 أعلاه.

178 M. Roscini، الحاشية 126 أعلاه، الصفحة 178. انظر أيضًا، وإن جرى التعبير عنه بموجب القانون العرفي، دليل تالين 2، الحاشية 13 أعلاه، الفقرة 5 من شرح القاعدة 93؛ وانظر:
Michael N. Schmitt, "'Attack' as a Term of Art in International Law: The Cyber Operations Context", in Christian Czosseck, Rain Ottis and Katharina Ziolkowski (eds), *4th International Conference on Cyber Conflict: Proceedings*, NATO CCD COE Publications, Tallinn, 2012, pp. 283-293, 289-290.

السيبرانية بخلاف الهجمات قد تكون موجهة ضد المدنيين أو الأعيان المدنية.[179] وقد يبدو من الصعب التوفيق بين هذا التأكيد والمادة 48 بالنسبة للدول الأطراف في البروتوكول، أو على الأقل سيحتاج إلى توضيحه بدقة. وفي الواقع، أشار الخبراء إلى أنه "رغم... وجود فرق بين العمليات العسكرية والهجمات، فهذا لا يعني أن الهجمات غير العنيفة على شبكات الكمبيوتر يمكن بالتالي شنها ضد أعيان مدنية".[180] وينبع هذا الاستنتاج من قواعد تفسير المعاهدات التي تتطلب تفسير الأحكام على أنها "ذات محتوى مفيد وليست زائدة عن الحاجة".[181]

وكما ذُكر أعلاه، تُفهم "العمليات العسكرية" على أنها أي تحركات ومناورات وأنشطة أخرى أيًا كان نوعها تقوم بها القوات المسلحة بهدف القتال" أو "المتعلقة بالأعمال العدائية. والمناورة جزء لا يتجزأ من العمليات السيبرانية.[182] فعلى سبيل المثال، قد يكون إنشاء إمكانية الوصول عن بُعد لنظام أو جهاز خطوة نحو الوصول إلى نظام أو جهاز آخر أو مهاجمته.[183] وبافتراض أن النظام أو الجهاز الأول مدني بطبيعته والثاني هدف عسكري، فقد يثور السؤال حول ما إذا كان إنشاء الوصول إلى النظام أو الجهاز المدني سيشكل عملية عسكرية محظورة. ويرى مؤلفو هذا المقال أن هذا السيناريو لا يتعارض على ما يبدو مع المادة 48، شريطة ألا يتضرر أو يتعطل النظام أو الجهاز المدني أثناء العملية، لأن العملية موجهة في نهاية المطاف إلى هدف عسكري.[184] ويمكن بالفعل تقييم هذه العمليات السيبرانية بنفس طريقة تقييم العمليات العسكرية التقليدية - على سبيل المثال، عندما يتحرك جندي كوماندو عبر منزل مدني لمهاجمة هدف عسكري يقع خلفه. ومع ذلك، تظل الالتزامات الأخرى ذات صلة، مثل الالتزام بتوخي الحرص الدائم على تجنب إصابة الأعيان المدنية.

ويرى المؤلفون أن المادة 48 يجب أن تُفسر، وحدها أو بالاقتران مع المادتين 51 (1) و57 (1) من البروتوكول الإضافي الأول على أنها تحظر العمليات الإلكترونية التي تهدف فقط إلى تعطيل خدمات الإنترنت للسكان المدنيين ولو كانت هذه العمليات السيبرانية لا تؤدي إلى تعطيل الأعيان أو تفضي من ناحية أخرى إلى تبعات تؤدي إلى تصنيفها كهجمات. وأصبح الاستخدام المدني لشبكة الإنترنت اليوم واسع الانتشار لدرجة أن أي تفسير آخر سيخلف فجوة مهمة في الحماية التي يوفرها القانون الدولي الإنساني للمدنيين من آثار الأعمال العدائية التي تنفذ بوسائل سيبرانية.[185]

179 الدليل العسكري النرويجي، الحاشية 118 أعلاه، الفقرة 9-57. انظر أيضًا: دليل قانون الحرب الصادر عن وزارة الدفاع، الحاشية 87 أعلاه، الفقرة 2-5-16.

180 H. Harrison Dinniss، الحاشية 124 أعلاه، الصفحة 199.

181 انظر أيضًا: سي. دروغيه، الحاشية 83 أعلاه، الصفحة 556.

182 انظر على سبيل المثال:

US DoD, *Cyberspace Operations*, Joint Publication 3-12, 8 June 2018, p. xii: "Movement and Maneuver.

وتتيح عمليات الفضاء السيبراني إسقاط القوة دون الحاجة إلى إقامة وجود فعلي في أراضٍ أجنبية. وتنطوي المناورة في قسم شبكة معلومات وزارة الدفاع أو الفضاء السيبراني الأزرق [الصديق] على تحديد مواقع القوات وأجهزة الاستشعار ووسائل الدفاع لتوفير أفضل تأمين لمناطق الفضاء السيبراني أو الانخراط في الإجراءات الدفاعية على النحو المطلوب. والمناورة في الفضاء السيبراني الرمادي [المحايد] والأحمر [العدو] إجراء لاستغلال الفضاء السيبراني، وتنطوي على أنشطة من قبيل الوصول إلى الروابط والعُقد الخاصة بالخصم أو العدو أو الوسيط وتشكيل هذا الفضاء السيبراني لدعم الإجراءات المستقبلية".

183 L. Gisel and L. Olejnik (eds)، الحاشية 11 أعلاه، الصفحة 57.

184 قارن بـ H. Harrison Dinniss، الحاشية 124 أعلاه، الصفحة 201.

185 ناقش الخبراء الذين صاغوا دليل تالين ما إذا كان تعطيل جميع اتصالات البريد الإلكتروني في جميع أنحاء بلد أثناء نزاع مسلح يصل إلى حد الهجوم - وهو مفهوم أضيق من العمليات العسكرية. وترى مجموعة قليلة أن المجتمع الدولي سيعتبر هذه العملية عمومًا هجومًا، إلا أن الأغلبية ترى أن القانون الدولي الإنساني لا يمتد إلى هذا الحد في الوقت الراهن، غير أنها اعتبرت أن توصيف هذه العمليات على أنها هجمات يستند إلى أساس منطقي.

وكما تبين أعلاه، يرى البعض أنه ليست جميع العمليات السيبرانية التي تعطل الأعيان، أو تحذف البيانات أو تتلاعب بها، تشكل هجمات. ونتيجة لهذه التفسيرات، فإن نطاقًا أوسع بكثير من العمليات السيبرانية لن يخضع لقواعد الهجمات، بما فيها العمليات التي يترتب عليها احتمال كبير لوقوع الضرر. لذلك، من الأهمية بمكان لحماية السكان المدنيين أن يوضح من يفسرون مفهومي "الهجوم" و"الأعيان" تفسيرًا محدود النطاق ما إذا كانوا يرون أن العمليات السيبرانية التي تؤدي فقط إلى تعطيل الأعيان أو حذف البيانات تصل إلى حد "العمليات العسكرية"، ومدلول ذلك بالنسبة لتطبيق مبدأ التمييز على هذه العمليات - وعلى وجه الخصوص، ما تقتضيه المادة 48 من البروتوكول الإضافي الأول بأن تقوم أطراف النزاعات المسلحة "بتوجيه عملياتها ضد الأهداف العسكرية دون غيرها". فعلى سبيل المثال، يمكن على الأقل الإبقاء على مستوى معين من الحماية إذا قبل من يفسرون مفهوم "الهجوم" تفسيرًا محدود النطاق أن العملية السيبرانية التي تعطل الأعيان فقط هي "عملية عسكرية" ولذلك يجب أن توجه ضد الأهداف العسكرية دون غيرها.

وحتى العمليات السيبرانية التي لا تدخل في نطاق مفهوم "العملية العسكرية" كما يفهم في البروتوكول الإضافي الأول قد تخضع لبعض قواعد القواعد الدولي الإنساني المنبثقة من مبدأ التمييز. فعلى سبيل المثال، ذُكر أن "توجيه" عمليات نفسية أو أنواع أخرى من الدعاية إلى المدنيين لا ينتهك المادة 48 من البروتوكول الإضافي الأول لأن هذه العمليات لا تندرج ضمن معنى "العمليات العسكرية" كما تفهم في المادة 48.[186] ومع ذلك، فإن العمليات النفسية لا تقع خارج نطاق الحماية الذي توفره معايير القانون الدولي الإنساني الأخرى. فعلى سبيل المثال، يجب ألا تصل إلى حد الأعمال المحظورة أو التهديدات بالعنف التي يكون الغرض الأساسي منها بث الرعب بين السكان المدنيين أو تشجيع انتهاكات القانون الدولي الإنساني.[187]

قد تنبع القيود المفروضة على العمليات السيبرانية بخلاف الهجمات أيضًا من مبدأ الضرورة العسكرية. واعتمادًا على القاعدة العرفية التي تعود إلى قواعد لاهاي لعام 1907، ينص دليل قانون الحرب الصادر عن وزارة الدفاع الأمريكية على أن "العملية السيبرانية التي لا تشكل هجومًا، ولكنها مع ذلك ستؤدي إلى مصادرة أو تدمير ممتلكات العدو، يجب أن تمليها ضرورات الحرب".[188] ويشير الدليل أيضًا إلى الضرورة العسكرية بطريقة أكثر عمومية، ويقرر أن العمليات السيبرانية التي لا تصل إلى حد الهجوم "يجب ألا تكون موجهة ضد المدنيين أو الأعيان المدنية للعدو ما لم تكن العمليات ضرورية من الناحية العسكرية".[189] وبالمثل، تشير أستراليا إلى أن "قواعد القانون الدولي الإنساني المنطبقة تسري أيضًا على العمليات السيبرانية في نزاع مسلح التي لا تشكل أو تصل إلى حد 'الهجوم'، بما في ذلك مبدأ الضرورة العسكرية".[190] وهذه الإحالات إلى الضرورة العسكرية كمبدأ تقييدي موضع ترحيب، غير أن هناك حاجة إلى مزيد من الوضوح بشأن ما ينص عليه مبدأ الضرورة العسكرية تحديدًا عند تنفيذ عمليات سيبرانية.

دليل تالين 2، الحاشية 13 أعلاه، الفقرة 13 من شرح القاعدة 92.

186 سي. دروغيه، الحاشية 83 أعلاه، الصفحة 556.

187 تقرير التحديات الصادر عن اللجنة الدولية لعام 2019، الحاشية 36 أعلاه، الصفحتان 28-29.

188 دليل قانون الحرب الصادر عن وزارة الدفاع، الحاشية 87 أعلاه، الفقرة 16-5-1.

189 المرجع نفسه، الفقرة 16-5-2.

190 وزارة الشؤون الخارجية والتجارة الأسترالية، الحاشية 94 أعلاه، الصفحة 4.

توضح هذه المناقشة الموجزة أن العمليات السيبرانية بخلاف الهجمات ليست خارج نطاق التنظيم. ومن ناحية أخرى، لا يزال النظام القانوني الذي يحكم العمليات العسكرية غير مكتمل ويفتقر إلى الدقة ويفرض متطلبات أقل مقارنة بالنظام القانوني الذي يحكم العمليات التي تصل إلى حد الهجمات بموجب القانون الدولي الإنساني. ولمعالجة فجوة الحماية المذكورة ولو بعض الشيء على أقل تقدير، اقترح شميت أن تطبق الدول - من الناحية السياساتية- تقييمًا محدثًا للتناسب على العمليات السيبرانية التي لا تصل إلى حد الهجمات.[191]

والحماية المحددة التي يوفرها القانون الدولي الإنساني لبعض الأشخاص والأعيان تفرض قيودًا أكبر على نطاق العمليات العسكرية المسموح بها.

قواعد القانون الدولي التي تحمي الأعيان التي لا غنى عنها لبقاء السكان المدنيين والخدمات الطبية وعمليات الإغاثة الإنسانية

بالإضافة إلى القواعد العامة المتعلقة بسير الأعمال العدائية، ينص القانون الدولي الإنساني على نظم محددة لفئات معينة من الأعيان والخدمات توفر حماية إضافية وأقوى من الحماية الممنوحة لجميع المدنيين والأعيان المدنية.

فعلى سبيل المثال، ينص القانون الدولي الإنساني تحديدًا على أن "مهاجمة أو تدمير أو نقل أو تعطيل الأعيان التي لا غنى عنها لبقاء السكان المدنيين" هي إجراءات غير قانونية.[192] وتحمي هذه القاعدة، على سبيل المثال "المواد الغذائية" و"المناطق الزراعية التي تنتجها" و"مرافق مياه الشرب وشبكاتها وأشغال الري".[193] ورأى الخبراء الذين صاغوا دليل تالين أن شبكة الإنترنت في حد ذاتها لا يمكن اعتبارها عينًا لا غنى عنه لبقاء السكان المدنيين، إلا أنهم أشاروا إلى أن "البنية التحتية السيبرانية التي لا غنى عنها لتشغيل المولدات الكهربائية وأشغال ومنشآت الري، ومنشآت مياه الشرب، ومرافق الإنتاج الغذائي قد أن تصنف على هذا النحو وذلك حسب الظروف".[194] ويجب أن تُفهم الإشارة الصريحة إلى "التعطيل" على أنها تشمل نطاقًا أوسع من العمليات التي قد تؤثر على هذه المقومات، بما يتجاوز الهجمات أو التدمير. وعلى النحو المشار إليه في شرح اللجنة الدولية للمادة 54 (2) من البروتوكول الإضافي الأول، استهدف القائمون على الصياغة "تغطية جميع الاحتمالات" لكيفية تعطيل الأعيان المخصصة لإعاشة السكان المدنيين.[195] واليوم، تُحظر العمليات السيبرانية التي يقصد بها أو يتوقع منها تعطيل الأعيان التي لا غنى عنها لبقاء السكان المدنيين بغض النظر عما إذا كانت تصل إلى حد الهجوم. وبالتالي، فإن الجدل الدائر حول ما إذا كانت العمليات العسكرية التي تستهدف هذه الأعيان تصل إلى حد الهجوم (على النحو المبين أعلاه)، هو موضع نقاش بالنسبة لهذه الأعيان.

191 M. N. Schmitt، الحاشية 67 أعلاه، الصفحة 347: "تلتزم الدول، من الناحية السياساتية، بالامتناع عن تنفيذ عمليات سيبرانية لا تنطبق عليها قواعد القانون الدولي الإنساني التي تحكم الهجمات عندما تكون الآثار السلبية الملموسة المتوقعة على الأشخاص المدنيين أو السكان المدنيين مفرطة مقارنة بالفائدة الملموسة المتعلقة بالنزاع التي يتوقع الحصول عليها من خلال العملية".

192 انظر: البروتوكول الإضافي الأول، المادة 54 (2)؛ والبروتوكول الإضافي الثاني، المادة 14؛ ودراسة اللجنة الدولية للقانون العرفي، الحاشية 63 أعلاه، القاعدة 54.

193 البروتوكول الإضافي الأول، المادة 54 (2).

194 دليل تالين، الحاشية 13 أعلاه، الفقرة 5 من شرح القاعدة 141.

195 شرح اللجنة الدولية للبروتوكولين الإضافيين، الحاشية 110 أعلاه، الفقرتان 2101 و 2103.

ينص القانون الدولي الإنساني على توفير حماية محددة للخدمات الطبية. ونظرًا للأهمية الأساسية للرعاية الصحية بالنسبة لأي شخص يتضرر من النزاع المسلح، يجب على الأطراف المتحاربة احترام وحماية المرافق والطواقم الطبية في جميع الأوقات.[196] ويُفهم الالتزام بـ "احترام" المرافق والطواقم الطبية على أنه لا يحميهم من العمليات التي تصل إلى حد الهجمات فحسب- بل يُحظر "إلحاق الأذى بهم بأي شكل من الأشكال. وهذا يعني أيضًا أنه لا ينبغي أن يكون هناك أي تعطيل لعملها (على سبيل المثال، من خلال منع وصول الإمدادات) أو منع إمكانية مواصلة تقديم العلاج للجرحى والمرضى المشمولين بعنايتهم".[197] ويمتد نطاق الحماية الخاصة الممنوحة للمرافق الطبية ليشمل الاتصالات الطبية: رغم أن التشويش على اتصالات العدو يعتبر عمومًا أمرًا مسموحًا به، فلا يجوز السماح بإحداث "تعطيل متعمد لقدرة الوحدات [الطبية] على الاتصال لأغراض طبية"، حتى إذا كانت الوحدات الطبية تتواصل مع القوات المسلحة.[198] وعلاوة على ذلك، فإن الالتزام باحترام المرافق الطبية وحمايتها يشمل حظر حذف البيانات الطبية أو تغييرها أو التأثير سلبًا عليها بطريقة أخرى.[199] وقد يوفر أيضًا حماية من العمليات السيبرانية التي تستهدف سرية البيانات الطبية، والتي قد يكون من الصعب على الأقل في بعض الظروف التوفيق بينها وبين الالتزام بحماية واحترام المرافق الطبية.[200] وتشمل البيانات ذات الصلة في السياق الطبي "البيانات اللازمة للاستخدام السليم للمعدات الطبية وتتبع مخزون الإمدادات الطبية" بالإضافة إلى "البيانات الطبية الشخصية المطلوبة لعلاج المرضى".[201] وينطوي الالتزام بـ "حماية" المرافق الطبية، بما فيها بياناتها، على التزامات إيجابية.

196 انظر على سبيل المثال: اتفاقية جنيف الأولى، المادة 19؛ واتفاقية جنيف الثانية، المادة 12؛ واتفاقية جنيف الرابعة، المادة 18؛ والبروتوكول الإضافي الأول، المادة 12؛ والبروتوكول الإضافي الثاني، المادة 11؛ ودراسة اللجنة الدولية للقانون الدولي الإنساني العرفي، الحاشية 63، القواعد 25 و 28 و 29؛ و Tallinn Manual 2.0، الحاشية 13 أعلاه، القاعدتان 131-132. لا تتوقف حماية المرافق والطواقم الطبية إلا إذا ارتكبت أو استخدمت لارتكاب أعمال ضارة بالعدو خارج نطاق واجباتها الإنسانية. بيد أن هذه الحماية لا تتوقف إلا بعد توجيه إنذار تحدد فيه كلما كان ذلك ملائمًا مهلة معقولة ثم يبقى هذا الإنذار بلا استجابة. انظر: اتفاقية جنيف الأولى، المادة 21؛ واتفاقية جنيف الثانية، المادة 34؛ واتفاقية جنيف الرابعة، المادة 19؛ والبروتوكول الإضافي الأول، المادة 13؛ والبروتوكول الإضافي الثاني، المادة 11 (2)؛ ودراسة اللجنة الدولية للقانون الدولي الإنساني العرفي، الحاشية 63، القواعد 25 و 28 و 29؛ و Tallinn Manual 2.0، الحاشية 13 أعلاه، القاعدة 134.

197 شرح اللجنة الدولية للبروتوكولين الإضافيين، الحاشية 110 أعلاه، الفقرة 517. انظر أيضًا: تعليق اللجنة الدولية على اتفاقية جنيف الأولى، الحاشية 69 أعلاه، الفقرة 1799؛ وبيان أكسفورد، الحاشية 32 أعلاه، النقطة 5 ("أثناء النزاع المسلح، ينص القانون الدولي الإنساني احترام وحماية الوحدات الطبية ووسائل النقل والطواقم الطبية في جميع الأوقات. وفقًا لذلك، يجب على أطراف النزاعات المسلحة الالتزام بما يلي: ألا تعطل عمل مرافق الرعاية الصحية من خلال العمليات السيبرانية؛ ويجب أن تتخذ جميع الاحتياطات الممكنة لتجنب الضرر العرضي الناجم عن العمليات السيبرانية؛ ويجب أن تتخذ جميع التدابير الممكنة لتيسير عمل مرافق الرعاية الصحية ومنع تعرضها للضرر، بسبل منها العمليات السيبرانية")؛ دليل تالين، الحاشية 13 أعلاه، الفقرة 5 من شرح القاعدة 131 ("على سبيل المثال، هذه القاعدة [القاعدة 131 التي تنص على أنه" يجب احترام وحماية أفراد الخدمات الطبية والدينية والوحدات الطبية ووسائل النقل الطبي، ولا يجوز على وجه الخصوص تحويلها إلى هدف للهجوم السيبراني"] تحظر تغيير البيانات في النظام العالمي لتحديد المواقع العالمي لطائرة هليكوبتر طبية بغية تضليلها، رغم أن العملية لا تعتبر هجومًا على وسيلة نقل طبية").

198 شرح اللجنة الدولية للبروتوكولين الإضافيين، الحاشية 110 أعلاه، الفقرة 1804.

199 انظر: تقرير التحديات الصادر عن اللجنة الدولية لعام 2015، الحاشية 118 أعلاه، الصفحة 43.

200 انظر: L. Gisel and L. Olejnik (eds)، الحاشية 11 أعلاه، الصفحة 36، يناقش هذا المرجع فرضية اختراق السجلات الطبية أو الإدارية لمرفق طبي من أجل معرفة الموعد الطبي لقائد العدو لتحديد مكانه من أجل إيقاعه في الأسر أو قتله في طريقه إلى المرفق الطبي أو العودة منها. وقد يؤدي هذا بالفعل إلى إعاقة الأداء الطبي للمرفق دون مبرر وعرقلة قدرة العاملين في مجال الرعاية الصحية على التمسك بواجبهم الأخلاقي المتمثل في الحفاظ على السرية الطبية. ويقترح دليل تالين 2، الحاشية 13 أعلاه، الفقرة 2 من شرح القاعدة 132، ما يلي كمثال على عملية لا تنتهك القانون الدولي الإنساني: "استطلاع سيبراني غير ضار لتحديد ما إذا كان المرفق الطبي أو وسائل النقل الطبية (أو ما يرتبط بها من أجهزة الكمبيوتر وشبكات الكمبيوتر والبيانات) محل الاهتمام تُستغل لارتكاب أعمال ضارة من الناحية العسكرية".

201 دليل تالين 2، الحاشية 13 أعلاه، الفقرة 3 من شرح القاعدة 132.

ويجب على أطراف النزاع اتخاذ تدابير فعالة لحماية المرافق الطبية من الضرر قدر المستطاع، بما في ذلك الضرر الناجم عن العمليات السيبرانية.[202]

كما ينص القانون الدولي الإنساني على وجوب احترام وحماية العاملين في المجال الإنساني وإرساليات الغوث.[203] ويحظر هذا الالتزام بالتأكيد أي "هجمات" تستهدف العمليات الإنسانية. وعلى غرار الالتزام باحترام وحماية الطواقم والمرافق الطبية، ينبغي أيضًا فهم القواعد ذات الصلة على أنها تحظر "الأشكال الأخرى من السلوك الضار خارج نطاق سير الأعمال العدائية" التي تستهدف العاملين في المجال الإنساني أو التدخل غير المبرر في عملهم.[204] علاوة على ذلك، يتعين على أطراف النزاعات المسلحة الموافقة على عمليات الغوث الإنسانية والسماح بها وتسهيلها.[205] وفقًا لذلك، تنص القاعدة 145 من دليل تالين 2 على أنه "لا يجوز تصميم أو تنفيذ العمليات السيبرانية للتدخل غير المبرر في الجهود غير المتحيزة الرامية إلى تقديم المساعدة الإنسانية"، وتنص على أن هذه العمليات محظورة "حتى لو لم تصل إلى حد 'الهجوم'".[206] كما ينبغي فهم الالتزام باحترام وحماية طواقم وعمليات الإغاثة على أنها تحمي البيانات ذات الصلة.[207] وعلى الأقل بالنسبة للدول الأطراف في البروتوكول الإضافي الأول، ينبغي أن تشمل حماية البيانات الإنسانية البيانات التي تحتاج اللجنة الدولية إليها "لأداء المهام الإنسانية المسندة إليها بموجب اتفاقيات [جنيف] وهذا البروتوكول بقصد تأمين الحماية والعون لضحايا النزاعات".[208]

وتُظهر أشكال الحماية الخاصة المذكورة أن القانون الدولي الإنساني يوفر قواعد أكثر صرامة للعمليات العسكرية التي تستهدف سلعًا أو خدمات معينة ضرورية لبقاء السكان المدنيين وصحتهم ورفاههم.

أهمية المراجعات القانونية لوسائل وأساليب الحرب السيبرانية لضمان احترام القانون الدولي الإنساني

في ضوء التحديات الخاصة التي تطرحها خصائص الفضاء السيبراني أمام تفسير وتطبيق بعض مبادئ القانون الدولي الإنساني في سير الأعمال العدائية، يتعين على أطراف النزاعات المسلحة التي تقرر تطوير أو اقتناء أو استخدام أسلحة أو وسائل أو أساليب جديدة تعتمد على التكنولوجيا السيبرانية توخي الحذر في القيام بذلك. وفي هذا الصدد، فإن الدول الأطراف في

202 تعليق اللجنة الدولية على اتفاقية جنيف الأولى، الحاشية 69 أعلاه، الفقرات 1805-1808؛ ودليل تالين 2، الحاشية 13 أعلاه، الفقرة 6 من شرح القاعدة 131.

203 البروتوكول الإضافي الأول، المادتان 70 (4) و 71 (2)؛ ودراسة اللجنة الدولية للقانون العرفي، الحاشية 63 أعلاه، القاعدتان 31 و 32.

204 تعليق اللجنة الدولية على اتفاقية جنيف الأولى، الحاشية 69 أعلاه، الفقرتان 1358 و 1799.

205 انظر على سبيل المثال: اتفاقية جنيف الرابعة، المادة 59؛ والبروتوكول الإضافي الأول، المادتان 69-70؛ ودراسة اللجنة الدولية للقانون العرفي، الحاشية 63 أعلاه، القاعدة 55.

206 دليل تالين 2، الحاشية 13 أعلاه، الفقرة 4 من شرح القاعدة 80.

207 للاطلاع على المزيد من المناقشات، انظر:
Tilman Rodenhäuser, "Hacking Humanitarians? IHL and the Protection of Humanitarian Organizations against Cyber Operations", *EJIL: Talk!*, 16 March 2020, available at: www.ejiltalk.org/hacking-humanitarians-ihl-and-the-protection-of-humanitarian-organizations-against-cyber-operations/.

208 البروتوكول الإضافي الأول، المادة 81. وتشمل هذه البيانات، على سبيل المثال، البيانات اللازمة لإنشاء وكالات البحث عن المفقودين لجمع المعلومات عن الأشخاص المبلغ عن فقدانهم في سياق نزاع مسلح، أو البيانات التي تجمعها اللجنة الدولية عند زيارة المحتجزين وإجراء مقابلات معهم دون شهود.

البروتوكول الإضافي الأول التي تقوم بتطوير أو اقتناء قدرات الحرب السيبرانية - سواء لأغراض هجومية أو دفاعية - عليها التزام بتقييم ما إذا كان استخدام السلاح السيبراني أو وسائل أو أساليب القتال محظورًا بموجب القانون الدولي في بعض الظروف أو كلها.[209] ولا غنى عمومًا عن المراجعات القانونية لجميع الدول لضمان احترام قواتها المسلحة للقانون الدولي الإنساني،[210] بحيث لا تستخدم سوى الأسلحة أو وسائل أو أساليب الحرب، وما يعتمد منها على التكنولوجيا السيبرانية، التي تمتثل لالتزامات الدولة بموجب القانون الدولي الإنساني.[211] وينبغي الاستعانة في هذه المراجعات بفريق متعدد التخصصات يضم خبراء قانونيين وعسكريين وتقنيين حسب الاقتضاء.[212] ويجب إجراء هذه المراجعات القانونية في وقت أبكر وبعمق أكبر من تحليل مشروعية الاستخدام الفعلي للأداة في الظروف المحددة للهجوم.

وفي ضوء حداثة التقنية، من المهم أن تحظى المراجعة القانونية للأسلحة ووسائل وأساليب الحرب السيبرانية باهتمام خاص. وقد يكون حظر الأسلحة العشوائية بطبيعتها أمرًا ذا صلة بشكل خاص بالنظر إلى قدرة بعض الأدوات السيبرانية على الانتشار الذاتي من تلقاء نفسها.[213] ومع ذلك، قد تطرح المراجعة القانونية للأسلحة ووسائل وأساليب الحرب السيبرانية عددًا من التحديات. ونوضح بعض المسائل في الأجزاء التالية التي لا تتسم بطابع حصري.

أولًا، يتعين على الدولة التي تجري مراجعة قانونية تحديد المعايير القانونية التي تقوم بمراجعة الأداة السيبرانية في ضوئها. بمعنى آخر، تحتاج الدولة إلى إجابات لبعض الأسئلة التي نوقشت أعلاه، مثل ما إذا كان استخدام أداة معينة يعتبر هجومًا وبالتالي يخضع لطائفة واسعة من قواعد القانون الدولي الإنساني. وبالنسبة للمسائل التي يتسم فيها القانون بالغموض أو عدم الحسم، قد يكون هناك ما يبرر اتباع نهج حذر لتجنب ما يبدو لاحقًا من أن استخدام أداة سيبرانية كان غير قانوني أو كان ينبغي اعتباره كذلك.

ثانيًا، يتعين على الدول تحديد المسائل التي يجب مراجعتها. وقد لا يكون هذا واضحًا بالضرورة في سياق بالأدوات السيبرانية أو القدرات السيبرانية، كما يتضح من الاستخدام الواسع النطاق لهذه المصطلحات بدلًا من مفاهيم مثل الأسلحة السيبرانية. وناقش المعلقون ما إذا كانت الأدوات أو القدرات السيبرانية تعتبر من الأسلحة أو وسائل وأساليب القتال، وأيها يعتبر كذلك، وما هي الآثار المترتبة في سياق مراجعتها القانونية.[214] وعلى أي حال، كما هو مذكور أعلاه، يجب على الدول الأطراف في البروتوكول الإضافي الأول مراجعة جميع الأدوات أو القدرات السيبرانية التي تعتبر من الأسلحة أو وسائل وأساليب الحرب. وبالنسبة للدول التي ليست طرفًا في البروتوكول الإضافي الأول، فإن الالتزام باحترام وكفالة احترام القانون الدولي الإنساني من قبل قواتها المسلحة وحداثة استخدام التقنيات السيبرانية كسلاح أو وسيلة أو أسلوب حرب سيجعل من الحكمة توسيع نطاق البحث من حيث القدرات قيد المراجعة.[215]

209 البروتوكول الإضافي الأول، المادة 36.

210 انظر: المادة 1 المشتركة؛ ودراسة اللجنة الدولية للقانون العرفي، الحاشية 63 أعلاه، القاعدة 139.

211 ICRC, *A Guide to the Legal Review of New Weapons, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977*, Geneva, 2006, p. 1.

212 المرجع نفسه، الصفحتان 22-23.

213 انظر: دراسة اللجنة الدولية للقانون العرفي، الحاشية 63 أعلاه، القاعدة 71. للاطلاع على توضيح لبعض المسائل التي أثارتها المراجعة القانونية للأسلحة السيبرانية، انظر: "Scenario 10: Cyber Weapons Review",in K.Mačák, T. Minárik and T. Jančárková (eds)، الحاشية 68 أعلاه.

214 Jeffrey T. Biller and Michael N. Schmitt, "Classification of Cyber Capabilities and Operations as Weapons, Means, or Methods of Warfare", *International Law Studies*, Vol. 95, 2019, p. 219.

215 على سبيل المثال، في حين أن وزارة الدفاع الأمريكية تطبق سياسة إجراء مراجعة قانونية للأسلحة، بما في ذلك الأسلحة التي تستخدم القدرات السيبرانية

ثالثًا، لا ينبغي تقييم السلاح أو وسائل الحرب بمعزل عن طريقة استخدامها، وهذا يعني أن الاستخدام العادي أو المتوقع للسلاح أو وسائل الحرب يجب أن يؤخذ في الاعتبار في المراجعة القانونية. ومع ذلك، قد تكون القدرات العسكرية السيبرانية أقل ثباتًا من الأسلحة الحركية، خاصة إذا كانت مصممة لعملية معينة. وهذا يعني أن المراجعة يجب أن تتم في ضوء البيئة السيبرانية المحددة التي يُحتمل أن يستخدم فيها السلاح.

رابعًا، وفي هذا السياق، ينبغي للدولة إجراء مراجعة قانونية لا تقتصر على السلاح أو وسائل وأساليب الحرب التي تعتزم اقتناءها أو استخدامها لأول مرة، بل أيضًا عندما تقوم بتعديل السلاح أو وسائل وأساليب الحرب التي اجتازت أصلًا مراجعة قانونية. وقد يشكل هذا تحديًا في سياق الأدوات السيبرانية التي يُحتمل أن تخضع للتكيف المتكرر، ويشمل ذلك الاستجابة لتحديثات أمن البرامج التي يخضع لها الهدف المحتمل. وفي حين أن مسألة نوع ومدى التغيير الذي يتطلب مراجعة قانونية جديدة قد تحتاج إلى مزيد من التوضيح، يجب إجراء مراجعة قانونية جديدة، لا سيما عند تعديل السلاح أو وسائل وأساليب الحرب بطريقة تغير وظيفتها أو عندما يكون للتعديل تأثير بطريقة أخرى على توافق السلاح أو وسائل وأساليب الحرب مع القانون.[216] وقد لوحظ في هذا الصدد في سياق الأسلحة السيبرانية أن "تقييم ما إذا كان التغيير سيؤثر على تشغيل البرنامج يجب أن يكون نوعيًا وليس كميًا في طبيعته".[217] ولكي تكون المراجعات القانونية فعالة، يجب على الدول التي تقوم بدراسة أو تطوير أو اقتناء أو استخدام أسلحة أو وسائل وأساليب جديدة تعتمد على التقنيات الجديدة أن تعالج هذه التعقيدات وغيرها. بمعنى آخر، يجب أن تتكيف نظم الاختبار مع الخصائص الفريدة للتكنولوجيا السيبرانية. وفي ضوء التعقيدات المذكورة أعلاه، من الممارسات الجيدة لكفالة احترام القانون الدولي الإنساني من قبل جميع الدول تبادل المعلومات بشأن آليات المراجعة القانونية للدولة، وبقدر الإمكان، بشأن النتائج الموضوعية للمراجعات القانونية.[218] ويكتسي هذا الإجراء أهمية خاصة عند ظهور مشكلات توافق السلاح مع القانون الدولي الإنساني، وذلك لتجنب تعرض دول أخرى للمشكلات نفسها وإخطار الدول الأخرى بالاستنتاجات التي خلصت إليها الدولة القائمة بالاختبار ومفادها أن هذه الأدوات محظورة بموجب القانون الدولي الإنساني. وقد يساعد تبادل المعلومات بشأن المراجعات القانونية للأسلحة أو الوسائل أو الأساليب التي تعتمد على التقنيات الجديدة أيضًا في تراكم الخبرة وتسهيل تحديد الممارسات الجيدة، الأمر الذي قد يساعد الدول التي ترغب في إنشاء أو تعزيز آليات المراجعة القانونية الخاصة بها.[219]

(دليل قانون الحرب الصادر عن وزارة الدفاع، الحاشية 87 أعلاه، الفقرة 16-6)، فإن تعليمات القوات الجوية الأمريكية ذات الصلة تقرر مراجعة الأسلحة والإمكانيات السيبرانية: وزارة القوات الجوية الأمريكية، المراجعات القانونية للأسلحة والقدرات السيبرانية، تعليمات وزارة الدفاع 51-402، 27 تموز/يوليو 2011.

216 اللجنة الدولية، الحاشية 211 أعلاه، الصفحة 10.

217 Gary D. Brown and Andrew O. Metcalf, "Easier Said than Done: Legal Reviews of Cyber Weapons", *Journal of National Security Law and Policy*, Vol. 7, 2014, p. 133.

218 تم اقتراح ذلك في الكلمة التمهيدية التي ألقتها هيلين دورهام، مديرة القانون الدولي والسياسات باللجنة الدولية للصليب الأحمر، خلال الجلسة العامة التي نظمتها في 22 كانون الثاني/يناير 2019 اللجنةُ العالمية المعنية باستقرار الفضاء السيبراني (بيان موجود لدى اللجنة الدولية).

219 تقرير التحديات الصادر عن اللجنة الدولية لعام 2019، الحاشية 36 أعلاه، الصفحة 35.

الخاتمة

لحماية السكان المدنيين والبنية التحتية المدنية في النزاعات المسلحة، من المهم في المقام الأول الاعتراف بأن العمليات السيبرانية التي تُنفذ أثناء النزاعات المسلحة لا تحدث في فراغ قانوني، بل تخضع للقانون الدولي، وعلى الأخص القانون الدولي الإنساني. وكما يبين هذا المقال، فإن الاعتراف بانطباق القانون الدولي الإنساني ليس نهاية الحديث. فهناك حاجة إلى إجراء مزيد من المناقشة - ولا سيما بين الدول - بشأن كيفية تفسير القانون الدولي الإنساني في الفضاء السيبراني. وينبغي أن تسترشد أي مناقشة من هذا القبيل بفهم متعمق لتطور القدرات العسكرية السيبرانية، والتكلفة البشرية المحتملة التي قد تترتب عليها، والحماية التي توفرها أحكام القانون الحالية. ويهدف هذا المقال إلى توفير أساس لهذه المناقشات. ويتطور استخدام العمليات السيبرانية أثناء النزاعات المسلحة وكذلك تكلفتها البشرية المحتملة والمواقف القانونية للدول بشأن هذا الموضوع، إلا أن التحليل الوارد في هذا المقال يقدم عددًا من الاستنتاجات.

أولًا، على المستوى العملياتي، أضحى استخدام العمليات السيبرانية أثناء النزاع المسلح سمة واقعية من سمات النزاعات المسلحة ومن المرجح أن يزداد بروزًا في المستقبل. ويمكن أن تسبب أضرارًا جسيمة للسكان المدنيين، لا سيما إذا أثرت على البنية التحتية المدنية الحيوية مثل المرافق الطبية أو الكهرباء أو المياه أو الصرف الصحي. وفي حين أن مخاطر التسبب في حدوث التكلفة البشرية لا تبدو مرتفعة للغاية بناءً على الملاحظات الحالية، لا سيما بالنظر إلى الدمار والمعاناة اللذين تسببهما النزاعات دائمًا، فإن تطور العمليات السيبرانية يتطلب اهتمامًا دقيقًا بسبب الغموض الحالي والوتيرة السريعة للتغيير.

ثانيًا، ترى اللجنة الدولية أنه ليس ثمة شك في أن القانون الدولي الإنساني ينظم العمليات السيبرانية أثناء النزاعات المسلحة- شأن أي سلاح أو أساليب ووسائل القتال التي يلجأ إليها أي طرف من الأطراف المتحاربة في النزاع، سواء كانت قديمة أو حديثة. ولئن كانت هذه المسألة لا تحظى باتفاق شامل (بعد)، فإن الفحص الدقيق لمختلف الحجج التي أثيرت في المناقشات المتعددة الأطراف يُظهر أن تأكيد انطباق القانون الدولي الإنساني لا يضفي الشرعية على عسكرة الفضاء السيبراني أو استخدام العمليات السيبرانية الضارة. ويجب على الدولة التي تفكر في تنفيذ عملية سيبرانية ضد دولة أخرى أن تحلل شرعية هذه العملية بموجب ميثاق الأمم المتحدة والقانون الدولي الإنساني. فهذان الإطاران مكملان لبعضهما البعض عندما يتعلق الأمر بحماية البشر من الحرب وآثارها. فبينما يستخدم الإطاران بعض المصطلحات المتشابهة، فهما مستقلان عن بعضهما البعض من الناحية القانونية ويتطلبان تحليلات مختلفة، حيث إن المصطلحات المماثلة لها أحيانًا معنى مختلف. فعلى سبيل المثال، فإن تقديم استنتاج مفاده أن عملية سيبرانية تؤدي إلى انطباق القانون الدولي الإنساني لا يعني بالضرورة أنها تصل إلى حد هجوم مسلح يؤدي إلى نشوء حق الدفاع عن النفس.

ثالثًا، تشكل الطبيعة غير المادية جزئيًا -أي الرقمية- للفضاء السيبراني والترابط بين الشبكات العسكرية والمدنية تحديات عملية وقانونية في تطبيق مبادئ القانون الدولي الإنساني العامة والقواعد التي تحمي المدنيين والأعيان المدنية. وهذا صحيح على وجه الخصوص في سياق مفهوم "الهجوم" بموجب القانون الدولي الإنساني، ومسألة ما إذا كانت البيانات المدنية

تتمتع بحماية مماثلة بوصفها من "الأعيان المدنية"، وحماية البنية التحتية السيبرانية ذات "الاستخدام المزدوج".

مسألة وصول أو عدم وصول عملية معينة إلى حد "الهجوم" على النحو المحدد في القانون الدولي الإنساني، هي مسألة أساسية لتطبيق العديد من القواعد المستمدة من مبادئ التمييز والتناسب والاحتياط، التي توفر حماية بالغة الأهمية للمدنيين والأعيان المدنية. وعلى مدى سنوات طويلة، اتخذت اللجنة الدولية موقفًا مفاده أن العملية التي تهدف إلى تعطيل جهاز كمبيوتر أو شبكة كمبيوتر أثناء نزاع مسلح تشكل هجومًا على النحو المحدد في القانون الدولي الإنساني سواء تم تعطيل العين من خلال التدمير أو بأي طريقة أخرى. ويرد هذا الرأي أيضًا في مواقف عدد من الدول.

وفي حين أن العديد من القواعد العامة المتعلقة بسير الأعمال العدائية تقتصر على الأعمال التي تصل إلى حد الهجمات على النحو المحدد في القانون الدولي الإنساني، فإن بعض قواعد القانون الدولي الإنساني التي تحكم سير الأعمال العدائية تنطبق على مجموعة أوسع من العمليات. ويشمل القانون الدولي الإنساني عددًا من القواعد التي تنطبق على جميع "العمليات العسكرية"، مثل الالتزام بتوخي الحرص الدائم على تجنب إصابة الأعيان المدنية. وعلاوة على ذلك، ينص القانون الدولي الإنسان على قواعد محددة تحمي فئات من الأشخاص والأعيان، مثل الأعيان التي لا غنى عنها لبقاء السكان المدنيين والخدمات الطبية وعمليات الغوث الإنساني. ويمتد نطاق الحماية التي توفرها هذه القواعد ليتجاوز الحماية العامة الممنوحة للمدنيين والأعيان المدنية.

وتكتسي حماية البيانات من العمليات السيبرانية الخبيثة أثناء النزاع المسلح أهمية متزايدة لأن البيانات ركن أساسي في المجال الرقمي وحجر زاوية للحياة في العديد من المجتمعات. وترى اللجنة الدولية أنه يبدو من الصعب التوفيق بين الاستنتاج القائل بأن العمليات التي يقصد بها أو يتوقع منها حذف بيانات أساسية أو التلاعب بها لا يحظرها القانون الدولي الإنساني في عالم اليوم الأكثر اعتمادًا على الفضاء السيبراني، وأهداف وأغراض هذه المجموعة من القواعد، وهي مسألة تثير قدرًا كبيرًا من القلق.

من أجل حماية البنية التحتية المدنية الحيوية التي تعتمد على الفضاء السيبراني، من الضروري أيضًا حماية البنية التحتية للفضاء السيبراني نفسه. ودرج الفهم على أن العين المدنية قد تتحول إلى هدف عسكري عندما يفي استخدامها للأغراض العسكرية بتعريف الهدف العسكري حتى لو اُستخدمت في نفس الوقت لأغراض مدنية. ومن ناحية أخرى، يجب على أي طرف في نزاع يفكر في تنفيذ هجوم على البنية التحتية للفضاء السيبراني أن يحلل الأجزاء المتميزة من البنية التحتية التي تساهم مساهمة فعالة في العمل العسكري، وما إذا كان تدميرها أو تعطيلها، في الظروف السائدة آنذاك، سيوفر ميزة عسكرية أكيدة. علاوة على ذلك، يجب على هذا الطرف اتخاذ جميع الاحتياطات الممكنة لتجنب الضرر الذي يلحق بالمدنيين في النهاية أو التقليل منه إلى أدنى حد، بما في ذلك الضرر الناجم عن الآثار غير المباشرة أو الارتدادية، ويجب عليه الامتناع عن تنفيذ الهجوم إذا كان من المتوقع أن يكون هذا الضرر مفرطًا.

رابعًا، في ضوء التحديات الخاصة التي تطرحها خصائص الفضاء السيبراني أمام تفسير وتطبيق بعض مبادئ القانون الدولي الإنساني في سير الأعمال العدائية، يتعين على أطراف

النزاعات المسلحة التي تقرر تطوير أو اقتناء أو استخدام أسلحة أو وسائل أو أساليب جديدة تعتمد على التكنولوجيا السيبرانية توخي الحذر في القيام بذلك. ولئن كانت المراجعات القانونية للأسلحة ووسائل وأساليب القتال الجديدة إلزامية على الدول الأطراف في البروتوكول الإضافي الأول، تكتسب المراجعات القانونية أهمية حاسمة لجميع الدول لضمان ألا تستخدم قواتها المسلحة إلا الأسلحة أو وسائل وأساليب الحرب التي تمتثل لالتزامات الدولة بموجب القانون الدولي الإنساني.

وختامًا، فإن الاعتراف بأن القانون الدولي الإنساني ينطبق على الفضاء السيبراني والمشاركة في مناقشات حول كيفية معالجته للتحديات المختلفة التي تطرحها الخصائص المحددة للمجال السيبراني وما إذا كانت أحكام القانون الحالية مناسبة وكافية لا يستبعد أن تكون القواعد الجديدة مفيدة أو حتى ضرورية. ونرى أن الإجابة على هذا السؤال تتوقف بشكل خاص على كيفية تفسير الدول للالتزامات القائمة بموجب القانون الدولي الإنساني. ففي حالة اعتماد تفسيرات محدودة، فقد تظهر ثغرات كبيرة في حماية السكان المدنيين والبنية التحتية، وقد يحتاج الإطار القانوني الحالي إلى تعزيز. ومن ناحية أخرى، في حالة وضع قواعد جديدة، فنرى أن من الأهمية بمكان أن تستند إلى الإطار القانوني القائم أصلًا وأن تعززه- ولا سيما القانون الدولي الإنساني.