مختـــــارات مـن
المجلة الدوليـة
للصلـيب الأحمـــر

مجلد 94 (886) صيف 2012

لا تقترب من حدود فضائي الإلكتروني: الحرب الإلكترونية والقانون الدولي الإنساني وحماية المدنيين

«كوردولا دوريجي»*

تشغل «كوردولا دوريجي» منصب رئيسة وحدة القانون التنفيذي التابعة للشعبة القانونية باللجنة الدولية للصليب الأحمر (اللجنة الدولية)

ملخص

تتبوأ الحرب الإلكترونية مكانة بارزة على جدول أعمال المسؤولين عن وضع السياسات العامة والقادة العسكريين في جميع أنحاء العالم. وتنشأ وحدات جديدة تهدف إلى كفالة أمن الفضاء الإلكتروني على مختلف مستويات الحكومة، بما فيها القوات المسلحة. غير أن العمليات الإلكترونية في حالات النزاع المسلح قد يكون لها عواقب وخيمة للغاية، خاصة وأن تأثيرها لا يقتصر على بيانات النظام الحاسوبي أو أجهزة الكمبيوتر المستهدفة. وفي الواقع، تهدف العمليات الإلكترونية عادة إلى إحداث تأثير في «العالم الواقعي». فعلى سبيل المثال، من خلال العبث بالنظم الحاسوبية، يمكن للشخص أن يتلاعب في نظم مراقبة الحركة الجوية، أو نظم التدفق عبر أنابيب النفط، أو المحطات النووية لدى العدو. وتخلف بعض العمليات الإلكترونية تأثيرًا هائلاً على السكان المدنيين. ومن ثم، من الضروري مناقشة قواعد القانون الدولي الإنساني التي تحكم هذه العمليات لأن من الأهداف الرئيسية لهذا الفرع من القانون هو حماية السكان المدنيين من أضرار العمليات الحربية. ويهدف هذا المقال إلى التعاطي مع بعض الأسئلة التي تثار عند تطبيق القانون الدولي الإنساني- وهو مجموعة القواعد القانونية التي وضعت بينما كانت الحروب التقليدية الحركية في الحسبان- على تكنولوجيا الفضاء الإلكتروني. والسؤال الأول: متى تدخل حرب الفضاء الإلكتروني ضمن المعنى الحقيقي «للنزاع المسلح»؟ وبعد مناقشة هذا السؤال، ينتقل المقال إلى النظر في بعض من أهم القواعد التي تحكم سير العمليات العدائية وتفسير تلك القواعد في العالم الإلكتروني، وهي مبادئ التمييز والتناسب والاحتياط. وفيما يتعلق بهذه القواعد جميعها، يفرض العالم الإلكتروني عددًا من الأسئلة التي لم تجد إجابة بعد. وعلى وجه الخصوص، يفرض الترابط الذي يتسم به الفضاء الإلكتروني تحديًا أمام الافتراض الأساسي الذي تستند

* يطيب لي أن أتقدم بالشكر إلى زملائي بـ«اللجنة الدولية»، «كنوت دورنان»، و«برونو ديمبير»، و«رايموند سميث»، و«تريستان فيرارو»، و«جيلينا بيتش»، و«غاري براون» على ما قدموه من تعليقات وافية على النسخ السابقة، وكذلك إلى «نيلي فيرليندن» على ما قدمته من مساعدة في المراجع.
جميع مراجع الإنترنت جرى الاطلاع عليها في تشرين الأول/ أكتوبر 2012 ما لم يبين خلاف ذلك.
كتب هذا المقال بصفة شخصية ولا يعكس بالضرورة آراء «اللجنة الدولية».

معرّف الوثيقة رقم:10.1017/S1816383113000246

إليه القواعد الخاصة بسير العمليات العدائية، ومفادها إمكانية بل وضرورة حماية المدنيين والأعيان المدنية في جميع الأحوال. ومن ثم، لا يزال النظر مستمرًا فيما إذا كانت القواعد التقليدية للقانون الدولي الإنساني ستوفر حماية كافية للمدنيين من تأثير حروب الفضاء الإلكتروني. ويحتاج تفسير هذه القواعد بالتأكيد إلى النظر بعين الاعتبار إلى الخصوصيات التي تميز الفضاء الإلكتروني. وفي ظل غياب معرفة أفضل بالتأثير المحتمل لحروب الفضاء الإلكتروني، لا يمكن أن نستبعد أن يكون من الضروري وضع قواعد أكثر صرامة.

كلمات أساسية: أمن الفضاء الإلكتروني، حرب الفضاء الإلكتروني، الهجوم الإلكتروني، القانون الدولي الإنساني، العمليات الإلكترونية، الأسلحة الإلكترونية، النزاع المسلح في الفضاء الإلكتروني، سير العمليات العدائية، التمييز، التناسب، الهجمات العشوائية، الاحتياطات.

: : : : : :

المقدمة

يتبوأ أمن الفضاء الإلكتروني مكانة بارزة على جدول أعمال المسؤولين عن وضع السياسات العامة والقادة العسكريين في جميع أنحاء العالم. وتصف دراسة نشرها مؤخرًا معهد الأمم المتحدة لبحوث نزع السلاح التدابير التي اتخذتها ثلاث وثلاثون دولة أدرجت على وجه التحديد حرب الفضاء الإلكتروني في تخطيطها وتنظيمها العسكري، وتقدم هذه الدراسة لمحة عامة عن نهج أمن الفضاء الإلكتروني المتبع في ست وثلاثين دولة أخرى.[1] وتشمل هذه المجموعة دولًا لديها بيانات متطورة للغاية عن العقيدة وتنظيمات عسكرية توظف مئات أو آلاف الأفراد وترتيبات أساسية تدمج الهجوم الإلكتروني في قدراتها الحالية الخاصة بالحرب الإلكترونية. ويعمل عدد من الدول على إنشاء وحدات متخصصة داخل أو خارج قواتها المسلحة للتعامل مع العمليات الإلكترونية.[2] وورد أيضًا أن اثنتي عشرة من أقوى القوات المسلحة الخمس عشرة على مستوى العالم تعمل على بناء برامج لحروب الفضاء الإلكتروني.[3]

أمن الفضاء الإلكتروني على وجه العموم وحروب الفضاء الإلكتروني على وجه الخصوص

في خضم المناقشات حول أمن الفضاء الإلكتروني على وجه العموم، لا يعرف الجمهور إلا قليلًا عن الخطط والسياسات العسكرية للدول فيما يتعلق بحروب الفضاء الإلكتروني.

1 Center for Strategic and International Studies, *Cybersecurity and Cyberwarfare – Preliminary Assessment*
,*of National Doctrine and Organization*, UNIDIR Resources Paper, 2011
متاح عبر الرابط التالي:
http://www.unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfare-preliminary-assess-
;ment-of-national-doctrineand-organization-380.pdf
انظر أيضًا:
Eneken Tikk, *Frameworks for International Cyber Security*, CCD COE Publications, Tallinn, 2011.

2 انظر على سبيل المثال:
Ellen Nakashima, 'Pentagon to boost cybersecurity force', in *The Washington Post*, 27 January 2013; Gordon Corera, 'Anti-cyber threat centre launched', in *BBC News*, 27 March 2013.

3 Scott Shane, 'Cyberwarfare emerges from shadows of public discussion by US officials', in The New York
Times, 26 September 2012, p. A10.

ويبدو أن أغلب الاستراتيجيات الحكومية تتألف من مزيج يجمع بين الاستراتيجيات الدفاعية والهجومية. فمن ناحية، تسعى الدول على نحو متزايد إلى حماية بنيتها الأساسية الحيوية من الهجمات الإلكترونية. ومن ناحية أخرى، يبدو أنها تعمل أيضًا على بناء القدرات التكنولوجية حتى تكون قادرة على شن عمليات إلكترونية ضد خصومها في أوقات النزاع المسلح.[4]

ويدخل المسؤولون عن وضع السياسات العامة والمعلقون في مناقشة حول ما إذا كانت «الأسلحة الإلكترونية» الجديدة ينبغي حظرها، كلها أو بعضها، حظرًا تامًا، وما إذا كان الاهتمام ينبغي أن يوجه إلى تدابير بناء الثقة (التي تشبه التدابير الخاصة بنزع السلاح النووي)،[5] وما إذا كان ينبغي وضع «قواعد الطريق» لضبط السلوك في الفضاء الإلكتروني.[6] دارت مناقشة على مدى أكثر من عقد حول ضرورة إبرام معاهدة جديدة بشأن أمن الفضاء الإلكتروني. وظل الاتحاد الروسي يدعو إلى معاهدة من هذا القبيل منذ أواخر التسعينيات، في حين رأت الولايات المتحدة الأمريكية (الولايات المتحدة) والدول الغربية عدم وجود حاجة إليها.[7] وفي رسالة موجهة إلى الأمين العام للأمم المتحدة، اقترح الاتحاد الروسي وأوزباكستان مدونة قواعد سلوك دولية لأمن المعلومات في أيلول/ سبتمبر 2011، على أن يكون لها نطاق أوسع بكثير من حالات النزاع المسلح.[8] وجدير بالذكر أن الصين، والاتحاد الروسي، وكازاخستان، وقرغيزستان، وطاجيكستان، وأوزبكستان هي أيضًا أطراف في اتفاقية اعتمدت في إطار منظمة شنغهاي للتعاون في عام 2009.[9] أما الهند، وجمهورية إيران الإسلامية، ومنغوليا، وباكستان، فيشاركون بوصفهم مراقبين. وتبين ترجمة إنجليزية غير رسمية أن هذه الاتفاقية تبدو وكأنها توسع نطاق مفاهيم «الحرب»

4 المرجع السابق.

5 Ben Baseley-Walker, 'Transparency and confidence-building measures in cyberspace: towards norms of
behaviour', in UNIDIR, *Disarmament Forum*, 'Confronting cyberconflict', Issue 4, 2011, pp. 31–40,
متاح عبر الرابط التالي:
http://www.unidir.org/files/publications/pdfs/confronting-cyberconflict-en-317.pdf ،
James Andrew Lewis, *Confidence-building and international agreement in cybersecurity*,
متاح عبر الرابط التالي: http://www.unidir.org/pdf/articles/pdf-art3168.pdf.

6 انظر: William Hague, 'Security and freedom in the cyber age – seeking the rules of the road'، كلمة أمام مؤتمر ميونيخ للأمن، 4 شباط/ فبراير 2011. متاح عبر الرابط التالي: https://www.gov.uk/government/speeches/security-and-freedom-in-the-cyber-age-seeking-the-rules-of-the-road,
وانظر: 'Foreign Secretary opens the London Conference on Cyberspace'، 1 تشرين الثاني/ نوفمبر 2011، متاح عبر الرابط التالي: https://www.gov.uk/government/speeches/foreign-secretary-opens-the-london-conference-on-cyberspace.

7 انظر مشروع القرار الذي قدمه الاتحاد الروسي إلى اللجنة الأولى التابعة للجمعية العامة في عام 1998، رسالة مؤرخة 23 أيلول/ سبتمبر 1998 من المندوب الدائم للاتحاد الروسي إلى الأمين العام للأمم المتحدة، وثيقة الأمم المتحدة رقم A/C.1/53/3، 30 أيلول/ سبتمبر 1998؛
E. Kramer, 'US and Russia differ on a treaty for cyberspace', in John Markoff and Andrew *The New York Times*, 28 June 2009, p. A1; John Markoff and Andrew E. Kramer, 'In shift, US talks to Russia on internet security', in *The New York Times*, 13 December 2009, p. A1;
وانظر: Adrian Croft, 'Russia says many states arming for cyber warfare', in Reuters, 25 April 2012، متاح عبر الرابط التالي:
http://www.reuters.com/article/2012/04/25/germany-cyberidUSL6E8FP40M20120425؛
Keir Giles, 'Russia's public stance on cyberspace issues', paper given at the4 2012 th International Conference on Cyber Conflict, C. Czosseck, R. Ottis and K. Ziolkowski (eds), NATO CCD COE Publications, Tallinn, 2012,
متاح عبر الرابط التالي: http://www.conflictstudies.org.uk/files/Giles-Russia_Public_Stance.pdf.

8 رسالة مؤرخة 12 أيلول/ سبتمبر 2011 من المندوبين الدائمين للاتحاد الروسي، وأوزباكستان، والصين، وطاجيكستان لدى الأمم المتحدة إلى الأمين العام، وثيقة الأمم المتحدة رقم A/66/359، بتاريخ 14 أيلول/ سبتمبر 2011.

9 اتفاق بين حكومات الدول الأعضاء في منظمة شنغهاي للتعاون على التعاون في مجال أمن المعلومات على الصعيد الدولي.

و«السلاح» لتتجاوز معانيها التقليدية الواردة في القانون الدولي الإنساني.[10]

ولا تزال هذه المناقشة- التي يتهم فيها جميع الأطراف غيرهم بالتجسس ونشر الأسلحة، بالتصريح أو التلميح بطريقة أو بأخرى-[11] تتسم بالعمومية الشديدة من المنظور القانوني. فعلى وجه الخصوص، لا يوجد فرق بين حالات النزاع المسلح والحالات الأخرى، على الرغم من أن انطباق القانون الدولي الإنساني يعتمد على هذا الفرق. ويبدو أن معظم القلق يركز على التجسس ضد الدولة وكذلك ضد المصالح الاقتصادية، غير أن هناك كذلك حديثًا يدور حول الحرب الإلكترونية وضرورة تجنب انتشار الأسلحة في الفضاء الإلكتروني. ولا يوجد عمومًا فرق بين حالات النزاع المسلح والحالات الأخرى التي تتهدد فيها العمليات الإلكترونية أمن الدول أو الشركات أو الأسر الخاصة. ولا تتطرق المناقشات الدائرة حول أمن الفضاء الإلكتروني حتى إلى حالات النزاع المسلح، وليس من الواضح ما إذا كانت هذه الحالات مدرجة ضمنًا. وفي الواقع، وفي كثير من الجوانب، لا سيما فيما يتعلق بحماية البنية الأساسية الحاسوبية من التسلل أو التلاعب أو التلف، ليس هناك فرق بين هجوم إلكتروني ينفذ في إطار نزاع مسلح أو إطار غيره. فالوسائل التقنية لحماية البنية الأساسية ستظل كما هي دون تغيير في أغلب الحالات. ومع ذلك، ولئن كان من قبيل الإنصاف أن نقول إن أغلب التهديدات في العالم الإلكتروني لا ترتبط ارتباطًا مباشرًا بحالات نزاع مسلح بل تنبثق بالأحرى من نشاط التجسس الاقتصادي أو أشكال التجسس الأخرى أو الجريمة الإلكترونية المنظمة، فمن الواضح أيضًا أن اللجوء إلى الأسلحة الإلكترونية أو العمليات الإلكترونية يضطلع بدور متزايد في النزاعات المسلحة وأن الدول تستعد بنشاط لهذا التطور الجديد.

وفي الوقت ذاته، هناك خلط بشأن انطباق القانون الدولي الإنساني على الحرب الإلكترونية- ربما كان مرجعه في الواقع إلى اختلاف الأفكار حول مفهوم الحرب الإلكترونية ذاتها، والتي قد تمتد من فهمها بوصفها عمليات إلكترونية تنفذ في إطار نزاعات مسلحة كما تفهم في إطار القانون الدولي الإنساني، إلى النظر إليها على أنها أنشطة إلكترونية إجرامية

10 متاح عبر الرابط التالي:
http://media.npr.org/assets/news/2010/09/23/cyber_treaty.pdf،
المرفق الأول يعرف «حرب المعلومات» على أنها «مواجهة بين دولتين أو أكثر في مجال المعلومات تهدف إلى الإضرار بنظم وعمليات وموارد المعلومات، والهياكل المهمة للغاية وغيرها، وتقويض النظم السياسية والاقتصادية والاجتماعية. والقيام بغسيل الأدمغة النفسي الشامل من أجل زعزعة استقرار المجتمع والدولة، فضلًا عن إرغام الدولة على اتخاذ قرار في صالح الطرف المعادي». ويصف المرفق الثاني تهديد «تطوير واستخدام أسلحة المعلومات، والتحضير لحرب المعلومات وشنها» بأنها تنبثق «من إنشاء وتطوير أسلحة معلومات تشكل تهديدًا مباشرًا للهياكل الحيوية في الدول، مما قد يؤدي إلى سباق تسلح جديد ويشكل تهديدًا خطيرًا في مجال أمن المعلومات على الصعيد الدولي. ومن بين سماته استخدام أسلحة المعلومات للتحضير لحرب المعلومات وشنها، والتأثير على نظم النقل والاتصالات والمراقبة الجوية، ومرافق الدفاع الصاروخي والأنواع الأخرى من مرافق الدفاع، نتيجة لذلك تفقد الدولة قدراتها الدفاعية في مواجهة الطرف المعتدي وتخفق في ممارسة حقها المشروع في الدفاع عن النفس؛ واختراق تشغيل البنية الأساسية للمعلومات، مما يؤدي إلى انهيار النظم الإدارية ونظم اتخاذ القرار في الدول؛ وإحداث تأثير مدمر على الهياكل الحيوية».

11 Kenneth Lieberthal and Peter W. Singer, ‘Cybersecurity and US–China relations’, in China ,US Focus, 23 February 2012
متاح عبر الرابط التالي:
http://www.chinausfocus.com/library/think-tank-resources/us-lib/peacesecurity-us-lib/brookings-cybersecurity-and-u-s-china-relations-february-23-2012/; Mandiant Intelligence Centre ,Report, *APT1: Exposing one of China’s Cyber Espionage Units*
متاح عبر الرابط التالي:
http//:intelreport.mandiant.com?/gclid=CKD67-Oo3LUCFalxOgod8y8AJg؛
Ellen Nakashima, ‘US said to be target of massive cyber-espionnage campaign’, in The Washington Post, 11 February 2013; ‘North Korea says US “behind hack attack” ’, in *BBC News*, 15 March 2013.

من جميع الأشكال. وأكدت بعض الدول، مثل الولايات المتحدة،[12] والمملكة المتحدة لبريطانيا العظمى وأيرلندا الشمالية،[13] وأستراليا،[14] أن القانون الدولي الإنساني ينطبق على الحرب الإلكترونية.[15]

ومع ذلك، لا تتطرق المواقف المعلنة حتى الآن إلى التفاصيل بشأن مسائل من قبيل المستوى المحدد للنزاعات المسلحة أو تعريف «الهجمات» في القانون الدولي الإنساني أو عواقب الحرب الإلكترونية على ما يسمى الأعيان ذات الاستخدام المزدوج. وتردد أن الصين لا تقبل انطباق القانون الدولي الإنساني على الحرب الإلكترونية.[16] ولكن من غير الواضح ما إذا كان هذا هو موقف الصين الرسمي فعلاً في حالة نشوب نزاع مسلح في إطار المعنى المقصود في القانون الدولي الإنساني. وثمة رأي آخر مفاده ما يلي:

> يذهب موقف الصين إلى أن دول العالم ينبغي لها أن تقدر قيمة الفضاء الإلكتروني- فهو أول فضاء اجتماعي يخلقه البشر- وينبغي لها أن تعارض بشدة عسكرة الإنترنت... وهي ترى أن ميثاق الأمم المتحدة الحالي وقوانين النزاع المسلح القائمة فضلاً عن المبادئ الأساسية للقانون الدولي الإنساني التي تتصل بالتهديد باستعمال القوة أو استخدامها لا تزال تنطبق جميعها على الفضاء الإلكتروني- ولا سيما ضرورات «عدم استعمال القوة» و«تسوية المنازعات الدولية بالوسائل السلمية»، فضلاً عن مبدأي التمييز والتناسب فيما يتعلق بوسائل وأساليب القتال.[17]

وكما يبدو، فإن الاتحاد الروسي لم يتخذ موقفًا رسميًا بشأن انطباق القانون الدولي الإنساني

12 Harold Koh, 'International law in cyberspace', speech at the US Cyber Command Inter-Agency Legal Conference, 18 September 2012,
متاح عبر الرابط التالي:
http://opiniojuris.org/2012/09/19/harold-koh-oninternational-law-in-cyberspace/؛
وتقرير الأمين العام عن المستجدات في مجال المعلومات والاتصالات في سياق الأمن الدولي (ويشار إليه فيما يلي باسم «تقرير الأمين العام»)، 15 تموز/ يوليو 2011، وثيقة الأمم المتحدة رقم A/66/152، الصفحة 19؛ وانظر أيضًا استراتيجية وزارة الدفاع الأمريكية للعمليات في الفضاء الإلكتروني: «تنطبق القواعد الدولية القائمة منذ زمن طويل التي توجه سلوك الدول- في زمن السلم والنزاع- أيضًا على الفضاء الإلكتروني. ومع ذلك، تستلزم السمات الفريدة التي تتسم بها التكنولوجيا المتشابكة العمل من أجل توضيح كيفية تطبيق هذه القواعد وما هي أوجه الفهم الإضافية التي قد تكون لازمة لاستكمالها»، US Department of Defense، Strategy for Operating in Cyberspace، تموز/ يوليو 2011، متاحة عبر الرابط التالي:
http://www.defense.gov/news/d20110714cyber.pdf.

13 تقرير الأمين العام، 23 حزيران/ يونيو 2004، وثيقة الأمم المتحدة رقم A/59/116، الصفحة 11؛ وتقرير الأمين العام المؤرخ 20 تموز/ يوليو 2010، وثيقة الأمم المتحدة رقم A/65/154، الصفحة 15.

14 تقرير الأمين العام، الحاشية 12 أعلاه، الصفحة 6.

15 انظر أيضًا: المقترح الذي تقدم به الممثل السامي للاتحاد الأوروبي للشؤون الخارجية والأمن والسياسة والاتصال المشترك إلى البرلمان الأوروبي والمجلس الأوروبي الاقتصادي والاجتماعي ولجنة الأقاليم بعنوان:
Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – Cyber Security Strategy of the European Union: an Open, Safe and Secure Cyberspace, Brussels, 7.2.2013, JOIN (2013) 1 final.

16 انظر أيضًا: Adam Segal, 'China, international law and cyber space', in *Council on Foreign Relations*, 2 October 2012، متاح عبر الرابط التالي:
http://blogs.cfr.org/asia/2012/10/02/china-international-law-and-cyberspace/.

17 Li Zhang, 'A Chinese perspective on cyber war', in this edition
ذكر سفير الصين، في كلمته أمام اللجنة الأولى في أيلول/ سبتمبر 2011، أن الصين اقترحت أن «تلزم البلدان نفسها بالامتناع عن استخدام المعلومات والتكنولوجيا الإلكترونية للمشاركة في أنشطة عدائية تضر بالسلم والأمن الدوليين والامتناع عن نشر المعلومات والأسلحة الإلكترونية» وأن «تعمل على الحيلولة دون تحول المعلومات والفضاء الإلكتروني إلى ميدان معركة جديد»؛ لا توجد إشارة إلى القانون الدولي الإنساني. انظر البيان الخاص بأمن المعلومات والفضاء الإلكتروني الذي ألقاه سعادة السفير «وانغ كون» أمام اللجنة الأولى خلال الدورة السادسة والستين للجمعية العامة، «العمل على بناء فضاء معلوماتي وإلكتروني يتسم بالسلم والأمن والإنصاف»، نيويورك، 20 تشرين الأول/ أكتوبر 2011، متاح عبر الرابط التالي:
http://www.fmprc.gov.cn/eng /wjdt/zyjh/t869580.htm

على الحروب الإلكترونية.[18]

ومن وجهة نظر قانونية، من المهم التمييز بين الحرب الإلكترونية بمفهوم العمليات الإلكترونية المنفذة في سياق النزاعات المسلحة في إطار المعنى المقصود في القانون الدولي الإنساني، والعمليات الإلكترونية خارج هذه السياقات. ولا تنطبق قواعد القانون الدولي الإنساني إلا في سياق النزاعات المسلحة، مما يفرض قيودًا محددة على الأطراف المشاركة في النزاع.[19] وبالتالي، فإن مصطلح «الحرب الإلكترونية» في هذا المقال سيشير إلى وسائل وأساليب القتال التي تشمل العمليات الإلكترونية التي تصل إلى حد النزاع المسلح أو تنفذ في سياقه وذلك في إطار المعنى المقصود في القانون الدولي الإنساني فقط. وتوجه العمليات الإلكترونية المذكورة- التي يشار إليها كثيرًا بوصفها هجمات على شبكات الكمبيوتر- ضد جهاز كمبيوتر أو نظام حاسوبي أو عبرهما من خلال مسار لتدفق البيانات.[20] ويمكن أن تسعى إلى تحقيق أهداف مختلفة، منها على سبيل المثال التسلل إلى نظام حاسوبي وجمع أو إخراج أو تدمير أو تعديل أو تشفير البيانات أو إطلاق عمليات أو تعديلها أو التلاعب بطريقة أخرى في هذه العمليات التي يسيطر عليها النظام المختَرق. وبمعنى آخر، يتناول التحليل التالي العمليات العدائية التي تشمل تطوير شفرة حاسوبية وإرسالها من جهاز كمبيوتر أو أكثر إلى أجهزة الكمبيوتر المستهدفة.

الشواغل الإنسانية

يرتبط الشاغل الإنساني لدى اللجنة الدولية للصليب الأحمر (اللجنة الدولية) أساسًا بالتأثير المحتمل على السكان المدنيين، لا سيما لأن العمليات الإلكترونية قد تؤثر تأثيرًا خطيرًا على البنية الأساسية المدنية[21] نتيجة لسمات عدة تميز العالم الإلكتروني. أولًا، نتيجة لاعتماد البنية الأساسية المدنية على نطاق واسع ومتزايد على النظم الحاسوبية، فإنها معرضة بدرجة كبيرة للهجمات على شبكات الكمبيوتر. وعلى وجه الخصوص، يعتمد عدد من المنشآت الخطيرة، مثل محطات الكهرباء والمحطات النووية والسدود ونظم معالجة وتوزيع المياه ومحطات تكرير البترول وأنابيب الغاز والنفط والنظم المصرفية ونظم المستشفيات والسكك الحديدية

18 لا تشير العقيدة العسكرية المذكورة للاتحاد الروسي إلى القانون الدولي الإنساني فيما يتعلق بحرب المعلومات؛ انظر «العقيدة العسكرية للاتحاد الروسي المعتمدة بموجب المرسوم الرئاسي للاتحاد الروسي بتاريخ 5 شباط/ فبراير 2010»، متاح عبر الرابط التالي: http://www.sras.org/military_doctrine_russian_federation_2010; ولا يشير إليه كذلك K. Giles، الحاشية 7 أعلاه؛ وانظر:
Roland Heikerö, 'Emerging threats and Russian Views on information warfare and informa-,tion operations', FOI Swedish Defence Research Agency, March 2010, p. 49
متاح عبر الرابط التالي: http//:www.highseclabs.com/Corporate/foir2970.pdf، ويشير إلى أن الاتحاد الروسي اقترح «تطبيق قوانين إنسانية تحظر الهجمات على غير المقاتلين وحظر الخداع في الفضاء الإلكتروني».

19 بالنسبة للجنة الدولية للصليب الأحمر (اللجنة الدولية)، من المهم لفت الانتباه إلى الحالة الخاصة للعمليات الإلكترونية التي تصل إلى حد النزاعات المسلحة أو تنفذ في سياقها- أي الحرب الإلكترونية بمعنى ضيق. ويرجع السبب في هذا إلى أن «اللجنة الدولية» مكلفة بمهمة محددة في إطار اتفاقيات جنيف لعام 1949 وهي مساعدة وحماية ضحايا النزاعات المسلحة. وهي مكلفة أيضًا من المجتمع الدولي بالعمل على فهم ونشر القانون الدولي الإنساني. انظر على سبيل المثال، المادة 125 (5) من اتفاقية جنيف الثالثة، والمادة 143 (5) من اتفاقية جنيف الرابعة، والمادة 5 (2) (ز) من النظام الأساسي للحركة الدولية للصليب الأحمر والهلال الأحمر.

20 وزارة الدفاع الأمريكية، *قاموس المصطلحات العسكرية والمصطلحات المرتبطة بها*، 8 تشرين الثاني/ نوفمبر 2010 (بصيغته المعدلة في 31 كانون الثاني/ يناير 2010)، واشنطن العاصمة، 2010: «الهجمات على شبكات الكمبيوتر هي إجراءات تتخذ من خلال استخدام شبكات الكمبيوتر لتعطيل أو منع أو تقويض أو تدمير المعلومات المخزنة في أجهزة الكمبيوتر وشبكات الكمبيوتر، أو أجهزة الكمبيوتر والشبكات نفسها».

21 في قانون سير العمليات العدائية، «المدنيون» و«السكان المدنيون» و«الأعيان المدنية» هي مفاهيم قانونية مختلفة تنطبق عليها قواعد مختلفة. ولكن عندما يتحدث هذا المقال عن تأثير العمليات الإلكترونية على السكان المدنيين، فهو يشير أيضًا إلى الأضرار التي تلحق بالبنية الأساسية المدنية، وهي أكثر الطرق احتمالًا لتأثير العمليات الإلكترونية على السكان المدنيين.

ومراقبة الحركة الجوية، على ما يسمى نظام التحكم الإشرافي وتجميع البيانات ونظم التحكم الموزع. وهذه النظم، التي تشكل الرابط بين العالم الرقمي والعالم المادي، معرضة للغاية للتدخل الخارجي من جانب أي مهاجم تقريبًا.[22]

ثانيًا، يشكل الترابط البيني الذي تتسم به شبكة الإنترنت تهديدًا للبنية الأساسية المدنية. ففي واقع الأمر، تعتمد الشبكات العسكرية على البنية الأساسية الحاسوبية، ذات الطابع التجاري أساسًا، مثل كابلات الألياف البصرية الممتدة تحت البحر أو الأقمار الصناعية أو أجهزة التوجيه أو مراكز الاتصال؛ وفي المقابل، تُزود المركبات وأنشطة الشحن ونظم مراقبة الحركة الجوية المدنية على نحو متزايد بنظم الملاحة التي تعتمد على الأقمار الصناعية لنظام تحديد المواقع العالمي، والتي تستخدمها أيضًا القوات المسلحة. وبالتالي، من المستحيل إلى حد بعيد التمييز بين البنية الأساسية الحاسوبية المدنية البحتة والعسكرية البحتة. وكما سيتبين لاحقًا، فإن هذا يشكل تحديًا خطيرًا أمام أحد المبادئ الرئيسية للقانون الدولي الإنساني، أن لا وهو مبدأ التمييز بين الأهداف العسكرية والأعيان المدنية. بالإضافة إلى ذلك، فحتى إذا لم تكن أجهزة الكمبيوتر أو النظم الحاسوبية العسكرية والمدنية كلها واحدة ولا فرق بينها، فإن الترابط البيني يعني أن تأثير هجوم على هدف عسكري قد لا يقتصر على ذلك الهدف. في الواقع، قد يخلف الهجوم الإلكتروني تبعات على مختلف النظم الأخرى، بما في ذلك النظم والشبكات المدنية، على سبيل المثال من خلال نشر برامج ضارة مثل الفيروسات أو الديدان إذا خرجت عن نطاق السيطرة. ويعني هذا أن الهجوم على نظام حاسوبي عسكري قد يؤدي أيضًا إلى تلف النظم الحاسوبية المدنية التي قد تكون بدورها حيوية لبعض الخدمات المدنية مثل الإمداد بالمياه أو الكهرباء أو نقل الأصول.

وليس لدينا في الوقت الراهن أمثلة واضحة على هجمات إلكترونية أثناء النزاعات المسلحة أو أمثلة تضرر فيها السكان المدنيون تضررًا بالغًا بالهجمات على شبكة حاسوبية أثناء النزاعات المسلحة. ومع ذلك، يبدو أن الخبراء التقنيين يتفقون على أنه من الممكن من الناحية التقنية، وإن كان صعبًا، التدخل عمدًا في نظم مراقبة الحركة الجوية أو غيرها من نظم النقل أو السدود أو محطات الكهرباء عبر الفضاء الإلكتروني. ولا يمكن تجاهل السيناريوهات الكارثية المحتملة، مثل تصادم الطائرات أو إطلاق الإشعاع من المحطات النووية أو إطلاق مواد كيميائية سامة من المحطات الكيميائية أو تعطيل البنية الأساسية والخدمات الحيوية، مثل شبكات الكهرباء أو المياه.

والسيناريوهات المذكورة قد لا تكون هي أكثر السيناريوهات احتمالًا من حيث وقوعها؛ فالعمليات الإلكترونية تحمل كل درجات ترجيح احتمال استعمالها للتلاعب في البنية الأساسية المدنية، مما يؤدي إلى إصابتها بخلل في أداء وظائفها أو تعطلها دون التسبب في الوفاة أو الإصابة الفورية. والتأثير الذي تخلفه هذه الوسائل والأساليب «غير الدموية» للقتال قد لا يكون مأساويًا على السكان المدنيين كالقصف بالمدافع أو القنابل. ورغم ذلك قد يكون شديدًا، على سبيل المثال في حالة تعطل الإمداد بالكهرباء أو المياه، أو في حالة انهيار شبكات الاتصالات أو النظام المصرفي. ويجب من ثم أن يوضح هذا التأثير وكيفية أخذه في الحسبان في إطار قواعد القانون الدولي الإنساني.

دفع بعض المعلقين بأن تهديد الهجمات على شبكات الكمبيوتر المسؤولة عن تشغيل البنية الأساسية المدنية على نطاق واسع ينبغي أن لا يُبالغ في تقديره ولا سيما لأن الأسلحة الإلكترونية الهجومية يجب أن تُصمم بطريقة شديدة الخصوصية لكي تؤثر على النظم الحاسوبية

22 يحلل Stefano Mele السيناريوهات المحتملة للتدخل في الأنواع المختلفة من النظم العسكرية والمدنية ويشير إلى أن التلاعب في نظم إدارة شبكات الكهرباء ربما يشكل أكبر تهديد في الوقت الراهن. انظر:
Stefano Mele, 'Cyber warfare and its damaging effects on citizens', September 2010, متاح عبر الرابط التالي: http://www.stefanomele.it/public/documenti/185DOC-937.pdf.

المستهدفة على وجه التحديد (مثل فيروس «ستوكسنت» Stuxnet على سبيل المثال)،[23] ومن ثم ليس من السهل إعادة توجيهها نحو أهداف أخرى.[24] كذلك، في نظام الإنترنت الذي يتسم بالترابط البيني على الصعيد الدولي ووسط اقتصاد العولمة، قد تعزف الدول عن تدمير بعضها البعض لأن العواقب، التي تطال النظم المالية على سبيل المثال، قد تلحق بها أضرارًا قدر ما تلحق بخصومها.[25] وقد يكون هذا صحيحًا أو غير صحيح. ولما كانت الهجمات على شبكات الكمبيوتر قادرة على استهداف الأعيان المدنية، أو قد تكون عشوائية في بعض الأحوال أو تستخدم بطريقة عشوائية، أو يمكن أن يكون لها عواقب عرضية مدمرة تلحق بالبنية الأساسية المدنية والسكان المدنيين، فإن هذه كلها أسباب كافية لتوضيح القواعد المنطبقة على سير العمليات العدائية التي يجب على أطراف النزاع مراعاتها.

دور القانون الدولي الإنساني

في ضوء هذه المقدمة، هل يعالج القانون الدولي الإنساني العواقب المحتملة للحرب الإلكترونية على السكان المدنيين؟

لا تشير أحكام القانون الدولي الإنساني على وجه التحديد إلى العمليات الإلكترونية. ولهذا السبب، ولما كان استغلال التكنولوجيا الإلكترونية ظاهرة جديدة نسبيًا ويبدو أنها تؤدي في بعض الأحيان إلى استحداث تغيير نوعي كامل في وسائل وأساليب القتال، يدفع البعض من حين لآخر بأن القانون الدولي الإنساني غير متوائم مع العالم الإلكتروني ولا يمكن تطبيقه على الحرب الإلكترونية.[26] ومع ذلك، فإن عدم وجود إشارات محددة في القانون الدولي الإنساني إلى العمليات الإلكترونية لا يعني أن هذه العمليات غير خاضعة لقواعد القانون

23 أطلق ما يسمى فيروس «ستوكسنت» على مرفق تخصيب اليورانيوم الإيراني في «نطنز»؛ حيث تشير التقارير إلى أنه أدى إلى تدمير ألف جهاز طرد مركزي. وأشارت التقارير التي أوردتها الصحف إلى أن الولايات المتحدة أو إسرائيل أو كلتيهما كانتا وراء إطلاق هذا الفيروس، غير أن هذا أمر لم يُعترف به رسميًا.
David Albright, Paul Brannan and Christina Walrond, 'Did Stuxnet take out 1,000 centrifuges ,at the Natanz enrichment plant? Preliminary assessment', ISIS Report, 22 December 2010
متاح عبر الرابط التالي:
http//:isis-online.org/isisreports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/;
David E. Sanger, 'Obama order sped up wave of cyberattacks against Iran', in The New York Times, 1 June 2012,
متاح عبر الرابط التالي:
http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattack-sagainst-iran. html?pagewanted=all&_moc.semityn.www

24 Thomas Rid, 'Think again: cyberwar', in *Foreign Policy*, March/April 2012, pp. 5 ff.,
متاح عبر الرابط التالي:
http://www.foreignpolicy.com/articles/2012/02/27/cyberwar?print=yes&hidecomments=yes&page=full;
Thomas Rid and Peter McBurney, 'Cyber-weapons', in *The RUSI Journal*, February–March ,2012
Vol. 157, No. 1, pp. 6–13;
وانظر أيضًا:
Maggie Shiels, 'Cyber war threat exaggerated claims security expert', in *BBC News*, 16 ,February 2011
متاح عبر الرابط التالي: http://www.bbc.co.uk/news/technology-12473809.

25 يرى Stefano Mele (الحاشية 22 أعلاه) أن هذا هو السبب في أن شن هجمات إلكترونية ضخمة على النظم المالية في الدول الأجنبية أمر غير مرجح.

26 Charles J. Dunlap Jr., 'Perspectives for cyber strategists on law for cyberwar', in *Strategic Studies Quarterly*, Spring 2011, p. 81.

الدولي الإنساني. فالتكنولوجيات الجديدة من جميع الأنواع تُطور طوال الوقت ويتسع القانون الدولي الإنساني بما فيه الكفاية لاستيعاب هذه التطورات الجديدة. ويحظر القانون الدولي الإنساني أو يقيد استخدام أسلحة معينة على وجه التحديد (الأسلحة الكيماوية أو البيولوجية أو الألغام المضادة للأفراد على سبيل المثال). وهو كذلك ينظم، من خلال قواعده العامة، جميع وسائل وأساليب القتال، بما في ذلك استعمال جميع الأسلحة. وعلى وجه التحديد، تنص المادة 36 من البروتوكول الإضافي الأول لاتفاقيات جنيف 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 الملحق «البروتوكول» أو أية قاعدة أخرى من قواعد القانون الدولي التي يلتزم بها الطرف السامي المتعاقد.

وبخلاف الالتزام المحدد الذي يفرضه على الدول الأطراف في البروتوكول الإضافي الأول، تبين هذه القاعدة أن قواعد القانون الدولي الإنساني تنطبق على التكنولوجيا الجديدة.

ومع ذلك، فإن الحرب الإلكترونية تتحدى بعضًا من أكثر الافتراضات الأساسية للقانون الدولي الإنساني. أولًا، يفترض القانون الدولي الإنساني أن أطراف النزاع معلومة ومحددة. ولا يمكن التسليم بهذا الأمر دائمًا حتى في النزاعات المسلحة التقليدية، ولا سيما النزاعات المسلحة غير الدولية. ومع ذلك، في العمليات الإلكترونية التي تحدث يوميًا، فإن عدم الكشف عن الهوية هو القاعدة وليس الاستثناء. ويبدو من المستحيل في بعض الحالات تتبع مصدر هذه العمليات، وحتى عندما يكون هذا ممكنًا، فإنه يستغرق وقتًا طويلًا في معظم الحالات. ولما كان القانون كله قائمًا على إسناد المسؤولية (في القانون الدولي الإنساني إلى طرف في النزاع أو إلى فرد)، تنشأ صعوبات رئيسية على وجه الخصوص، إذا لم يكن من الممكن تحديد هوية مرتكب عملية معينة ومن ثم لا يمكن تحديد علاقة العملية بنزاع مسلح معين، فسيكون من الصعب للغاية تحديد ما إذا كان القانون الدولي الإنساني ينطبق حتى على العملية. ومن ثم، على سبيل المثال، إذا تعرضت البنية الأساسية لحكومة ما لهجوم ولكن لم يكن من الواضح من يقف وراء الهجوم، فمن الصعب تحديد من هي أطراف النزاع المسلح، ومن ثم تحديد ما إذا كان هناك نزاع مسلح أصلًا. وبالمثل، حتى إذا كانت أطراف النزاع معلومة، قد يكون من الصعب إسناد الفعل إلى طرف واحد معين. ثانيًا، يستند القانون الدولي الإنساني إلى افتراض أن وسائل وأساليب القتال سيكون لها آثار عنيفة في العالم المادي. ومن المرجح أن يكون للكثير من العمليات الإلكترونية آثار تخريبية ولكنها ليست مدمرة من الناحية المادية بشكل مباشر. ثالثًا، يتأسس هيكل القواعد التي تحكم سير العمليات العدائية بأسره- ولا سيما مبدأ التمييز- على افتراض أن معظم الأعيان المدنية والأهداف العسكرية يمكن تمييزها. وفي مسرح عمليات الحرب الإلكترونية، من المرجح أن يكون هذا هو الاستثناء وليس القاعدة، لأن أغلب البنية الأساسية الإلكترونية حول العالم (الكابلات الممتدة تحت البحر، وأجهزة التوجيه، والخوادم، والأقمار الصناعية) تخدم الاتصالات المدنية والعسكرية على حد سواء.

يسعى التحليل التالي من ثم إلى استكشاف كيفية تفسير قواعد القانون الدولي الإنساني لكي تكون منطقية في العالم الإلكتروني، وكيف يمكن للتكنولوجيا الإلكترونية أن تتماس مع حدود هذه القواعد. وكما سيتبين فيما يلي، لعل من المبكر للغاية أن نقدم إجابات قاطعة عن الكثير من الأسئلة المثارة لأن الأمثلة قليلة والحقائق غير واضحة على الإطلاق ولا تزال ممارسات الدول فيما يتعلق بتفسير القواعد المنطبقة وتنفيذها في حاجة إلى تطوير. وحتى الآن، يعد دليل تالين المتعلق بالقانون الدولي المنطبق على عمليات حرب الفضاء الإلكتروني (يشار إليه فيما يلي باسم «دليل تالين») هو الإجراء الأشمل الذي يسعى إلى تفسير قواعد

القانون الدولي (الحق في الحرب وقانون الحرب) في إطار الحرب الإلكترونية.[27] وقد صاغ هذا الدليل مجموعة من الخبراء بناء على دعوة من مركز الامتياز التعاوني للدفاع عن الفضاء الإلكتروني التابع لمنظمة حلف شمال الأطلسي، وهو يقدم مجموعة مفيدة من القواعد التي تقترن بتعليق يعكس مختلف الآراء بشأن المسائل الشائكة التي تثيرها هذه التكنولوجيا الجديدة. وشاركت «اللجنة الدولية» في مداولات مجموعة الخبراء بوصفها مراقبًا، إلا أنها لا توافق على جميع الآراء الواردة في الدليل.

انطباق القانون الدولي الإنساني على العمليات الإلكترونية: ما هو النزاع المسلح في الفضاء الإلكتروني؟

لا ينطبق القانون الدولي الإنساني إلا إذا نُفذت العمليات الإلكترونية في سياق نزاع مسلح وكانت مرتبطة به. وبالتالي، ينبغي أن لا يُثار أي جدل إزاء الرأي القائل بأن العمليات الإلكترونية حين تنفذ في سياق نزاع مسلح دائر، فإنها تخضع لقواعد القانون الدولي الإنساني ذاتها التي يخضع لها النزاع: على سبيل المثال، إذا قام أحد أطراف النزاع، بالتزامن مع قصف بالمدفعية أو القذائف أو بالإضافة إليها، أيضًا بإطلاق هجوم إلكتروني على النظم الحاسوبية لخصمه.

ومع ذلك، فإن عددًا من العمليات التي يشار إليها على أنها من قبيل الحرب الإلكترونية قد لا تُنفذ في سياق نزاع مسلح على الإطلاق. وقد تؤدي مصطلحات مثل «الهجمات الإلكترونية» أو «الإرهاب الإلكتروني» إلى استدعاء فكرة أساليب الحرب، إلا أن العمليات التي تشير إليها لا تُنفذ بالضرورة في نزاع مسلح. ويمكن للعمليات الإلكترونية أن تستخدم، بل هي تستخدم فعلًا، في جرائم ترتكب في حالات يومية لا تتعلق بالحرب على الإطلاق.

ويكون التصنيف أصعب في الحالات الأخرى التي تقع في مرتبة متوسطة بين حالات النزاعات المسلحة القائمة التي تُحارب باستخدام الوسائل التقليدية والعمليات الإلكترونية، وكذلك الحالات التي تقع بالكلية خارج نطاق النزاع المسلح. وهذا هو الحال، لا سيما، عندما تكون الهجمات على شبكات الكمبيوتر هي العمليات العدائية الوحيدة التي تُنفذ بل وأكثر من ذلك إذا ظلت أفعالًا منفردة. وهذا السيناريو ليس سابقًا لأوانه تمامًا. ففيروس «ستوكسنت»، الذي يبدو أنه استهدف مرفق تخصيب اليورانيوم في جمهورية إيران الإسلامية في «نطنز»، يظل إلى الوقت الراهن هجومًا منفردًا على شبكة الكمبيوتر (حتى إذا نُفذ على مدى فترة زمنية)، وربما أطلقته دولة أو أكثر ضد جمهورية إيران الإسلامية. وعلى الرغم من أن تصنيف الهجوم على أنه نزاع مسلح لم يظهر في محادثات الدول، ذهب بعض المعلقين في تفكيرهم إلى أن الهجوم إذا نفذته دولة، فإنه يصل إلى حد النزاع المسلح الدولي.[28] ثمة

27 Michael N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, Cambridge, 2013 (forthcoming).
«دليل تالين» متاح عبر الرابط التالي: http://www.ccdcoe.org/249.html.

28 Michael N. Schmitt, 'Classification of cyber conflict', in *Journal of Conflict and Security Law*, Vol. 17, Issue 2, Summer 2012, p. 252;
انظر أيضًا:
Gary Brown, 'Why Iran didn't admit Stuxnet was an attack', in *Joint Force Quarterly*, Issue 63, 4th Quarter 2011, p. 71,
متاح عبر الرابط التالي: http://www.ndu.edu/press/why-iran-didntadmit-stuxnet.html . لا يعالج G. Brown مسألة تصنيف النزاع، بل يرى أن فيروس «ستوكسنت» يصل بوضوح إلى حد الهجوم، وربما يخالف الحظر المفروض على استخدام القوة وقانون الحرب.

سيناريو آخر متصور وهو العمليات الواسعة النطاق والمستمرة التي تنفذها جماعة مسلحة منظمة غير حكومية ضد البنية الأساسية الحكومية. فهل يمكن أن تصل هذه العمليات إلى حد النزاع المسلح غير الدولي؟

في إطار قواعد القانون الدولي الإنساني الحالية، هناك نوعان- ونوعان فقط- من النزاع المسلح: النزاعات المسلحة الدولية، والنزاعات المسلحة غير الدولية. ولن تُناقش في هذا المقال جميع معايير وجود النزاعات المذكورة. بل ستُعالج بعض الجوانب التي يبدو أنها تؤدي إلى إثارة أسئلة بالغة الصعوبة فيما يتعلق بالعمليات الإلكترونية.

النزاعات المسلحة الدولية

تنص المادة 2 المشتركة بين اتفاقيات جنيف الأربع لعام 1949 على أن النزاع المسلح الدولي هو أي «حالة حرب معلنة أو اشتباك مسلح آخر ينشب بين طرفين أو أكثر من الأطراف السامية المتعاقدة، حتى لو لم يعترف أحدها بحالة الحرب».

لا يوجد أي تعريف آخر للنزاعات المسلحة الدولية في أي معاهدة أخرى، ومن المقبول الآن، أن النزاع المسلح الدولي، على حد تعبير المحكمة الجنائية الدولية ليوغوسلافيا السابقة ينشب «عندما يكون هناك لجوء إلى القوة المسلحة بين الدول».[29] ويعتمد تطبيق القانون الدولي الإنساني على الحالة الواقعية وليس على إدراك حالة النزاع المسلح من جانب الأطراف فيه. والسؤال المحدد الذي يثار في سياق الحرب الإلكترونية هو ما إذا كان النزاع المسلح الدولي يمكن أن يبدأ بهجوم على شبكة كمبيوتر في ظل غياب أي استخدام (حركي) آخر للقوة. وتعتمد الإجابة على ما إذا كان الهجوم على شبكة الكمبيوتر (1) يمكن إسناده إلى الدولة (2) ويصل إلى حد اللجوء إلى القوة- وهو مصطلح ليس له تعريف في إطار القانون الدولي الإنساني.

إسناد التصرف إلى الدولة

يمكن أن تؤدي مسألة إسناد عملية معينة إلى دولة معينة إلى إثارة أسئلة بالغة الصعوبة في الفضاء الإلكتروني حيث يكون عدم الكشف عن الهوية هو القاعدة وليس الاستثناء. ومع ذلك، ما دامت الأطراف لا يمكن تحديد هويتها كدولتين أو أكثر، فمن المستحيل أن يُصنف النزاع على أنه نزاع مسلح دولي. وعلى الرغم من أن هذا التحدي يتعلق بالوقائع لا بالناحية القانونية، فمن سبل التغلب على عدم اليقين الذي يعتري الحقائق استخدام الافتراضات القانونية. فعلى سبيل المثال، إذا كان الهجوم على شبكة الكمبيوتر يُشن من البنية الأساسية الحكومية لدولة معينة، فإن الافتراض الذي يمكن تقديمه هو أن العملية تسند إلى الدولة- خاصة في ضوء قاعدة القانون الدولي التي تنص على أن الدول يجب عليها أن لا تسمح، عن علم، بأن تستخدم أراضيها للقيام بأفعال تتعارض مع حقوق دول أخرى.[30] ومع ذلك، هناك اعتراضان على هذا النهج.

الأول، أن قواعد القانون الدولي القائمة لا تؤيد هذا الافتراض. فعلى سبيل المثال، لا تتضمن المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دوليًا أي قواعد بشأن

29 International Criminal Tribunal for the Former Yugoslavia (ICTY), *Prosecutor v. Tadic*, Case No. IT-94-1-A, Appeals Chamber Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, 2 October1995, para. 70 (emphasis added).

الحالات المنصوص عليها في المادة 1 (4) من البروتوكول الإضافي الأول تعتبر أيضًا نزاعات مسلحة دولية للدول الأطراف في البروتوكول الإضافي الأول.

30 محكمة العدل الدولية، قضية *قناة كورفو (المملكة المتحدة ضد ألبانيا)*، الحكم الصادر في 9 نيسان/ أبريل 1949، الصفحة 22؛ وانظر أيضًا: القاعدة 5 من «دليل تالين» الحاشية 27 أعلاه.

31 محكمة العدل الدولية، قضية *منصات النفط (قضية جمهورية إيران الإسلامية ضد الولايات المتحدة الأمريكية)*، الحكم الصادر في

افتراض إسناد التصرف إلى دولة معينة. أيضًا، وضعت محكمة العدل الدولية حدًا مرتفعًا لإسناد التصرف إلى دولة معينة في سياق حق الدفاع عن النفس. فقد قررت المحكمة فعليًا، في قضية منصات النفط، أن عبء الإثبات يقع على عاتق الدولة التي تحتج بحق الدفاع عن النفس:

> المحكمة ببساطة عليها أن تقرر ما إذا كانت الولايات المتحدة قد أثبتت أنها ضحية «هجوم مسلح» شنته إيران حتى تبرر لها استخدامها القوة المسلحة في الدفاع عن النفس؛ ويقع عبء إثبات الوقائع التي تبين وجود الهجوم المذكور على عاتق الولايات المتحدة.[31]

وعلى الرغم من أن هذه العبارة صدرت في سياق حق الدفاع عن النفس في إطار حق اللجوء إلى القوة، فيمكن تعميمها على جميع المسائل الواقعية المتعلقة بإسناد التصرف إلى دولة معينة. وبما أنه افتراض حول الوقائع، فسيكون من غير المنطقي افتراض حقائق لغرض واحد معين وليس لغرض آخر.

ثانيًا، من شأن هذا الافتراض أيضًا أن يكون بعيد المدى للغاية في السياق المحدد للحرب الإلكترونية. فنظرًا لصعوبة تحصين البنية الأساسية الحاسوبية من التلاعب، والسهولة التي يمكن للشخص أن يتحكم بها عن بُعد في جهاز كمبيوتر ويتخفى تحت هوية مختلفة في الفضاء الإلكتروني، فإن هذا سيلقي بعبء ضخم للغاية على الحكومات من حيث تحميلها مسؤولية جميع العمليات التي تُطلق من أجهزة الكمبيوتر الخاصة بها دون أي دليل آخر.[32]

ثمة مسألة أخرى تخضع للمناقشة المتكررة وهي إسناد المسؤولية إلى الدولة عن الهجمات الإلكترونية التي تطلقها أطراف خاصة، مثل مجموعات القرصنة. فبعيدًا عن المسائل الواقعية التي يثيرها عدم الكشف عن هوية منفذي العمليات الإلكترونية، ترد القواعد القانونية الخاصة بإسناد مسؤولية الأفعال التي ترتكبها أطراف خاصة إلى الدولة في المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دوليًا.[33] وعلى وجه الخصوص، تتحمل الدولة المسؤولية عن تصرف شخص أو مجموعة من الأشخاص «إذا كان الشخص أو مجموعة الأشخاص يتصرفون في الواقع بناء على تعليمات تلك الدولة أو بتوجيهات منها أو تحت رقابتها لدى القيام بذلك التصرف».[34] ويجب توضيح ما يعنيه «التوجيه أو الرقابة» على وجه التحديد في إطار القانون الدولي بمرور الوقت. وتشترط محكمة العدل الدولية، لكي يُسند فعل طرف خاص (سواء كان فردًا أو عضوًا في جماعة منظمة) إلى الدولة، أن يتعين إثبات الرقابة أو السيطرة الفعلية للدولة على العملية في السياق الذي ارتُكبت فيه الانتهاكات المزعومة، وليس بشكل عام إزاء مجمل التصرفات التي يقوم بها الأشخاص أو مجموعات الأشخاص الذين ارتكبوا الانتهاكات.[35] وفي ظل غياب هذه الرقابة على العملية المحددة،

6 تشرين الثاني/ نوفمبر 2003، الفقرة 57.

32 يتخذ «دليل تالين» وجهة نظر قانونية مماثلة في القاعدة 7: «إن مجرد أن عملية إلكترونية قد أطلقت أو وجهت بطريقة أخرى من بنية أساسية إلكترونية حكومية لا يعد دليلًا كافيًا على إسناد مسؤولية تلك العملية إلى هذه الدولة، بل هو مؤشر على أن الدولة المذكورة لها صلة بالعملية».

33 لجنة القانون الدولي، مشاريع المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دوليًا، حولية لجنة القانون الدولي، 2001، المجلد الثاني (الجزء الثاني). أعيد إصدار النص بحيث يبدو كما يرد في مرفق قرار الجمعية العامة 83/56 الصادر في 12 كانون الأول/ ديسمبر 2001، والمنقح بالوثيقة رقم A/56/49(Vol. I)/Corr.4 (ويشار إليها فيما يلي باسم «المواد المتعلقة بمسؤولية الدول»).

34 المادة 8 من المواد المتعلقة بمسؤولية الدول.

35 محكمة العدل الدولية، *الأنشطة العسكرية وشبه العسكرية في نيكاراغوا وضدها (نيكاراغوا ضد الولايات المتحدة الأمريكية)*، الحكم الصادر في 27 حزيران/ يونيو 1986، الفقرتان 115 و116 (يشار إليها فيما يلي باسم «قضية نيكاراغوا»)؛ ومحكمة العدل الدولية، *القضية المتعلقة بتطبيق اتفاقية منع جريمة الإبادة الجماعية والمعاقبة عليها (البوسنة والهرسك ضد صربيا والجبل الأسود)*، الحكم الصادر في 26 شباط/ فبراير 2007، الفقرات 400-406.

فلا يمكن إسنادها إلى الدولة حتى في حالة ارتكابها على يد جماعة ذات درجة كبيرة من الاعتماد على سلطات الدولة.[36] وفي السياق ذاته، يشترط شرح المواد المتعلقة بمسؤولية الدول أن توجه الدولة العملية المحددة أو تراقبها وأن يكون التصرف جزءًا لا يتجزأ من تلك العملية.[37] وذهبت المحكمة الجنائية الدولية ليوغوسلافيا السابقة خطوة أبعد ودفعت بأنه حيثما كانت جماعة منظمة، من قبيل جماعات المعارضة المسلحة، فيكفي أن تمارس سلطات الدولة «رقابة عامة» على هذه الجماعة المنظمة ذات الهيكل القيادي المتسلسل دون الحاجة إلى ممارسة سيطرة أو توجيه محدد على التصرفات الفردية.[38] ومع ذلك، فقد أقرت المحكمة أيضًا أنه عندما تكون الدولة المسيطرة ليست هي الدولة الإقليمية، «يلزم تقديم المزيد من الأدلة الموسعة والدامغة لإثبات أن الدولة تسيطر فعلًا على الوحدات والجماعات»- مما يعني أن من الأصعب إثبات مشاركة الدولة في تخطيط العمليات العسكرية أو دورها التنسيقي.[39] ينص شرح لجنة القانون الدولي على ما يلي: «ستكون مسألة تقدير في كل حالة من حيث ما إذا كان تصرف معين قد نُفذ أو لم يُنفذ تحت رقابة الدولة بالقدر الذي ينبغي به أن يسند إليها السلوك الخاضع للرقابة».[40] إلا أن هذه المناقشة ليست حكرًا على الفضاء الإلكتروني. فما أن تثبت الوقائع، تنطبق المعايير القانونية ذاتها التي تنطبق في أي حالة أخرى تسند فيها إلى دولة ما تصرفات أطراف خاصة. ومن المرجح بدرجة كبيرة أن تكمن الصعوبة، مرة أخرى في هذا الصدد، في تقييم الوقائع.

اللجوء إلى القوة المسلحة

المعيار الثاني الذي يجب تحقيقه هو معيار «اللجوء إلى القوة المسلحة» بين الدول.

وقبل الانتقال إلى المسائل التي تثيرها الحرب الإلكترونية في هذا الصدد، يجدر أن نوضح بشكل موجز جدًا أن تصنيف أي نزاع على أنه نزاع مسلح دولي في إطار القانون الدولي الإنساني (قانون الحرب) منفصل عن مسألة الحق في اللجوء إلى القوة. ويتداخل فرعا القانون في كثير من المجالات، بما في ذلك الحرب الإلكترونية. فبموجب الحق في اللجوء إلى القوة، يكون السؤال هو ما إذا كانت العمليات الإلكترونية- ومتى- تصل إلى حد استخدام القوة في إطار المعنى المقصود في المادة 2 (4) من ميثاق الأمم المتحدة و/ أو إلى هجوم مسلح في إطار المعنى المقصود في المادة 51 من ميثاق الأمم المتحدة، وفي أي ظروف تؤدي إلى تفعيل الحق في الدفاع عن النفس.[41] وأيًا كانت الآراء الواردة في هذه المناقشة حول

36 قضية *نيكاراغوا*، الحاشية 35 أعلاه، الفقرة 115.

37 تقرير لجنة القانون الدولي عن أعمال دورتها الثالثة والخمسين (من 23 نيسان/ أبريل إلى 1 حزيران/ يونيو ومن 2 تموز/ يوليو إلى 10 آب/ أغسطس 2011)، وثيقة الأمم المتحدة رقم A/56/10، التعليق على المادة 8 من مشاريع المواد المتعلقة بمسؤولية الدول، الفقرة 3.

38 ICTY, *Prosecutor v. Dusko Tadic*, IT-94-1, Appeals Chamber Judgment of 15 July 1999, para. 120.
يقال في بعض الأحيان إن المسألة المعروضة أمام المحكمة كانت تتعلق بتصنيف النزاع كنزاع غير دولي أو دولي؛ إلا أن الدفع أن المسألتين منفصلتان تمامًا غير مقنعة إذ أنها تؤدي إلى الاستنتاج بأن دولة ما يمكن أن تكون طرفًا في نزاع بحكم سيطرتها على جماعة مسلحة منظمة ولكنها ليست مسؤولة عن الأفعال المرتكبة أثناء ذلك النزاع.

39 المرجع السابق، الفقرات 138-140.

40 التعليق على المادة 8 من مشاريع المواد المتعلقة بمسؤولية الدول، الحاشية 37 أعلاه، الفقرة 5.

41 Marco Roscini, 'World wide warfare – jus ad bellum and the use of cyber force', in *Max*

الحق في اللجوء إلى القوة، ينبغي الإشارة إلى أن أهداف تنظيم حق اللجوء إلى القوة وقانون الحرب مختلفة تمامًا: فبينما ينظم الحق في اللجوء إلى القوة على وجه التحديد العلاقات بين الدول واشتراطات اللجوء المشروع إلى القوة بين الدول، ينظم قانون الحرب سلوك أطراف النزاع وهدفه، وغرضه هو حماية ضحايا الحرب من العسكريين والمدنيين. ومن ثم، فإن فعلًا معينًا قد يشكل لجوءًا إلى القوة لأغراض تصنيف نزاع مسلح دولي، دون الإخلال بالسؤال المطروح حول ما إذا كان يشكل أيضًا استخدامًا للقوة في إطار المعنى المقصود في المادة 2 (4) من ميثاق الأمم المتحدة (على الرغم من أنه أمر محتمل)، ناهيك بالهجوم المسلح في إطار المادة 51. وينطبق هذا التمييز بالتساوي على العمليات الإلكترونية.

ننتقل إلى قانون الحرب، فنقول إنه لا يوجد تعريف في المعاهدات لمعنى القوة المسلحة في القانون الدولي الإنساني لأنه معيار من معايير الفقه القانوني. وتقليديًا، يتمثل الهدف من الحرب في الانتصار على العدو، وفي الحرب التقليدية، يتضمن النزاع نشر الوسائل العسكرية بما يفضي إلى المواجهة العسكرية. وبالتالي، عندما تُستخدم وسائل وأساليب القتال التقليدية- مثل القصف بالمدافع أو القنابل أو نشر القوات- فلا خلاف على أن هذه التصرفات تصل إلى حد القوة المسلحة. بيد أن الهجمات على شبكات الكمبيوتر لا تتضمن استخدام أسلحة من هذا القبيل.

وفي ظل غياب الأسلحة التقليدية والقوة الحركية، ما الذي يمكن اعتبار أنه يصل إلى حد القوة المسلحة في العالم الإلكتروني؟

الخطوة الأولى هي مقارنة تأثير الهجمات على شبكات الكمبيوتر بالتأثير الناجم عن القوة الحركية. يرى أغلب المعلقين أنه إذا كان من الممكن إسناد المسؤولية عن هجوم على شبكة الكمبيوتر إلى دولة معينة وكان له التأثير نفسه الذي يحققه اللجوء الحركي إلى القوة، فإن هذا من شأنه أن يؤدي إلى نزاع مسلح دولي.[42] وفي الواقع، إذا تسبب الهجوم على شبكة الكمبيوتر في تصادم الطائرات أو القطارات، مما يؤدي إلى الوفاة أو الإصابة أو انتشار الفيضانات وما يترتب عليها من تبعات واسعة النطاق، فلن تكون هناك أسباب كثيرة تبرر معاملة الحالة معاملة مختلفة عن الهجمات المكافئة المنفذة من خلال وسائل أو أساليب القتال الحركية.

Planck Yearbook of United Nations Law, Vol. 14, 2010, p. 85; Michael N. Schmitt, 'Computer network attack and the use of force in international law: thoughts on a normative framework', in *Columbia Journal of Transnational Law*, Vol. 37, 1998–1999, p. 885; Herbert S. Lin, 'Offensive cyber operations and the use of force', in *Journal of National Security Law and Policy*, Vol. 4, 2010, p. 63; David P. Fidler, 'Recent developments and revelations concerning cybersecurity and cyberspace: implications for international law', in ASIL Insights, 20 June 2012, Vol. 16, no. 22; *Tallinn Manual*, above note 27, Rules 10–17.

42 M. N. Schmitt, 'Classification of cyber conflict', الحاشية 28 أعلاه، الصفحة 251; Knut Dörmann, 'Applicability of the Additional Protocols to Computer Network Attacks', ICRC, 2004, p. 3, متاح عبر الرابط التالي: http://www.icrc.org/eng/resources/documents/misc/68lg92.htm؛ Heather Harrison Dinniss, *Cyber Warfare and the Laws of War*, Cambridge University Press, Cambridge, 2012, p. 131; Nils Melzer, *Cyberwarfare and International Law*, UNIDIR Resources Paper, 2011, p. 24, متاح عبر الرابط التالي: http://www.unidir.ch/pdf/ouvrages/pdf-1-92-9045-011-L-en.pdf يرى Nils Melzer أنه لما كان وجود نزاع مسلح دولي يعتمد على وقوع عمليات عدائية مسلحة بين الدول، فإن العمليات الإلكترونية لا تؤدي إلى نزاع مسلح من خلال إحداث الوفاة أو الإصابة أو الدمار فحسب، بل أيضًا من خلال التأثير سلبًا على العمليات العسكرية أو القدرة العسكرية للدولة.

هذه المقارنة مفيدة من ثم للحالات التي تؤدي فيها الهجمات على شبكات الكمبيوتر إلى وفاة أو إصابة أو أضرار مادية أو دمار في البنية الأساسية. ولكن، قد لا يكون من الكافي تسجيل النطاق الكامل للتأثير المحتمل للعمليات الإلكترونية والأضرار التي قد تسببها، والتي قد لا تشبه بالضرورة التأثير المادي للأسلحة التقليدية. والعمليات الإلكترونية يُلجأ إليها في كثير من الأحيان لا من أجل إلحاق التدمير أو الضرر المادي بالبنية الأساسية العسكرية أو المدنية، بل من أجل التأثير على عملها، على سبيل المثال عن طريق التلاعب فيها، بل أيضًا القيام بذلك دون اكتشاف التلاعب. فعلى سبيل المثال، يمكن ترك شبكة الكهرباء دون أن تُمس، ولكن تُعطل عن طريق هجوم على شبكة الكمبيوتر. وبالمثل، يمكن التلاعب في النظام المصرفي في بلد ما دون أن يلحق أي ضرر مادي بالبنية الأساسية ودون أن يُلاحظ التلاعب في النظام الأساسي لبعض الوقت. وللوهلة الأولى، وحتى في ظل غياب الوسائل العسكرية التقليدية أو حتى الدمار المادي المباشر، فإن التأثير المحتمل لهذه الأعطال- الذي قد يكون أوسع أو أشد بكثير من تدمير مبنى معين أو مجموعة من المباني على سبيل المثال- على السكان، يؤيد تصنيفها على أنها لجوء إلى القوة. ولكن، قد تسعى الدول- وحتى الدول الضحية- إلى تجنب تصعيد المواجهات الدولية أو قد يكون لديها أسباب تجعلها تتجنب التعامل مع أنواع الهجمات من هذا القبيل على أنها تفضي إلى نزاع مسلح. ومن الصعب في هذه المرحلة استنتاج أي مواقف قانونية، لأن الدول يبدو أنها تلتزم الصمت في أغلب الأحوال في مواجهة الهجمات الإلكترونية.[43] وفي ظل غياب ممارسات واضحة للدول، هناك نُهج عديدة محتملة لمعالجة هذه المسألة.

ومن النُهج المتبعة النظر إلى أي عملية إلكترونية عدائية تؤثر على عمل الأعيان على أنها لجوء إلى القوة المسلحة. وإن هدف القانون الدولي الإنساني وغرضه على وجه العموم، ولا سيما في ظل غياب مستوى العنف الذي يحدد وجود نزاع مسلح دولي- وهو تجنب وجود فجوة في الحماية، ولا سيما حماية السكان المدنيين من أضرار الحرب- يؤيدان إدماج العمليات الإلكترونية من هذا القبيل في تعريف القوة المسلحة لأغراض بدء نزاع مسلح. وكذلك، بالنظر إلى أهمية أن تولي الدولة أهمية لحماية البنية الأساسية الحيوية في استراتيجياتها الإلكترونية، فمن المتوقع أن تتعامل مع الهجمات على شبكات الكمبيوتر التي تشنها دولة أخرى بهدف تعطيل هذه البنية الأساسية على أنها بداية نزاع مسلح.[44] وبالإضافة

43 انظر أيضًا G. Brown، الحاشية 28 أعلاه.

44 N. Melzer، الحاشية 42 أعلاه، الصفحة 14. يرى Mezler أن الإشارة قد تتم إلى مفهوم البنية الأساسية الحيوية للنظر في «نطاق وتأثيرات» هجوم معين على شبكة الكمبيوتر لأغراض تحديد نزاع مسلح في إطار المعنى المقصود في المادة 51 من ميثاق الأمم المتحدة. للاطلاع على السياسة الفرنسية، انظر:
Agence Nationale de la Sécurité des Systèmes d'Information, Défense et sécurité des systèmes d'informations, متاحة عبر الرابط التالي: http://www.ssi.gouv.fr/IMG/pdf/2011-02 15_De-fense_et_securite_des_systemes_d_information_strategie_de_la_France.pdf; وللاطلاع على السياسة الألمانية، انظر: Bundesamt für Sicherheit in der Informationstechnik, Schutz Kritischer In-frastrukturen, متاحة عبر الرابط التالي:
https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Strategie/Kritis/Kritis_node.html;
وللاطلاع على السياسة الكندية، انظر: National Strategy for Critical Infrastructure، متاحة عبر الرابط التالي:
http://www.publicsafety.gc.ca/prg/ns/ci/ntnl-eng.aspx;
وللاطلاع على سياسة المملكة المتحدة، انظر: The UK Cyber Security Strategy، متاحة عبر الرابط التالي:
http://www.cabinetoffice.gov.uk/resource-library/cyber-security-strategy;
وللاطلاع على السياسة الأسترالية، انظر: CERT Australia, Australia's National Computer Emergency Response Team متاحة عبر الرابط التالي:.https://www.cert.gov.au/

إلى ذلك، وفي ظل عدم وجود نزاع مسلح، فإن هذه الحالة لن تخضع لنطاق الحماية التي يوفرها القانون الدولي الإنساني. وفي هذه الحالة، قد تنطبق فروع أخرى من القانون مثل الحق في اللجوء إلى القوة أو قانون الجريمة الإلكترونية أو قانون الفضاء أو قانون الاتصال وتوفر حمايتها الخاصة. ولا يدخل تحليل تأثيرها ضمن نطاق هذا المقال، ومع ذلك فإن فروع القانون الأخرى كلها تطرح مجموعة الأسئلة الخاصة بها. فعلى سبيل المثال، قد ينطبق القانون الدولي لحقوق الإنسان، ولكن هل يستوفي الهجوم على شبكة كمبيوتر، الذي يُنفذ من الجانب الآخر من العالم ضد البنية الأساسية المدنية، شرط السيطرة الفعلية لأغراض انطباق قانون حقوق الإنسان؟ أيضًا، إلى أي مدى يوفر قانون حقوق الإنسان حماية كافية من تعطيل البنية الأساسية الذي لا يتحدد تأثيره على حياة السكان المدنيين بالضرورة بشكل فوري؟

ثمة نهج آخر يتمثل في عدم التركيز حصرًا على التأثيرات المتماثلة للعملية الإلكترونية، بل النظر في مجموعة من العوامل التي تدل على اللجوء إلى القوة المسلحة. وتشمل هذه العوامل مستوى معينًا لشدة التبعات المترتبة على العمليات الإلكترونية، والوسائل المستخدمة، واشتراك القوة المسلحة أو فروع أخرى من الحكومة في العملية العدائية، وطبيعة الهدف (عسكري أم لا)، ومدة العملية. ولنأخذ على ذلك مثالًا خارج العالم الإلكتروني، فإذا قتل رئيس أركان القوات المسلحة لدولة ما في هجوم جوي شنته دولة أخرى، فإن هذا يعتبر بالتأكيد فعلًا يصل إلى حد النزاع المسلح الدولي. ولكن إذا قتل بسبب إرسال خطاب مسمم، فهل يعتبر هذا أيضًا في حد ذاته فعلًا يصل إلى حد النزاع المسلح الدولي؟[45] وماذا إذا كان الهدف مدنيًا؟ وهل وسائل تدمير البنية الأساسية ذات صلة بالمسألة؟ فعلى سبيل المثال، إذا خُربت أجزاء من منشأة نووية بفعل عناصر أجنبية متسللة، فهل يصل هذا أيضًا إلى حد اللجوء إلى القوة المسلحة؟ وهل يختلف الأمر إذا كان الهدف عسكريًا أو مدنيًا؟

من الممكن في العالم الإلكتروني على سبيل المثال أن تتعامل الدول مع الهجمات على شبكات الكمبيوتر الخاصة ببنيتها الأساسية العسكرية بأسلوب يختلف عن الهجمات التي تؤثر على نظمها المدنية. ولعل هذا الأمر ليس منطقيًا تمامًا من الناحية التقنية لأن استخدام القوة هو استخدام القوة، سواء ضد هدف عسكري أو عين مدنية. إلا أن مستوى الضرر الذي تستعد الدولة لتقبله قد يكون أقل عندما يتعلق الأمر بالعمليات الموجهة نحو إضعاف قدراتها العسكرية.

وباتباع هذا النهج، إذا كان الهجوم على شبكة الكمبيوتر دقيقًا ومدته قصيرة فقط، فقد لا يعتبر من قبيل القوة المسلحة إلا إذا وصلت تبعاته إلى مستوى معين من الشدة. ويبدو أن مثال الهجوم بفيروس «ستوكسنت» الذي أفادت عنه الصحافة يدل على أن الهجمات على شبكات الكمبيوتر ربما تظل- على أقل تقدير لبعض الوقت- أفعالًا عدائية منفصلة تقوم بها دولة ضد دولة أخرى، دون أن تقترن بعمليات حركية أخرى، خاصة إذا كان المهاجم يرغب في أن يظل مجهول الهوية، أو يرغب في أن يظل الهجوم دون أن يُكتشف لفترة من الوقت، أو يرغب (لأسباب سياسية أو غيرها) في تجنب تصعيد القوة واستمرار العمليات العدائية والنزاع المسلح. فإذا اعتمدنا على ما إذا كان الهجوم الحركي الذي يحقق التأثيرات نفسها يصل إلى حد القوة المسلحة، فربما كان علينا أن نخلص إلى استنتاج مفاده أن الهجوم المذكور يشكل قوة مسلحة لأن التقارير أفادت أن فيروس «ستوكسنت» قد تسبب في التدمير المادي لألف جهاز طرد مركزي من طراز IR-1 مما استلزم الاستعاضة عنه بمرفق تخصيب

45 في كتاب *كيف يوفر القانون الحماية في الحرب؟* المجلد الأول، الطبعة الثالثة، «اللجنة الدولية»، جنيف، 2011، الصفحة 122، يميِّز «ماركو ساسولي»، و«أنطوان بوفييه»، و«آن كوينتن» بين القوة التي تنفذها القوات المسلحة أو غيرها من عناصر الدولة: «عندما تلتقي القوات المسلحة التابعة لدولتين، تكفي رصاصة واحدة تُطلق أو شخص واحد يقع في الأسر (وفقًا لتعليمات الحكومة) لكي ينطبق القانون الدولي الإنساني، بينما في حالات أخرى (على سبيل المثال، الإعدام دون محاكمة بمعرفة عميل سري ترسله حكومته إلى الخارج)، من الضروري وجود مستوى أعلى من العنف».

اليورانيوم في «نطنز».[46] وفي الواقع، لو أن أجهزة الطرد المركزي في منشأة نووية قد دُمرت بفعل قصف قامت به القوات الجوية لدولة أخرى، فإن هذا الهجوم يعتبر من قبيل اللجوء إلى القوة المسلحة ويؤدي إلى نزاع مسلح دولي. ولكن نظرًا لأن أساليب الهجوم لم تكن حركية ولم ترد أي تقارير عن هجمات أخرى ذات صلة بها، ولم تسبب أي أضرار معروفة خارج أجهزة الطرد المركزي، فهناك من يقول إنها لا تصل إلى حد القوة المسلحة المفضي إلى نزاع مسلح دولي.

وخلاصة القول: لم يتضح بعد ما إذا كانت الدول- وتحت أي ظروف- ستعامل الهجمات على شبكات الكمبيوتر على أنها لجوء إلى القوة المسلحة. وأن مجرد التلاعب في نظام مصرفي أو غيره من أشكال التلاعب في البنية الأساسية الحيوية، حتى إذا أدى إلى خسارة اقتصادية فادحة، ربما سيؤدي إلى توسيع نطاق مفهوم القوة المسلحة بما يتجاوز الهدف والغرض منه- فالتأثير ليس مكافئًا للدمار الذي تتسبب فيه الوسائل المادية. إلا أن تدمير البنية الأساسية الحيوية من قبيل نظم الإمداد بالكهرباء أو المياه، الذي سيؤدي حتمًا إلى مصاعب شديدة يعاني منها السكان إذا استمر فترة زمنية معينة، حتى إذا لم يفض إلى الوفاة أو الإصابة، ربما يجب اعتباره من قبيل القوة المسلحة. وعلى الرغم من أن التأثيرات ليست مكافئة للتأثيرات المادية، فهي بالتحديد من فئة التبعات الخطيرة التي يسعى القانون الدولي الإنساني إلى حماية السكان المدنيين منها.

وصحيح أن الدول لا تستطيع التحايل على التزاماتها بموجب القانون الدولي من خلال إطلاق تسمياتها الخاصة على الفعل. وقد انفصل تطبيق قانون النزاع المسلح الدولي عن الحاجة إلى إصدار إعلانات رسمية قبل عقود طويلة من أجل تجنب حالات قد تمنع فيها الدول الحماية التي يوفرها هذا الفرع من القانون. وتوضح هذا المادة 2 المشتركة حيث يشير تعليق «اللجنة الدولية» عليها إلى ما يلي:

> يمكن للدولة دائمًا أن تتظاهر، حين ترتكب فعلًا عدائيًا ضد دولة أخرى، بأنها لا تشن حربًا، بل تقوم بمجرد إجراء شرطي أو تتصرف في إطار الدفاع المشروع عن النفس. وإن تعبير «النزاع المسلح» يجعل هذه الحجج أقل سهولة.[47]

وعلى الرغم من ذلك، وإن كان صحيحًا أن تصنيف النزاع، في حادثة معينة، لا يعتمد على موقف الدول المعنية، فإن ممارسات الدول والاجتهاد القانوني يحددان تفسير تعريف «النزاعات المسلحة الدولية» في إطار القانون الدولي. ومن المحتمل أن لا يتحدد تصنيف النزاعات الإلكترونية بطريقة حاسمة إلا من خلال ممارسات الدول في المستقبل.

النزاعات المسلحة غير الدولية

فيما يتعلق بالنزاعات المسلحة غير الدولية في العالم الإلكتروني، يتمثل السؤال الرئيسي في كيفية التمييز بين السلوك الإجرامي والنزاع المسلح. فمن الشائع أن نسمع أو نقرأ أن أعمال القراصنة أو غيرها من المجموعات، بما في ذلك مجموعات مثل «أنونيموس»

46 هذا هو رأي M. N. Schmitt، الحاشية 28 أعلاه، الصفحة 252؛ حول الأضرار الناجمة، انظر D. Albright و P. Brannan و C. Walrond، الحاشية 23 أعلاه؛ D. E. Sanger، الحاشية 23 أعلاه.

47 Jean Pictet (ed.), *Commentary on the Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field*, ICRC, Geneva, 1952, p. 32.
هذه مسألة مختلفة تتعلق بنية القتال: فالأعمال المنفردة في بعض الأحيان لا تصنف على أنها تصل إلى حد النزاع المسلح، ولا يرجع السبب في هذا إلى أنها لا تصل إلى مستوى شدة معين، بل لأنها تفتقر إلى نية القتال، ومنها على سبيل المثال التوغلات العرضية عبر الحدود؛ انظر:
UK Joint Service Manual of the Law of Armed Conflict, Joint Service Publication 383, 2004, para. 3.3.1, متاح عبر الرابط التالي:
http://www.mod.uk/NR/rdonlyres/82702E75-9A14-4EF5-B414-49B0D7A27816/0/JSP3832004Edition.pdf.

(Anonymous) أو «ويكيليكس» (Wikileaks)، يشار إليها على أنها «حرب».[48] وبطبيعة الحال، لا تشير هذه التصريحات بالضرورة إلى وجود نزاع مسلح أو بشكل أدق نزاع مسلح غير دولي، بالمفهوم القانوني. ومع ذلك، يجدر توضيح معايير تصنيف حالة معينة على أنها نزاع مسلح غير دولي.

وفي ظل عدم وجود تعريف في المعاهدات، أدت ممارسات الدول والفقه القانوني إلى وضع تعريف للنزاعات المسلحة غير الدولية أوجزته المحكمة الجنائية الدولية ليوغوسلافيا السابقة على النحو التالي: يوجد نزاع مسلح غير دولي «حيثما كان هناك... عنف مسلح طويل الأمد بين سلطات حكومية وجماعات مسلحة منظمة أو بين هذه الجماعات داخل دولة ما».[49] وقد اندرج شرط «الأمد الطويل» بمرور الوقت تحت شرط يقتضي أن يصل العنف إلى مستوى شدة معين. وبالتالي، يحدد المعياران وجود نزاع مسلح غير دولي: يجب أن تصل المواجهة المسلحة إلى حد أدنى من الشدة ويجب أن تظهر الأطراف المشاركة في النزاع حدًا أدنى من التنظيم.[50]

الجماعات المسلحة المنظمة

لكي تُصنف جماعة على أنها جماعة مسلحة منظمة يمكنها أن تكون طرفًا في نزاع في إطار المعنى المقصود في القانون الدولي الإنساني، يجب أن يكون لديها مستوى من التنظيم يتيح لها أن تنفذ أعمالاً حربية مستمرة وأن تمتثل للقانون الدولي الإنساني. وتشمل العناصر الاسترشادية وجود جدول تنظيمي يبين هيكل القيادة، وهيئة تطلق العمليات وتجمع الوحدات المختلفة، والقدرة على تجنيد وتدريب مقاتلين جدد، ووجود قواعد داخلية.[51] وعلى الرغم من أن الجماعة لا تحتاج إلى أن يكون لديها مستوى التنظيم نفسه الذي لدى القوات المسلحة التابعة للدولة، فيتعين عليها أن تمتلك مستوى معينًا من تدرج السلطة ونظامًا للتأديب والقدرة على تنفيذ الالتزامات الأساسية للقانون الدولي الإنساني.[52]

وفيما يتعلق بالقراصنة أو غيرهم من المجموعات المماثلة، فإن السؤال الذي يثار هو

48 انظر على سبيل المثال:
Mark Townsend et al., 'WikiLeaks backlash: The first global cyber war has begun, claim ,hackers', in *The Observer*, 11 September 2010
متاح عبر الرابط التالي
http://www.guardian.co.uk/media/2010/dec/11/wikileaks-backlash-cyber-war;
Timothy Karr, 'Anonymous declares cyberwar against "the system"', in *The Huffington Post*, 3 June 2011, متاح عبر الرابط التالي:
http://www.huffingtonpost.com/timothy-karr/anonymousdeclares-cyberw_b_870757.html.

49 المحكمة الجنائية الدولية ليوغوسلافيا السابقة، Prosecutor v. Tadic، الحاشية 29 أعلاه، الفقرة 70.

50 هناك نوعان من النزاعات المسلحة غير الدولية. وجميع النزاعات المسلحة غير الدولية مشمولة في المادة 3 المشتركة بين اتفاقيات جنيف؛ بالإضافة إلى أن أحكام البروتوكول الإضافي الثاني تنطبق على النزاعات المسلحة غير الدولية «التي تدور على إقليم أحد الأطراف السامية المتعاقدة بين قواته المسلحة وقوات مسلحة منشقة أو جماعات نظامية مسلحة أخرى وتمارس تحت قيادة مسؤولة على جزء من إقليمه من السيطرة ما يمكنها من القيام بعمليات عسكرية متواصلة ومنسقة، وتستطيع تنفيذ هذا البروتوكول» (المادة 1 (1) من البروتوكول الإضافي الثاني).

51 للاطلاع على استعراض بالعوامل الاسترشادية التي أخذت بها المحكمة الجنائية الدولية ليوغوسلافيا السابقة في سوابقها القضائية، انظر:
ICTY, Prosecutor v. Boskoski, IT-04-82-T, Trial Chamber Judgement of 10 July 2008, paras 199–203.
وانظر أيضًا: ICTY, Prosecutor v. Limaj, IT-03-66-T, Trial Chamber Judgement of 30 November 2005, paras 94–134; ICTY, Prosecutor v. Haradinaj, IT-04-84-T, Trial Chamber Judgement of 3 April 2008, para. 60.

52 المحكمة الجنائية الدولية ليوغوسلافيا السابقة، Prosecutor v. Boskoski، المرجع السابق، الفقرة 202.

ما إذا كانت الجماعات المنظمة تمامًا عبر شبكة الإنترنت يمكن أن تشكل جماعات مسلحة في إطار المعنى المقصود في القانون الدولي الإنساني. وكما يقول «مايكل شميت»:

إن أعضاء المنظمات الافتراضية ربما لا يلتقون أبدًا بل وربما لا يعرفون النشاط الفعلي لبعضهم البعض. ومع ذلك، فيمكن لهذه المجموعات أن تتصرف بطريقة منسقة ضد الحكومة (أو جماعة مسلحة منظمة)، وأن تتلقى أوامر من قيادة افتراضية، وأن تكون منظمة للغاية. فعلى سبيل المثال، من العناصر التي قد تُكلف بها المجموعة تحديد نقاط الضعف في الأنظمة المستهدفة، وقد يكون العنصر الثاني هو تطوير برامج ضارة لاستغلال نقاط الضعف المذكورة، وقد يكون العنصر الثالث تنفيذ العمليات، وقد يكون العنصر الرابع الحفاظ على دفاعات إلكترونية ضد الهجمات المضادة.[53]

ومع ذلك، فإن اشتراط أن يكون بالجماعات المسلحة المنظمة بعض أشكال القيادة المسؤولة والقدرة على تنفيذ القانون الدولي الإنساني، يبدو وكأنه يستبعد المجموعات المنظمة افتراضيًا من تصنيفها ضمن الجماعات المسلحة المنظمة؛ فقد يكون من الصعب على سبيل المثال إقامة نظام تأديب فعال داخل هذه الجماعة من أجل كفالة احترام القانون الدولي الإنساني.[54] وبمعنى آخر، من غير المرجح أن تمتلك مجموعات القراصنة التي ترتبط فقط عبر الاتصال الافتراضي، التنظيم أو هيكل القيادة (والتأديب) اللازم لتشكيل طرف في النزاع.[55]

الشدة

ينظم القانون الدولي الإنساني العمليات الإلكترونية التي تُنفذ في سياق نزاع مسلح غير دولي قائم وتتصل به. والسؤال الذي يثار، على الرغم من أنه قد يبدو سابقًا لأوانه في هذه المرحلة، هو ما إذا كان مستوى الشدة المطلوب لتحقيق نزاع مسلح غير دولي يمكن الوصول إليه في حالة استخدام الوسائل الإلكترونية فقط (على افتراض أن هناك طرفين أو أكثر في النزاع).

وعلى عكس تصنيف النزاعات المسلحة الدولية، هناك اتفاق على أن النزاع المسلح غير الدولي لا يوجد إلا إذا وصلت العمليات العدائية إلى مستوى شدة معين. وقد أشارت المحكمة الجنائية الدولية ليوغوسلافيا السابقة إلى عدد من العوامل الاسترشادية التي يجب أخذها في الحسبان لتقييم شدة النزاع، مثل الطابع الجماعي للعمليات العدائية، واللجوء إلى القوة العسكرية وليس مجرد القوة الشرطية، وخطورة الهجمات، وما إذا كانت هناك زيادة في الاشتباكات المسلحة، وانتشار الاشتباكات على الأرض وعلى مدى فترة زمنية، وتوزيع الأسلحة بين طرفي النزاع، وعدد المدنيين الذين يضطرون إلى النزوح من مناطق القتال، وأنواع الأسلحة المستخدمة، ولا سيما استخدام الأسلحة الثقيلة وغيرها من العتاد العسكري، مثل الدبابات وغيرها من المركبات الثقيلة، وحجم الدمار، وعدد الإصابات الناجمة عن القصف أو القتال.[56] فهل يمكن للعمليات الإلكترونية وحدها أن تصل إلى مستوى الشدة المطلوب؟

53 M. N. Schmitt، الحاشية 28 أعلاه، الصفحة 256.
54 المرجع السابق، الصفحة 257.
55 انظر المناقشة الواردة في «دليل تالين» حول الأنواع المختلفة من الجماعات التي يمكن وضعها في الاعتبار، الحاشية 27 أعلاه، التعليق على القاعدة 23، الفقرات 13-15.
56 انظر على سبيل المثال: ICTY, Prosecutor v. Limaj، الحاشية 51 أعلاه، الفقرات 135-170؛ والمحكمة الجنائية الدولية ليوغوسلافيا السابقة، Prosecutor v. Haradinaj، الحاشية 51 أعلاه، الفقرة 49؛ وProsecutor v. Boskoski، الحاشية 51 أعلاه، الفقرات 177-178.

ونقول مرة أخرى إن نقطة البداية تتمثل في مقارنة شدة التبعات بشدة التبعات المترتبة على العمليات الحركية. ولا يوجد سبب يجعل العمليات الإلكترونية لا تحقق التبعات العنيفة نفسها التي تحققها العمليات الحركية، إذا استخدمت على سبيل المثال لفتح بوابات السدود، أو التسبب في تصادم الطائرات أو القطارات. وفي هذه الحالات، وإذا لم يكن هذا العنف مجرد عنف متقطع، فربما يستوفي المستوى المحدد لنشوب نزاع مسلح غير دولي.

ولكن العمليات الإلكترونية في حد ذاتها لا تُحدث الكثير من التأثيرات المذكورة أعلاه كمؤشرات شدة العنف (الاشتباكات المسلحة، ونشر القوات المسلحة، واستخدام الأسلحة الثقيلة، وما إلى ذلك). ومن المرجح أن تكون تبعات العمليات الإلكترونية وحدها هي التي تكون شديدة بما يكفي للوصول إلى مستوى الشدة المطلوب، مثل التدمير الواسع النطاق أو التأثيرات الكارثية التي تلحق بأجزاء كبيرة من السكان من خلال الهجمات المتكررة.

الملخص

من المرجح أن لا يثار خلاف على الفكرة التي تقول إن القانون الدولي الإنساني ينطبق على العمليات الإلكترونية التي تُنفذ في إطار نزاع مسلح دولي أو غير دولي تدور رحاه بجانب العمليات الحركية. أما في ظل غيات العمليات الحركية، فإن الحرب الإلكترونية «البحتة» تُستبعد من النظرية، ولكن لم يتضح بعد ما إذا كنا سنرى الكثير من الأمثلة في الواقع العملي في المستقبل القريب.

ولا يزال من غير الواضح على وجه الخصوص في أي اتجاه ستسير ممارسات الدول. فنظرًا لعزوف الدول عن الاعتراف بحالات النزاع المسلح، ولا سيما النزاع المسلح غير الدولي، فقد نجد أننا أمام توجه نحو تجنب الحديث عن النزاع المسلح. ولا يرجع السبب في هذا إلى احتمال عدم الكشف عن هوية مرتكبي الكثير من الهجمات على شبكات الكمبيوتر والمشكلات العملية المتعلقة بإسناد المسؤولية فحسب، بل أيضًا إلى حقيقة أن أغلب الحالات لا تصل إلى حد حالات خطيرة تشهد تدميرًا ماديًا ناتجًا عن الهجوم على شبكات الكمبيوتر، بل بالأحرى إلى درجة تلاعب منخفض المستوى بالبنية الأساسية لا تنتج عنه إراقة الدماء. وقد تختار الدول التعامل مع هذه الحالات في إطار إنفاذ القانون والقانون الجنائي ولا تنظر إليها على أنها تخضع للإطار القانوني المنطبق على النزاعات المسلحة.

تطبيق القواعد التي تحكم سير العمليات العدائية

إذا كانت العمليات الإلكترونية تُنفذ في إطار نزاع مسلح، فهي تخضع لقواعد القانون الدولي الإنساني، ولا سيما القواعد التي تحكم سير العمليات العدائية. ولما كانت الأسلحة الإلكترونية تعتمد على التكنولوجيات الجديدة، فإنها لا تشكك في حد ذاتها في انطباق القانون الدولي الإنساني عليها.

غير أن الحرب الإلكترونية تشكل تحديات خطيرة أمام المبادئ الأساسية التي يستند إليها القانون الدولي الإنساني، ولا سيما التمييز- وهو القدرة المحتملة على التمييز- بين الأهداف العسكرية والأعيان المدنية. وبالتالي، فإن السؤال المطروح لا يتعلق كثيرًا بما إذا كانت القواعد التي تحكم سير العمليات العدائية تنطبق على الحرب الإلكترونية، بل بالأحرى كيف ستُطبق؛ أي كيف يمكن ترجمتها بحيث يكون لها مدلول منطقي في هذا العالم الجديد.

ما الأفعال التي تخضع لقواعد القانون الدولي الإنساني التي تحكم سير العمليات العدائية؟

قبل الانتقال إلى القواعد التي تحكم سير العمليات العدائية- ولا سيما مبادئ التمييز والتناسب والاحتياط- من المهم معالجة مسألة ظلت موضوعًا للمناقشة لفترة من الوقت، أن لا وهي نوع السلوك، ولا سيما نوع العملية الإلكترونية، الذي يؤدي إلى تطبيق القواعد التي تحكم سير العمليات العدائية. والسؤال بالغ الأهمية. فإذا كانت عملية إلكترونية معينة خاضعة لمبدأ التمييز، فمن المحظور توجيهها مباشرة ضد البنية الأساسية المدنية، وإذا وُجّهت صوب هدف عسكري، فإن التأثيرات العرضية التي تلحق بالبنية الأساسية المدنية يجب أن تؤخذ في الاعتبار إذا كانت العملية خاضعة لمبدأ التناسب.

والسبب الذي يؤدي إلى إثارة هذه المناقشة هو أن الفضاء الإلكتروني يختلف عن مسارح الحروب التقليدية في أن وسائل وأساليب الهجوم لا تتضمن استخدام القوة الحركية التقليدية، أو ما يفهم عمومًا على أنه عنف. وبالتالي، يمكن لعدد من العمليات الإلكترونية أن تلحق تأثيرًا شديدًا على العين المستهدفة من خلال تعطيلها عن العمل، ولكن دون إلحاق الأضرار المادية بالعين التي تحدث في الحرب التقليدية.

وبالتالي، من المهم للغاية أن توضح هذه المسألة في حالة السكان المدنيين. فحسبما يرى الشخص، من منظور ضيق أو منظور واسع، أنواع العمليات الإلكترونية التي تخضع للقواعد التي تحكم سير العمليات العدائية، يمكن أن تكون الأعمال التالية محظورة أو قانونية في سياق نزاع مسلح:

- تعطيل شبكة الكهرباء المدنية أو نظام لمعالجة المياه (دون إلحاق أضرار مادية بها).
- توجيه هجوم يترتب عليه حرمان نظام مصرفي من خدمة الإنترنت مما يكون له تأثير كبير على قدرة عدة ملايين من عملاء المصرف على الحصول على الخدمات المصرفية.[57]
- تعطيل الموقع الإلكتروني لهيئة سوق المال لدولة معادية دون التأثير على أعمال التداول بها.[58]
- توجيه هجوم يترتب عليه الحرمان من الخدمات المقدمة عبر نظام خاص لحجز رحلات الطيران عبر الإنترنت من أجل التسبب في إزعاج السكان المدنيين.
- حجب موقعي «الجزيرة»، أو «بي بي سي» لاحتوائهما على معلومات تسهم في تقديم الصورة الميدانية للعدو.
- منع جميع السكان من الدخول على موقع «فيسبوك» لاحتوائه على دعاية تدعو إلى التمرد؛
- إغلاق شبكة الإنترنت وشبكات الهاتف المحمول في منطقة معينة من البلد لمنع الدعاية التي يطلقها الخصم.[59]

57 حدث هذا في إستونيا في أيار/ مايو 2007؛ انظر: Larry Greenemeier, 'Estonian attacks raise concern over cyber «nuclear winter» ', in *Information Week*, 24 May 2007, متاح عبر الرابط التالي: http://www.informationweek.com/estonian-attacks-raise-concern-over-cybe/199701774.

58 انظر على سبيل المثال: Yolande Knell, 'New cyber attack hits Israeli stock exchange and airline', in *BBC News*, 16 January 2012, متاح عبر الرابط التالي: http://www.bbc.co.uk/news/world-16577184.

59 في مصر، قطعت الحكومة خدمة الإنترنت وشبكة الهاتف المحمول لمدة خمسة أيام لردع المتظاهرين: 'Internet blackouts: reaching for the kill switch', in The Economist, 10 February 2011, متاح عبر الرابط التالي: http//:www.economist.com/node .18112043/
اتخذت الحكومة الصينية تدابير مماثلة ردًا على الاضطرابات في «شينجيانغ» و«التبت»: Tania Branigan, 'China cracks down on text messaging in Xinjiang', in *The Guardian*, 29 February 2010, متاح عبر الرابط التالي: http://www.guardian.co.uk/world/2010/jan/29/xinjiangchin وانظر أيضًا: Tania Branigan, 'China cut off internet in area of Tibetan unrest', in *The Guardian*, 3 February

يؤدي هذا إلى سؤالين: الأول، هل قواعد القانون الدولي الإنساني الأساسية التي تحكم سير العمليات العدائية- وهي مبادئ التناسب والتمييز والاحتياط- لا تنطبق إلا على الهجمات الإلكترونية في إطار المعنى المقصود في القانون الدولي الإنساني، أم أنها تنطبق على العمليات العسكرية بصورة أكثر عمومًا؟ والثاني، أي العمليات الإلكترونية تشكل هجمات في إطار المعنى المقصود في القانون الدولي الإنساني؟

ما الذي يؤدي إلى تطبيق القواعد التي تحكم سير العمليات العدائية: «الهجمات» أم «العمليات العسكرية» أم «العمليات العدائية»؟

فيما يتعلق بالسؤال الأول، ينشأ الاختلاف في وجهات النظر من القاعدة العامة التي تحكم سير العمليات العدائية، بصيغتها الواردة في المادة 48 وما يليها من البروتوكول الإضافي الأول والمعترف بها على نطاق واسع ضمن القانون العرفي. تنص المادة 48 من البروتوكول الإضافي الأول على ما يلي:

> تعمل أطراف النزاع على التمييز بين السكان المدنيين والمقاتلين وبين الأعيان المدنية والأهداف العسكرية، ومن ثم توجه عملياتها ضد الأهداف العسكرية دون غيرها، وذلك من أجل تأمين احترام وحماية السكان المدنيين والأعيان المدنية. (إضافة تأكيد)

أما القواعد التالية التي تحكم سير العمليات العدائية فهي من ثم مصاغة في صورة قيود على الهجمات بشكل أكثر تحديدًا. فالمادة 51 من البروتوكول الإضافي الأول على سبيل المثال، بعد أن تبين في فقرتها الأولى أن «السكان المدنيين والأشخاص المدنيين يتمتعون بحماية عامة ضد الأخطار الناجمة عن العمليات العسكرية»، تستطرد لتنص على أنه «لا يجوز أن يكون السكان المدنيون بوصفهم هذا، وكذا الأشخاص المدنيون، محلًا للهجوم» وأن «الهجمات العشوائية محظورة». ويعرف الهجوم المخالف لمبدأ التناسب في المادة 51 (5) (ب) من البروتوكول الإضافي الأول على أنه «الهجوم الذي يمكن أن يتوقع منه أن يسبب خسارة في أرواح المدنيين أو إصابة بهم أو أضرارًا بالأعيان المدنية، أو أن يُحدث مزيجًا من هذه الخسائر والأضرار، يفرط في تجاوز ما ينتظر أن يسفر عنه ذلك الهجوم من ميزة عسكرية ملموسة ومباشرة». وتحظر المادة 51 (6) «هجمات الردع ضد السكان المدنيين أو الأشخاص المدنيين». وتنص المادة 52 على أن «تقصر الهجمات على الأهداف العسكرية فحسب». وينص مبدأ الاحتياط في المادة 57 على أن يتخذ عدد من الاحتياطات «فيما يتعلق بالهجمات». وهناك كثير من المواد التي تستخدم مصطلح «الهجوم» عند تقييد حقوق الأطراف المتحاربة.[60]

وبالتالي، تدور الحجة الأولى حول مسألة ما إذا كانت القواعد التي تحكم سير العمليات العدائية مقتصرة على تلك الأعمال العدائية التي تشكل هجمات (على النحو الوارد بالتعريف في المادة 49 من البروتوكول الإضافي الأول) أو ما إذا كانت تنطبق على طائفة أوسع من العمليات العسكرية. وقد اقترحت ثلاث وجهات نظر في إطار الحديث على نطاق أوسع.

يرى أغلب المعلقين أن هيكل البروتوكول الإضافي الأول وصياغته تبينان أن المادة

2012,

متاح عبر الرابط التالي :

http://www.guardian.co.uk/world/2012/feb/03/china-internet-links-tibetan-unrest.

60 انظر على سبيل المثال المواد 12 و54 و55 و56 من البروتوكول الإضافي الأول.

48 وإن كانت توفر مبدأ عامًا لحماية السكان المدنيين، فإن هذا المبدأ العام «مُفعّل» في المواد اللاحقة. فالعمليات الإلكترونية التي تشكل هجمات هي فقط التي تخضع لمبادئ التمييز والتناسب والاحتياط.[61] دفع «مايكل شميت» في هذا الصدد برأي مفاده أن بعض العمليات العسكرية يمكن أن تُوجه عمدًا ضد المدنيين، ومنها على سبيل المثال العمليات النفسية- التي تبين في رأيه أن العمليات العسكرية ليست كلها خاضعة لمبدأ التمييز.[62]

ويرى «نيلس ميلزر» أن النقاش حول مفهوم الهجوم لا يقدم إجابة شافية للسؤال لأن القواعد التي تحكم سير العمليات العدائية لا تنطبق على الهجمات فحسب، إذا تحدثنا بشكل دقيق، بل على عمليات أخرى كذلك. وهو يرى ما يلي:

> يقتضي الفهم الدقيق للقيود التي يفرضها القانون الدولي الإنساني على سير العمليات العدائية القول بأن انطباق هذه القيود على العمليات الإلكترونية لا يعتمد على ما إذا كانت العمليات المذكورة تصنف على أنها «هجمات» (وهي الصيغة الغالبة من تنفيذ العمليات العدائية)، بل على ما إذا كانت تشكل جزءًا من «العمليات العدائية» في إطار المعنى المقصود في القانون الدولي الإنساني.[63]

وهو يرى أن العمليات الإلكترونية التي تهدف إلى الإضرار بالخصم، سواء عن طريق التسبب مباشرة في الوفاة أو الإصابة أو الدمار أو عن طريق التأثير سلبًا على العمليات العسكرية أو القدرة العسكرية، يجب أن تعتبر عمليات عدائية.[64] فعلى سبيل المثال، فإن العمليات الإلكترونية التي تهدف إلى تعطيل أو تعجيز نظم الرادار أو نظم الأسلحة أو الإمداد بالخدمات اللوجستية أو شبكات الاتصال التي يتحكم فيها العدو عن طريق الكمبيوتر، تُصنف على أنها عمليات عدائية حتى إذا لم تتسبب في ضرر مادي. أما العمليات الإلكترونية التي تنفذ لتحقيق الغرض العام المتمثل في جمع المعلومات الاستخباراتية فلا تندرج ضمن العمليات العدائية. وفيما يتعلق بالتعطيل غير المدمر للأعيان المدنية، لا يخلص «ميلزر» إلى استنتاج قاطع، بل يشير إلى الإشكالية القائمة بين اعتماد تفسير للقانون مقيد للغاية أو متساهل للغاية.[65]

تتسم حجة «ميلزر» بالجاذبية في أنها تُعمِل الهدف والغرض المحدد للقواعد التي تحكم سير العمليات العدائية، أن لا وهو «ضرورة إبعاد المدنيين الأبرياء عن دائرة العمليات العدائية قدر الإمكان وأن يتمتعوا بالحماية العامة من الأخطار الناجمة عن العمليات العدائية».[66] ومع ذلك، تترك هذه الحجة أهم سؤال بلا إجابة، وهو ما إذا كانت العمليات العدائية التي تعطل البنية الأساسية المدنية دون تدميرها تندرج ضمن مفهوم العمليات العدائية.

ترى «هيذر هاريسون دينيس» أن حظر استهداف السكان المدنيين والأعيان المدنية لا يقتصر على الهجمات.[67] بل إنها تشير إلى صياغة المادة 48 من البروتوكول الإضافي

61 M. N. Schmitt, 'Cyber operations and the jus in bello: key issues', in *Naval War College International Law Studies*, Vol. 87, 2011, p. 91; Robin Geiss and Henning Lahmann, 'Cyber warfare: applying the principle of distinction in an interconnected space', in *Israeli Law Review*, Vol. 45, No. 3, November 2012, p. 2.

62 M. N. Schmitt، المرجع السابق، الصفحة 91.

63 N. Melzer ، الحاشية 42 أعلاه.

64 المرجع السابق، الصفحة 28.

65 المرجع السابق.

66 Y. Sandoz, C. Swinarski and B. Zimmermann (eds), Commentary on the Additional Protocols of 8 June1977 to the Geneva Conventions of 12 August 1949, ICRC/Martinus Nijhoff Publishers, Dordrecht, 1987, para. 1923

(ويشار إليه فيما يلي بالتعليق على البروتوكولين الإضافيين).

67 H. H. Dinniss، الحاشية 42 أعلاه، الصفحات 196-202.

الأول والعبارات الأولى من المادتين 51 و57 لتدفع بضرورة أن لا تقتصر حماية السكان المدنيين على الهجمات فحسب، بل كذلك بشكل أكثر عمومًا من تأثير العمليات العسكرية. وهي من ثم تسلم بأن مبادئ التمييز والتناسب والاحتياطات تنطبق كذلك على الهجمات على شبكات الكمبيوتر التي تندرج ضمن تعريف العملية العسكرية. ولكي يندرج ضمن التعريف، «يجب أن يكون الهجوم على شبكة الكمبيوتر مقترنًا بالقوة المادية، إلا أنه لا يتعين بالضرورة أن يفضي إلى تبعات عنيفة في حد ذاته».[68]

وعلى الرغم من هذه الآراء المؤيدة لتوسيع نطاق أنواع العمليات التي يجب أن تنطبق عليها القواعد التي تحكم سير العمليات العدائية، من الواضح أن الدول ميزت بالفعل في البروتوكول الإضافي الأول بين المبادئ العامة الواردة في افتتاحية كل من قواعد التمييز والاحتياط والقواعد المحددة ذات الصلة بالهجمات، وأنها خلصت إلى ضرورة تعريف الهجمات تعريفًا محددًا في المادة 49 من البروتوكول. ومن الصعب الخروج عن هذا الانقسام بين العمليات العسكرية والهجمات.

ومع ذلك، فإن الحجة التي تسوقها «دينيس» تعطي مدلولًا لحقيقة أن المواد 48 و51 و57 تتضمن قواعد عامة تفرض قيودًا على العمليات العسكرية وليس الهجمات فحسب، وسيكون من الصعب شرح مضمونها بطريقة أخرى. والتفسير المنهجي لهذه القواعد يعني أن الافتتاحية لها محتوى ذو دلالة وليست نصًا زائدًا. كذلك، فإن الرأي الذي قدمه «مايكل شميت» ومفاده أن بعض العمليات، مثل العمليات النفسية، يمكن توجيهها ضد المدنيين، مما يعني أن بعض العمليات العسكرية يمكن توجيهها ضد المدنيين، يستند إلى فهم خاطئ لمفهوم العمليات العسكرية. وفي الواقع، وإن كان صحيحًا أن بعض العمليات الإلكترونية، مثل العمليات النفسية، يمكن توجيهها ضد السكان المدنيين، يرجع السبب في هذا إلى أنها لا تندرج ضمن فئة العمليات العسكرية أو العمليات العدائية في إطار المعنى الذي يقصده واضعو البروتوكول. ويشير تعليق «اللجنة الدولية» إلى أن مصطلح «العمليات» في المادة 48 يعني العمليات العسكرية ويشير إلى «جميع التحركات والأعمال المرتبطة بالعمليات العدائية التي تضطلع بها القوات المسلحة».[69] ويوصف مصطلح «العمليات العسكرية» في المادة 51 بأنه «جميع التحركات والأنشطة التي تضطلع بها القوات المسلحة فيما يتعلق بالعمليات العدائية».[70] وفي المادة 57، فإنها «ينبغي أن تُفهم على أنها تعني أي تحركات أو مناورات أو أنشطة أخرى أيًا كان نوعها وتضطلع بها القوات المسلحة بهدف القتال».[71] وبمعنى آخر، لا تندرج العمليات من قبيل الدعاية أو التجسس أو العمليات النفسية ضمن مفاهيم العمليات العدائية أو العمليات العسكرية، ولا تخضع من ثم لمبادئ التمييز والتناسب والاحتياط، حتى إذا نفذتها القوات المسلحة.

وبالتالي، بينما قد يعمل بعض المضمون الأكثر تحديدًا في المادتين 51 و57 من البروتوكول الإضافي الأول على معالجة خصوصيات الهجمات، هناك حجة جيدة تذهب إلى أن العمليات العسكرية الأخرى لا يمكن استثناؤها تمامًا من الالتزامات بالتمييز والتناسب والاحتياط، وإلا فإن المادة 48 وافتتاحية المادتين 51 و57 ستصبح زائدة. ولكن لمّا كان هناك خلاف حول هذه المسألة، كان من الحكمة رغم ذلك إمعان النظر في تعريف «الهجوم» وأي أنواع العمليات الإلكترونية تندرج ضمنه. وفي الواقع، تندرج أغلب العمليات الإلكترونية الواردة في الأمثلة المذكورة أعلاه ضمن مفهوم الهجوم، وستُحظر إذا كانت موجهة نحو

68 المرجع السابق، الصفحة 201.
69 التعليق على البروتوكولين الإضافيين، الحاشية 68 أعلاه، الفقرة 1875.
70 المرجع السابق، الفقرة 1936.
71 المرجع السابق، الفقرة 2191.

البنية الأساسية المدنية. وبالتالي، سيتبين أن العمليات المذكورة في أغلب الأمثلة المقدمة أعلاه تصل إلى حد الهجمات، وبالتالي فإن مسألة ما إذا كانت الهجمات فقط أم «العمليات العدائية» أو «العمليات العسكرية» أيضًا تخضع للقواعد التي تحكم سير العمليات العدائية، إنما هي مسألة خلافية.

ما هو الهجوم؟

كما ذُكر آنفًا، تختلف العمليات في الفضاء الإلكتروني عن الحرب التقليدية في أن وسائل وأساليب الهجوم لا تتضمن استخدام القوة الحركية التقليدية أو ما يُفهم عمومًا على أنه عنف. ومع ذلك، ورد تعريف الهجمات في المادة 49 (1) من البروتوكول الإضافي الأول (الذي يعكس القانون الدولي الإنساني العرفي) على أنها «أعمال العنف الهجومية والدفاعية ضد الخصم». وكان هذا التعريف يدل على العنف المادي في أذهان واضعي البروتوكول.

أولًا، ينبغي الإشارة إلى أنه، استنادًا إلى حقيقة أن الهجوم يجب أن يكون عملًا من أعمال العنف، هناك اتفاق واسع النطاق اليوم على أن العنف لا يشير إلى وسائل الهجوم- التي تشمل الوسائل الحركية فقط.[72] والعمليات العسكرية التي تؤدي إلى تبعات عنيفة تشكل هجمات. فعلى سبيل المثال، لا خلاف على أن استخدام العناصر البيولوجية أو الكيماوية أو الإشعاعية يشكل هجومًا، حتى إذا لم يتضمن الهجوم استخدام القوة المادية.[73] وبالتالي، كان من المقبول لفترة طويلة أن ما يحدد الهجوم ليس عنف الوسائل، بل عنف التبعات.[74] ومن ثم، فحتى تدفق البيانات التي تمر عبر الكابلات أو القمر الاصطناعي يمكن أن تندرج ضمن مفهوم الهجوم.

ويكمن الخلاف في الجانب المتعلق بتأثيرات العمليات الإلكترونية. فهو ينتقل إلى تلك العمليات التي لا تسبب الوفاة أو الإصابة بين الأشخاص أو التدمير المادي أو الأضرار في الأعيان كما تفعل العمليات الحركية، بل تعطل عمل الأعيان دون أن تُحدث أضرارًا مادية فيها- كما هو الحال في الأمثلة المذكورة أعلاه. وكما تبين هذه الأمثلة، فإن تبعات العمليات الإلكترونية ليس لها بالضرورة تأثير عنيف ويظهر هذا في أنها لا تتسبب في تلف أو تدمير مادي. في الأمثلة المقدمة أعلاه، تكون التبعات في العالم المادي غير مباشرة في أغلب الأحوال: فعلى سبيل المثال، إذا تعطلت شبكة الكهرباء، فقد يؤدي هذا إلى انقطاع الكهرباء عن الخدمات الحيوية مثل المستشفيات. وفي بعض الحالات، تقتصر التبعات على القدرة على الاتصال أو مباشرة الأنشطة التجارية، كما يحدث عند تعطيل النظام المصرفي. فهل يمكن اعتبار هذه العمليات هجمات في إطار المعنى المقصود في المادة 49 من البروتوكول الإضافي الأول؟

72 Yoram Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflict*, Cambridge University Press, Cambridge, 2004, p. 84; M. N. Schmitt, الحاشية 61 أعلاه، الصفحة 5.

73 ICTY, *Prosecutor v. Dusko* Tadic´, Decision on the Defence Motion for Interlocutory Appeal, 2 October 1995, paras. 120 and 124 (بشأن الأسلحة الكيميائية)؛ و ودليل تالين، الحاشية 27 أعلاه، التعليق على القاعدة 30، الفقرة 3؛

Emily Haslam, 'Information warfare: technological changes and international law', in *Journal of Conflict and Security Law*, Vol. 5, No. 2, 2000, p. 170.

74 Michael N. Schmitt, 'Wired warfare: computer network attack and jus in bello', in *International Review of the Red Cross*, Vol. 84, No. 846, June 2002, p. 377; ودليل تالين، الحاشية 27 أعلاه، التعليق على القاعدة 30، الفقرة 3.

طرح رأيان فيما يتعلق بهذه المسألة. يشير «مايكل شميت» في كتاباته الأولى إلى أن:

العملية الإلكترونية، شأنها شأن أي عملية أخرى، هي هجوم عندما تؤدي إلى الوفاة أو الإصابة بين الأفراد، مدنيين كانوا أو مقاتلين، أو تفضي إلى الإضرار بالأعيان أو تدميرها، سواء كانت أهدافًا عسكرية أو أعيانًا مدنية.[75]

والضرر، في وجهة النظر المذكورة، يشير إلى الضرر المادي فقط. فالهجمات على شبكات الكمبيوتر التي لا تتسبب إلا في الإزعاج أو مجرد انقطاع مؤقت في عمل الأعيان، لا تشكل هجمات ما لم تترتب عليها معاناة بشرية. وبشكل حاسم، فإن مجرد تعطل عمل عين، بما لا يصل إلى حد التسبب في معاناة بشرية أو التسبب في أضرار مادية أو الخسارة الكاملة والدائمة لعمل العين المستهدفة، لا يصل إلى حد الهجوم.[76]

ويرى «كنوت دورمان» أن العمليات الإلكترونية يمكن أن تشكل أيضًا هجمات حتى إذا لم تؤد إلى تدمير العين. ويستند هذا الرأي إلى تعريف الهدف العسكري في المادة 52 (2) من البروتوكول الإضافي الأول التي تنص على أن الأهداف العسكرية هي تلك الأهداف التي «يحقق تدميرها التام أو الجزئي أو الاستيلاء عليها أو تعطيلها في الظروف السائدة حينذاك ميزة عسكرية أكيدة». ويتبين من مصطلح «تعطيل» أن من غير المهم ما إذا كانت العين قد عُطلت من خلال التدمير أو بأي وسيلة أخرى.[77] ويجيب النقاد قائلين إن تعريف الأهداف العسكرية ليس صحيحًا تمامًا لأنه يفترض ضمنًا وجود هجوم في المقام الأول ولا يعرف الهجوم في حد ذاته.[78] يخفق هذا النقد في الإقرار بأن مصطلح «تعطيل» يقصد به أن يشمل «أي هجوم يهدف إلى حرمان العدو من استعمال العين دون تدميرها بالضرورة».[79] ويبين هذا أن واضعي النص لم يكن في ذهنهم الهجمات الموجهة إلى تدمير الأعيان أو إلحاق الأضرار بها فحسب، بل كذلك الهجمات التي تهدف إلى حرمان العدو من استعمالها دون تدميرها بالضرورة. وبالتالي، على سبيل المثال، يمكن تعطيل نظام الدفاع الجوي لدى العدو من خلال عملية إلكترونية تمتد فترة معينة عن طريق التدخل في نظامه الحاسوبي ولكن دون تدمير بنيته الأساسية أو إلحاق الأضرار بها بالضرورة.[80]

75 M. N. Schmitt، الحاشية 61 أعلاه، الصفحة 6.

76 يتخذ Michael Schmitt رأيًا مختلفًا بعض الشيء ويدفع بأن «التدمير يشمل العمليات التي (تعطل) العين وإن لم تُلحق بها ضررًا ماديًا، مما يجعلها غير صالحة للعمل، كما في حالة العملية الإلكترونية التي تتسبب في تعطل نظام يعتمد على الكمبيوتر ما لم يتم إصلاحه»؛
International Attack, as a term of art in international law: the cyber operations context', in *2012 4th Conference on Cyber Conflict*, C. Czosseck, R. Ottis and K. Ziolkowski (eds), 2012, NATO ;CCD COE Publications, Tallinn, p. 291

وانظر أيضًا: M. N. Schmitt، الحاشية 28 أعلاه، الصفحة 252.

77 K. Dörmann، الحاشية 42 أعلاه، الصفحة 4.

78 M. N. Schmitt، الحاشية 61 أعلاه، الصفحة 8.

79 Michael Bothe, Karl Josef Partsch and Waldemar A. Solf, *New Rules for Victims of Armed Conflicts: Commentary to the Two 1977 Protocols Additional to the Geneva Conventions of 1949*, Martinus Nijhoff Publishers, Dordrecht, 1982, p. 325.

80 تشير التقارير إلى حدوث ذلك في هجوم جوي قامت به إسرائيل في أيلول/ سبتمبر 2007 على منشأة سورية يعتقد أنها تحوي برنامجًا لتطوير الأسلحة النووية. واخترقت إسرائيل الدفاعات الجوية السورية وتحكمت فيها أثناء الهجوم؛ انظر
'Arab & Israeli cyber-war', in *Day Press News*, 22 September 2009,
متاح عبر الرابط التالي:
http//:www.dp-news.com/en/detail.aspx?articleid55075=

ويعرف «دليل تالين» مؤخرًا الهجوم الإلكتروني بأنه «عملية إلكترونية، هجومية أو دفاعية، يتوقع منها بشكل معقول أن تحدث إصابة أو وفاة في صفوف الأشخاص أو أضرارًا أو دمارًا في الأعيان».[81] ومع ذلك، كما يبين التعليق، اختلف الخبراء حول ما يُفهم بالضبط على أنه «ضرر» يلحق بالأعيان، وما إذا كان تعطيل عمل عين معينة يندرج ضمن تعريفه وما نوع ذلك التعطيل.[82]

يكمن الضعف في الرأي الأول في أنه يفتقر إلى الشمول. أولًا، لن يكون من المنطقي أن نعتبر أن العين المدنية إذا أصبحت عديمة النفع، بغض النظر عن الطريقة التي تم بها ذلك، فإنها ليست متضررة. وإن تعطل شبكة الكهرباء عن العمل بفعل ضرر مادي أو تدخل في النظام الحاسوبي الذي تدار عن طريقه، لا يمكن أن يكون معيارًا مناسبًا. أما الرأي المعارض فيؤدي إلى استنتاج مفاده أن تدمير منزل واحد عن طريق القصف يعتبر هجومًا، إلا أن تعطيل شبكة الكهرباء التي تمد الآلاف أو ملايين السكان لا يعتبر كذلك.

ثانيًا، تعطي الإشارة إلى مبدأ التناسب مؤشرًا للتأثيرات العرضية التي تسعى القواعد التي تحكم سير العمليات العدائية إلى حماية المدنيين منها، أي الإفراط في «الخسارة العرضية لحياة المدنيين أو إلحاق الإصابة في صفوف المدنيين أو إلحاق الأضرار بالأعيان المدنية». ويختلف «الضرر» عن «التدمير». فهو يعني «الضرر... الذي يعطل قيمة شيء ما أو الانتفاع به...»[83] وبالتالي، فإن تعطيل عمل نظم معينة عن طريق التدخل في النظم الحاسوبية الأساسية المشغلة له يمكن أن يصل إلى حد الضرر ما دام يعطل الانتفاع به.

ثالثًا، فإن وجهة النظر التي ترى أن الفقدان الكامل والدائم للخصائص الوظيفية دون إلحاق ضرر مادي ليس له سند منطقي في مجال تكنولوجيا المعلومات. فلما كانت البيانات يمكن دائمًا استعادتها أو تغييرها، فلا يوجد فقدان دائم وكامل للخصائص الوظيفية لعين ما دون وقوع ضرر مادي. وبالتالي، يجب أن يُفهم الهجوم على أنه يشمل العمليات التي تعطل عمل الأعيان دون أن يلحق بها ضرر مادي أو تدمير، حتى إذا كان التعطيل مؤقتًا.

ومع ذلك، فإن التفسير الشديد العمومية لمصطلح «الهجوم» يعني أن جميع التدخلات في النظم الحاسوبية المدنية من شأنها أن تصل إلى حد الهجمات: تعطيل الاتصالات التي تتم عن طريق البريد الإلكتروني أو شبكات التواصل الاجتماعي أو تعطيل نظم الحجز أو التسوق عن طريق الإنترنت وما إلى ذلك. وإن المساواة بين هذه الأعطال التي تلحق في الأساس بنظم الاتصال والهجمات، ربما تتجاوز نطاق ما كانت تتصوره القواعد التي تحكم سير العمليات العدائية. وقد سعت هذه القواعد تقليديًا إلى منع إلحاق الضرر بالبنية الأساسية المدنية التي تتجلى على نحو ظاهر في العالم المادي، وليس التدخل في الدعاية أو الاتصالات أو الحياة الاقتصادية. وفي عالم اليوم، يؤدي اعتماد الحياة المدنية على نظم الاتصالات إلى غموض هذه الخطوط الفاصلة، وليس باليسير التمييز بين ما هو «مجرد» اتصال وما يتجاوز ذلك.

تقدم قواعد القانون الدولي الإنساني الحالية والهدف والغرض من هذه القواعد عددًا من المؤشرات للتمييز بين العمليات التي تصل إلى حد الهجمات والعمليات التي ليست كذلك.

81 Tallinn Manual، الحاشية 27 أعلاه، القاعدة 30.
82 المرجع السابق، التعليق على القاعدة 30، الفقرات 10-12.
83 *Concise Oxford Dictionary*.

أولًا، كما قيل آنفًا، لا يشمل مفهوم «الهجمات» نشر الدعاية أو حالات الحظر أو الوسائل غير المادية للحرب النفسية أو الاقتصادية.[84] أما العمليات الإلكترونية المكافئة للتجسس أو لنشر الدعاية أو لحالات الحظر أو للوسائل غير المادية للحرب النفسية أو الاقتصادية، فلا تندرج في تعريف «الهجمات».

ثانيًا، لا يحظر القانون الدولي الإنساني الحصار أو العقوبات الاقتصادية التي لا تقتصر على الاستهداف العمدي للقوات المسلحة بل تستهدف السكان المدنيين والاقتصاد كذلك. وبالتالي، فإن مصطلح «الهجمات» لا يشكل العمليات الإلكترونية التي من شأنها أن تكون مساوية للعقوبات الاقتصادية. ولا يعني هذا أن هذه العمليات لا حدود لها في إطار القانون الدولي الإنساني (من قبيل حظر تدمير أو نقل أو تعطيل الأعيان التي لا غنى عنها للسكان المدنيين أو الالتزام باحترام مرور الغوث الإنساني)، ولكن لمّا كانت لا تشكل هجمات، فلا يوجد حظر في القانون الدولي الإنساني على توجيهها ضد المدنيين.

ثالثًا، لا تهدف القواعد التي تحكم سير العمليات العدائية إلى حظر جميع العمليات التي تتدخل في نظم الاتصالات. فعلى سبيل المثال، ليست كل أشكال الحرمان من العمليات الخدمية،[85] مثل حجب البث التليفزيوني أو موقع إلكتروني تابع لجامعة معينة، تصل إلى حد الهجوم. ولعل المفهوم الموازي لهذه العمليات في العالم المادي هو التشويش على الاتصالات اللاسلكية أو البث التليفزيوني- وهو ما لا يعتبر هجومًا في مفهوم القانون الدولي الإنساني.

وللتمييز بين تلك العمليات التي تصل إلى حد الهجمات والعمليات التي ليست كذلك، تطرح في بعض الأحيان معايير الإزعاج.[86] ولا ينبغي الأخذ بحجة الإزعاج، من قبيل تقنين الأغذية» في الاعتبار لتحديد «الأضرار العرضية في صفوف المدنيين». وبالتالي، فإن الشيء الذي يسبب مجرد الإزعاج لا يمكن أن يصل إلى حد الهجوم. وعلى الرغم من أن معيار الإزعاج لا يخلو من مزايا، فقد يكون هناك اختلاف على ما يشكل إزعاجًا فيما يتعلق بحالات التدخل في التكنولوجيا والاتصالات الإلكترونية. فعلى سبيل المثال، بينما من الممكن الاتفاق على أن تعطيل نظام للحجز عن طريق الإنترنت يتسبب في مجرد إزعاج، فقد يكون التوصل إلى توافق في الآراء أصعب حول مسائل من قبيل التدخل في الخدمات المصرفية. ولا يزال من غير الواضح الطريقة التي سيُنظر بها إلى هذه التدخلات في المستقبل، ولا سيما في إطار ممارسات الدول.

الملخص

الخلاصة أن العمليات الإلكترونية يمكن أن تشكل هجومًا في إطار المعنى المقصود في القانون الدولي الإنساني عندما تتسبب في وفاة أو إصابة أو تدمير مادي أو أضرار، وكذلك

84 M. Bothe وآخرون، الحاشية 29 أعلاه، الصفحة 289.

85 يعني هذا العمليات الإلكترونية التي تجعل الخدمة في جهاز الكمبيوتر المستهدف غير متاحة للمستخدمين أو العملاء المعتادين.

86 M. N. Schmitt, above note 74, p. 377; Program on Humanitarian Policy and Conflict Research at Harvard
University, *Commentary on the HPCR Manual on International Law Applicable to Air and Missile Warfare*, 2010, Commentary on Article 1(d), para. 7
متاح عبر الرابط التالي:
http//:www.ihlresearch.org/amw/aboutmanual.php
(ويشار إليه فيما يلي باسم التعليق على دليل HPCR Manual on Air and Missile Warfare)؛
Michael N. Schmitt, 'Cyber operations in international law: the use of force, collective security, self-defense and armed conflict', in National Research Council, *Proceedings of a Workshop on Deterring Cyber Attacks*, Washington, DC, The National Academies Press, 2010, p. 155.

إذا كانت تتدخل في عمل عين عن طريق تعطيل نظامها الحاسوبي. وبالتالي، إذا تعطل نظام للدفاع الجوي بفعل عملية إلكترونية، أو إذا أدت عملية إلكترونية إلى تعطيل عمل شبكة كهرباء، أو إذا تعطل النظام المصرفي، فإن هذا يصل إلى حد الهجوم. ومع ذلك، فليست جميع العمليات الإلكترونية الموجهة نحو تعطيل عمل البنية الأساسية تصل إلى حد الهجمات. وعندما لا تكون العملية موجهة نحو البنية الأساسية المادية التي تعتمد على النظام الحاسوبي، بل أساسًا إلى تعطيل الاتصالات، فهي أقرب ما تكون إلى التشويش على الإشارات اللاسلكية أو البث التليفزيوني- إلا إذا كانت بطبيعة الحال جزءًا من هجوم، من قبيل تعطيل نظام الدفاع الجوي. ويكمن الاختلاف في أن وظيفة الاتصالات في الفضاء الإلكتروني هي التي تستهدف فقط؛ أما في حالات أخرى، فيكون المستهدف هو عمل العين بما يتجاوز حدود الفضاء الإلكتروني في العالم المادي. وعلى الرغم من أن التدخل في النظم الإلكترونية الذي يؤدي إلى التعطيل في العالم المادي يشكل هجمات، فإن مسألة التدخل في نظم الاتصالات، مثل نظم أو وسائط البريد الإلكتروني، لم تحل بشكل كامل.

مبدأ التمييز

يُلزم مبدأ التمييز الدول بأن تميز في جميع الأحوال بين المدنيين والمقاتلين وبين الأعيان المدنية والأهداف العسكرية.[87] وهو مبدأ أساسي من مبادئ القانون الدولي الإنساني، على حد قول محكمة العدل الدولية.[88] ولا يجوز توجيه الهجمات إلا نحو المقاتلين أو الأهداف العسكرية. ويعني هذا أنه عند تخطيط وتنفيذ العمليات الإلكترونية، فإن الأهداف المسموح بها فقط في إطار القانون الدولي الإنساني هي الأهداف العسكرية، مثل أجهزة الكمبيوتر أو النظم الحاسوبية التي تحقق مساهمة فعالة في العمليات العسكرية الملموسة. ولا يجوز توجيه الهجمات عبر الفضاء الإلكتروني نحو النظم الحاسوبية المستخدمة في منشآت مدنية بحتة.

ويعد بعض النقاش حول الأهداف العسكرية في الفضاء الإلكتروني مدعاة للقلق من وجهة نظر حماية السكان المدنيين. في الواقع، يبدو أن العمليات الإلكترونية قد تكون مناسبة على وجه الخصوص لاستهداف أعيان مدنية معينة، لأنها تُمكّن المقاتلين من الوصول إلى بعض الأهداف التي ربما كانت فرص الوصول إليها أقل فيما سبق، مثل الشبكات المالية أو شبكات البيانات الطبية.[89] ودفع البعض بأن الحرب الإلكترونية قد تؤدي إلى شكل من «قائمة الأهداف الموسعة»[90] بالمقارنة بالحرب التقليدية. وأيضًا، لأن العمليات الإلكترونية يمكنها تعطيل عمل عين دون إلحاق أضرار مادية بها، ذهب بعض المعلقين إلى أن استخدام العمليات الإلكترونية يوسع نطاق الأهداف المشروعة لأنه يسمح بشن هجمات ذات تأثيرات يمكن عكسها على أعيان سيكون من المحظور مهاجمتها بطريقة أخرى.[91] وقيل أيضًا إن:

87 المواد 48 و51 و52 من البروتوكول الإضافي الأول؛ و«جون- ماري هنكرتس» و«لويز دوزوالد- بك» (المحرران)، القانون الدولي الإنساني العرفي، المجلد الأول، القواعد (يشار إليه فيما يلي باسم «دراسة القانون الدولي الإنساني العرفي»)، اللجنة الدولية للصليب الأحمر، 2005، القواعد 1-10.

88 محكمة العدل الدولية، *مشروعية التهديد باستخدام الأسلحة النووية*، فتوى، 8 تموز/ يوليو 1996، الفقرة 78.

89 Michael N. Schmitt, 'Ethics and military force: the jus in bello', Carnegie Council for Ethics in International Affairs, 7 January 2002, متاح عبر الرابط التالي: http://www.carnegiecouncil.org/studio/multimedia/20020107/index.html

90 هذا هو التعبير الذي استخدمه Eric Talbot Jensen، في مقاله المعنون:
Unexpected consequences from knock-on effects: a different standard for computer network' operations?', in *American University International Law Review*, Vol. 18, 2002–2003, p. 1149.

91 Mark R. Shulman, 'Discrimination in the law of information warfare', in *Columbia Journal of Transnational Law*, 1999, pp. 963 ff.

الطبيعة غير القاتلة المحتملة للأسلحة الإلكترونية قد تخيم على تقييم مشروعية هجوم معين، مما يؤدي إلى انتهاكات متكررة لمبدأ التمييز في هذا الشكل الجديد من الحرب أكثر من الحرب التقليدية.[92]

وفي ضوء هذه المقدمة، من المهم الإشارة إلى قواعد القانون الدولي الإنساني التي تحكم الهجمات على الأعيان ومعالجة عدد من المشكلات القانونية المحددة التي قد تطرأ من خلال استخدام الهجمات على شبكات الكمبيوتر.

الأعيان المدنية، في إطار القانون الدولي الإنساني، هي كل الأعيان التي ليست بأهداف عسكرية.[93] والأهداف العسكرية معرفة في المادة 52 (2) من البروتوكول الإضافي الأول على أنها:

> الأهداف التي تسهم مساهمة فعالة في العمل العسكري سواء كان ذلك بطبيعتها أم بموقعها أم بغايتها أم باستخدامها، والتي يحقق تدميرها التام أو الجزئي أو الاستيلاء عليها أو تعطيلها في الظروف السائدة حينذاك ميزة عسكرية أكيدة.

وتنص المادة 52 (3) من البروتوكول الإضافي الأول على أن الأعيان التي تكرس عادة لأغراض مدنية يفترض أنها لا تستخدم في تقديم مساهمة فعالة للعمل العسكري. وبالتالي، على سبيل المثال، إذا كانت بعض البنى الأساسية المدنية ذات الحساسية البالغة، مثل أغلب المصانع الكيميائية، تعتمد على شبكة كمبيوتر مغلقة، فيجب أن يُفترض أن هذه الشبكة مدنية.

وكما توضح صياغة المادة 52 (2)، يجب أن تكون هناك علاقة واضحة بين الهدف المحتمل والعمل العسكري. ويشير مصطلح «العمل العسكري» إلى القدرات القتالية للعدو في الحرب. وتتأسس العلاقة من خلال المعايير الأربعة للطبيعة والموقع والغاية والاستخدام. وتشير الطبيعة إلى الطابع المتأصل للهدف، مثل السلاح. فالأعيان التي ليست لها طبيعة عسكرية قد تقدم أيضًا مساهمة فعالة في العمل العسكري بحكم موقعها الخاص أو غايتها أو استخدامها الحالي.

وفي هذا الصدد، ينبغي أن يسلط الضوء على أربع مسائل قد يكون لها نتائج خطيرة محتملة على البنية الأساسية المدنية: والأهم من ذلك، أن أغلب البنية الأساسية الإلكترونية يطلق عليها في الواقع العملي البنية الأساسية ذات الاستخدام المزدوج؛ ومسألة ما إذا كانت المصانع التي تنتج الأجهزة والبرامج التي تستخدمها القوات المسلحة تصبح أهدافًا عسكرية، واستهداف الأعيان باستخدام ما يسمى القدرة على استدامة الحرب، والتوابع القانونية لاستخدام شبكات التواصل الاجتماعي لأغراض عسكرية، مثل جمع معلومات عن الأهداف.

الأعيان ذات الاستخدام المزدوج في الفضاء الإلكتروني

ما يسمى الأعيان ذات الاستخدام المزدوج- وهو مصطلح غير موجود بصفته هذه في أحكام القانون الدولي الإنساني- هي تلك الأعيان التي تستخدم لأغراضٍ مدنية وعسكرية على حد السواء. وبسبب استخدامها لأغراض عسكرية، فهي تصبح أهدافًا عسكرية في إطار المادة 52 (2) من البروتوكول الإضافي الأول وأهدافًا مشروعة للهجوم. ومن الأمثلة المتكررة

92 Jeffrey T. G. Kelsey, 'Hacking into international humanitarian law: the principles of distinction and neutrality in the age of cyber warfare', in *Michigan Law Review*, Vol. 106, 2007–2008, p. 1439.

93 المادة 52 (1) من البروتوكول الإضافي الأول التي تعكس قواعد القانون الدولي العرفي، دراسة القانون الدولي الإنساني العرفي، الحاشية 87 أعلاه، القاعدة 9.

الأجزاء من البنية الأساسية المدنية التي تمد القوات المسلحة بأغراض عملياتها، مثل محطات الطاقة أو شبكات الكهرباء.

وحسب وجهة النظر السائدة اليوم، لا يمكن لهدف أن يكون مدنيًا وعسكريًا في الوقت ذاته. فما إن يستخدم للعمل العسكري، يصبح هدفًا عسكريًا بشكل كامل (إلا إذا ظلت أجزاء منه مدنية- على سبيل المثال المباني المختلفة في مستشفى).[94] وعلى عكس المقترح الذي قدمته «اللجنة الدولية» في عام 1956، الذي ذكر، خارج نطاق المواد والمنشآت ذات الطبيعة العسكرية البحتة، الاتصالات ووسائل النقل المدنية أو الصناعة «ذات الأهمية العسكرية الأساسية» أو «ذات الأهمية الأساسية لسير الحرب»،[95] يعتبر بشكل عام اليوم أن العين تصبح هدفًا عسكريًا حتى إذا كان استخدامها لأغراض عسكرية استخدامًا هامشيًا فقط بالمقارنة باستخدامها للأغراض المدنية. فعلى سبيل المثال، إذا كانت هناك محطة تزود نسبة صغيرة من الوقود المستخدم في العمليات العسكرية، فهي تتحول إلى هدف عسكري حتى لو لم يكن هذا هو غرضها الأساسي.

الأخطار في الفضاء الإلكتروني واضحة: فالبنية الأساسية الإلكترونية الدولية كلها تقريبًا- وهي تشمل أجهزة الكمبيوتر وأجهزة التوجيه والكابلات والأقمار الاصطناعية- تستخدم في الاتصالات المدنية والعسكرية على حد سواء.[96] والكابل الذي يمتد تحت البحر وينقل الاتصالات العسكرية يصبح هدفًا عسكريًا- ويستتبع ذلك (عملاً بقواعد القانون الدولي الإنساني الأخرى، ولا سيما التناسب) أن لا يصبح هدفًا لعملية إلكترونية تهدف إلى تعطيل الاتصالات العسكرية فحسب، بل يمكن تدميره أيضًا. وبالمثل، فإن «الخادم» الذي يحتوي على نسبة 5 في المائة في صورة بيانات عسكرية يصبح هدفًا مشروعًا. ومن الأهمية بمكان أن نضع هذا في الحسبان في حقبة زمنية تشهد تزايد الحوسبة السحابية، حيث لا يكون مستخدمو الحوسبة السحابية عادة على دراية بأي «الخوادم» تُخزن بياناتهم عليها وبأي البيانات الأخرى التي تُخزن على ذلك «الخادم». وتفيد التقارير بأن نحو 98 في المائة من اتصالات الحكومة الأمريكية تستخدم شبكات يملكها ويشغلها مدنيون.[97]

والخطر الذي تشكله إمكانية استهداف أي جزء من البنية الأساسية الإلكترونية هو خطر شديد الواقعية. وفي الواقع، بينما قد تسعى الدول في ظروف معينة إلى تعطيل الوظائف

94 *The Commander's Handbook on the Law of Naval Operations*, Department of the Navy/Department of Homeland Security, USA, July 2007, para. 8.3; و«دليل تالين»، الحاشية 27 أعلاه، التعليق على القاعدة 39، الفقرة 1.

95 في «مشروع قواعد (اللجنة الدولية) للحد من الأخطار التي يتكبدها السكان المدنيون في زمن الحرب»، كانت القائمة التي وضعتها المنظمة بمساعدة الخبراء العسكريين وقُدمت كنموذج، يخضع للتعديل، على النحو التالي: «أولاً: الأهداف التي تنتمي إلى الفئات التالية هي تلك الأهداف التي تعتبر ذات أهمية عسكرية معترف بها بصورة عامة... (6) الفئة الخاصة بخطوط ووسائل الاتصال (خطوط السكك الحديدية، والطرق، والجسور، والأنفاق، والقنوات) ذات الأهمية العسكرية الأساسية، (7) منشآت البث الإذاعي ومحطات التليفزيون، ومحطات الهاتف والتلغراف ذات الأهمية العسكرية الأساسية، (8) الصناعات ذات الأهمية الأساسية لسير الحرب: (أ) الصناعات الخاصة بتصنيع الأسلحة...، (ب) الصناعات الخاصة بتصنيع الإمدادات والمواد ذات الطبيعة العسكرية...، (ج) المصانع أو المحطات التي تشكل مراكز الإنتاج أو التصنيع الأخرى ذات الأهمية الأساسية لسير الحرب، مثل الصناعات المعدنية والهندسية والكيميائية، ذات الطبيعة أو الغرض المهمين من الناحية العسكرية، (د) منشآت التخزين والنقل التي تتمثل مهمتها الأساسية في خدمة الصناعات المشار إليها في الفقرات (أ)-(ج)، (هـ) المنشآت التي توفر الطاقة أساسًا للدفاع الوطني، مثل الفحم أو أنواع الوقود الأخرى أو الطاقة الذرية والمحطات التي تنتج الغاز أو الكهرباء أساسًا للاستهلاك العسكري» (إضافة تأكيد). انظر: Rules for the Limitation of the Dangers incurred by the Civilian Population in Time of Draft War, ICRC, 1956, متاحة عبر الرابط التالي: http://www.icrc.org/ihl/INTRO/420?OpenDocument.

96 انظر أيضًا: R. Geiss وH. Lahmann، الحاشية 61 أعلاه، الصفحة 3.

97 Eric Talbot Jensen, 'Cyber warfare and precautions against the effects of attacks', in *Texas Law Review*, Vol. 88, 2010, p. 1534

المحددة للغاية التي تضطلع بها البنية الأساسية العسكرية للخصم، فإن حقيقة أن الفضاء الإلكتروني كله يستخدم للعمليات العسكرية يعني أن في أي نزاع مسلح سيكون من قبيل المصلحة الاستراتيجية المهمة إضعاف شبكات الاتصالات لدى الخصم وقدرته على الوصول إلى الفضاء الإلكتروني. وسيعني هذا حرمان الخصم من القدرة على الوصول إلى المسارات المهمة للغاية في الفضاء الإلكتروني، وتعطيل مساراته الرئيسية أو إمكانية وصوله إلى شبكات الاتصالات الرئيسية، وليس مجرد استهداف نظم حاسوبية محددة في البنية الأساسية العسكرية.[98] وعلى العكس مما يحدث في مسارح الحروب المعتادة، مثل الأرض أو الفضاء، يعني مسرح عمليات الفضاء الإلكتروني الذي صممه الإنسان أن الأطراف المتحاربة لن تركز على السلاح المتنقل فحسب بل ستركز أيضًا على المسارات نفسها.[99] فعلى سبيل المثال، في الفضاء الجوي، نجد أن الطائرات فقط هي التي تصنف كهدف عسكري؛ أما في الحرب الإلكترونية، فإن البنية الأساسية المادية التي تنقل الأسلحة الإلكترونية (الشفرات الضارة) تصنف كأهداف عسكرية.

وتثير العواقب الإنسانية المترتبة على هذه الحالة قلقًا بالغًا على حماية السكان المدنيين. ففي عالم يعتمد فيه قطاع كبير من البنية الأساسية المدنية، والاتصالات المدنية، والشؤون المالية، والاقتصاد والتجارة على البنية الأساسية الإلكترونية الدولية، يصبح من السهل للغاية أن تقوم الأطراف بتدمير هذه البنية الأساسية. وليس ثمة حاجة إلى الدفع بأن الشبكة المصرفية تستخدم للعمل العسكري، أو بأن الشبكة الكهربائية ذات استخدام مزدوج. وسيُبرر تعطيل الكابلات الرئيسية أو الشبكات أو أجهزة التوجيه أو الأقمار الاصطناعية التي تعتمد عليها هذه النظم، دائمًا بحقيقة أن هذه المسارات تستخدم لنقل معلومات عسكرية، وهي من ثم تصنف كأهداف عسكرية.

يشير «دليل تالين» إلى ما يلي:

> إن الظروف التي يمكن فيها أن تتعرض شبكة الإنترنت بالكامل للهجوم [هي] ظروف غير محتملة إلى حد بعيد بما يجعل هذا الاحتمال أمرًا نظريًا بحتًا في الوقت الحاضر. وعوضًا عن ذلك، اتفق الفريق الدولي للخبراء على أن أي هجوم تقريبًا يستهدف شبكة الإنترنت يجب أن يكون مقتصرًا على أجزاء منفصلة من الشبكة، وذلك من الناحية القانونية والعملية.[100]

ويذكر الدليل أيضًا أن مبدأي الاحتياط والتناسب، يجب احترامهما في حال تعرضت شبكة الإنترنت أو أجزاء كبيرة منها للهجوم. ولكن على الرغم من أن هذا قد يبدو مطمئنًا للوهلة الأولى، فهو يترك إشكالية حول ما إذا كان من الممكن أو غير الممكن استهداف شبكة الإنترنت بالكامل، أو استهداف أجزاء منها إذا كانت تستخدم في الاتصالات العسكرية وكان تدميرها أو تعطيلها يوفر ميزة عسكرية أكيدة (مرة أخرى رهنًا بالتناسب والاحتياطات).

وبالإضافة إلى ذلك، يتسم الفضاء الإلكتروني بالمرونة، بمعنى أن المعلومات إذا لم تتمكن من التدفق عبر قناة واحدة، فهناك مسارات وبدائل متعددة، ويمكن عادة نقل المعلومات عبر طريق آخر. وكما يشير «دليل تالين»:

98 US Department of Defense, *Quadrennial Defence Review Report*, February 2010, pp. 37–38,
متاح عبر الرابط التالي:
http//:www.defense.gov/qdr/images/QDR_as_of12_Feb10_1000.pdf.

99 R. Geiss and H. Lahmann، الحاشية 61 أعلاه، الصفحة 9.

100 Tallinn Manual، الحاشية 27 أعلاه، التعليق على القاعدة 39، الفقرة 5.

تشكل العمليات الإلكترونية تحديات فريدة في هذا الصدد. ولنتخيل شبكة تستخدم لأغراض عسكرية ومدنية على حد السواء. قد يكون من المستحيل أن نعرف عبر أي جزء من الشبكة ستمر المعلومات العسكرية، بما يميزها عن المعلومات المدنية. وفي هذه الحالات، تُصنف الشبكة بالكامل (أو على الأقل تلك الأجزاء التي يحتمل أن يتم النقل فيها) كهدف عسكري.[101]

والنتيجة المترتبة على ذلك أن جميع أجزاء الإنترنت تقريبًا في بعض الظروف تصنف كهدف عسكري لأنها كلها مسارات محتملة لنقل المعلومات العسكرية.

ولا يخلو التفسير الواسع النطاق السائد للأعيان ذات الاستخدام المزدوج على أنها أهداف عسكرية بالفعل من مشكلات في العالم المادي.[102] ففي الفضاء الإلكتروني، يمكن أن تتفاقم العواقب إلى أقصى حد حيث لا يبقى أي شيء على طابعه المدني، وتصبح القاعدة الأساسية التي تنص على وجوب تمتع السكان المدنيين بالحماية من الأخطار الناجمة عن العمليات العسكرية، خالية من مضمونها، وتخضع المسألة فقط لمبدأي التناسب والاحتياط.

وأخيرًا، إذا كانت أغلب البنى الأساسية الإلكترونية في جميع أنحاء العالم ذات طابع مزدوج من حيث الاستخدام ويمكن اعتبارها هدفًا عسكريًا، فإن هذا يثير المسألة الأساسية المتعلقة بالحدود الجغرافية للنزاع المسلح. فلا توجد حدود فعلية في الفضاء الإلكتروني، فالنظم الحاسوبية يمكن مهاجمتها من أي مكان (عن بُعد) أو التلاعب فيها أو تحويلها إلى وسائل للقتال وأهداف عسكرية. ويجب أن نضع في الحسبان أن العقبات لن تقتصر على أن أجهزة الكمبيوتر المذكورة ستتعرض للقرصنة المضادة بواسطة النظم الحاسوبية التي تعرضت للهجوم. ونظريًا، يمكن تدميرها من خلال الوسائل الحركية بوصفها أهدافًا عسكرية. فعلى سبيل المثال، يمكن استخدام روبوت لإطلاق هجوم يعمل على تدمير البنية الأساسية الإلكترونية للخصم. ولتنفيذ عملية من هذا القبيل، فإن طرف النزاع الذي يطلق الهجوم سيسيطر عن بُعد على آلاف أو ملايين أجهزة الكمبيوتر في جميع أنحاء العالم، مما سيؤدي إلى نقل البرنامج الضار إلى أجهزة الكمبيوتر المستهدفة. وإذا كان هذا الروبوت سيؤدي إلى تحديد جميع ملايين أجهزة الكمبيوتر التي يستخدمها في جميع أنحاء العالم على أنها أهداف عسكرية معرضة للهجوم، فستكون النتيجة نوعًا من الحرب الإلكترونية الشاملة. والنتيجة المنطقية، وهي أن جميع أجهزة الكمبيوتر على مستوى العالم ستصبح أهدافًا عسكرية، تتعارض مع أساسيات قانون الحياد في النزاعات المسلحة الدولية (وأصلًا

101 المرجع السابق، التعليق على القاعدة 39، الفقرة 3.

102 انظر أيضًا:

Marco Sassòli, 'Legitimate targets of attacks under international humanitarian law', Background Paper prepared for the Informal High-Level Expert Meeting on the Reaffirmation and Development of International Humanitarian Law, Cambridge, 27–29 January 2003, HPCR, ,2003, pp. 3–6

متاح عبر الرابط التالي:

;http://www.hpcrresearch.org/sites/default/files/publications/Session1.pdf

and the environment', in *Vermont Law Review*, Vol. 25, William M. Arkin, 'Cyber warfare ,2001, p. 780

ويصف الآثار التي ترتبت في عام 1991 على الهجمات الجوية على محطة الكهرباء العراقية والتي لم تقتصر على إمداد المدنيين بالكهرباء، بل امتد تأثيرها ليشمل توزيع المياه، وتنقيتها، والصرف الصحي، والبنية الأساسية الصحية؛ وانظر: R. Geiss and H. Lahmann، الحاشية 61 أعلاه، الصفحة 16.

مع الأساس المنطقي الذي يقوم عليه، وهو تجنيب البلدان الأخرى وسكانها تأثير الأعمال العدائية) ومع القيود الجغرافية لميدان المعركة في النزاعات المسلحة غير الدولية.[103] ففي النزاع المسلح الدولي، يفرض قانون الحياد قيودًا معينة على حق الدولة التي تعرضت للهجوم في الدفاع عن نفسها عن طريق مهاجمة البنية الأساسية في أرض محايدة.[104] أولًا، يجب على الدولة التي تعرضت للهجوم أن تخطر الدولة المحايدة وأن تمنحها فترة زمنية مناسبة لإنهاء الانتهاك؛ ثانيًا، لا يسمح للدولة التي تعرضت للهجوم بإنهاء انتهاك الحياد إلا إذا كان ذلك الانتهاك يشكل تهديدًا خطيرًا ومباشرًا لأمنها وإذا لم تكن هناك بدائل أخرى تتسم بالجدوى وحسن التوقيت للرد على التهديد. وهذه القيود واسعة النطاق نسبيًا، ولكي توفر حماية فعلية للسكان المدنيين في الدولة المحايدة، فمن المفترض أن تفسر في إطار ضيق. أما في النزاعات المسلحة غير الدولية، فلا ينطبق قانون الحياد. ومع ذلك، فإن التعامل مع النزاع المسلح على أنه يدور في أي مكان يستخدم فيه جهاز كمبيوتر أو كابل أو شبكة للعمل العسكري (ومن ثم يشكل هدفًا عسكريًا بشكل طبيعي)، سيؤدي إلى كسر الحدود الجغرافية لميدان المعركة في النزاعات المسلحة غير الدولية.

والخلاصة، يتضح أن مبدأ التمييز، في الفضاء الإلكتروني، على ما يبدو، لا يتيح بصيص أمل لحماية البنية الأساسية الإلكترونية المدنية وجميع البنى الأساسية المدنية التي تعتمد عليها. وفي هذه الحالات، ستتمثل الحماية القانونية الأساسية للبنية الأساسية المدنية في مبدأ التناسب الذي سيُناقش في الأجزاء التالية.[105]

المشكلة في أن أغلب البنى الأساسية في الفضاء الإلكتروني ذات استخدام مزدوج، وهي تمثل بالتأكيد أهم شاغل وتبدو المسائل القانونية الأخرى أقل إلحاحًا، وإن كان بعضها سيُناقش في الفقرات التالية.

الشركات التي تنتج تكنولوجيا المعلومات المستخدمة في العمل العسكري

لمّا كانت الأجهزة والبرامج تستخدم في كثير من الآلات العسكرية، فإن شركات تكنولوجيا المعلومات التي تنتجها يمكن أن ينظر إليها على أنها «أهداف عسكرية تدعم الحرب»[106]- شأنها شأن مصانع الذخيرة. ومن المرجح أن يعني هذا أن عددًا من شركات تكنولوجيا المعلومات في جميع أنحاء العالم ستشكل أهدافًا مشروعة؛ إذ إن كثيرًا منها قد يزود القوات المسلحة بالبنية الأساسية لتكنولوجيا المعلومات.[107] يتساءل «إريك تالبوت جنسن» عما إذا كانت شركة مايكروسوفت تشكل هدفًا مشروعًا «استنادًا إلى الدعم الذي تقدمه إلى المجهود

103 تعد حدود أرض المعركة في النزاعات المسلحة غير الدولية من المسائل الخلافية وتتجاوز نطاق هذا المقال- إلا أن الصعوبات التي تثيرها الحرب الإلكترونية تكاد لا تجد لها إجابة في هذا الصدد. للاطلاع على وجهة نظر «اللجنة الدولية»، انظر: اللجنة الدولية للصليب الأحمر، تقرير عن القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة، المؤتمر الدولي الحادي والثلاثون للصليب الأحمر والهلال الأحمر، جنيف، 28 تشرين الثاني/ نوفمبر- 1 كانون الأول/ ديسمبر 2011، تقرير من إعداد اللجنة الدولية للصليب الأحمر، تشرين الأول/ أكتوبر 2011، الصفحتان 21 و22، وللاطلاع على مناقشة حول التأثيرات الجغرافية للحرب الإلكترونية، انظر «دليل تالين»، الحاشية 27 أعلاه، التعليق على القاعدة 21.

104 تستمد هذه القيود من المادة 22 من «دليل سان ريمو بشأن أحكام القانون الدولي الإنساني المنطبقة على النزاعات المسلحة في البحر»، الصادر بتاريخ 12 حزيران/ يونيو 1994، النسخة الإنجليزية متاحة عبر الرابط التالي:
https//:ihl-databases.icrc.org/ihl/INTRO?560/OpenDocument

105 التعليق على دليل *HPCR Manual on Air and Missile Warfare*، الحاشية 86 أعلاه، التعليق على القاعدة 22 (د)، الفقرة 7؛ و«دليل تالين»، الحاشية 27 أعلاه، التعليق على القاعدة 39، الفقرة 2؛ و E. T. Jensen، الحاشية 90 أعلاه، الصفحة 1157.

106 M. N. Schmitt، الحاشية 61 أعلاه، الصفحة 8.

107 يتردد أن وزارة الدفاع الأمريكية ستستضيف مقاولين يرغبون في اقتراح تكنولوجيات جديدة للحرب الإلكترونية: انظر S. Shane، الحاشية 3 أعلاه.

الحربي للولايات المتحدة من خلال تيسير عملياتها العسكرية». وهو يرى أن «كون الشركة ومقرها يقدمان منتجًا تجده القوات المسلحة أساسيًا لعملها، فضلًا عما تقدمه من خدمة العملاء لدعم ذلك المنتج، قد يوفر ما يكفي من الحقائق لاستنتاج أنها تشكل هدفًا ذا استخدام مزدوج» إلا أنه يشك في إمكانية تحقق ميزة عسكرية أكيدة من هذا الهجوم.[108]

يوضح المثال أن التشابه مع مصانع الذخيرة ينبغي أن لا يأخذ أكبر من حجمه. وينص المعيار ذو الصلة الوارد في المادة 52 (2) من البروتوكول الإضافي الأول على أن العين يجب أن تحقق، من خلال استخدامها، مساهمة فعالة في العمل العسكري. أولًا، هذه الشركات ليست أعيانًا مادية، بل هي كيانات اعتبارية، وبالتالي فإن السؤال المطروح يجب أن يتعلق بدلًا من ذلك بما إذا كان أي من مواقعها (أي المباني) قد بات هدفًا عسكريًا. ثانيًا، هناك فرق بين الأسلحة وأدوات تكنولوجيا المعلومات. فالأسلحة، بطبيعتها، أهداف عسكرية، في حين أن نظم تكنولوجيا المعلومات العامة ليست كذلك. وبالتالي، يتعين على المرء التمييز بين المصانع التي تطور فعليًا ما قد يطلق عليه أسلحة إلكترونية، وهي عبارة عن شفرات/ بروتوكولات محددة تستخدم في شن هجوم على شبكة كمبيوتر معينة (على سبيل المثال، الموقع الذي يجري فيه تطوير فيروس معين مثل «ستوكسنت»)، والمصانع التي تزود القوات المسلحة بمستلزمات تكنولوجيا المعلومات العامة التي تختلف، على سبيل المثال، عن الإمدادات الغذائية.[109]

القدرة على القتال في الحرب أم القدرة على استدامة الحرب؟

في الحرب الإلكترونية، حيث يكون الإغراء باستهداف البنية الأساسية المدنية ربما أعلى مما هو عليه في الحرب التقليدية، من المهم أن نضع في الاعتبار أن العين المدنية لكي تتحول إلى هدف عسكري، فإن مساهمتها في العمل العسكري يجب أن توجه صوب القدرات الفعلية على القتال في الحرب لدى أحد أطراف النزاع. أما إذا كانت العين تسهم فقط في القدرة على استدامة الحرب لدى أحد أطراف النزاع (مجهوده الحربي العام)، فإنها لا تصنف كهدف عسكري.

في دليل القائد الأمريكي لقانون العمليات البحرية، جرى توسيع نطاق التعبير «تسهم مساهمة فعالة في العمل العسكري» المستمد من المادة 52 (2) من البروتوكول الإضافي الأول، والاستعاضة عنه بتعبير «تسهم مساهمة فعلية في القدرة على القتال في الحرب أو القدرة على استدامة الحرب لدى العدو».[110] يُوجه هذا الرأي أساسًا نحو الأهداف الاقتصادية، التي قد تعمل بشكل غير مباشر على دعم أو استدامة القدرة العسكرية للعدو.[111] يشير تقييم

108 E. T. Jensen، الحاشية 90 أعلاه، الصفحتان 1160 و1168؛ انظر أيضًا: E. T. Jensen، الحاشية 97 أعلاه، الصفحة 1544: «إذا قامت شركة مدنية لأجهزة الكمبيوتر بإنتاج أو صيانة أو دعم النظم الإلكترونية التابعة للحكومة، فيبدو من الواضح أن العدو يمكن أن يقرر أن الشركة تستوفي شروط المادة 52 ويجوز استهدافها».

109 لا يخلص «دليل تالين» أيضًا إلى استنتاج حاسم بشأن هذه المسألة: «تتضمن الحالة الصعبة مصنعًا ينتج أصنافًا غير مخصصة تحديدًا للقوات المسلحة، ولكنها رغم ذلك توضع في كثير من الأحيان تحت تصرف القوات المسلحة. وعلى الرغم من أن جميع الخبراء اتفقوا على أن مسألة ما إذا كان مصنع معين يصنف كهدف عسكري بحكم الاستخدام تعتمد على نطاق وحجم وأهمية مقتنيات القوات المسلحة، لم يتمكن الفريق من التوصل إلى أي استنتاج حاسم بشأن المستويات الدقيقة».

110 *The Commander's Handbook on the Law of Naval Operations*, الحاشية 94 أعلاه، الفقرة 8-2.

111 M. N. Schmitt, 'Fault lines in the law of attack', in S. Breau and A. Jachec-Neale (eds), *Test-ing the Boundaries of International Humanitarian Law*, British Institute of International and Comparative Law, London, 2006, pp. 277–307.
للاطلاع على الأسس المنطقية التي يستند إليها هذا النهج، انظر على سبيل المثال:
Charles J. Dunlap, 'The end of innocence, rethinking noncombatancy in the post-Kosovo

أجراه المستشار القانوني لوزارة الدفاع الأمريكية فيما يتعلق بالعمليات الإلكترونية في عام 1999 إلى أن:

> يجب أن لا تتعرض البنى الأساسية ذات الطبيعة المدنية البحتة للهجوم إلا إذا كانت القوة المهاجمة قادرة على أن تثبت أن ميزةً عسكرية أكيدة متوقعةٌ من هذا الهجوم... وفي نزاع مسلح طويل وممتد، قد يؤدي إلحاق الضرر باقتصاد العدو وقدراته البحثية والتنموية إلى تقويض مجهوده الحربي، ولكن في نزاع قصير ومحدود، قد يكون من الصعب تحديد الميزة العسكرية المتوقعة من مهاجمة الأهداف الاقتصادية.[112]

تتجاهل هذه النُهج القيود القانونية التي يفرضها القانون الدولي الإنساني. فإلحاق الضرر بالاقتصاد المدني للعدو وقدراته البحثية والتنموية في حد ذاتها، هو تصرف لا يجيزه القانون الدولي الإنساني على الإطلاق، بغض النظر عن الميزة العسكرية المتوخاة وبغض النظر عن مدة النزاع. وإلا، فلن تكون هناك حدود على الحرب حيث يمكن اعتبار الاقتصاد ككل في بلد ما مما يساعد على استدامة الحرب.[113] ومن المهم على وجه الخصوص التذكير بهذا في سياق الحروب الإلكترونية والإشارة إلى العواقب المدمرة المحتملة التي تلحق بالسكان المدنيين نتيجة لوضع تعريف واسع النطاق للأهداف العسكرية.

وسائل الإعلام وشبكات التواصل الاجتماعي

يعالج «دليل تالين» المسألة الشائكة المتعلقة باستخدام شبكات التواصل الاجتماعي للأغراض العسكرية:[114]

> أبرزت النزاعات الأخيرة استخدام شبكات التواصل الاجتماعي للأغراض العسكرية. فعلى سبيل المثال، يستخدم موقع «فيسبوك» لتنظيم عمليات القوات المسلحة، ويستخدم موقع «تويتر» لنقل معلومات ذات قيمة عسكرية. ومن الضروري إبداء ثلاث ملاحظات

era', in Strategic Review, Vol. 28, Summer 2000, p. 9; Jeanne M. Meyer, 'Tearing down the façade: a critical look at current law on targeting the will of the enemy and Air Force doctrine', ;in *Air Force Law Review*, Vol. 51, 2001, p. 143

وانظر: J. T. G. Kelsey، الحاشية 92 أعلاه، الصفحة 1447، الذي يدعو إلى صياغة تعريف جديد للأهداف العسكرية بحيث تُدرج بعض البنى الأساسية والخدمات المدنية.

112 Department of Defense Office of General Counsel, *An Assessment of International Legal Issues in Information Operations*, May 1999, p. 7, متاح عبر الرابط التالي: http://www.au.af.mil/au/awc/awcgate/dod-io-legal/dod-io-legal.pdf. يتسم موقف الولايات المتحدة في التقرير الأخير للأمين العام بالغموض في أحسن الأحوال عندما يشير إلى أن مبادئ قانون الحرب «تحظر شن الهجمات على الهياكل الأساسية المدنية البحتة التي قد لا يعود تعطيلها أو تدميرها بأي مكاسب عسكرية تذكر». وإذا كان يُقصد بهذا أن يشير ضمنًا إلى أن الهجمات على الهياكل الأساسية المدنية البحتة لن يُسمح بها إذا كان تدميرها أو تعطيلها سيؤدي إلى ميزة عسكرية مهمة، فإن هذا لا يتفق مع القانون الدولي الإنساني الذي لا يسمح على الإطلاق بالهجمات على أعيان مدنية بحتة (تقرير الأمين العام، 15 تموز/ يوليو 2011، وثيقة الأمم المتحدة رقم A/66/152، الصفحة 26).

113 M. Sassòli، الحاشية 102 أعلاه.

Stephan Oeter, 'Means and methods of combat', in Dieter Fleck (ed.), *The Handbook of Humanitarian Law in Armed Conflicts*, Oxford University Press, Oxford, 1995, para. 442.5.

114 أشارت التقارير على سبيل المثال إلى أن حلف شمال الأطلسي أقر بأن شبكات التواصل الاجتماعي مثل «تويتر»، «وفيسبوك»، «ويوتيوب» أسهمت في عمليات الاستهداف التي نفذها في ليبيا، بعد التحقق منها مقارنة بمصادر أخرى:
Graeme Smith, 'How social media users are helping NATO fight Gadhafi in Libya', in The Globe and Mail, 14 June 2011; Tim Bradshaw and James Blitz, 'NATO draws on Twitter for Libya strikes', in *The Washington Post*, 16 June 2011.

تحذيرية. أولًا، يجب تذكر أن هذه القاعدة [التي تقول إن العين المستخدمة لأغراض مدنية وعسكرية هي هدف عسكري] لا تخل بقاعدة التناسب واشتراط اتخاذ الاحتياطات في الهجوم... ثانيًا، تعتمد مسألة مشروعية العمليات الإلكترونية ضد شبكات التواصل الاجتماعي على ما إذا كانت هذه العمليات تصل إلى حد الهجوم. فإذا كانت العمليات لا تصل إلى هذا الحد، فإن مسألة تصنيفها كهدف عسكري تصبح خلافية... ثالثًا، لا يعني هذا أن موقع «فيسبوك» أو موقع «تويتر» بوصفهما هذا يجوز استهدافهما؛ فلا يجوز أن يوجه الهجوم إلا نحو تلك المكونات فيهما التي تستخدم لأغراض عسكرية [ما دام الهجوم يلتزم بالاشتراطات الأخرى التي يحددها قانون النزاع المسلح].[115]

يطرح تصنيف شبكات التواصل الاجتماعي، مثل «فيسبوك»، و«تويتر»، على أنها أهداف عسكرية عددًا من المشكلات. في الواقع، تحتوي هذه الشبكات على كميات هائلة من البيانات- أغلبها لا يرتبط تمامًا بالمعلومات المحددة التي يجب استهدافها- حتى إنه يصعُب تصنيف أي من هذه الشبكات على أنها هدف عسكري واحد. وثمة سؤال آخر عما إذا كان من الممكن من الناحية التقنية أن يقتصر الهجوم على تلك المكونات التي تستخدم لأغراض عسكرية فقط من بين البيانات غير المنظمة في هذه الشبكات.

ويُطرح سؤال مماثل من حيث درجة الصعوبة فيما يتعلق بوسائل الإعلام. يشير «دليل تالين» إلى ما يلي:

من الأمثلة المهمة التقارير الإعلامية. فإذا كانت هذه التقارير تسهم مساهمة فعالة في الصورة العملياتية للعدو، فإن حرمان العدو منها قد يوفر ميزة عسكرية أكيدة. وذهب بعض أعضاء الفريق الدولي للخبراء إلى أن البنية الأساسية الإلكترونية التي تعزز نقل هذه التقارير تُصنف كهدف عسكري، على الرغم من تحذيرهم من أن البنية الأساسية لا يجوز مهاجمتها إلا بموجب القواعد المتعلقة بالهجوم، ولا سيما تلك المتعلقة بالتناسب... والاحتياطات في الهجوم... وأشاروا على وجه الخصوص إلى أن الشرط الأخير من شأنه أن يؤدي عادة إلى اشتراط أن يقتصر الأمر على شن هجمات إلكترونية تهدف إلى حظر البث المذكور. ودفع خبراء آخرون إلى أن الصلة بين مساهمة البنية الأساسية الإلكترونية في العمل العسكري تتم عن مسافة بعيدة للغاية تحول دون تصنيف البنية الأساسية على أنها هدف عسكري. واتفق جميع أعضاء الفريق الدولي للخبراء على أن هذه التقييمات تخضع بالضرورة للسياق إلى حد بعيد.[116]

وحتى إذا كان تقرير معين يسهم مساهمة فعالة في العمل العسكري، فلا ينبغي أن يؤدي هذا إلى استنتاج أن المؤسسة الإعلامية المسؤولة أو أن البنية الأساسية التي تبث التقرير يمكن أن تكون هدفًا للهجوم. وفيما يتعلق بالمؤسسات الإعلامية، ستكون العواقب المحتملة لقبول تعرضها للاستهداف خطيرة. ولنأخذ «بي بي سي» مثالًا على محطة إذاعية دولية. أولًا، يعد تعبير «تسهم في الصورة العملياتية للعدو» تعبيرًا فضفاضًا للغاية، وهو أوسع نطاقًا من تقديم مساهمة مباشرة في العمل العسكري للعدو، حسبما تقتضي ذلك المادة 52 (2) من البروتوكول الإضافي الأول. ثانيًا، حتى إذا كان التقرير الإعلامي يحتوي على

115 Tallinn Manual، الحاشية 27 أعلاه، الصفحة 114.
116 المرجع السابق، الصفحة 113.

معلومات تكتيكية، بشأن أهداف محددة على سبيل المثال، فإن افتراض أن الشركة الإعلامية يمكن استهدافها يثير إشكالية كبيرة. فبخلاف الشركة نفسها، إذا اعتبرنا أن البنية الأساسية الإلكترونية التي تُبث التقارير عبرها هدف عسكري، فإن هذا سيعني أن جزءًا كبيرًا من البنية الأساسية في العالم- مرة أخرى كما هو الحال مع الأعيان ذات الاستخدام المزدوج، مع الأخذ في الحسبان أن تبعات اعتبار عين ما هدفًا عسكريًا تتمثل في إمكانية استهدافها أيضًا باستخدام الوسائل الحركية، مما يعني أن الموقع المادي الذي تُبث التقارير منه وعبره- يمكن إلحاق الأضرار به وتدميره. وأخيرًا، كما قيل آنفًا، يشكل المثال الخاص بالمؤسسات الإعلامية تناقضًا حادًا مع مشكلة الحدود الجغرافية لميدان المعركة. كذلك، فإن قانون الحياد يفرض عددًا من الحدود في النزاع المسلح الدولي على قدرة الدولة على استهداف البنية الأساسية في دولة محايدة.[117]

حظر الهجمات العشوائية ووسائل وأساليب القتال العشوائية

تُحظر الهجمات العشوائية،[118] وهي تلك الهجمات:

- التي لا توجه إلى هدف عسكري محدد.
- أو التي تستخدم طريقة أو وسيلة للقتال لا يمكن أن توجه إلى هدف عسكري محدد.
- أو التي تستخدم طريقة أو وسيلة للقتال لا يمكن حصر آثارها على النحو الذي يتطلبه القانون الدولي الإنساني.

ومن ثم فإن من شأنها أن تصيب، في كل حالة كهذه، الأهداف العسكرية والأشخاص المدنيين أو الأعيان المدنية دون تمييز. ويتعين على أطراف النزاع «من ثم أن لا تستخدم على الإطلاق أسلحة غير قادرة على التمييز بين الأهداف المدنية والعسكرية».[119]

وكما ذكر آنفًا، فإن حقيقة أن أغلب الفضاء الإلكتروني يمكن اعتباره من قبيل الاستخدام المزدوج، من المرجح أن تجعل من الصعب فصل البنية الأساسية العسكرية عن المدنية. ومع ذلك، فحتى في الحالات التي يمكن فيها فصل البنية الأساسية العسكرية وتمييزها عن البنية الأساسية المدنية، ثمة خطورة أخرى تتمثل في أن الهجمات ستكون عشوائية بسبب ترابط الفضاء الإلكتروني.[120] يتكون الفضاء الإلكتروني من نظم حاسوبية لا حصر لها متشابكة في جميع أنحاء العالم. وحتى إذا كانت النظم الحاسوبية العسكرية منفصلة عن المدنية، فإنها كثيرًا ما تتصل بالنظم التجارية المدنية وتعتمد عليها كليًا أو جزئيًا. وبالتالي، قد يكون من المستحيل إطلاق هجوم إلكتروني على البنية الأساسية العسكرية وتحديد الهجوم أو تأثيراته بحيث يقتصر على ذلك الهدف العسكري. والفيروسات والديدان من الأمثلة على أساليب الهجوم على شبكات الكمبيوتر التي تندرج ضمن هذه الفئة إذا كانت تأثيراتها محددة بمعرفة من صنعوها. وإن استخدام دودة تنسخ نفسها ولا يمكن التحكم فيها وقد تسبب من ثم أضرارًا كبيرة في البنية الأساسية المدنية من شأنه أن يشكل انتهاكًا للقانون

117 انظر القسم أعلاه «الأعيان ذات الاستخدام المزدوج في الفضاء الإلكتروني».
118 دراسة القانون الدولي الإنساني العرفي، القاعدة 12؛ المادة 51 (4) من البروتوكول الإضافي الأول.
119 محكمة العدل الدولية، الحاشية 88 أعلاه، الفقرة 78.
120 K. Dörmann، الحاشية 42 أعلاه، الصفحة 5.

الدولي الإنساني.[121]

رفض بعض المعلقين هذا الشاغل باعتباره أمرًا مبالغًا فيه، لا سيما استنادًا إلى حقيقة مفادها أنه لما كانت أغلب العمليات الإلكترونية لن تكون فعالة إلا إذا كانت موجهة نحو نظم محددة للغاية وشديدة التخصص، فإن تأثيرها على أجهزة الكمبيوتر الأخرى لن يكون ضارًا. والمثال المقدم في هذه الحالة هو فيروس «ستوكسنت» الذي صُمم بدقة شديدة ليستخدم ضد المنشآت النووية في جمهورية إيران الإسلامية.[122]

وفي الواقع، إذا أُدخل فيروس إلى نظام عسكري مغلق أو صُمم للحيلولة دون انتشاره إلى النظم الأخرى، فقد لا يكون هناك أي خطرٍ على البنية الأساسية المدنية الواقعة خارج هذا النظام. ولكن من الممكن تمامًا أن نتخيل طرفًا في نزاع لا يأخذ هذه الاحتياطات أو يطور أسلحة إلكترونية لها تأثيرات على شبكات لم يكن يتوقعها. وإذا كان من الممكن تصميم أسلحة إلكترونية غير عشوائية، فإن هذا لا يعني أن لا يوجد احتمال كبير لوقوع هجمات عشوائية. وحتى فيروس «ستوكسنت»- كما ورد في وسائل الإعلام- يبين مدى صعوبة السيطرة على تأثيرات الفيروسات؛ فقد أشارت التقارير إلى أن هذا الفيروس لم يكن مقصودًا به إصابة أجهزة الكمبيوتر خارج النظم المستهدفة في المنشآت النووية، ومع ذلك فقد نسخ نفسه بطريقة أو بأخرى خارج إيران.[123] وعلى الرغم من أن انتشار الفيروس خارج النطاق الذي قصده مطوروه ربما لم يسبب أي أضرار، فهو يبين مدى صعوبة التحكم في ذلك الانتشار.

ومن ثم، هناك عبء مزدوج ملقى على عاتق الأطراف المتحاربة. أولًا، فهي قد لا تستخدم أسلحة إلكترونية عشوائية بطبيعتها، مثل الفيروسات أو الديدان التي تنسخ نفسها دون أي احتمال للسيطرة عليها (بما يشبه الأسلحة البكتريولوجية على سبيل المثال). ويجب تجريم استخدام هذا النوع من الأسلحة أثناء استعراض السلاح عند تطويره أو الحصول عليه- إذا لم يكن من الممكن على الإطلاق استخدامه دون ضرب الأهداف العسكرية والمدنية على حد سواء، وإذا لم يكن متوافقًا مع متطلبات القانون الدولي الإنساني.[124] ثانيًا، في كل هجوم، يتعين على الطرف المحارب أن يتحقق مما إذا كان السلاح الإلكتروني المستخدم، في الظروف المحددة في كل حالة، يمكن توجيهه أو يوجه بالفعل نحو هدف عسكري وما إذا كان تأثيره يمكن السيطرة عليه في إطار المعنى المقصود في القانون الدولي الإنساني.

مبدأ التناسب

بالنظر إلى طبيعة الاستخدام المزدوج التي تتسم بها أغلب البنى الأساسية الإلكترونية من ناحية، ومخاطر التبعات على البنية الأساسية المدنية في حالة استهداف أجهزة كمبيوتر أو نظم حاسوبية عسكرية بحتة بسبب ترابط الفضاء الإلكتروني من ناحية أخرى، هناك

121 إما أن الدودة لا يمكن توجيهها إلى هدف عسكري محدد (راجع دراسة القانون الدولي الإنساني العرفي، القاعدة 12 (ب)، والمادة 51 (4) (ب) من البروتوكول الإضافي الأول، وإما أن لها تأثيرات لا يمكن تقييدها على النحو الذي يقتضيه القانون الدولي الإنساني (انظر: دراسة القانون الدولي الإنساني العرفي، القاعدة 12 (ج)، والمادة 51 (4) (ج) من البروتوكول الإضافي الأول).

122 T. Rid، الحاشية 24 أعلاه.

123 D. E. Sanger، الحاشية 23 أعلاه.

124 لا ينبثق هذا من المادة 36 من البروتوكول الإضافي الأول التي تنطبق على الدول الأطراف في البروتوكول، بل كذلك من الالتزام العام للأطراف المتحاربة بعدم استخدام أسلحة عشوائية.

قلق شديد من تأثر البنية الأساسية المدنية بشكل كبير بالعمليات الإلكترونية في النزاعات المسلحة. وبالتالي، يصبح مبدأ التناسب قاعدة بالغة الأهمية لحماية السكان المدنيين.

يصاغ مبدأ التناسب في المادة 51 (5) (ب) من البروتوكول الإضافي الأول، وهي تعكس قواعد القانون الدولي العرفي.[125] ويحظر الهجوم إذا كان «يتوقع منه أن يسبب خسارة في أرواح المدنيين أو إصابة بهم أو أضرارًا بالأعيان المدنية، أو أن يُحدث مزيجًا من هذه الخسائر والأضرار، يفرط في تجاوز ما ينتظر أن يسفر عنه ذلك الهجوم من ميزة عسكرية ملموسة ومباشرة».

وكما ذكر سابقًا، يعني إلحاق الضرر بالأعيان «الضرر... الذي يعطل قيمة شيء ما أو الانتفاع به...».[126] وبالتالي من الواضح أن الضرر الذي يجب أخذه في الحسبان لا يشتمل على الضرر المادي فحسب، بل يتضمن أيضًا فقدان الخواص الوظيفية للبنية الأساسية المدنية حتى في حالة انتفاء الضرر المادي. وقد قيل إن «الهجمات الإلكترونية قد تغير الأهمية الممنوحة للتبعات المؤقتة» في تقييم التناسب،[127] غير أن هذا لا يستند إلى أساس قانوني في القانون الدولي الإنساني. وكما اقترح «جيس» و«لهمان»، فإن أي قراءة أخرى ستترتب عليها العواقب التالية:

> في حين أن تدمير سيارة مدنية منفردة من شأنه أن يصل إلى حد «الضرر العرضي» ذي الصلة من الناحية القانونية وإن كان غير مهم، فإن فصل خدمة الإنترنت وغيرها من خدمات الاتصالات عن آلاف أو ملايين الأسر والشركات والخدمات العامة، أو قطع المعاملات المالية التي تتم عن طريق الإنترنت عن اقتصاد بلد بالكامل وما يترتب على ذلك من تأثيرات اقتصادية مجتمعية على هذا النحو، لا تُحسب على أنها عناصر تؤخذ في الاعتبار في معادلة التناسب.[128]

ومع ذلك، ينبغي الإقرار بأن الهجمات على شبكات الكمبيوتر حين تتسبب في إلحاق الضرر بالبنية الأساسية المدنية، بسبل منها تعطيلها مؤقتًا، فإن مبدأ التناسب تعترضه عدد من القيود (كما يحدث أيضًا في الحرب التقليدية).

أولًا، كما هو الحال في جميع حالات تطبيق مبدأ التناسب، لا يزال هناك قدر من الشك بشأن ما يمكن اعتباره أضرارًا عرضية مفرطة تلحق بالأعيان المدنية بالمقارنة بالميزة العسكرية الملموسة والمباشرة. وتبدو النتائج التي تبين أن الأضرار العرضية التي تلحق بالبنية الأساسية المدنية تكون مفرطة بالمقارنة بالميزة العسكرية، قليلة ومتباعدة.[129] ولا

125 دراسة القانون الدولي الإنساني العرفي، الحاشية 87 أعلاه، القاعدة 14.

126 *Concise Oxford Dictionary*.

127 Oona Hathaway et al., 'The law of cyber-attack', in California Law Review, Vol. 100, No. 4, 2012, p. 817.

128 R. Geiss and H. Lahmann، الحاشية 61 أعلاه، الصفحة 17.

129 انظر:

Louise Doswald-Beck, 'Some thoughts on computer network attack and the international law of armed conflict', in Michael N. Schmitt and Brian T. O'Donnell (eds), *Computer Network Attack and International Law*, International Law Studies, Vol. 76, 2002, p. 169:

«... الأمثلة الموجودة... كانت دائمًا... إما حالات كان فيها الهدف المحتمل شيئًا ذا طبيعة عسكرية لكنه غير قابل للاستخدام في ظل الظروف السائدة، وإما أن قيمة العين كهدف عسكري لا يمكن التحقق منها». انظر أيضًا: المحكمة الجنائية الدولية ليوغوسلافيا السابقة، التقرير النهائي المقدم إلى المدعي العام من اللجنة المشكلة لاستعراض حملة القصف التي شنها حلف شمال الأطلسي ضد جمهورية يوغوسلافيا الاتحادية (ويشار إليها فيما يلي باسم «التقرير المقدم إلى المدعي العام»)، 13 حزيران/ يونيو 2000، الفقرة 19. ردًا على قيام قوات الناتو بقصف مجمع «بانشيفو» الصناعي ومصفاة للنفط في «نوفي ساد» خلال حرب كوسوفو عام 1999، والتي أدت إلى إطلاق نحو 80 ألف طن من النفط الخام إلى التربة بالإضافة إلى أطنان كثيرة من المواد المسممة الأخرى، ذكرت

يعني هذا أن التناسب لا يفرض حدودًا على جميع الهجمات. ولكن يبقى أن نرى كيف سيتم تفسيره فيما يتعلق بالهجمات الإلكترونية.

فمن ناحية، قد يقال إن العمليات الإلكترونية ما دامت لا تزال في مهدها، فلا يُعرف عنها الكثير ولا يمكن أن نتوقع من القادة استشراف تأثيرها، ومن الصعب معرفة ما هي الخسارة أو الأضرار العرضية المدنية «المتوقعة» في الحرب الإلكترونية. ومن ناحية أخرى، فإن هذا الشك كمي وليس نوعيًا؛ فتحديدًا بسبب الشبكات المترابطة، فإن التبعات التي تلحق بالبنية الأساسية المدنية تكون واضحة. وبمعنى آخر، يجب توقع الأضرار العرضية في أغلب الحالات، حتى إذا كان من الصعب تقييم حجمها الدقيق.

ثانيًا، على الرغم من عدم وجود خلاف الآن على نطاق واسع على أن التأثيرات الارتدادية- وهي تأثيرات المستوى الثاني أو الثالث غير المباشرة الناجمة عن هجوم معين- يجب أن تؤخذ في الاعتبار، لا يزال بعض النقاش دائرًا حول نطاق هذا الالتزام.[130] وبالنظر إلى صياغة المادة 51 (5) (ب) من البروتوكول الإضافي الثاني («يمكن أن يتوقع منه»)، من المنطقي الدفع بأن الأضرار المتوقعة يجب أن توضع في الاعتبار، حتى إذا كانت طويلة الأجل أو كانت أضرارًا من المستوى الثاني والثالث.[131] وبسبب ترابط الشبكات في الفضاء الإلكتروني، قد يكون توقع التأثيرات أصعب مما هي عليه في حالة السلاح التقليدي الحركي، ولكن في الوقت نفسه من المهم للغاية القيام بكل جهد مستطاع لتقييم تلك التأثيرات. ومن الناحية العملية، يؤدي هذا أساسًا إلى طرح المسألة المتعلقة بالاحتياطات الواجب اتخاذها في الهجمات. وبالنظر إلى ترابط شبكات المعلومات والنظم التي تعتمد عليها، ما الذي يمكن توقعه من قائد من حيث التحقق من أجل تقدير التأثيرات الارتدادية للهجوم على شبكة الكمبيوتر؟[132]

مبدأ الاحتياط

يتضمن مبدأ الاحتياط في القانون الدولي الإنساني جانبين: الاحتياطات في الهجوم والاحتياطات لمواجهة تأثيراته.[133]

الاحتياطات في الهجوم

عند تنفيذ العمليات العسكرية، يجب توخي العناية الدائمة من أجل تجنيب السكان المدنيين والأعيان المدنية.[134] وتشمل الاحتياطات المحددة التي يقتضيها القانون الدولي الإنساني بذل كل جهد مستطاع للتحقق من أن الأهداف هي أهداف عسكرية،[135] واتخاذ جميع الاحتياطات المستطاعة عند تخير وسائل وأساليب القتال من أجل تجنب إحداث خسائر في أرواح

اللجنة أنه «من الصعب تقييم القيم النسبية التي ستحدد الميزة العسكرية المتحققة والضرر الذي يلحق بالبيئة الطبيعية، وأن تطبيق مبدأ التناسب نظريًا أسهل من تطبيقه عمليًا».

130 انظر على سبيل المثال: التعليق على دليل *HPCR Manual on Air and Missile Warfare*، الحاشية 86 أعلاه، التعليق على القاعدة 14، الفقرة 4، وانظر:
Michael N. Schmitt, 'Computer network attack: the normative software', in *Yearbook of International Humanitarian Law*, The Hague, TMC Asser Press, 2001, p. 82

131 Tallinn Manual، الحاشية 27 أعلاه، التعليق على القاعدة 51، الفقرة 6؛ R. Geiss and H. Lahmann، الحاشية 61 أعلاه، الصفحة 16.

132 يجب تمييز هذا عن الهجوم العشوائي الذي يمكن السيطرة فيه على التأثيرات.

133 انظر: المادتان 57 و58 من البروتوكول الإضافي الأول؛ دراسة القانون الدولي الإنساني العرفي، الحاشية 87 أعلاه، القواعد 15-24.

134 المادة 57 (1) من البروتوكول الإضافي الأول؛ دراسة القانون الدولي الإنساني العرفي، الحاشية 87 أعلاه، القاعدة 15.

135 المادة 57 (2) (أ) (أولًا) من البروتوكول الإضافي الأول؛ دراسة القانون الدولي الإنساني العرفي، الحاشية 87 أعلاه، القاعدة 16.

المدنيين، أو إلحاق الإصابة بهم أو الإضرار بالأعيان المدنية، وذلك بصفة عرضية، وعلى أي الأحوال حصر ذلك في أضيق نطاق.[136] وهو أيضًا يلزم أطراف النزاع بإلغاء أو تعليق أي هجوم إذا تبين أنه سيحدث «أضرارًا عرضية» مفرطة.[137]

وبالتالي، قد تتضمن الاحتياطات التزامات من قبيل اتخاذ تدابير لجمع كافة المعلومات المتاحة من أجل التحقق من الهدف والتأثيرات العرضية المحتملة لأي هجوم.[138] وفي الحرب الإلكترونية، قد تشمل الاحتياطات تصميم خريطة بشبكة الخصم،[139] التي تكون عادة جزءًا من تصميم الهجمات على شبكات الكمبيوتر في أي حالة إذا كانت مصممة خصيصًا للهجوم على نظام حاسوبي مستهدف بعينه. وإذا كانت المعلومات المتاحة غير كاملة- كما هو الحال في الفضاء الإلكتروني بسبب ما يتسم به من ترابط- فيجب تحديد نطاق الهجوم بحيث يقتصر على تلك الأهداف التي تتوافر عنها معلومات كافية.[140]

وقد يتطلب مبدأ الاحتياط خبرة تقنية خاصة. ينص «دليل تالين» على أنه «بالنظر إلى تعقد العمليات الإلكترونية، وارتفاع احتمالات الإضرار بالنظم المدنية، والفهم المحدود في بعض الأحيان لطبيعتها وتأثيرها لدى المسؤولين عن اعتماد العمليات الإلكترونية، ينبغي أن تتاح لمخططي المهام، حيثما أمكن، الاستعانة بالخبرة التقنية الموجودة لمساعدتهم في تحديد ما إذا كانت التدابير الاحتياطية الملائمة قد اتُخذت.[141] وإذا كانت الخبرة، ومن ثم القدرة على تقييم طبيعة الهجوم والخسائر والأضرار العرضية بين المدنيين، غير متاحة، فقد يتعين على المهاجم الامتناع عن الهجوم.

ومع ذلك، من المرجح أن تكون الكثير من الهجمات الإلكترونية التي تتم في إطار الدفاع، آلية؛ أي إنها عمليات إلكترونية مبرمجة من قبل لمواجهة التدخلات التي تتم من الخارج.[142] وهذه «الهجمات المضادة» تكون آلية وتستهدف بكل بساطة أجهزة الكمبيوتر التي يبدأ منها التدخل؛ ولمّا كانت تتصدى لمشكلة تقنية، فهي لا تُعنى بالطبيعة المدنية أو العسكرية لأجهزة الكمبيوتر. وفي هذه الظروف، وبالنظر إلى أن هذه الهجمات الإلكترونية مصدرها آلاف بل وحتى ملايين أجهزة الكمبيوتر، سيتعين على الدول أن تتوخى العناية في تقييم مشروعية هذه الهجمات المضادة في ضوء مبدأ الاحتياط.

ومن زاوية أخرى، يمكن لمبدأ الاحتياط، في بعض الحالات، أن يتضمن التزامًا باللجوء إلى التكنولوجيا الإلكترونية عندما تكون متاحة. وفي الواقع، قد تتسبب العمليات الإلكترونية أيضًا في أضرار عرضية أقل بين المدنيين أو في البنية الأساسية المدنية مما تسببه العمليات الحركية. فعلى سبيل المثال، قد يكون تعطل خدمات معينة تستخدم لأغراض عسكرية ومدنية أقل ضررًا من تدمير البنية الأساسية بالكامل. ومع ذلك، فإن مسألة نطاق الالتزام باللجوء إلى تكنولوجيا أكثر تطورًا- التكنولوجيا الإلكترونية في هذه الحالة- لم تُسو بالكامل. وفي الواقع، لا يوجد حتى الآن توافق دولي على أن الأطراف المتحاربة يجب عليها

136 المادة 57 (2) (أ) (ثانيًا) من البروتوكول الإضافي الأول؛ دراسة القانون الدولي الإنساني العرفي، الحاشية 87 أعلاه، القاعدة 17.
137 المادة 57 (2) (ب) من البروتوكول الإضافي الأول؛ دراسة القانون الدولي الإنساني العرفي، الحاشية 87 أعلاه، القاعدة 19.
138 المحكمة الجنائية الدولية ليوغوسلافيا السابقة، التقرير النهائي المقدم إلى المدعي العام، الفقرة 29: وصفت اللجنة المشكلة لاستعراض حملة القصف التي شنها حلف شمال الأطلسي ضد جمهورية يوغوسلافيا في تقريرها النهائي هذا الالتزام على النحو التالي: «يجب على القائد العسكري إنشاء نظام فعال لجمع المعلومات من أجل جمع وتقييم المعلومات المتعلقة بالأهداف المحتملة. ويجب على القائد كذلك توجيه قواته إلى استخدام الوسائل التقنية المتاحة لتحديد الأهداف بشكل صحيح أثناء العمليات. ويجب على القائد وطاقم الطائرات المشاركة فعليًا في العمليات أن يكون لديها شيء من السلطة التقديرية لتحديد أي الموارد المتاحة يجب استخدامه وبأي طريقة».
139 E. T. Jensen، الحاشية 90 أعلاه، الصفحة 1185.
140 Tallinn Manual، الحاشية 27 أعلاه، القاعدة 53، الفقرة 6.
141 المرجع السابق، القاعدة 52، الفقرة 6.
142 وفقًا للمادة 49 من البروتوكول الإضافي الأول، هذه العمليات الدفاعية هي أيضًا هجمات يجب أن تلتزم بمبادئ التمييز والتناسب والاحتياط.

في جميع الأحوال أن تستخدم السلاح الأكثر دقة أو الأكثر تقدمًا من الناحية التكنولوجية (تدور المناقشة حول هذه المسألة أساسًا فيما يتعلق بالذخائر الدقيقة التوجيه).[143] ومع ذلك، يتضمن مبدأ الاحتياط التزامًا بعدم التقيد بمبدأ التمييز والتناسب فحسب، بل أيضًا اتخاذ كل التدابير المستطاعة من أجل «تجنب إحداث خسائر في أرواح المدنيين، أو أضرار بالأعيان المدنية، وذلك بصفة عرضية، وعلى أي الأحوال حصر ذلك في أضيق نطاق». وفي هذه الحالات، يعني مبدأ الاحتياط ضمنًا أن القادة ينبغي لهم أن يختاروا أقل الوسائل ضررًا المتاحة في زمن الهجوم من أجل تحقيق هدفهم العسكري.[144]

الاحتياطات لمواجهة تأثيرات الهجمات

يقتضي مبدأ الاحتياطات لمواجهة تأثيرات الهجمات أن تقوم أطراف النزاع، ضمن إجراءات أخرى «قدر المستطاع، بالسعي جاهدة إلى نقل ما تحت سيطرتها من السكان المدنيين والأفراد المدنيين والأعيان المدنية بعيدًا عن المناطق المجاورة للأهداف العسكرية» وأن «تتخذ الاحتياطات الأخرى اللازمة لحماية ما تحت سيطرتها من سكان مدنيين وأفراد وأعيان مدنية من الأخطار الناجمة عن العمليات العسكرية».[145] ويعني هذا أن الدول عليها التزام إما بإبقاء الأهداف العسكرية بعيدًا عن السكان المدنيين والأعيان المدنية، أو (ولا سيما إذا لم يكن هذا الإجراء ممكنًا) اتخاذ تدابير أخرى لحماية السكان المدنيين والبنية الأساسية المدنية من الأخطار الناجمة عن العمليات العسكرية.

وكما يشير «دليل تالين»، قد يشمل هذا «فصل البنية الأساسية الإلكترونية العسكرية عن المدنية؛ وفصل النظم الحاسوبية التي تعتمد عليها البنية الأساسية المدنية الحيوية عن شبكة الإنترنت؛ واتخاذ ترتيبات مسبقة لضمان الإصلاح الفوري للنظم الحاسوبية المهمة تحسبًا لأي أنواع متوقعة من الهجوم الإلكتروني، والتسجيل الرقمي للأعيان الثقافية أو الروحية المهمة لتسهيل إعادة الإعمار في حالة تدميرها أثناء النزاع المسلح، واستخدام تدابير مكافحة الفيروسات لحماية النظم المدنية التي قد تتأثر بالأضرار أو التدمير أثناء هجوم على البنية الأساسية الإلكترونية المدنية».[146]

وفي الواقع، غالبًا ما تتم الدعوة إلى ضرورة الفصل بين الشبكات العسكرية والمدنية.[147] وكما يوصي التقييم القانوني الذي أجرته وزارة الدفاع الأمريكية، «حيثما يكون هناك اختيار، ينبغي إبقاء النظم العسكرية منفصلة عن البنى الأساسية المستخدمة لأغراض مدنية أساسية».[148] ومع ذلك، فهو أمر بعيد عن الواقع. ففي الأيام الأولى التي شهدت ظهور شبكة الإنترنت، مضى بناؤها دون أي مراعاة لهذه المسائل. هناك بطبيعة الحال شبكات

143 انظر:
Jean-François Quéguiner, ‘Precautions under the law governing the conduct of hostilities’, in *International Review of the Red Cross*, Vol. 88, No. 864, December 2006, p. 801; *Commentary on HPCR Manual on Air and Missile Warfare*, above note 86, Commentary on Rule 8, para. 2.

144 K. Dörmann، الحاشية 42 أعلاه؛
Michael N. Schmitt, ‘The principle of discrimination in 21st century warfare’, in *Yale Human Rights and Development Law Journal*, Vol. 2, 1999, p. 170; Commentary on HPCR Manual on Air and Missile Warfare,
الحاشية 86 أعلاه، التعليق على القاعدة 32 (ب)، الفقرة 3 بشأن الأسلحة ذات مستوى الدقة الأكبر أو قوة التفجير الأقل.

145 المادة 58 من البروتوكول الإضافي الأول؛ دراسة القانون الدولي الإنساني العرفي، الحاشية 89 أعلاه، القاعدتان 22 و24.

146 Tallinn Manual، الحاشية 27 أعلاه، التعليق على القاعدة 59، الفقرة 3.

147 E. T. Jensen، الحاشية 97 أعلاه، الصفحات 1533-1569؛
Adam Segal, ‘Cyber space governance: the next step’, Council on Foreign Relations, Policy Innovation Memorandum No. 2, 14 November 2011, p. 3,
متاح عبر الرابط التالي: http://www.cfr.org/cybersecurity/cyberspace-governance-next-step/p24397

148 Department of Defense Office of General Counsel، الحاشية 112 أعلاه، الصفحة 7.

عسكرية مغلقة، وتُفصل أيضًا بعض البنى الأساسية المدنية البالغة الحساسية عن الشبكات الخارجية. ولكن بالنظر إلى الضعف المتأصل في القاعدة المتعلقة بفصل الأعيان المدنية عن الأهداف العسكرية (المادة 58 -أ- من البروتوكول الإضافي الأول) التي تُلزم فقط الدول بالسعي جاهدة إلى فصل الأهداف العسكرية عن الأعيان المدنية وفقط بالقدر المستطاع، من غير المرجح بصورة كبيرة أن تُفسر في ممارسات الدول على أنها تتضمن التزامًا بفصل الشبكات المدنية عن العسكرية. وإن كان القيام بهذا ممكنًا من الناحية النظرية، فإنه سيكون غير عملي ومكلفًا إلى الحد الذي يجعله غير قابل للتطبيق بمفهوم المادة 58 من البروتوكول الإضافي الأول. وسيتعين على الحكومات إنشاء خطوط الاتصالات العسكرية الخاصة بها، بما في ذلك الكابلات وأجهزة التوجيه والأقمار الاصطناعية، في جميع أنحاء العالم.[149]

بالإضافة إلى ذلك، فإن فصل البنية الإلكترونية العسكرية عن المدنية يعتمد على افتراض أنهما متميزتان وينبغي الإبقاء عليهما متميزتين. وبالمعنى الدقيق للكلام، لا تحظر المادة 58 الاستخدام المزدوج: فهي تعتمد على افتراض أن هناك تمييزًا بين الأعيان المدنية والأهداف العسكرية، حتى إذا كانت بعض الأعيان المدنية تستخدم كأهداف عسكرية. وبالفعل في العالم المادي، تستخدم أجزاء كبيرة من البنية الأساسية المهمة لأغراض مزدوجة، ومنها على سبيل المثال شبكات الكهرباء، وكذلك في حالات كثيرة أنابيب النفط، ومحطات الطاقة، وشبكات الطرق. أما في الفضاء الإلكتروني، فيصبح المبدأ خاليًا من أي معنى نسبيًا، حيث لا تتمثل المشكلة في اشتراك البنى الأساسية المدنية والعسكرية في الموقع، بل في حقيقة أنهما شيء واحد ولا فرق بينهما.[150]

والسؤال في هذه الحالة هو عما إذا كانت المادة 58 (ج) من البروتوكول الإضافي الأول تشترط أن تتوفر الحماية لبعض البنى الأساسية المدنية على أقل تقدير (محطات الطاقة النووية، والمصانع الكيميائية، والمستشفيات على سبيل المثال) من الأضرار في حالة الهجوم الإلكتروني، مما يُلزم الدول بأن تتخذ إجراءات للإبقاء على خصائصها الوظيفية. فعلى سبيل المثال يوصي «إريك تالبوت جنسن» الولايات المتحدة، لكي تمتثل لالتزامها في إطار المادة 58، بأن تتخذ عددًا من التدابير مثل إعداد خريطة توضح النظم والشبكات والصناعات المدنية التي ستتحول إلى أهداف عسكرية، وأن تكفل توفير حماية كافية للقطاع الخاص، وأن تعمل على إنشاء أو صيانة حلول للهجمات المضادة، أو أن تنشئ احتياطات استراتيجية من قدرات شبكة الإنترنت.[151] وبالتأكيد يسير عدد كبير من البلدان نحو حماية بنيته الأساسية الحيوية في هذا الطريق- وإن كان من غير المرجح أن تتصور الحكومات هذه الحماية في إطار الاحتياطات السلبية بالمعنى المقصود في المادة 58 (ج).

الخلاصة

كما ورد في المقدمة، ستتضمن العمليات الإلكترونية وسائل وأساليب جديدة للقتال، لا تزال تأثيراتها لم تختبر بعد أو هي غير مفهومة فهمًا جيدًا. ولكن يبدو أن استخدام تكنولوجيا المعلومات لأغراض عسكرية يشكل تحديات خطيرة أمام تطبيق القانون الدولي الإنساني، ولا سيما فيما يتعلق بالفرضية الأساسية التي تقول إن السكان المدنيين والأعيان المدنية يمكن بل ويجب تمييزهم في النزاع المسلح. ومن أجل الحصول على بيانات واضحة بشأن ما تعتزم الدول القيام به من أجل احترام مبادئ التمييز والتناسب والاحتياط، ينبغي طرح هذه المسألة لمناقشة أكثر صراحة ووضوحًا مما عليه الحال الآن.

وفي ضوء الأخطار التي تشكلها الحرب الإلكترونية على البنية الأساسية المدنية، يقترح عدد من الحلول في ضوء القانون القائم والقانون المنشود. ومن هذه الاقتراحات أن

149 E. T. Jensen، الحاشية 97 أعلاه، الصفحتان 1551 و1552.
150 R. Geiss and H. Lahmann، الحاشية 61 أعلاه، الصفحة 14.
151 E. T. Jensen، الحاشية 97 أعلاه، الصفحة 1563.

تصدر الدول بيانات تفصيلية عن ملاذات رقمية آمنة، أي أهداف مدنية تعتبر بها الدول خارج حدود سير العمليات الإلكترونية.[152] وإذا جرى الاتفاق على هذا بين الأطراف، فإن هذا سيكون أقرب إلى المناطق المنزوعة السلاح المنصوص عليها في المادة 60 من البروتوكول الإضافي الأول. وسيستلزم هذا عملية الحوار وتدابير بناء الثقة التي تتم الدعوة إليها حاليًا، وهي تتجاوز موضوع هذا المقال. يقول «آدم سيغال» إنه «من المرجح أن يتحقق توافق سهل نسبيًا على بعض المجالات- المستشفيات والبيانات الطبية- واتفاق أقل بكثير حول مجالات أخرى مثل النظم المالية، وشبكات الكهرباء، والبنية الأساسية لشبكة الإنترنت».[153] وعلى الرغم من أن هذا مسار مثير للاهتمام ينبغي استكشافه- وربما يُستكشف في النهاية في إطار حوار دولي بشأن تدابير بناء الثقة- فربما لا يكون من قبيل التشاؤم المفرط التشكيك في جدوى هذا المسار على المدى القصير. وبالنظر إلى الطبيعة الخفية لكثير مما يبدو أنه التلاعب الحالي بالفضاء الإلكتروني والتسلل إليه، من غير الواضح حجم الثقة التي ستوضع في الاتفاقات أو البيانات المتعلقة بالمناطق الإلكترونية التي ستكون خارج حدود الاستخدام العسكري.

ثمة اقتراح آخر قدمه «جيس» و«لهمان» بتوسيع قائمة «الأعمال والمنشآت التي تحوي قوى خطرة» الواردة في المادة 56 من البروتوكول الإضافي الأول عن طريق القياس.[154] ويمكن أن ينطبق هذا على عناصر معينة في البنية الأساسية الإلكترونية، مثل شبكات التبادل الرئيسية في شبكة الإنترنت أو «الخوادم» المركزية التي تعتمد عليها ملايين من الوظائف المدنية المهمة. وشأنها شأن السدود والجسور ومحطات توليد الطاقة النووية، لا يجوز أن تكون هدفا للهجوم، حتى إذا كانت تشكل أهدافًا عسكرية؛ لأن الأخطار على السكان المدنيين تتجاوز في جميع الأحوال الميزة العسكرية المتحققة من مهاجمتها. ومع ذلك، يقر «جيس» و«لهمان» أيضًا بأن من غير المرجح أن يلاقي اقتراح من هذا القبيل تأييدًا بين الدول. فعلى وجه الخصوص، على الرغم من أن التأثيرات الارتدادية لتعطيل أو تدمير البنية الأساسية الإلكترونية قد تكون خطيرة، فسيكون من الصعب الدفع بأنها قابلة للمقارنة مع إطلاق الانبعاثات مثل المواد المشعة أو مياه السدود. ولكن، إذا كانت لها هذا التأثيرات الكارثية المشابهة، فإن المبرر المنطقي الذي تستند إليه المادة 56 من البروتوكول الإضافي الأول يمكن أن يوفر حجة مقنعة لحماية البنية الأساسية الإلكترونية.

وبالمضي قدمًا، أدت التحديات التي يفرضها العالم الإلكتروني أيضًا إلى إثارة المسألة المتعلقة بما إذا كان ينبغي أن تُحظر (بعض) وسائل وأساليب الحرب الإلكترونية حظرًا تامًا أو تنظم بموجب معاهدة دولية. وكما ورد في المقدمة، دعت بعض الدول إلى صياغة معاهدة جديدة في هذا الصدد، على الرغم من أن حدود ما ينبغي ولا ينبغي السماح به ليست واضحة تمامًا في جميع الأحوال. تدور مناقشة متزامنة بين الخبراء والأكاديميين المتخصصين في الأمن الإلكتروني. فقد اقترح البعض صياغة معاهدات جديدة بشأن الحرب الإلكترونية،[155] في حين يدفع آخرون بضرورة وجود شكل من أشكال معاهدة نزع السلاح تفرض حظرًا على جميع الأسلحة الإلكترونية أو بعضها على أقل تقدير.[156] ولا يزال البعض

152 A. Segal، الحاشية 147 أعلاه.

153 المرجع السابق.

154 R. Geiss and H. Lahmann، الحاشية 61 أعلاه، الصفحة 11.

155 Mark R. Shulman, 'Discrimination in the law of information warfare', in *Columbia Journal of Transnational Law*, Vol. 37, 1999, p. 964; Davis Brown, 'A proposal for an international convention to regulate the use of information systems in armed conflict', in *Harvard International Law Journal*, Vol. 47, No. 1, Winter 2006, p. 179; Duncan B. Hollis, 'Why states need an international law for information operations', in *Lewis and Clark Law Review*, Vol. 11, 2007, .p. 1023

156 Mary Ellen O'Connell, 'Cyber mania', in *Cyber Security and International Law*, Meeting Summary, Chatham House, 29 May 2012,

متاح عبر الرابط التالي:
http://www.chathamhouse.org/sites/default/files/public/Research/International%20Law/290512summary.pdf;

الآخر يعارض هذا الرأي قائلين؛ إن أي معاهدة لن تكون قابلة للتنفيذ بسبب صعوبات إسناد المسؤولية، وإنه سيكون من المستحيل من الناحية التقنية التمييز بين أدوات الحرب الإلكترونية والتجسس الإلكتروني، وإن الأسلحة المحظورة قد تكون أقل تدميرًا من الأسلحة التقليدية، وإن مسألة التحقق ستكون مستحيلة.[157]

يقترح بعض المعلقين حلولًا أخرى من قبيل «تعددية غير رسمية للأطراف»،[158] أو تكوين منظمة دولية تعنى بالأمن الإلكتروني، على غرار الوكالة الدولية للطاقة الذرية، لتعمل كمنبر مستقل للتعاون الدولي بهدف وضع معاهدات للسيطرة على الأسلحة الإلكترونية.[159]

ومن الصعب أن نعرف، في هذه المرحلة، المسار الذي ستؤدي إليه هذه المناقشات، ولا سيما إذا كانت الدولة مستعدة لمناقشة الأخطار الحقيقية للحرب الإلكترونية بشكل صريح واتخاذ التدابير الرامية لمنع أسوأ السيناريوهات. وفي الوقت ذاته، إذا اختارت أطراف النزاع الأسلحة الإلكترونية أثناء النزاعات المسلحة، فعليها أن تكون على دراية بالإطار القانوني القائم كحد أدنى من القواعد التي يجب احترامها على الرغم من قيودها. ويتعين على الدول أن تعلم وأن تدرب قواتها المسلحة وفقًا لذلك. ومن المهم تشجيع مناقشة هذه المسائل، ورفع مستوى الوعي بضرورة تقييم الأثر الإنساني لتطوير التكنولوجيات، وضمان عدم استخدامها قبل الأوان في ظل ظروف لا يمكن فيها ضمان احترام القانون.

وفي الختام، لا يوجد شك في أن القانون الدولي الإنساني ينطبق على الحرب الإلكترونية. ولكن، إذا كان القانون يوفر قدرًا كافيًا من الحماية للسكان المدنيين، لا سيما عن طريق حماية البنية الأساسية المدنية من الأضرار، فإن هذا يعتمد على أسلوب تفسير القانون الدولي الإنساني- الذي لم يتصور واضعوه هذه العمليات- فيما يتعلق بها. ولن يكون من الممكن حماية البنية الأساسية المدنية من تعرضها للاستهداف المباشر أو من الأضرار التي يمكن أن تكون كارثية على السكان المدنيين إلا إذا فسر القانون على أساس من حسن النوايا ومن خلال توخي أقصى درجات العناية. وحتى في هذه الحالة، فبالنظر إلى أوجه الضعف المحتملة التي تعتري مبادئ التمييز والتناسب والاحتياط- وفي ظل غياب معرفة أوسع بالقدرات والتأثيرات الهجومية- لا يمكن أن نستبعد احتمال الحاجة إلى قواعد أكثر صرامة.

Misha Glenny, 'We will rue Stuxnet's cavalier deployment', in *The Financial Times*, 6 June 2012, citing Russian antivirus expert Eugen Kaspersky; Scott Kemp, 'Cyberweapons: bold steps in a digital darkness?', in Bulletin of the Atomic Scientists, 7 June 2012, متاح عبر الرابط التالي:
http://thebulletin.org/web-edition/op-eds/cyberweapons-bold-steps-digital-darkness ؛
Bruce Schneier, 'An international cyberwar treaty is the only way to stem the threat', in US News, 8 June 2012,
http://www.usnews.com/debate-club/should-there-be-an-international-trea- متاح عبر الرابط التالي:
ty-on-cyberwarfare/an-international-cyberwar-treaty-is-the-only-way-to-stem-the-threat;
Duncan Holis, 'An e-SOS for cyberspace', in Harvard International Law Journal, Vol. 52, No. 2, Summer 2011, who argues for a system of e-sos.

157 Herb Lin and Thomas Rid, 'Think again: cyberwar', in Foreign Policy, March/April 2012, p. 7, متاح عبر الرابط التالي:
http://www.foreignpolicy.com/articles/2012/02/27/cyberwar?print=yes&hidecom-ments=yes&page=full;
Jack Goldsmith, 'Cybersecurity treaties: a skeptical view', in Peter Berkowitz (ed.), *Future Challenges in National Security and Law* (forthcoming), متاح عبر الرابط التالي:
http://media.hoover.org/sites/default/files/documents/FutureChallenges_Goldsmith.pdf.

158 A. Segal، الحاشية 108 أعلاه.

159 Eugene Kaspersky, 'Der Cyber-Krieg kann jeden treffen', in Süddeutsche, 13 September 2012, متاح عبر الرابط التالي:
http://www.sueddeutsche.de/digital/sicherheit-im-internet-der-cyber-krieg-kann-jeden-tref-.fen-1.1466845