اللجوء للحق في اتخاذ إجراءات مضادّة ومدى ملاءمته كخيار للرد على الهجمات السيبرانية المعادية

أ. د. ياسر يوسف الخلايلة
كلية القانون – جامعة قطر

وأ. د. مخلد إرخيّص الطراونة
قسم القانون – كلية الشرطة – قطر

الملخّص :

بلغت الثورة التكنولوجيّة ذروتها مع دخول العالم الرقمي إلى كل مناح الحياة اليوميّة، منها ما له آثار إيجابية ومنها ما له آثار سلبية، ومنها ما له أثر مباشر على الأفراد وما له أثر يصيب الدول ذات السيادة. ونحن نشهد الآن استخدامات للشبكة العنكبوتية كوسيط يتم من خلاله تنفيذ هجمات سيبرانية غير مشروعة دولياً باعتبار أنها تؤثر في سيادة الدول المستهدفة. وعليه، يثير هذا البحث سؤالاً متعلقاً بالإمكانات المتاحة للدول لأن ترد على تلك الأنشطة حال حصولها، وتكون فيه ضحيّة لها، بعيداً عن استخدامها لحقّها المتمثّل بالدفاع الشرعي عن نفسها المُشار إليه في المادة 51 من ميثاق الأمم المتحدة. فهذا الحق، وإن كان يعكس عرفًا من أعراف القانون الدولي المستقرّة، إلّا أنّه في اللجوء إليه مباشرة تجاهلًا كبيراً لإمكانات أخرى يوفّرها القانون الدولي، متمثّلة بالحق في اتخاذ تدابير مضادّة وردت الإشارة إليها صراحةً في المادة 22 من مشروع المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دوليًا. ويقترح هذا البحث أن هذه التدابير يمكن أن تكون ناجعة، وأنّها جاءت تحديدًا تحت الفصل الخاص ب «الإجراءات البديلة المضادّة المتعلّقة بالأعمال غير المشروعة».

لذلك، يسعى هذا البحث إلى تثبيت فكرة ضرورة الإبقاء على اللجوء للتدابير المضادّة كوسيلة أساسية يّلجأ إليها في المقام الأوّل، سواء في المساومة السياسية أو القانونية، قبل الالتجاء لغيرها من الإجراءات. وذلك بسبب صعوبة الوقوف على ما إذا كانت الهجمات السيبرانية ترقى لمستوى العمليات «العسكرية» المعادية للتمكّن من إثارة المادة 51 من ميثاق الأمم المتحدة. ولبناء هذه النتيجة، يجيب البحث عمّا إذا كانت

العمليات السيبرانية المعادية تخوّل الدول المعتدى عليها بداية من استخدام حقّها في اللجوء إلى التدابير المضادة في إطار مشروع المواد المتعلّقة بمسؤولية الدول عن الأعمال غير المشروعة دوليًا.

المقدّمــة :

تنوّعت وتسارعت وتيرة استخدام الفضاء الإلكتروني في تنفيذ عمليات غير مشروعة دوليًا تؤثر وبشكل مباشر على سيادة الدولة وسياساتها وقدرتها على النهوض باقتصادها. ومع كثرة هذا النوع من الأنشطة السيبرانية المُعادية يثار التساؤل: كيف يمكن للدول أن ترد على الأنشطة الإلكترونية السيبرانية الخارجية المعادية؟ سؤال طالما تعرّضت له الأبحاث الفقهية بالارتكاز على الحق العام المتمثّل بالدفاع الشرعي المُشار إليه في المادة 51 من ميثاق الأمم المتحدة، والذي يعكس عرفًا من أعراف القانون الدولي المستقرّة، كحق عام لأي دولة في الدفاع عن نفسها ضمن ثوابت محددة مدارها السماح باستخدام القوة، إن لزم الأمر، على «الهجمات المُسلحة»، بما في ذلك العمليات السيبرانية التي ترقى إلى مصاف الهجوم العسكري[1].

والحقيقة أن النظرة الفقهية لمفهوم الدفاع عن النفس قد تبلورت بشكل أكبر في أعقاب أحداث 9/11، وذلك إثر تخوف المجتمع الدولي من تكرار أحداث إرهابية مماثلة، بحيث أصبح الناتج الفكري في هذا الموضوع متركّزًا على محاولة تجاوز المعنى اللغوي لنص المادة 51 من ميثاق الأمم المتحدة، ومتجاهلًا إلى حد كبير إمكانية اتخاذ تدابير مضادّة وردت الإشارة إليها صراحةً في المادة 22 من

(1) تحدد المادة 51 من ميثاق الأمم المتحدة أن حق الدفاع الشرعي مرتبط بوجود هجوم عسكري كشرط سابق لتفعيل هذا الحق. ويمكن الرجوع إلى عدد كبير من السوابق القضائية التي تدل على وجود عرف دولي ثابت بخصوص استخدام هذا الحق مثل قرار محكمة العدل الدولية في قضية نيكاراجوا (Nicaragua v. U.S., I.C.J. 14, 176, 27 June 1986). انظر أيضًا: فتوى محكمة العدل الدولية بخصوص مدى قانونية التهديد باستخدام السلاح النووي (ICJ Advisory Opinion, I.C.J. 226, 38, 41, 8 July 1996). أيضًا، قضية موانئ البترول بين أمريكا وإيران (Iran v. U.S., I.C.J. 161, 74, 6 Nov. 2003).

مشروع المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دوليًا[2]. هذه التدابير جاءت تحديدًا تحت الفصل الخامس الخاص بالظروف النافية لعدم المشروعية، كإجراءات بديلة يمكن استخدامها بكفاية عالية بدلًا من حق الدفاع عن النفس المذكور في المادة 21 من ذات الفصل[3].

(2) مشروع المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دوليًا، 2002، السجلات الرسمية للجمعية العامّة، الدورة السادسة والخمسون، الملحق رقم ١٠ (A/56/10)، الفصل الرابع، الفقرة 76. انظر: النسخة العربية من المشروع على الموقع الإلكتروني:

http://www.un.org/arabic/documents/GADocs/56/A_56_589.pdf

جميع المواقع الإلكترونية في هذه الدراسة تم زيارتها بتاريخ 2 فبراير 2016.

(3) أيضًا يمكن الرجوع في موضوع الحق في الدفاع عن النفس في مجال الاعتداء السيبراني إلى «مدوّنة مبادئ تالين» الإرشادية الخاصّة بالقانون الدولي المستخدمة في الحروب السيبرانية وخصوصًا المبادئ 13 – 17:

https://www.usnwc.edu/getattachment/Departments---Colleges/International-Law/Tallinn-Manual/Tallinn.pdf.aspx

ولقد نشر حلف شمال الأطلسي «الناتو» هذه المدوّنة من 282 صفحة؛ لتصبح المرجع للقوانين الدولية المطبقة في حالة نشوب حروب الإلكترونية وأيضًا لتنظيم قواعد الاشتباك عبر الإنترنت. جاءت هذه المدوّنة على أثر تخوّف مسؤولين عسكريين أمريكيين من هجمات إلكترونية مستمرة تتعرض لها الولايات المتحدة من قبل الصين، وحيث ساد اعتقاد عند مسؤولين عسكريين بحلف شمال الأطلسي أن الحرب الإلكترونية أصبحت سلاحًا مدمرًا حاله حال السلاح الحربي. وتعطي مدوّنة تالين حقًا للدولة التي تتعرض لهجوم إلكتروني في شن حرب هجومية إلكترونية مضادة، بل وتسمح باستخدام القوة العسكرية في حالة كان من نتيجة شن الهجوم الإلكتروني المعادي خسائر بالأرواح البشرية. انظر في هذا الصدد:

https://blog.cyberkov.com/270.html.

ولا يخفى أنّه من المتوقّع أن تقوم الولايات المتحدة باستعمال هذه القوانين لصالحها، وذلك بشن هجمات مضادة على الدول واعتبارها أهدافا شرعية وبدعم من حلف الناتو، وخصوصًا في غياب رؤية صينية روسية واضحة لهذا القانون. انظر: ما جاء بخصوص مبادئ تالين عمومًا المذكرات التفسيرية لمايكل شميت (Michael Schmitt ed., 2013).

وانظر أيضًا ماثيو واكسمان:

M. C. Waxman, Self-defensive Force Against Cyber Attacks: Legal, Strategic and Political Dimensions, 89 INT'L L. STUD. 109 (2013);

وأيضًا:

M. N. Schmitt, Cyber Operations and the Jus ad Bellum Revisited, 56 VILL. L. REV. 569, 586–603 (2011)

وأيضًا:

Y. Dinstein, Computer Network Attacks and Self-Defense, 76 INT'L L. STUD. 99 (2002)

هذا البحث[4] يُناقش ويُجادل بضرورة الإبقاء على اللجوء للتدابير المضادّة كوسيلة أساسية في المساومة السياسية والقانونية، فالواقع يشير مثلاً إلى أنه من الصعوبة بمكان أن ترقى العمليات السيبرانية المعادية دائمًا إلى مصاف العمليات «العسكرية» المعادية بوصفها المذكور في المادة 51 من ميثاق الأمم المتحدة. فعلى سبيل المثال، هناك خلاف حول إمكانية وصف عملية "ستوكس نت" عام 2010 (والمعروفة بأنها كانت موجّهة لتحجيم مشروع إيران النووي والتي أدّت إلى تخريب ما يقارب 1000 جهاز طرد مركزي نووي إيراني) على أنها اعتداء عسكري عدائي يتفق والوصف الوارد في المادة 51 [5].

ويبقى السؤال هنا ـ وبعيدًا عن الحق التقليدي في الدفاع الشرعي الوارد في المادة 51 من ميثاق الأمم المتحدة ـ هل تخوّل العمليات السيبرانية المعادية الدول المعتدى عليها استخدام حقّها في اللجوء إلى التدابير المضادة في إطار مشروع المواد المتعلّقة بمسؤولية الدول عن الأعمال غير المشروعة دوليًا[6]؛ خصوصًا إذا لم ترتقِ هذه العمليات إلى كونها عمليات عسكرية بالمعنى الحرفي الوارد في المادة 51 من ميثاق الأمم

(4) يرتكز هذا البحث في مجمله على مبادئ تالين، المرجع السابق، وعلى مشروع المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دوليًا، 2002، وقد تم تأسيسه على ترجمة لمفاصل الدراسة التي قدّمها مايكل شميت، أستاذ القانون الدولي في الكلّية البحرية الأمريكية في بحثه المعنون بـ:

"Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law, 3 Virginia Journal of International Law, vol. 54;

وأيضًا على دراسة تحليلية لجورمان:

S. Gorman, China Hackers Hit U.S. Chamber, WALL ST. J., Dec. 21, 2011, at: http://online.wsj.com/news/articles/SB10001424052970204058404577110541568535300

وعلى دراسة تحليلية لجروس:

M. J Gross, Enter the Cyber-Dragon, VANITY FAIR, Sept. 2011, http://www.vanityfair.com/culture/features/201109//chinese-hacking-201109

وبيرلوث:

N. Perlroth, Washington Post Joins List of News Media Hacked by the Chinese, N.Y. TIMES, Feb. 1, 2013, http://www.nytimes.com/201302/02//technology/washington-posts-joins-list-of-media-hacked-by-the-chinese.html

(5) انظر: مدوّنة مبادئ تالين الإرشادية، المرجع 3 سابق الإشارة إليه، الصفحة 58.

(6) المرجع 3 سابق الإشارة إليه.

المتحدة والمخوّل للحق في الدفاع الشرعي (علمًا بأن هذه المادة لا تُعطي مدلولًا نوعيًا واضحًا لماهية «الهجوم العسكري»)؟.

ستقوم هذه الدراسة بالتعرّض لهذه المسائل عمومًا لكن دون الخوض في دلالات الحق في استخدام الدفاع الشرعي السيبراني ضد الاعتداء الخارجي بمفهومه التقليدي، كما ستعنى فقط بمسؤولية الدول في حال الاعتداء السيبراني دون التعرّض لمسؤولية المنظمات الدولية في هذا الخصوص(7)، وستقوم تحديدًا بسبر غور الشروط الواجب توافرها قبل نشوء حق الدول للّجوء لتلك التدابير المضادّة للهجمات السيبرانية، وذلك بعد الوقوف على طبيعة تلك التدابير. وستحاول الدراسة إثبات أن اللجوء لهذه التدابير وحدودها له فوائد جمّة يمكن التعويل عليها كرد مناسب للاعتداءات الدولية التي لا ترقى لأن تتصف بأنها اعتداء عسكري، بيد أنها أيضًا موشّحة بالعديد من المعوّقات التي تحد من الاستخدام الأمثل لها وقت الحاجة. من هذا المنطلق ـ ونظرًا لأهمية هذا الموضوع ـ فإننا نرتئي تقسيمه إلى ثلاثة مباحث، نتناول في المبحث الأول عموميات في حق اللجوء إلى التدابير المضادة، وندرس في المبحث الثاني الشروط السابقة لحق اللجوء إلى التدابير المضادّة، ونركز في المبحث الثالث على حدود وقيود التدابير المضادّة ومدى تناسبها.

(7) في هذا الخصوص انظر:

Int›l L. Comm›n, Responsibility of International Organizations, U.N. Doc. A/CN.4/L.778

المبحث الأول
عموميات في حق اللجوء إلى التدابير المضادّة

سنتناول دراسة هذا الموضوع في هذا المبحث في ثلاثة مطالب، نبحث في المطلب الأول مفهوم الهجوم السيبراني وأشكاله، وفي الثاني نتعرّض لتعريف التدابير المضادة ومدى شرعيتها، ونناقش في المطلب الثالث مسألة التفرقة بين التدابير المضادّة وغيرها من الإجراءات الدولية المشابهة لها.

المطلب الأول
مفهوم الهجوم السيبراني وأشكاله

يُعد الاعتداء السيبراني من المفاهيم الحديثة نسبياً، ولذلك، يعتبر الوقوف على تعريفه، وتحديد طبيعته وعناصره، وما يترتب على إتيانه من مسؤولية دولية، جنائية كانت أم مدنية، حريا بالبحث والدراسة، والحقيقة أن هناك غموضاً يكتنف الاعتداء السيبراني فيما يتعلّق بالتعريف به[8]، ولكن لغايات هذا البحث، رأينا أن يشمل مفهوم الهجمات السيبراني جميع الأعمال التي تشكّل فقط اعتداءً على دولة ذات سيادة عن طريق استخدام أنظمة إلكترونية معيّنة تخدم مصالح المعتدي، سواء أكانت على شكل «هجوم سيبراني» أو «حرب سيبرانية»[9].

(8) انظر في مفهوم الهجوم السيبراني وأشكاله أحمد عيسى نعمة الفتلاوي، الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي، كلية القانون، جامعة بابل 2015. ولا شك بأن غياب تعريف واضح للهجوم السيبراني يشكل عائقاً بوجه المختصين. انظر في ذلك عموماً:

Oona` A.Hathway , Rebecca Crootof , Philip Levtiz , aley Nix, Aileen Nowlan ,William Perdue and Julia Spiegel, «The Law of Cyber –Attack», California Law Review, 2012 , p.7.

(9) للوقوف على التفرقة بينها انظر:

K. Saalbach,»Cyber War, Methods and Practice», Version 9.0, University of Osnabruck, 17 Jun 2014, p. 6; Shin, Beomchul,» The Cyber Warfare and the Right of Self –Defense: Legal Perspectives and the Case of the United States, IFANS, Vol.19, No1, June 2011, p. 104; and Scoot Shckelford, ,» State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem», University of Cambridge, Department of politics and International Studies, Cambridge, UK,2009, p. 194.

ولا بد من الإشارة هنا إلى أن استخدام النشاط الإلكتروني قد يكون موجّهاً لتحقيق أهداف عسكرية كجزء من هجوم عسكري، فهنا، وبقراءة نص المادة 1/49 من البروتوكول الإضافي الأوّل لعام 1977، الملحق باتفاقيات جنيف الأربعة لعام 1949، نجد أن المقصود بالهجمات هو «أعمال العنف الهجوميّة والدفاعيّة ضد الخصم». وبالرغم من أنّه لا يشترط بالهجمات السيبرانية أن يرافقها أعمال عنف مسلّح بشكل ملموس ومباشر، إلّا أننا لا يمكننا التسليم بأن كل عمل على شكل قرصنة سيبرانية لا يشكّل عمل عنف مسلّح، حيث إنّه بالنظر إلى الآثار التي ترتبها تلك العمال السيبرانية قد تتجاوز في تأثيرها وجسامتها الهجمات العسكرية التقليدية، خصوصاً أنّ المادة 2/51 من نفس الاتفاقية تنص على أنّه «لا يجوز أن يكون المدنيون بوصفهم هذا وكذا الأشخاص المدنيون محلاً للهجوم، وتحظر أعمال العنف أو التهديد به الرامية أساساً إلى بث الذعر بين السكان المدنيين».

ولكن بالنظر إلى أشكال الهجمات السيبرانية نظرة شمولية، فإنّه لا بد من القول بأنّه يصعب حصر جميع أنواع الهجمات الممكنة، بيد أنّه يمكن عرض بعض نماذج الهجمات السيبرانية التي حدثت منذ العقد الثمانين من القرن المنصرم. ففي عام 1982 مثلاً، شنّت الولايات المتحدة الأمريكية هجوماً سيبرانياً ضد منظومة التحكّم العالمية صناعياً في أنبوب نفط (Chelyabinsk) السوفييتي، محدثةً انفجاراً كبيراً امتد لثلاث كيلومترات[10]. وفي عام 1999، استهدف سلاح الجو التابع لحلف شمال الأطلسي شبكة الهاتف اليوغسلافية عن طريق هجمات سيبرانية منظّمة،[11] تلاه استهداف بعض قراصنة صينيين لمواقع إلكترونية تابعة للبيت الأبيض كرد للاعتداء على سفارة الصين في بلغراد[12]. وبين الأعوام

(10) انظر:

Diego Rafael Canabarro and Thiago Borne,»Reflection on the fog of Cyber War», National Center for Digital Government, Policy working Paper No. 13:001, March 1, 2013.

(11) انظر:

Thomas W. Smith,» The New Law of War: Legitimizing Hi-Tech and Infrastructural,» International Studies Quarterly, 2002, Vol. 46, p.366.

(12) المرجع السابق.

1998– 2000، تعرّضت أنظمة اتصال إلكترونية أمريكية رفيعة المستوى (تابعة لوزارة الدفاع، ولوكالة الفضاء الأمريكية، ووكالة الطاقة الأمريكية) لهجمات سيبرانية لسرقة آلاف من الملفّات المصنّفة على أنها سرّية للغاية[13].

وقد يكون للهجمات السيبرانية شكلاً متصلاً اتصالاً مباشراً بالقدرات الهجومية أو الدفاعية لدولة ما، من ذلك ردّة فعل الصين تجاه الولايات المتحدة الأمريكية، بعد استهدافها لمواقع إلكترونية عسكرية صينية تتعلّق بتطوير مقاتلات EP–3 ومقاتلات Fighter Jet، بأن قامت بمهاجمة مواقع إلكترونية أمريكية كانت حصيلتها تقدّر بملياري دولار أمريكي[14]. ومن ذلك أيضاً، الهجمات الإلكترونية المتلاحقة عام 2007 على استونيا من قبل روسيا الاتحاديّة، والتي أدّت إلى تعطل كامل لشبكات الاتصال الإلكتروني في استونيا من ضمنها شبكة الاتصال الخاصّة برئيس وزرائها ورئيس برلمانها[15]. هذا الهجوم له أهميّة واضحة، إذ إنّه نُظر إليه كاختبار لمدى إمكانية قيام حلف شمال الأطلسي على الرد باعتبار أن استونيا تنتمي إلى هذا الحلف[16]. ومن نفس هذا النمط الهجوم الإلكتروني الذي تعرّضت له مواقع إلكترونية في سوريا من قبل سلاح الجو الإسرائيلي عام 2007، واستهدف

(13) انظر:

Scott J. Shackelford,»Analogizing Cyber: from Nuclear War to Net War Attacks in International Law», p.14.

(14) وجّهت أمريكا تهماً رسميّة للصين ومحمّلة إيّاها عواقب هذه الهجمات. للمزيد حول هذا الموضوع أنظر:

Kenneth Grees, Darien Kindlind, Ned Moran, Rob Rachwald,»World War C: Understanding Nation-States Motives behind Today›s Advanced Cyber Attaches». Fire Eyes report, p. 6, at: https://www.fireeye.com/resources/pdfs/fireeye-wwc-report.pdf

(15) انظر:

Scott J. Shackelford, «Analogizing Cyber: From Nuclear War to Net War Attacks in International Law", op.cit 13, p. 205.

(16) تقدّمت استونيا بطلب لعقد اجتماع أمني طارئ لأعضاء حلف الناتو على إثر هذا الهجوم، وذلك على اعتبار أن هذا الهجوم يهدد دول الحلف جميعاً استناداً إلى المادة 5 من اتفاقية الناتو لعام 1959، والتي تنص على أنّه: «يتّفق الأطراف، على أن أي هجوم، أو عدوان مسلّح ضد أي طرف منهم أو عدّة أطراف في أوروبا أو أمريكا الشمالية، يُعدّ عدواناً عليهم جميعاً، وبناء عليه فإنّهم متفقون على أنه في حالة وقوع مثل هذا العدوان المسلّح، فإنّ على كل طرف منهم، تنفيذاً لما جاء في المادة 51 من ميثاق الأمم المتّحدة عن حق الدفاع الذاتي عن أنفسهم بشكل فردي أو جماعي..».

إحداث شلل تام في أنظمة اتصال في وزارة الدفاع السورية[17]، وكذلك الهجوم الروسي الجورجي عام 2008 بعد إعلان انفصال جورجيا عن روسيا[18].

والواقع أيضًا أن جُلَّ العمليات السيبرانية لا ترقى أساسًا لمستوى العمليات «العسكرية» بوصفها أعلاه، فعلى سبيل المثال، هناك خلاف حول إمكانية وصف عملية «ستوكس نت» عام 2010 على أنها اعتداء عسكري عدائي يتفق والوصف الوارد في المادة 51، بالرغم ما هو معروف بأنها كانت موجّهة لتحجيم مشروع إيران النووي وأنّها أدّت إلى تخريب ما يقارب 1000 جهاز طرد مركزي نووي إيراني[19]. وتدعو المؤشرات للاعتقاد بوجود العديد من العمليات السيبرانية المعادية التي يصعب تصنيفها بالعمليات العسكرية بالشكل المطلق. فعلى سبيل المثال، تتكرّر الأخبار في انطلاق عمليات سيبرانية من إقليم دولة الصين بالذات، وعلى أيدي قراصنة شبكة الإنترنت (أو ما يسمون بالهاكرز)، واختراقها لحسابات بنكيّة لمراكز مالية عالمية كمركز «مورغان ستانلي» وغرفة تجارة الولايات المتحدة الأمريكية، وحتى اختراق شبكات إعلامية أمريكية عالمية مثل شبكة «نيويورك تايمز» وصحيفة «وول ستريت» وصحيفة «واشنطن بوست»[20]. هذه العمليات، في مجملها، يصعب تصنيفها بالعمليات العسكرية البحتة[21].

(17) أنظر:

Eshel, David,, "Israel adds cyber-attack to IDF", Aviation Week's DTI, 9 Feb. 2010: http://infosecisland.com/blogview/5160-Analysis-on-Defense-and-Cyber-Warfare.html

(18) الهجوم أضعف قدرة جورجيا على استخدام دفاعها الجوي. أنظر:

Jonathan A. OPHARD, "Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow›s Battlefield", DUKE Law & Technology Review, No. 3, p. 3.

وأيضاً:

Thomas W. Smith, "The New Law of War: Legitimizing Hi-Tech and Infrastructural", International Studies Quarterly, 2002, Vol. 46, p. 366.

(19) انظر: مدوّنة مبادئ تالين الإرشادية، المرجع 3 سابق الإشارة إليه، الصفحة 58.

(20) انظر: في هذا الخصوص جورمان؛ جروس وبلروث، المرجع 4 سابق الإشارة إليه.

(21) للتعرّف على المصادر والتقنيات المستخدمة لمثل هذه الاعتداءات السيبرانية، انظر:

K. Geers Et Al., Fireeye Labs, World War C: Understanding Nation-State Motives Behind Today's Adbavanced Cyber Attacks, (2013);

انظر أيضًا: مايكل شميت، المرجع 4 سابق الإشارة إليه.

وعلى مستوى يمكن تصنيفه بأنّه لا يرقى لهجوم عسكري، نرى أن الهجمات السيبرانية تمادت لتطال البنى التحتيّة الاقتصادية أو الإعلامية، أو حتى الشؤون السياسيّة الأكثر أهميّة في دول أخرى، من ذلك التشويش الذي تعرضت له قناة الجزيرة الرياضية منذ سنوات قليلة خلال نقلها لمباريات كأس العالم لكرة القدم[22]. وحديثاً، كان هناك ادعاءات بأن روسيا قد تدخّلت عن طريق هجمات سيبرانية في نتائج الانتخابات الأمريكية، وشنّها لهجمات سيبرانية تدخلاً منها في حملة الانتخابات الرئاسية الفرنسية[23]، ونقلت صحيفة «الشرق الأوسط» السعودية منذ شهور قليلة أن دوائر استخباراتية أوروبية قامت بإحباط هجوم إلكتروني شنّته مجموعة متسللين يُطلق عليها اسم «روكيت كيتين» يُعتقد أنها مرتبطة بالحرس الثوري الإيراني، واستهدفت شخصيات سياسية واقتصادية بارزة على مستوى العالم بينهم أمراء ومسؤولون سعوديون وقطريون[24]. وهناك خلاف، كما أشرنا سابقاً، حول إمكانية وصف عملية «ستوكس نت» عام 2010 (والمعروفة بأنها كانت موجّهة لتحجيم مشروع إيران النووي والتي أدّت إلى تخريب ما يقارب 1000 جهاز طرد مركزي نووي إيراني) على أنها اعتداء عسكري عدائي يتفق والوصف الوارد في المادة 51 [25].

إلّا أنه لا يفوتنا الإشارة إلى أن هذه معظم الهجمات السيبرانية، كما قدّمنا أعلاه، كانت ولا زالت، تُستخدم من دول ذات سيادة ضد دول أخرى ذات سيادة، فدولة الصين ذاتها كانت متّهمةً باستخدام قراصنة شبكة الإنترنت ضد دول أخرى كما هي الحال في عملية «كومنت كرو» التي اشتهرت بأنّها أدّت إلى النفاذ إلى

(22) انظر في دواعي التشويش الإلكتروني على المحطات الإذاعية:

التشويش–من–وراءه–ولماذا http://www.aljazeera.net/programs/infocus/2015/5/17/

(23) انظر الخبر على الموقع الالكتروني:

http://www.bbc.com/arabic/world-38344457
http://www.france24.com/ar

(24) كشفت شركة «تشيك بوينت تكنولوجيز» التي تُعنى بالأمن المعلوماتي عن أن المجموعة استهدفت تحديدًا أمراء وشخصيات بارزة في أوساط اقتصادية وحكومية سعودية، وصحفيين ووكالات أنباء وعلماء نوويين، فضلًا عن المؤسسات التعليمية وناشطي حقوق الإنسان. انظر صحيفة الشرق على الموقع الإلكتروني:

http://www.al-sharq.com/news/details/383883#.VkNnnl_XeJJ

(25) انظر: مدوّنة مبادئ تالين الإرشادية، المرجع 3 سابق الإشارة إليه، الصفحة 58.

شبكة الدفاع عن صناعات الولايات المتحدة الأمريكية[26]، والولايات المتحدة من ناحيتها أيضًا لديها قوة سيبرانية عالمية متطوّرة لا يقاربها فيها أي دولة أخرى، وهي متّهمة بشن هجمات سيبرانية. كما أن دولا أخرى، ككوريا الشمالية لديها أجهزة حكومية خاصّة للقيام بعمليات سيبرانية تم توجيهها ضد دول الجوار بالذات[27]. كما أن دولتي الهند والباكستان التي يظهر أنهما تقومان باستخدام مكثّف لهذا النوع من العمليات للكشف عن النواحي الاستخبارية لكل منهما ضد الأخرى؛ نظرًا لظروف الصراع القائم بينهما. أمّا في سوريا، فهناك قوّة عسكرية خاصة بهذا النوع من العمليات، ونُسب لها عمليات التشويش على اتصالات جماعات حقوق الإنسان المناهضة للرئيس الأسد، والتشويش على محطات إعلامية مثل: «شبكة الجزيرة»، والـ «بي بي سي»، وحقوقية مثل «هيومن رايتس ووتش»، وغيرها[28].

وتجدر الإشارة هنا إلى أنّه ربّما يخرج عن مفهوم الاعتداء السيبراني في هذه الدراسة الجريمة السيبرانية الاعتيادية التي تغطّيها اتفاقية مجلس أوروبا المتعلّقة بالجريمة السيبرانية (Convention on Cybercrime) في الحالات التي لا يتم فيها الاعتداء السيبراني على سيادة دولة أخرى بشكل مباشر، الأمر الذي يمكّنها من حق اللجوء إلى تدابير مضادّة ضد دولة أخرى كما سيأتي شرحه. هذا بالرغم

(26) انظر بهذا الخصوص:

D. E. Sanger, D. Barboza & N. Perlroth, Chinese Army Unit is Seen as Tied to Hacking Against U.S., N.Y. TIMES, Feb. 18, 2013,
http://www.nytimes.com/201319/02//technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html?pagewanted=all

انظر أيضًا: مايكل شميت، المرجع 4 سابق الإشارة إليه.

(27) M. Fisher, South Korea Under Cyber Attack: Is North Korea Secretly Awesome at Hacking?
http://www.washingtonpost.com/blogs/worldviews/wp/201320/03//south-korea-under-cyber-attack-is-north-korea-secretly-awesome-at-hacking/

(28) أنظر:

H. Tsukayama & P. Farhi, Syrian Hackers Claim Responsibility for Disrupting Twitter,
http://www.washingtonpost.com/lifestyle/style/syrian-hackers-claim-responsibility-for-hacking-twitter-new-york-times-web-site/201320500/27/08/f580-f5c-11e3-bdf6-e4fc677d94a1_story.html;

انظر أيضًا: مايكل شميت، المرجع 4 سابق الإشارة إليه.

من أنّ هذه الاتفاقية أوردت في المادة الخامسة منها أنّه: «تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الفعل التالي في قانونها الوطني، إذا ما ارتكب عمداً وبغير حق الإعاقة الخطيرة لعمل منظومة الكمبيوتر عن طريق إدخال أو إرسال أو إتلاف أو محو أو تغيير أو تبديل أو تدمير بيانات الكمبيوتر»، وعليه، يكون للحديث عن تسريب معلومات سرية، ذات طابع دبلوماسي وأمني وسياسي وغيره، إلى موقع «ويكيليكس» الإلكتروني ونشرها من قبل هذا الأخير شأن آخر يخرج عن مدار هذه الدراسة، إذ إن ما نشر على هذا الموقع يمثّل بوجهة نظرنا جريمة على المستويات الوطنيّة باعتبارها أداة تعمل على تشويه المجتمع البشري، والذي لا بد منه في هذه الحالة هو أن يقوم المجتمع الدولي ومؤسساته الدولية، وعلى رأسها الأمم المتحدة ومنظماتها ومحاكمها، بتشكيل لجان من هيئات دولية ومنظمات حقوقية وقانونية دولية، لمحاكمة مرتكبي تلك الخروقات التي تمثل صورة لجريمة عابرة للحدود. إن فحوى التسريب ما كان يشكّل اعتداءً على دولة ذات سيادة بطريقة تخدم مصالح المعتدي، وترقى لأن تكون شكلاً من أشكال الهجوم السيبراني أو الحرب السيبرانية.

المطلب الثاني
التعريف بالتدابير المضادّة ومدى شرعيتها

تتضمّن مبادئ القانون الدولي العرفي لمسؤولية الدول ـ كما أشير إليها في مشروع المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دوليًا لعام 2002[29] ـ ما يبرّر تلك الأفعال غير المشروعة بصفة استثنائية باعتبار اتخاذها من قبيل التدابير المضادة[30]. ويعد استخدام التدابير المضادة كتدابير قسرية يُلجأ لها حصرًا عندما تتسبب دولة بضرر في حق دولة أخرى، وتستخدمها الدولة المتضررة من أجل حث تلك الأخيرة على احترام التزاماتها ولوقف السلوك غير المشروع دوليًا [31]، بل ويمكن لأي دولة كانت أن تتخذ تلك التدابير القانونية ضد دولة تقوم بانتهاكات من نوع خاص، كانتهاكات حقوق الإنسان أو الالتزامات

(29) المرجع 3 سابق الإشارة إليه.
(30) المرجع ذاته، المادة 22 بشأن التدابير المضادة المتعلقة بالأفعال غير المشروعة دوليًا.
(31) المرجع ذاته، المادة 49 بشأن موضوع التدابير المضادة وقيودها.

تجاه المجتمع الدولي بأكمله (الالتزامات في مواجهة الكافة)، وذلك ضمانًا لوقف الخرق وجبرًا تناله الدولة المتضررة أو المستفيدون من الالتزام الذي خُرق[32].

ومن المعروف أن عبارة «التدابير المضادّة» صعبة التعريف إذا ما جاءت كتدابير قسرية انفرادية، إذ إنّها غالبًا ما تعني اتخاذ تدابير اقتصادية من قبل دولة لحمل دولة أخرى على تغيير سياستها،[33] كالجزاء التجاري الذي يُفرض في شكل حظر و/أو مقاطعة، أو وقف للتدفقات المالية أو الاستثمارية للدولة المستهدفة، وفي بعض الحالات رفض وارداتها[34]، بل وكثيرًا ما يُشار أيضًا إلى الجمع بين القيود المفروضة على الواردات والصادرات كحظر تجاري[35].

وكما هو معروف، تتحمّل الدول عمومًا المسؤولية الناتجة عن تصرفاتها غير المشروعة على أساس القانون الدولي للمسؤولية الدولية وما تضمّنه مشروع المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دوليًا لعام 2002، وكما أقرته مجمل الأحكام ذات العلاقة الصادرة عن محكمة العدل الدولية، خصوصًا في قضيتي قناة كورفو لعام 1949 وقضية نيكاراجوا لعام 1986[36]، هاتان القضيتان –وغيرهما الكثير–[37] كانت ولا زالت ركائز صياغة مشروع المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دوليًا الآنف ذكرها، والتي بدورها شملت الأعمال السيبرانية بالقواعد الخاصّة بمسؤولية الدول[38].

(32) المرجع ذاته، المادة 54 بشأن التدابير المتخذة من جانب دول خلاف الدولة المضرورة.

(33) انظر:

A. F. Lowenfeld, International Economic Law (Oxford, Oxford University Press, (2002) p. 698.

(34) M. P. Doxey, International Sanctions in Contemporary Perspective (Basingstoke, Palgrave Macmillan, 1996)

(35) انظر: مايكل شميت، المرجع 4 سابق الإشارة إليه، وأيضًا:

C. C Joyner, "Boycott", Max Planck Encyclopedia of Public International Law (Oxford University Press, 2011), available from www.mpepil.com.

(36) انظر: قضية كورفو، ألبانيا وبريطانيا (1949 I.C.J 4، 23)، وقضية نيكارجوا، المرجع 1 سابق الإشارة إليه، 292.

(37) انظر: قضية مشروع غابتشيكوفو– ناغيماروس بين هنجاريا وسلوفاكيا:

Gabcikovo-Nagymaros Project (Hungary/Slovakia), ICJ 97, Judgment of 25 September 1997.

وقد توصلت محكمة العدل الدولية الدائمة إلى ذات النتيجة في قضية فوسفات المغرب (Preliminary Objections, 1938 P.C.I.J., ser. A/B, No. 74)، الصفحات 10 و 28؛ وأيضًا في قضية ويمبلدون بين بريطانيا وفرنسا (P.C.I.J, ser. A, No. 1 1923)، الصفحات 15و 30: وأيضًا في قضية مصنع شورزو بين ألمانيا وبولندا (1927 P.C.I.J, ser. A, No. 9)، الصفحات 3، 29 و 30.

(38) المبدأ رقم 6 من مبادئ تالين الإرشادية الخاصّة بالقانون الدولي المستخدمة في الحروب السيبرانية، المرجع رقم 3 سابق الإشارة إليه.

وبالرغم من أن مشروع المواد المتعلّقة بمسؤولية الدول عن الأعمال غير المشروعة دوليًا لا تعد من قبيل الاتفاقية الدولية بالمعنى المعروف (باعتبار أنها لا تُعدُّ من الاتفاقيات الملزمة كما تقرر في ذلك قواعد اتفاقية فيينا لقانون المعاهدات)، إلّا أنها تتمتّع بصفة القواعد القانونية ذات القوّة الملزمة باعتبار أنّ اللجنة الدولية للقانون الدولي قامت بتطوير هذه القواعد على مرّ عقود طويلة تجاوزت الخمسة، وتناوب أكثر من خمسة مقررين خاصّين بهذا المشروع عليها، ثمّ قيام الجمعيّة العمومية للأمم المتحدة بالتوصية بنفاذ بنودها، بل إنه يمكن القول بأن كثيرًا من قواعد هذا المشروع تعكس مضمونًا لقواعد عرفيّة ملزمة، ومن المؤشرات على ذلك التكرار الهائل في استخدام المحاكم الدولية لهذا المشروع في استصدارها لقراراتها والتي تجاوزت المائة والخمسين مرّة.[39] لذلك، يمكن الاستنتاج بأن قواعد القانون الدولي الخاصّة بالمسؤولية الدولية تأتي من قبيل القواعد الفاعلة التي يمكن أن يكون لها تطبيق مباشر على أفعال الدول غير المشروعة، ومنها قيامها بعمل غير مشروع على شكل نشاط سيبراني.

وينطوي تحت هذه القواعد بندٌ خاصٌّ بالتدابير المضادة التي يُمكن اللجوء إليها، فهذه التدابير لا تجوز في الأحوال العاديّة على أساس أن الفعل الذي يعبّر عنها يكون عادة مخالفًا لقواعد القانون الدولي، وهي بالتالي لا تعدو عن كونها تمكين لدولة متضررة من القيام بسلوك، أو الانتهاء عن القيام بسلوك، في وجه دولة أخرى متسببة بالضرر، ومن قبيل التدابير المضادة، بغية إرغام تلك الأخيرة على الرضوخ والعدول عن مخالفتها لالتزاماتها الدولية. إن هذه التدابير يُلجأ لها كوسيلة ضاغطة في غياب جبرية التقاضي الدولي أو إيقاع العقوبات الرادعة، والأصل هو منع مثل تلك التدابير في الأحوال الاعتيادية، إلّا أنّ المتمعّن بأحكام القضاء الدولي يجد بأن هناك جملة من القرارات القضائية الدولية التي سمحت ببعض التدابير المضادّة بسبب ما ينتج عنها من إيجابيات قد لا يدركه اللجوء للقضاء[40].

(39) انظر:

U.N. Doc. ST/LEG/SER.B/25 (2012)

(40) انظر: تحديدًا قضية مشروع غابتشيكوفو– ناغيماروس، مرجع سابق الإشارة إليه، الصفحات 82 و 83، وأيضًا: قضية نيكارجوا، مرجع سابق الإشارة إليه، صفحة 249.

وتؤكّد القرارات القضائية، وممارسات الدول، والنظريات الفقهية، مشروعية التدابير المضادة التي تستوفي شروطًا معينة من حيث المضمون والشكل، فالتدابير المضادة تُعد من الظروف النافية لعدم المشروعية سواء انطوى عليها إخلال بالتزام ناشئ بموجب قاعدة من قواعد القانون الدولي العام، أو بموجب معاهدة، أم بموجب صك أحادي الطرف، أو أي مصدر آخر، ما لم يُنص على خلاف ذلك، وهي لا تنهي الالتزام أو تلغيه، وإنّما تبرّر عدم الوفاء به ما دام ظرف استخدامها قائمًا. وقد سلّمت محكمة العدل الدولية في قضية "مشروع غابتشيكوفو- ناغيماروس» بأنه يمكن للتدابير المضادة أن تبرر تصرفًا، وإن كان تصرفًا غير مشروع، في حال تم القيام به «ردًا على فعل غير مشروع دوليًا قامت به دولة أخرى وكان موجهًا ضد تلك الدولة»[41]، شريطة استيفاء شروط معينة. ففي هذه القضية، نفت هنجاريا صفة عدم مشروعية توقفها عن العمل في مشروع السد المتنازع حوله مع تشيكوسلوفاكيا بموجب المعاهدة على أساس أنها أضرت بها، وكان رد المحكمة على هذا الدفع بأن «حالة الضرورة... تسمح بتأكيد أن هنجاريا... لن تتحمّل مسؤولية دولية لتصرفها»[42]، وورد في قرارات التحكيم في قضية «ناوليلا»[43] و«الاتفاق بشأن الخدمات الجوية»[44] ما يماثل هذا الاعتراف بشرعية التدابير المضادّة في حالات معينة.

المطلب الثالث
التفرقة بين التدابير المضادّة وغيرها من الإجراءات الدولية المشابهة لها

كان مصطلح «الانتقام» هو الشائع في وصف أي تدبير مضاد في النصف الأول من القرن الماضي. ومع أن المقصود بهذا المصطلح لم يتغيّر، باعتبار أن الدول تبحث

(41) انظر: القضية، المرجع السابق، الصفحة 55، الفقرة 83.

(42) انظر: المرجع السابق، ص 39، الفقرة 48.

(43) قضية مستعمرات البرتغال، حادثة نوليلا (UNRIAA, vol. II, 1928)، الصفحة 11.

(44) القضية الخاصّة باتفاقية الخدمات الجويّة 27 مارس 1946 بين الولايات المتحدة الأمريكية وفرنسا، قرار تاريخ 9 ديسمبر 1978 (UNRIAA, vol. XVIII - Sales No. E/F.80.V.7)، صفحة 415.

عن وسائل مختلفة لحفظ سيادتها في الظروف التي تهدد مصالحها، إلّا أن مصطلح الانتقام غدا من التاريخ القديم في وقتنا الحاضر، باعتبار أنّه من المفاهيم التي توسّع من أسباب استخدام القوة[45]، فلا سبيل اليوم لاستخدام القوّة المشروعة إلّا ضد من استخدم القوة العسكرية كما جاء به ميثاق الأمم المتحدة، وفي إطار المواد 2(4)، 39، 42، 51 التي باتت الآن من الأعراف الدولية الراسخة[46].

والحقيقة أنّه تمت الدلالة على التدابير المضادة من الناحية التاريخية عن طريق استخدام مصطلح «الأعمال الثأرية المشروعة» أو «الحماية الذاتية» أو «المساعدة الذاتية»، كما استخدم مصطلح «الجزاءات» للدلالة على التدابير التي تتخذ طبقًا للصك التأسيسي لبعض المنظمات الدولية، ولا سيما بموجب الفصل السابع من ميثاق الأمم المتحدة. أمّا في وقتنا الحاضر، وعلى الأقل منذ صدور قرار التحكيم في قضية الاتفاق بشأن الخدمات الجوية، فلم يعد تعبير «الأعمال الثأرية» مستخدمًا، وقد استبدل به مسمى «التدابير المضادة»، لذلك، وجب هنا التنويه إلى عدم الخلط بين التدابير المضادّة و «الأعمال الانتقامية الحربية» التي تكون خلال نزاع مسلح ومشكّلة بذاتها انتهاكًا للقانون الدولي الإنساني، وإن جاءت على شكل رد على سلوك عسكري غير قانوني من العدو[47].

كما أنه تجب التفرقة بين التدابير المضادّة و«الأعمال غير الصديقة» التي لا يشترط بها أن تكون تصرفات غير مشروعة ولا تنتمي أساسًا إلى مجموعة التصرفات غير المشروعة،[48] ومثال ذلك، كما هو مذكور في المبدأ الثاني من مبادئ تالين، قيام الدولة باعتراض موجات سيبرانية خارجية باعتبار أنها تتمتّع بسلطة

(45) انظر بهذا الخصوص:

M. Ruffert, Reprisals, 8 Max Planck Encyclopedia of International Law, 927 (2012);

(46) انظر: المؤشرات لذلك في التعليق على ميثاق الأمم المتحدة (Bruno Simma et al. eds., 3d ed. 2013)، الصفحات 200 – 213؛ وانظر: عمومًا مايكل شميت في التفرقة بين التدابير المضادّة وغيرها من الإجراءات الدولية المشابهة لها، المرجع 4 سابق الإشارة إليه.

(47) انظر في ذلك، وفي القانون الدولي الإنساني عمومًا:

F. Kalshoven, Belligerent Reprisals, 1971.

(48) انظر:

T. G. Retorsion, 8 Max Planck Encyclopedia of International Law, 976 (2012).

على المنشآت السيبرانية الموجودة على إقليمها[49]، فهذا التصرف هو تصرف قانوني، حتى وإن جاء معكرًا لمصالح الدولة التي انبعثت من أراضيها الموجات السيبرانية، طالما أنه لم يخالف اتفاقًا واضحًا مبرمًا بين الدولتين أو جاء مناقضًا لعرف دولي، بل إن إنهاء الاتفاق ذاته بشكل منفرد ـ وإن كان جائزًا بموجب الاتفاق ـ لا يُعد بذاته من قبيل التدابير المضادّة[50].

وكما تختلف التدابير المضادة أيضًا عن «الرد بالمثل»، أي التصرف غير الودي الذي لا يتلاءم مع أي التزام دولي للدولة التي تقوم به حتى لو كان ردًا على فعل غير مشروع دوليًا. وتشمل أفعال الرد بالمثل حظرَ العلاقات الدبلوماسية العادية أو غيرها من الاتصالات أو فرض قيود عليها، أو سحب برامج المعونة الطوعية. ومهما تكن دوافع مثل هذه الأفعال ـ ما دامت غير متعارضة مع الالتزامات الدولية للدول التي تقوم بها تجاه الدولة المستهدفة ـ فإنّها لا تنطوي على تدابير مضادة ولا تدخل ضمن نطاقها.

لا يعد من قبيل التدابير المضادّة أيضًا العقوبات التي يفرضها مجلس الأمن بالاستناد إلى الفصل السابع من ميثاق الأمم المتّحدة؛ والسبب في ذلك أن العقوبات التي يقررها مجلس الأمن طبقًا لهذا الفصل تكون مشروعة بحسب ميثاق الأمم المتحدة ذاته، والمجلس هو صاحب اختصاص في استصداره لهذه العقوبات، وبالتالي تُعد جميع الأعمال التي تصب في تحقق الغاية من هذه العقوبات من قبيل الأعمال المشروعة طالما انضبطت بقواعد القانون الدولي الإنساني. وعليه، يكون اعتراض الاتصالات ـ بموجب قرار من مجلس الأمن، واستنادًا على المادة 41 من الميثاق ـ مشروعًا لمن يقوم بتنفيذه، ولا يمكن وصف أعمال تحطيم وهدم البنية التحتيّة الخاصة بالشبكة العنكبوتية لدولة صدر بحقها مثل هذا القرار بالإجراءات المضادّة، وذلك باعتبار أنها أعمال مشروعة بموجب القرار الذي تم التوصل إليه.

(49) انظر: مبادئ تالين، المرجع 5 سابق الإشارة إليه؛ أيضًا: مايكل شميت، المرجع 4 سابق الإشارة إليه.
(50) انظر: بذلك المادة 42 من اتفاقية فينا لقانون المعاهدات (U.N.T.S. 331 1155 ,1969).

وأخيرًا، لا بد لنا من تمييز التدابير المضادّة عن الأعمال التي يُلجأ إليها بحجة الضرورة، ففي الحالات التي لا يمكن فيها درء خطر داهم على مصلحة دولية أساسية، فإن اللجوء إلى الأعمال المضادّة (سواء اتخذت شكل عمل سيبراني أو غير سيبراني) يصبح مشروعًا بحكم تلك الضرورة، طالما أن تلك الأعمال اتخذت في حدود دفع ذلك البلاء، أو المحافظة على تلك المصلحة الدولية الأساسية[51] أو كليهما معًا، وهنا لا بد من التنبيه إلى أن الأعمال التي تعتمد أساس الضرورة لها تختلف عن التدابير المضادّة في أوجه ثلاثة[52]، وهي:

أولًا: يشترط وجود عمل دولي غير مشروع لتسبيب اللجوء إلى أعمال الضرورة؛ بينما لا يُشترط ذلك للّجوء إلى التدابير المضادّة.

ثانيًا: لا يُشترط للّجوء لأعمال الضرورة أن يكون مصدر الخطر داهم أو مسبّبه ناشئًا عن تصرّفات صادرة عن دولة، أو حتى تحديد الجهة المسؤولة عنه (وهذا ما يهمّنا في هذه الدراسة المتعلّقة بالتصرفات التي تصدر عن مشغّلات سيبرانية لا تكون تابعة للدولة دائمًا)؛ بينما يُشترط ذلك إذا ما أرادت الدولة الدفع باللجوء إلى التدابير المضادّة كسبب لتصرّفها.

ثالثًا: لا يتم اللجوء لأعمال الضرورة إلّا في الحالات الاضطرارية الملحّة، وعوضًا عن ذلك يُتاح للدولة اللجوء للتدابير المضادّة للتصدّي للتصرفات الخارجية غير القانونية ولكن الأقل إلحاحًا. ولا نغفل أنّه في إطار الأعمال السيبرانية المعادية، يمكننا قبول أن يكون الرد مستندًا لمبدأ الضرورة في مواجهة التصرفات التي تُهدد البنية السيبرانية للدولة التي يقع عليها اعتداءً سيبراني خارجي.

51) انظر: في ذلك فتوى محكمة العدل الدولية في قضية حائط الفصل العنصري (I.C.J. 136, 140, 2004).

52) انظر: مايكل شميت، المرجع 4 سابق الإشارة إليه؛ وأيضًا: مبادئ تالين، المرجع 3 سابق الإشارة إليه، ولمزيد من التوضيح:

J. Crawford, The International Law Commission's Articles on State Responsibility: Introduction, Text and Commentaries, 178–86 (2002).

المبحث الثاني
الشروط السابقة لحق اللجوء إلى التدابير المضادّة

يظهر مما سبق أنه لا يمكن اللجوء للتدابير المضادّة إلّا في مواجهة تصرف دولي خارجي غير قانوني، ويجب في هذه التصرفات غير القانونية أن يتوفر فيها شرطان أساسان: أولًا، خرق لالتزام دولي في حق دولة أخرى، وثانيًا، وجود رابطة واضحة بين التصرف غير القانوني والدولة التي يُزعم بأنه نشأ عنها،[53] وهي الشروط ذاتها الخاصّة بنشوء المسؤولية الدولية بين دولة مسؤولة عن الضرر ودولة أخرى هي متضررة. ولذلك، يتولّد بتوافر هذين الشرطين حق عام للدولة المتضررة للجوء إلى تدابير احترازية مضادّة تفرضها طبيعة الاعتداء أيّا كان شكله. فعلى سبيل المثال، قامت القوّات المسلّحة الأمريكية بعمليّة مضادّة في عام 1998 ضد قراصنة الكمبيوتر المعروفين باسم «مسرح الاضطراب الإلكتروني» الذين قاموا بتهديد البنتاغون إلكترونيًا باعتراض وإجهاض الخدمة الإلكترونية فيه54. ولتصنيف هذه العملية بأنها من قبيل التدابير المضادّة المشروعة، كان لا بد أولًا من إثبات أنه كان هناك اعتداء مخالف لقواعد القانون الدولي من قبل من قاموا بالقرصنة وربط تصرُّفاتهم تلك بدولة أخرى. من هنا؛ ونظرًا لأهمية هذين الشرطين فإننا سنتعرّض لهما في مطلبين، نعالج في المطلب الأول وجود مخالفة لالتزام دولي إزاء دولة أخرى، وندرس في المطلب الثاني مسألة إسناد العمل غير المشروع للدولة في الجرائم السيبرانية على وجه الخصوص.

المطلب الأول
وجود مخالفة لالتزام دولي في حق دولة أخرى

يترتّب على عدم احترام الالتزامات الدولية من قبل أي دولة حقٌّ للدولة، أو الدول المتضررة بالتعويض عن الضرر الناتج عن الفعل غير المشروع، أساسه

(53) انظر: المادة 2 من مشروع مواد المسؤولية الدولية للدول الناجمة عن أعمال غير مشروعة، المرجع 3 سابق الإشارة إليه.

54) W. Schwartau, Striking Back, Network World Fusion: http://www.networkworld.com/news/0111vigilante.html

القواعد الخاصّة بمسؤولية الدولة المتسببة بالضرر[55]، وينجم عن هذا الحق القدرة على المطالبة بالكف عن العمل الضار أو وقف الاستمرار به، والتعويضان المادّي والمعنوي، أو حتى إعادة الحال لما كان عليه الوضع قبل الانتهاك إن كان ذلك ممكنًا[56].

ومن المعروف أن المخالفة تأتي إمّا على صورة مخالفة صريحة لاتفاقية أو على صورة مخالفة لعرف دولي مستقر، فعلى سبيل المثال، الدولة التي تقوم بأعمال سيبرانية معادية من على سفينة لها من داخل مياه إقليمية لدولة أخرى، وموجّهة ضد تلك الدولة، تكون بهذا العمل قد خرقت ليس فقط مبدأ «حق المرور البريء» المنصوص عليه في اتفاقية الأمم المتحدة لقانون البحار لعام 1982[57]، وإنّما أيضًا تكون قد خرقت الأعراف الدولية المستقرّة بهذا الشأن[58]. وبذات الطريقة، فإنّ قيام طائرة ملاحية لدولة ما بأعمال سيبرانية غير متّفق عليها خلال مرورها بأجواء دولة أخرى يُعد من قبيل المخالفة للأعراف الدولية[59].

ومن المعروف أيضًا أن من بين أهم المبادئ العرفية المستقرّة مبدأ سيادة الدولة

(55) المادة 2 من مشروع مواد المسؤولية الدولية للدول الناجمة عن أعمال غير مشروعة، المرجع 3 سابق الإشارة إليه، وانظر أيضًا: كروفورد، المرجع 38 سابق الإشارة إليه، على الصفحة 81. وأيضًا: قضية فوسفات المغرب، المرجع سابق الإشارة إليه، على الصفحة 48 منه؛ وأيضًا: قضية الدبلوماسيين الأمريكيين في طهران (1980 3 .I.C.J).

(56) وتعتبر المسؤولية الدولية من أهم الأسس التي يقوم عليها القانون الدولي العام، حيث إنها بمثابة محرّك الجزاء ضد الدولة التي تخالف التزاماتها التي يفرضها هذا القانون. هذه الحقيقة تؤكدها العديد من القرارات الدولية منها القرار الذي أصدرته محكمة العدل الدولية الدائمة بتاريخ 25/03/1926 بشأن مصنع شورزو والمتعلّق بتملّك بولونيا لمصنع ألماني دون دفع تعويض لألمانيا بمخالفة صريحة للاتفاقية المعقودة بينهما سنة 1922، وحيث رفع النزاع أمام المحكمة التي قررت أنه: «... من المبادئ المقبولة في القانون الدولي أن أي خرق للالتزامات الدولية سيتوجب تعويضا مناسبا ...». انظر تحليلًا في ذلك: د. السيد أبو عطية، الجزاءات الدولية بين النظرية والتطبيق، مؤسسة الثقافة الجامعية، الإسكندرية 2001.

(57) انظر: المواد 17 و 19 من اتفاقية الأمم المتحدة للبحار لعام 1982 (1833 397 .U.N.T.S) والتي دخلت حيّز النفاذ عام 1994.

(58) بالرغم من أن الولايات المتّحدة الأمريكية ليست عضوًا في اتفاقية الأمم المتحدة لقانون البحار لعام 1982 إلّا أنها تعترف بوجود عرف دولي يجعل من حق المرور البريء لازمة دولية كأحد أعراف القانون الدولي. انظر: في هذا «مدوّنة القادة» الأمريكية:

U.S. NAVY/U.S. MARINE CORPS/U.S. COAST GUARD, THE COMMANDER'S HANDBOOK ON THE LAW OF NAVAL OPERATIONS, NWP 114-M/MCWP 512.1-/COMDTPUB P5800.7A, 2.5.2.1 (July 2007).

(59) اتفاقية الملاحة الجويّة الدولية لعام 1944 (15 295 .U.N.T.S).

على إقليمها، حيث جاء في حكم التحكيم الدولي في قضية جزيرة بالماس أن: «... من مظاهر استقلال الدولة تمتّعها بصلاحيات ومهام الدولة ـ دون غيرها ـ على كافة إقليمها»[60]، فهذا يعني بهذا المقام إن الدولة لها ـ دون غيرها ـ أن تنظّم فضاءها السيبراني دون مؤثرات خارجية[61]، وعليه، فإن من نتائج مبدأ السيادة الإقليمية أن يكون للدولة الحق في حماية أراضيها وما فيها من بنية تحتيّة سواء أكانت مملوكة للدولة ذاتها (حكوميّة) أم كانت ملكيات خاصة لمواطنيها. وكنتيجة لذلك، يصنّف أي اعتداء سيبراني خارجي ضار على هذه البنية التحتية ـ سواء أكانت ذات ملكيّة عامّة أم ملكيّة خاصّة ـ بأنه اعتداء على سيادة الدولة ذاتها[62]، ما لم يكن الفعل الذي أقدمت عليه الدولة نتيجة لاستخدامها الطبيعي لحق الدفاع عن النفس، أو بسبب لجوئها لاتخاذ تدابير مضادّة كما سنبيّن ذلك لاحقًا.

ولا بد من الإشارة هنا أن بعض فقهاء القانون الدولي لا يشترطون تحقق وقوع الضرر في كل الحالات لقيام المسؤولية الدوليّة، كما هي الحال في حالة زرع برمجيات لمراقبة النشاطات الإلكترونية في دولة أخرى[63]، وهذا الطرح مبني على المقصود من الحق في «السيادة الإقليمية» والذي يعني قدرة الدولة صاحبة الحق ـ لا غيرها ـ على القيام بالنشاطات التي تراها مناسبة على إقليمها بما يحقق مصالحها دون تدخّل من دولة أخرى. ولذلك، يرفض أصحاب هذا الرأي القول بأن زرع برمجيات لمراقبة أنشطة الدولة من قبل دولة أخرى يُعد فقط من قبيل «أعمال التجسس»، فأعمال التجسس عندهم يمنعها القانون الدولي، وذلك لأنّ التجسّس إن احتوى على زرع برمجيات يؤدي حتمًا إلى تدمير منظومة حفظ المعلومات السرّية للدولة التي يتم التجسّس عليها، بل ويؤدي حتمًا إلى اختراق السيادة الإقليمية بدرجة كبيرة، وإلى إضعاف منظومة السيادة الإقليمية للدول بشكل ليس له مثيل.

وعليه، تعد أعمال القرصنة الإيرانية على شركات النفط الأمريكية، ومحاولتها الحصول على معلومات قد تؤثر في صنع القرار الأمريكي حول الطاقة النفطية، انتهاكا

(60) انظر: قضية جزيرة بالماس بين هولندا والولايات المتحدة الأمريكية (R.I.A.A. 829, 838 - Perm. Ct. Arb. 1928.2).

(61) انظر: الصفحات 15 و 16 من كراسة مبادئ تالين، المرجع 5 سابق الإشارة إليه؛ أيضًا: مايكل شميت، المرجع 4 سابق الإشارة إليه.

(62) انظر: الصفحة 16 من مدوّنة مبادئ تالين، المرجع السابق.

(63) المرجع السابق.

لسيادة الولايات المتّحدة الأمريكية على إقليمها حتّى وإن لم يثبت تحقق الضرر[64]، وبذات الطريقة، تكون إيران مسؤولة دوليًا ـ إذا ثبت تورّطها ـ بإطلاق فيروس «شامون» الإلكتروني وتعطيل ذاكرة آلاف محركات الأقراص الصلبة في أجهزة شركة «أرامكو» السعوديّة عام 2012، وإن لم تتعطّل تلك الأقراص بذاتها[65].

والحقيقة أنه لا بد لنا من التنبُّه إلى أن الأعمال التي تقوم بها دولة وتشكّل تدخلًا في شؤون دولة أخرى تأتي عمومًا على نمطين: فهي إمّا أن يكون الهدف منها «إجبار» الدولة المعتدى عليها على التصرف على نحو ما، أو أن يكون الهدف منها فقط «التأثير» على تلك الدولة لأن تنحى نحوًا سياسيًا معيّنًا. ولا يخفى أنه عندما تأخذ تلك الأعمال شكل التدخل السيبراني فإنها عادة ما تكون على النمط الجبري وليس لمجرد إحداث أثر في الموقف السياسي، وهنا، لنا أن نتصوّر كم أنّه من الصعب اشتراط ثبوت «تحقق الضرر» وأنّه بذلك يفترض ألّا يكون شرطًا في تحقق المسؤولية الدولية[66]. وهذا ما وضّحه قرار محكمة العدل الدولية في قضية نيكاراجوا، والذي جاء فيه بأن: «مبدأ السيادة الإقليمية يمنع جميع الدول من التدخّل المباشر أو غير المباشر في الشؤون الداخلية والخارجيّة لدولة أخرى»[67]، ففي هذه القضية، أشارت المحكمة إلى أنه بالرغم من أن قيام دولة بتزويد مقاتلي المليشيات في دولة أخرى بأموال لا ينطبق عليه وصف استخدام القوة بمفهومه اللغوي الوارد بنص المادة 2(4) من ميثاق الأمم المتّحدة، إلّا أن مثل هذه الأعمال غير مشروعة باعتبار أنها تمثّل تدخلًا غير مشروعٍ في شؤون دولة أخرى[68].

ولا بد في هذا السياق من الإشارة إلى أن القانون الدولي يفرض قيودًا على تمتّع الدولة بخصائص سيادتها الإقليمية بأن فرض عليها حسن تدبير شؤونها الداخلية

(64) انظر بهذا الرأي: مايكل شميت، المرجع 4 سابق الإشارة إليه، وأيضًا:

S. Gorman & D. Yadron, Iran Hacks Energy Firms, U.S. Says, WALL ST. J.: http://online.wsj.com/news/articles/SB10001424127887323336104578501601108021968

(65) انظر بهذا الرأي أيضًا: مايكل شميت، المرجع 4 سابق الإشارة إليه، وأيضًا:

C. Bronk & E. Tikk-Rigas, The Cyber Attack on Saudi Aramco, SURVIVAL, Apr–May 2013. P. 81.

(66) انظر: كراسة مبادئ تالين على الصفحات 43 – 45، المرجع 3 السابق الإشارة إليه.

(67) انظر: قضية نيكاراجوا، المرجع 3 سابق الإشارة إليه، 292، وأيضًا: قضية كورفو، ألبانيا وبريطانيا، (1949 I.C.J. 4, 23).

(68) «يمتنع أعضاء الهيئة جميعًا في علاقاتهم الدولية عن التهديد باستعمال القوة أو استخدامها ضد سلامة الأراضي أو الاستقلال السياسي لأية دولة أو على أي وجه آخر لا يتفق ومقاصد الأمم المتحدة». قضية نيكاراجوا، المرجع السابق، الصفحة 228.

بما لا يحدث ضررًا على سيادة الدول الأخرى، ومن هذا المنطلق، تكون الدولة مطالبة بالسيطرة على ما يحدث داخل إقليمها كما أقرّت بذلك محكمة العدل الدولية في قضية قناة كورفو والتي جاء في حكمها بأنه: «لا يكون للدولة أن تسمح، وبعلمها، استخدام أراضيها للقيام بأعمال مخالفة لحقوق الدول الأخرى»[69]. وتأسيسًا على ذلك، أقرّت مجموعة الخبراء الدوليين في صياغتهم لمبادئ تالين عام 2013 أنه: «على الدول عدم السماح باستخدام أراضيها للقيام بأعمال سيبرانية تسبب ضررًا لدولة أخرى إذا علمت بهذه الأنشطة»[70]، وأنّه عليها أن تقوم «بكل ما لديها من جهد» لتحقيق هذا الالتزام[71] باعتبار أن المتسبب بالضرر في مثل هذه الحالات عادة ما يكون جهات غير حكوميّة (أو ما يطلق عليهم مسمى قراصنة الإنترنت).

أمّا الدفوع التي يمكن استخدامها من قبل الدولة التي ثبت أنها كانت حاضنة لنشاط سيبراني معادي فهي نفس تلك الخاصّة بالأحكام العامّة المتعلّقة بموانع المسؤولية الدولية، فلا تقع المسؤولية في الحالة التي يثبت فيها وجود مسبق لرضا الدولة المتضررة من النشاطات السيبرانية، كما لا تقع المسؤولية في استخدام هذا النوع من النشاطات في سياق الدفاع عن النفس، أو عندما يسمح استخدامها بقرار من مجلس الأمن، وبالإضافة إلى ذلك، فإن القوّة القاهرة والضرورة تعتبران أسبابًا لعدم المسؤولية عن النشاط السيبراني الذي يتسبب بضرر لدولة أخرى[72]. وهنا، لا بد من الإشارة إلى أن مبادئ تالين أقرّت بأن للدولة المتضررة في هذا السياق أن تلجأ إلى التدابير المضادّة والتي قد تكون على شكل رد فعل سيبراني ضد الدولة التي ابتدأت النشاط السيبراني المُعادي، وفي هذه الحالة، لا يكون رد الفعل هذا عملاً غير مشروع طالما أنه اتسم بالتناسبية مع النشاط المتسبب أصلًا بالضرر[73].

---

(69) انظر: قرار محكمة العدل الدولية في قضية قناة كورفو، (Corfu Channel, 1949, I.C.J)، الصفحة 22، وكذلك قضية الدبلوماسيين الأمريكيين في طهران (USA Diplomatic Consular Staff in Tehran, 1980. I.C.J) صفحة 67–68.

(70) انظر: المبدأ 5 في كراسة مبادئ تالين، المرجع 3 سابق الإشارة إليه.

(71) انظر: التعليق على مبادئ تالين، المرجع 38 سابق الإشارة إليه، صفحة 140.

(72) انظر: نص المواد 20 و 21 من مشروع المسؤولية الدولية للدول الناجمة عن أعمال غير مشروعة، المرجع 3 سابق الإشارة إليه؛ وانظر أيضًا: المواد 42 و 51 من ميثاق الأمم المتّحدة، سابق الإشارة إليه.

(73) انظر: المبدأ 9 من كراسة مبادئ تالين، المرجع 3 سابق الإشارة إليه.

المطلب الثاني

إسناد العمل غير المشروع للدولة

انطلاقًا من مفهوم الإسناد، تؤكد النظرية التقليدية أن الشخص الدولي، متمثلًا بالدولة، هو وحده الذي يمكن أن يتحمل المسؤولية الدولية سواء بصورة مباشرة أم غير مباشرة، وسواء جاء الفعل غير المشروع بصورة قيام بعمل أم امتناع عن القيام بعمل، ذلك لأن هذه النظرية تفترض بأن الشخص الدولي هو وحده الذي يتحمل مسؤولية التعويض عن الضرر الناجم عن هذا الفعل. ويعني مفهوم «الإسناد» أن ينسب فعل معين ارتكبه شخص ما أو مجموعة من الأشخاص الطبيعيين إلى دولة ما، أو إلى شخص دولي، لأجل أن تثبت المسؤولية الدولية، ويعتبر الفعل أو النشاط غير القانوني وكأنه صادر عن الدولة ذاتها، أو ذلك الشخص الدولي ذاته، وبالتالي تنتج مسؤولية الدولة ذاتها عن ذاك النشاط.

وتنشأ المسؤولية الدولية المباشرة عن الأفعال المنسوبة إلى الدولة بأن تكون صادرة عن سلطاتها المختلفة، أي عن فرد أو هيئة يمنحها القانون الداخلي اختصاصًا، وبالتالي تُسأل الدولة عن الضرر الناجم عن هذه الأفعال. أما المسؤولية الدولية غير المباشرة للدولة فهي تنشأ عن أفعال صدرت عن أفراد عاديين يحملون جنسيتها أو عن أفراد من الأجانب يقيمون في إقليمها، وتلتزم الدولة في هذه الحالة بمعاقبة الفاعلين أو بإلزامهم بدفع التعويض إلى الأجنبي المتضرر. ولا تترتب على الدولة هذه المسؤولية غير المباشرة إلا إذا قصرت في الوفاء بهذا الالتزام؛ لأن تقصيرها في هذه الحالة يعتبر فعلًا غير مشروع.

ومن المسلّمات اتفاقًا أنّه لا يجوز اللجوء إلى التدابير المضادّة إلّا بتحقق شرط «الإسناد» بموجب قواعد المسؤولية الدولية[74]، لذلك ومن أجل أن نحدد نطاق السماح للّجوء إلى التدابير المضادّة، لا بد لنا من أن نفهم حدود مفهوم الإسناد في القانون الدولي. ويبدو الأمر واضحًا عندما تنشأ المسؤولية الدولية بقيام مسؤولين حكوميين من

(74) المادة (2/a) من مشروع المسؤولية الدولية، المرجع 3 سابق الإشارة إليه.

الدولة (كالعسكريين أو الاستخبارات) بأفعال مخالفة لقواعد القانون الدولي[75]، فعلى سبيل المثال، تعد جميع النشاطات الإلكترونية السيبرانية الصادرة عن وكالة الأمن القومي الأمريكية مسندة إلى الولايات المتحدة الأمريكية، وبالتالي تثار مسؤوليتها كدولة إزاء تلك النشاطات. فبموجب الأحكام العامّة في القانون الدولي، تعتبر الدولة مسؤولة عن القيام بالأعمال الصادرة عن موظفيها أو إداراتها العامة أو مؤسساتها العامة، أو عدم قيامهم بواجبهم، إذا نتج عن ذلك ضرر. وينطبق هذا بوجه خاص على كبار رجال الإدارة، أما فيما يتعلق بصغار الموظفين، فإن بعدهم النسبي عن سلطة الدولة غالبًا ما ينشئ مسؤولية الدولة غير المباشرة. ولا تترتب المسؤولية الحقيقية في هذه الحالة إلا إذا فشلت الدولة في إيقاع العقوبة على الموظف المذنب[76].

وهنا لا بد لنا من التذكير بأن نشاط الدولة قد يكون هو ذاته عرضة لسوء استخدام أحد الأفراد العاملين بالدولة سواء بقصد أم بدون قصد، وبدون أن يُسمح له بإتيان ذلك النشاط من الدولة أو حتى بدون علمها. ولربما يكون هناك من استطاع اختراق البنية التحتية السيبرانية لدولة ما وقام بتطويعها لمصلحته الخاصّة. وتتعقّد الأمور حتمًا إذا ما تدخلت الدولة بشكل سريع لإحباط هذا النوع من القرصنة؛ لأنها بذلك ـ أي الدولة ـ تخاطر بإمكانية الدفع بعدم إسناد العمل لها؛ لأنها ستبدو وكأنها هي التي ابتدأت النشاط المخالف للقانون. ولهذا السبب، جاء في المبدأ السابع من مدوّنة مبادئ تالين أنّه: «مجرّد إطلاق الفعل السيبراني عن أحد أجهزة الدولة أو صدوره عنه لا يُثبت علاقة الإسناد ... وإن كان يكفي للاعتقاد بوجود علاقة بين الدولة والنشاط ذاته»[77]، وبالتالي يتوجب على الدولة أن تتبيَّن مصدر هذا النشاط المُخادع، وأن تتولى بيان الأمر لمن تحقق الضرر بحقّه من الدول الأخرى؛ حتى تُزيل الشك من حولها.

(75) المادة (1/4) من مشروع المسؤولية الدولية، المرجع السابق.

(76) تعتبر قضية (Massey claim) عام 1927 (R.I.A.A. 155.4) مثالا على ذلك، حيث قُضي لصالح الولايات المتحدة وحُكم لها بمبلغ 15000 دولار على سبيل التعويض بسبب إخفاق السلطات المكسيكية في اتخاذ الإجراءات المناسبة لمعاقبة قاتل (Massey)، وهو مواطن أمريكي يعمل في المكسيك. جاء في رأي المفوض نيلسن: «ينجم عن سوء إدارة الأشخاص العاملين في خدمة الدولة إخفاق دولة في الوفاء بالتزاماتها المقررة بمقتضى القانون الدولي، وأنه يتوجب على الدولة أن تتحمل مسؤولية الأفعال غير القانونية المرتكبة من قبل موظفيها مهما كان مركزهم أو مقامهم الخاص بمقتضى القانون المحلي».

(77) مبادئ تالين، المرجع 3 سابق الإشارة إليه.

في هذا الصدد، جاء قرار محكمة العدل الدولية في قضية قناة كورفو مبيّنًا أن: «مجرّد سيطرة الدولة على إقليمها لا يعني دائمًا ضرورة الاستنتاج بأنها على دراية، أو أنها يجب أن تدري، بجميع النشاطات التي تحصل على إقليمها»[78]، وفي هذا الإطار لا بد من الإشارة إلى أنه، وبسبب تعقّد علوم استخدام الحاسوب وتقدّمها، يمكن أن نكون إزاء حالة هجوم إلكتروني على شاكلة الهجوم الذي قامت به كوريا الشمالية في عام 2013 عندما أنشأت أكثر من 100 عنوان حساب إلكتروني مفرد (IP address) في أكثر من أربعين دولة؛ كلها كانت تعمل للتأثير على حسابات وكمبيوترات حكومية وغير حكومية في كوريا الجنوبية، ومن الصعب إثبات علاقة الإسناد فيها[79].

وكما أبرزنا سابقًا، فإنه يبقى على الدولة التي ينتهي إلى علمها إتيان مثل هذه النشاطات على إقليمها أن تقوم بجميع الإجراءات الضرورية للحيلولة دون وقوع الضرر وإلّا تكون مسؤولة دوليًا، وكما أنه على الدولة التي لحقها ضرر وتختار اللجوء لإجراءات مضادة أن تتبع الحذر الشديد في طبيعة الإجراء الذي تتبناه، وعلى وجه الخصوص أن يكون الرد متناسبًا وقدرة الدولة على السيطرة على الأنشطة الإلكترونية على إقليمها، وعلى قدرتها للحيلولة دون وقوع نتائجها، وذلك بدلًا من التركيز على خطورة الهجوم السيبراني ذاته أو درجة وقع نتائجه. وباختصار، يجب أن يُتخذ التدبير الاحترازي لغاية أساسية هي إجبار الدولة التي وقع من عندها الاعتداء أن تفرض هيمنتها وسيطرتها على النشاطات الإلكترونية المعادية على أراضيها، وأن تتكلّف قدر المستطاع بدرئها.

أما النشاطات الإلكترونية التي يكون مصدرها أشخاصًا طبيعيين، أو هيئات غير حكومية، ولكنهم يتمتّعون بقدر من السلطة بموجب نظام أو قانون، فإن أعمالهم

(78) بين بريطانيا وألمانيا (I.C.J. 4، 18) عام 1949.

(79) انظر: بهذا الخصوص أيضًا مايكل شميت، المرجع 4 سابق الإشارة إليه، وأيضًا:

Y. Lee, South Korea Says North Korea Behind Computer Crash In March, HUFFINGTON POST (Apr. 10, 2013), at:
http://www.huffingtonpost.com/201310/04//north-korea-cyberattack_n_3050992.html.

فيما يتعلّق بهذه السلطة تُعزى للدولة ذاتها وإن تجاوز أولئك حدود السلطات المخوّلة لهم[80].

وفضلاً عمّا تقدّم، يوجد في القانون الدولي ما يشير إلى إمكانية اشتراك أكثر من دولة في المسؤولية عن الأضرار التي تتسبب من عدم احترام قواعده[81]، إذ يمكن لنشاط دولة ما أن يتسبب بمسؤولية دولة أخرى، وبالتالي إتاحة الفرصة بأن يتم استخدام التدابير المضادّة في مواجهة أكثر من دولة، فالدولة تكون مسؤولة بالاشتراك عند قيامها بمساعدة دولة أخرى على إتيان سلوك غير مشروع، إذا هي علمت بعدم مشروعية ذلك السلوك، كالسماح لها ـ مثلاً ـ باستخدام منشآتها الإلكترونية كواسطة لشن هجوم إلكتروني على دولة أخرى، بل وتكون مسؤولة بالاشتراك بمجّرد تمويلها مثل هذا النشاط. كما أن إكراه أو إجبار دولة ما على إتيان نشاط سيبراني معادي يجعل من الدولة التي قامت بذلك الإجبار مشتركة في المسؤولية[82]، ولكن لا بد لنا هنا من أن نفرّق بين نوع أو مدى التدابير المضادّة التي يمكن اللجوء إليها، وبين الحالة التي تكون الدولة المساندة مشتركة فعليًا في العملية السيبرانية المعادية أو أنها كانت مجرّد ممولة لبعض ذاك النشاط[83]، أو كانت هي المسيطر الفعلي على مجريات الأمور في الدولة التي انطلق منها النشاط [84]، كأن تكون هي الدولة الحامية أو المحتلّة لها.

(80) انظر: نص المادتين 6 و 7 من مشروع المسؤولية الدولية سابق الإشارة إليها. وجاء في قضية Caire Claim لعام 1929 بين فرنسا والمكسيك (5 .R.I.A.A. 516) ما يوضح ذلك؛ حيث طلب ضابطان مكسيكيان مبلغًا من المال من المدعو كير وهدداه بالموت إن لم يستجب لطلبهما. وبما أن المبلغ المطلوب لم يكن في متناول يده أمرا بإطلاق النار عليه. وأورد رئيس اللجنة التي نظرت هذه القضية بأنه: "تتحمل الدولة أيضًا مسؤولية دولية عن جميع الأفعال المرتكبة من قبل موظفيها أو أجهزتها والتي تعتبر تقصيرية طبقًا للقانون الدولي، بغض النظر عما إذا كان الموظف أو الجهاز الحكومي قد تصرف ضمن حدود اختصاصه أو أنه تجاوز تلك الحدود. وعلى كل حال، فلتبرير الأخذ بهذه المسؤولية الموضوعية للدولة عن الأفعال المرتكبة من قبل موظفيها أو جهازها خارج حدود اختصاصه، فإن من الضروري أن يكون قد تصرف، من حيث الظاهر على الأقل، على أنه موظف أو جهاز مفوض في ذلك، أو أنه، في معرض قيامه بالعمل، استعمل صلاحيات وتدابير تتلاءم مع صفته الرسمية". تجدر الإشارة إلى عدم اتفاق واضعي مدوّنة تالين بخصوص فيما لو كانت الدولة مسؤولة عن منع النشاطات المحتملة.

(81) انظر: نص المادة 16 من مشروع المسؤولية الدولية، المرجع 3 سابق الإشارة إليه.

(82) انظر: المادة 18 من مشروع المسؤولية الدولية، المرجع السابق. أيضًا: انظر المذكرات التفسيرية لجيمز كروفورد، المرجع سابق الإشارة إليه، على الصفحة 156.

(83) انظر: المذكرات التفسيرية لجيمز كروفورد، المرجع السابق، على الصفحة 151 منه.

(84) انظر: نص المادة 17 من مشروع المسؤولية الدولية، المرجع 3 سابق الإشارة إليه.

ويحوز شرط «الإسناد» على أهمية ونتائج خاصّة فيما يتعلّق بالتصرفات الخاصّة بالأفراد أو المجموعات، إذ إن أعمال هؤلاء لا تمثل الدولة ذاتها على أساس أنهم ليسوا من منتسبي أجهزتها التنفيذية أو التشريعية أو القضائية، أو أن نشاطهم لا يقع تحت دائرة سيطرة الدولة المباشرة، والأصل هنا أنه لا يجوز إسناد أعمال هؤلاء إلى الدولة ذاتها إلّا إذا تم منحهم سلطة لتمثيل الدولة، أو أنهم قاموا بتصرفاتهم بناء على توجيه من أحد أجهزة الدولة[85]. وتصبح الأمور أكثر تعقيدًا في حالة ما إذا قامت دولة ما برعاية تصرفات مجموعة من الأفراد من غير مواطنيها ويقطنون في دولة أجنبية وذلك بشنّهم عدوانًا إلكترونيًّا محلّيًّا أو خارجيًّا، وفي هذه الحالة، وحتى تثبت مسؤولية الدولة الراعية، لا بد من ثبوت ربط ذلك النشاط بها مباشرة، ولنا في التقارير الخاصّة بـ»مرتزقة الفضاء الافتراضي» توضيح لمدى تعقيد مثل هذه الأوضاع[86]، ولذلك لا يمكن اعتبار الارتباط العرضي أو السطحي محققًا شرط الإسناد، تمامًا كما لم تكفِ الدلائل بتورّط روسيا بأعمال القرصنة الإلكترونية المعادية التي وجّهت ضد إستونيا وجورجيا وقام بها مجموعة من قراصنة الإنترنت عامي 2007 و 2008 [87]، ومثال ذلك أيضًا، ما حصل عام 2013 عندما بُثّت تغريدة مفبركة على إحدى أكبر وكالات الأنباء الأمريكية «أسوشيتد برس» أفادت بوقوع انفجارين في البيت الأبيض وإصابة الرئيس باراك أوباما. فقد تسببت هذه التغريدة بحالة من الهلع داخل الولايات المتحدة وهبوط مؤشر «داو جونز» الصناعي بشكل حاد قبل أن يتضح أن الصفحة تعرضت لهجوم من قبل مجموعة من القراصنة (الهاكرز). ورغم الادّعاء حينها بمسؤولية الجيش السوري الإلكتروني عن اختراق حساب الوكالة الأمريكية، إلّا أن مزاعم الارتباط السطحي أو العرضي بين سوريا وذلك الاختراق الإلكتروني

(85) انظر: المادة 8 من مشروع المسؤولية الدولية، المرجع 3 سابق الإشارة إليه.

(86) انظر في ذلك:

J. Boone, Mercenary Hacker Group ‘Hidden Lynx’ Emerges as World›s Most Potent Cyber Threat, Globalpost (Sept. 18, 2013,) at:
http://www.globalpost.com/dispatches/globalpost-blogs/the-grid/hacker-mercenary-group-china-hidden-lynx-worlds-most-potent-cyber-threat.

(87) انظر في ذلك:

E. Tikk, K. Kaska & L. Vihul, International Cyber Incidents: Legal Considerations (2010).

يمنع حل اللجوء إلى التدابير المضادّة الممكنة[88].

وتثار في هذا الإطار مسألة في غاية الأهميّة تتمثّل في درجة ارتباط النشاط السيبراني بالدولة لثبوت مسؤوليتها القانونية، ففي قضية نيكاراجوا، أقرّت محكمة العدل الدولية بأنه: «من أجل أن ينتج عن الفعل مسؤولية الولايات المتّحدة القانونية لا بد من ثبوت سيطرتها الفعلية على سير العمليات العسكرية التي يُدّعى عدم مشروعيتها»[89]. وتجب التفرقة هنا بين معيار «السيطرة الفعلية» عن معيار «السيطرة الكاملة» الذي تم التعرّض له في قضية تاديتش المشهورة التي صدر بها قرار من المحكمة الجنائية الدولية بخصوص الجرائم ضد الإنسانية في يوغسلافيا[90]، مع أن المحكمة تعرّضت فقط لموضوع العلاقة بين الدولة والعناصر غير الحكومية (تحديدًا العلاقة التي تربط يوغسلافيا بالقوات الصربية البوسنية) لتمكّنها من تقرير فيما لو كان النزاع المسلّح في البوسنة يُعد من النزاعات الدولية، والحقيقة أن قرار محكمة العدل الدولية في قضية «جريمة الإبادة الجماعية» جاء مبينًا إلى حد كبير هذا الإطار المعياري في تقريرها بأن اشتراط «الإسناد» لقيام المسؤولية الدولية يجب أن يعتمد على إثبات سيطرة الدولة الفعلية وليس السيطرة الشاملة أو الكاملة على مجريات الأحداث المخالفة لقواعد القانون الدولي[91]. وبناءً على ذلك، لا يعد مجرد تقديم التمويل أو المساعدة اللوجستية من قبيل السيطرة الفعلية، وهي كما أقرّت المحكمة في قضية نيكاراجوا بأنه: «حتى السيطرة العامّة على القوّة المسلّحة ... لا تعني بالضرورة سيطرة فعلية إذا كانت القوّة تتمتّع بدرجة من الاستقلالية العالية»[92].

---

(88) انظر الموقع الإلكتروني:

http://archive.arabic.cnn.com/2013/world/423//false.obamaTweet/

وأيضًا:

S. Stalinsky, China Isn›t the Only Source of Cyberattacks, WALL ST. J. (May 21, 2013), at: http://online.wsj.com/news/articles/SB10001424127887324744104578475571183053736.

(89) انظر: قضية نيكاراجوا، المرجع 1 سابق الإشارة إليه، على الصفحة 11.

(90) انظر: قضية الادعاء العام ضد تادتش في محكمة يوغسلافيا 1999 (Case No. IT-94-1-A, Appeals Chamber Judgment, 117, 131–40, 145)

(91) انظر: القضية بين البوسنة وصربيا عام 2007 (I.C.J. 43, 403–05).

(92) قضية نيكاراجوا، المرجع 1 سابق الإشارة إليه، على الصفحة 115 منه.

في هذا المقام، وفي علاقة الأعمال التي تقوم بها الشركات بالدولة، لا بد لنا من التذكير بأنّه لا تُسند جميع أعمال الشركات المملوكة للدولة لها بمجرّد ثبوت هذه الملكيّة، فعلى سبيل المثال، لا يكفي مجرّد ثبوت ملكية الدولة لشركة اتصالات ما أو مؤسسة معلومات تقنيّة أن تُسند جميع تصرفاتها للدولة ذاتها، وبالتالي ليس للدولة المتضررة من تصرفات هذه الشركات الحق في اللجوء إلى تدابير مضادّة بحقّ دولة إلّا إذا ثبت أن الشركة المعنيّة قد تصرفت كمرفق حكومي أو كممثل لتلك للدولة، أو أنها قامت بتصرفاتها المخالفة برعاية، أو سيطرة، مباشرة من الدولة. ويستوي هذا فيما لو كانت تلك الشركة المملوكة للدولة موجودة داخل إقليم الدولة ذاتها أو خارجه، إذ لا اعتبار للمكان الجغرافي للشركات على إمكانية إسناد أنشطتها للدولة، وعليه، إذا قامت إحدى شركات الاتصالات الأجنبية والمملوكة لدولة ما بنشاط سيبراني مُعادي ـ سواء بحق دولة الموطن أم خارجه ـ يمكن إسناده لتلك الدولة، لأن هذه الأخيرة تكون مسؤولة دوليًا عن تلك التصرفات، غير أنه تجب الإشارة هنا ـ وبخلاف المادتين السادسة والسابعة من مشروع المواد المتعلّقة بمسؤولية الدول عن الأعمال غير المشروعة دوليًا، والخاصّة بتجاوز الأفراد الطبيعيين والمؤسسات الحكومية لحدود السلطات المخوّلة لهم ـ أنّه لا يثبت شرط الإسناد في حالة تجاوز الشركات المملوكة للحكومة إطار الصلاحيات المخوّلة لهم أو مخالفتهم لتعليمات الدولة، فقيام بعض قراصنة الشبكة العنكبوتية بالخارج بتجاوز التعليمات الصريحة لهم من دولتهم بعدم إتيان نشاطات محدّدة يعني بالتالي عدم توافر شرط الإسناد بحق الدولة إذا هم قاموا بتلك النشاطات المخالفة. وعليه، تفقد الدولة المتضررة حقّها في اللجوء إلى التدابير المضادّة ضد هذه الدولة.

المبحث الثالث
حدود وقيود التدابير المضادّة ومدى تناسبها

يتناول هذا الجزء شروط وحدود اتخاذ تدابير مضادة من جانب دولة متضررة من تهديد سيبراني، أي إنّه يتناول حدود تلك التدابير التي كان اتخاذها سيتعارض مع التزامات الدولة المتضررة لو تم اتخاذها في الحالات الاعتيادية تجاه الدولة المتسببة بالضرر. وقد علمنا أن هذه التدابير تأتي ردًّا على فعل غير مشروع دوليًا وتقوم به الدولة المتضررة من أجل ضمان الكف عن هذا الفعل الضار، والجبر حيثما أمكن، فالتدابير المضادة تعتبر نظامًا تحاول بواسطته الدول المتضررة إثبات حقوقها واستعادة العلاقة القانونية بالدولة المسؤولة، وهي علاقة قُطعت بسبب الفعل غير المشروع دوليًا. لذا فإننا سنقسم هذا المبحث إلى مطلبين، ندرس في المطلب الأول حدود اللجوء للتدابير المضادة، ونتناول في المطلب الثاني قيود اللجوء للتدابير المضادّة.

المطلب الأول
حدود اللجوء للتدابير المضادّة

لا بد من الإشارة بداية إلى أنّه بما أن التدابير المضادّة تمثّل شكلًا من أشكال دفع الضرر ومساعدة الذات، فإن للدولة المتضررة الحق في تقييم الوضع القائم، وتحديد فيما إذا كان هناك مخالفة للقانون الدولي أتت بها دولة أخرى بحقّها. وتقوم الدولة المتضررة بتقييم التهديد الموجه لها وتحديد الدولة المسؤولة عن ذلك، وهي بذلك عرضة لأن يكون تقييمها مصيبًا أو خاطئًا، فإذا ثبت أن تقديرها كان خاطئًا، تنتفي صفة «التدابير المضادّة» عن كل فعل قامت به، أو امتناع عن فعل، بل وتصبح هي بدورها محل مسؤولية دولية عن المخالفات التي تنتج عن سوء تقديرها، وعن الضرر الذي يلحق بالدولة الأخرى.

لذلك، ولمّا كان من الصعب التحقق دائمًا من شرط الإسناد في الأعمال الإلكترونية السيبرانية المخالفة، باعتبار أن اللجوء إليها ـ أساسًا ـ قد يكون من أجل تضليل المتضرر وعدم تمكينه من التعرّف على هوية الجناة، فإنه لا بد لمن يلجأ للتدابير

المضادّة من الدول أن تتوخّى الحيطة حتى لا تدور رحى المسؤولية وتصبح موجهة ضدّها، ومقدار الحيطة اللازمة هنا هو ما قررته محكمة تحكيمية في "قضية إيجر" بين أمريكا وإيران بأنّ المعيار هو «المعقولية في الاستنتاج»[93]، وذلك بالوصول إلى استنتاج معقول في تحديد المخالفة الدولية وهوية المسؤول عنها وإسناد العمل غير المشروع إلى دولة ما، وفي حال تحقّق هذا الشرط، وحدود اللجوء للتدابير المضادّة وقيودها كما سيأتي ذكره تاليًا، تنتفي صفة المسؤولية عن خطأ الدولة في تقديرها للأمور قبل تنفيذها لتدابير مضادّة.

وأيضًا، لا بد لنا من أن نتذكّر دائمًا بأن المسؤولية الدولية هي تلك التي تتعلّق بمساءلة الدول كشخص من أشخاص القانون الدولي، فلا يكون حق استخدام التدابير المضادّة إلّا من قبل دولة، وعليه، ليس هناك في القانون الدولي ما يخوّل الشركات الخاصّة (كشركات الاتصال وشركات المعلومات الإلكترونية) حق استخدام التدابير المضادّة بشكل منفرد، كرد على عمل دولي مخالف، حتى وإن كان مؤثرًا بشكل مباشر على أعمالها. على سبيل المثال، بالرغم من الارتباط بين الصين كدولة ومجموعة شركة جوجل العالمية، لم يكن هناك مسوّغ شرعي أو أدنى مبرر لشركة جوجل بالقيام بأعمال قرصنة سيبرانية كرد على أعمال لعصابة إنترنت قامت بالنفاذ إلى شبكتها[94]، بيد أنّه يجوز للدولة أن تستخدم مثل هذه الشركات إن هي أرادت أن تستخدم حقّها في التدابير المضادة[95] وتنسب حينها جميع ما تقوم به الشركة من باب مساعدة الدولة المتضررة إلى تلك الدولة إعمالًا لمبدأ الإسناد الآنف ذكره.

وكقاعدة عامّة، يجوز للدول المتضررة فقط حق اللجوء إلى التدابير المضادّة، وذلك باستثناء حالتين وُضّحتا في متن المادة 48 (1) من مشروع المواد المتعلقة بمسؤولية

(93) قضية إيجر ضد إيران عام 1987 (Yeager v. Iran, 17 Iran-U.S. Cl. Trib. Rep.)، الصفحات 101 و 102.

(94) انظر بهذا الصدد:

D.E. Sanger & J. Markoff, After Google's Stand on China, U.S. Treads Lightly, N.Y. TIMES (Jan. 15, 2010), at:
http://www.nytimes.com/201015/01//world/asia/15diplo.html?_r=0.

(95) مشروع مواد المسؤولية الدولية، المرجع 3 سابق الإشارة إليه. وانظر بهذا الخصوص:

Zach West, Young Fella, If You're Looking for Trouble I'll Accommodate You: Deputizing Private Companies for the Use of Hackback, 63 SYRACUSE L. REV. 119 (2012).

الدول عن الأفعال غير المشروعة دوليًا لعام 2002، تحت عنوان «احتجاج دولة غير مضرورة بمسؤولية دولة أخرى» بأنّه: «يحق لأي دولة خلاف الدولة المضرورة أن تحتج بمسؤولية دولة أخرى:

إذا كان الالتزام الذي خُرق واجبًا تجاه مجموعة من الدول تضم تلك الدولة، وكان الغرض منه هو حماية مصلحة جماعية للمجموعة؛ أو إذا كان الالتزام الذي خُرق واجبًا تجاه المجتمع الدولي ككل».[96]

ويستلزم في هذه الاستثناءات أن تكون صادرة عن مجموعة من الدول. ولذلك فإنّه لا يجوز لدولة منفردة غير متضررة أن تنخرط بأعمال تدابير مضادّة لحساب دولة أخرى متضررة، وذلك كما جاء في قرار محكمة العدل الدولية في قضية نيكاراجوا[97].

إنّ الهدف الأساس من اللجوء للتدابير المضادّة هو ما ورد في المادة 49 (1) من النصوص المتعلّقة بمسؤولية الدول عن الأفعال غير المشروعة دوليًا لعام 2002، والذي يتمثّل بمحاولة إرجاع الوضع غير المشروع إلى مسارٍ مشروع[98]، وعليه، فالدولة المعتدية ملزمة بأن: «تكف عن الفعل إذا كان مستمرًا ... وأن تقوم ... بتقديم التأكيدات والضمانات الملائمة بعدم التكرار إذا اقتضت الظروف ذلك ... وعلى الدولة المسؤولة ... الالتزام بجبر كامل الخسارة الناجمة عن الفعل غير المشروع دوليًا ... بحيث تشمل الخسارة ... أي ضرر سواء كان ماديًا أم معنويًا»[99].

وقد اختلفت الآراء أيضًا بشأن الأحكام المتعلقة بالتدابير المضادة الواردة في الفصل الثاني من الباب الثاني من مشروع النصوص المتعلّقة بالمسؤولية الدولية

(96) تتمثّل الحماية الجماعية بالاتفاقيات المتعلّقة بالمناطق أو الأقاليم الخالية من السلاح النووي، وكما أكثر ما يتمثل الالتزام تجاه المجتمع الدولي ككل (Erga Omnes) بالالتزامات المتعلّقة بمنع الاعتداء الدولي، التطهير العرقي والعبودية. من ذلك ما قامت به مجموعة من الدول بتجميد أرصدة حكوميّة عراقيّة عام 1990 إثر اجتياحها للكويت.

(97) قضية نيكاراجوا، المرجع 1 سابق الإشارة إليه، على الصفحة 249.

(98) مسودّة المشروع، المرجع 5 سابق الإشارة إليه. وانظر أيضًا: قضية آرشر دانيالز ضد المكسيك (Archer Daniels Midland Company v. Mexico) وخصوصًا دفاع المكسيك بأن الضريبة تكون مشروعة كإجراء مضاد وحكم المحكمة بنفي ذلك على أساس أن المكسيك لم تقم بفرض الضريبة لإجبار الولايات المتحدة الأمريكية للوفاء بالتزاماتها نحو المكسيك (ICSID Case No. ARB(AF)/04/05, Awa)، على الصفحات 134 وحتى 151.

(99) المادة 30، المرجع السابق.

عن الأفعال غير المشروعة دوليًا لعام 2002، فقد أعرب بعض من الأعضاء الذين اشتركوا بوضعه عن استحسانهم لاستبقاء هذا الفصل لسببين اثنين: أولهما، لأنه لا يمكن إنكار وجود التدابير المضادة كجزء معترف به في القانون الدولي، خصوصًا بعد تأكيد قرار محكمة العدل الدولية عليه في «قضية غابكيكوفو ناجيمروس» الذي بيّن أن الهدف من مثل هذه التدابير هو إرجاع العلاقات بين الدول إلى مشروعيتها كما كانت من قبل حيثما كان ذلك ممكنًا[100]؛ وثانيهما، لأن التدابير المضادة تؤدي دورًا حاسمًا في إعمال الغرض من المسؤولية الذي يتمثّل بِحثِّ الدولة المرتكبة للفعل غير المشروع على الامتثال بالتزاماتها، ثم ليس الكف عن الفعل فحسب، وإنما بجبر الضرر أيضًا.

وينتج عن هذه الحدود نتائج لا بد من إدراكها:

أولًا: لا يكون من قبيل التدابير المضادّة إذا كان اتخاذها سيفاقم المشكلة، وألّا يكون اتخاذها بمثابة انتقام. وجاء بشأن هذا ما وصفته محكمة تحكيم دولية في قرار لها بقضية الخدمات الجوّية بأن: «التدابير المضادة ما هي إلّا رهان على مدى حكمة الدولة بالتصرّف المعقول ... واستخدامها بروح من المنطقية والعزم على حل النزاع»[101]. هذا بالرغم من أن الحكمة لا تكون دائمًا ممكنة في الخلافات الدولية المتعلّقة بالهجمات الإلكترونية باعتبار أن رد الفعل السريع لدرئها لا يُتيح مجالًا لكثير من العقلانيّة.

ثانيًا: لأن الهدف من التدابير المضادّة هو إرجاع العلاقات إلى المشروعية بين الدول، فإنّه لا يجوز اللجوء إليها استباقًا، وهو ما انتهت إليه محكمة العدل الدولية في قضية «غابكيكوفو ناجيمروس» ـ سالفة الذكر ـ بأنه يمكن اللجوء إلى التدابير «كوسيلة مضادّة لعمل دولي سابق غير مشروع»[102].

ثالثًا: لا يجوز اللجوء إلى التدابير المضادّة كوسيلة من الوسائل الرادعة أو التأديبية، وبالتالي لا يجوز استخدامها في مواجهة ما تم وانتهى من أخطاء اقترفتها

(100) انظر: قضية كابكبكوفو، المرجع سابق الإشارة إليه، على الصفحة 87؛ انظر أيضًا: مايكل شميت، المرجع 4 سابق الإشارة إليه في جمع هذه الآراء.

(101) انظر: قضية الخدمات الجويّة، المرجع سابق الإشارة إليه، صفحة 91؛ انظر أيضًا: مايكل شميت، المرجع 4 سابق الإشارة إليه.

(102) قضية كابكيكوفو، المرجع 23 سابق الإشارة إليه، على الصفحة 83.

دولة أخرى ولا يُتوقّع تكرار الخطأ ذاته من جانبها، ولذلك، يصبح العامل الزمني مهمًا في مشروعية اللجوء للتدابير المضادّة حيث يقتصر استخدام التدابير المضادة على عدم الوفاء في الوقت الحاضر بالالتزامات الدولية للدولة المتخذة للتدابير تجاه الدولة المسؤولة(103).

رابعًا : وعليه، يبقى الحق بهذه التدابير قائمًا طالما أنّ خطأ الدولة المعتدية يمثّل جزءًا من سلسلة من الاعتداءات القائمة، أو أن الخطأ ينتج عنه لا محالة سلسلة من الأضرار المتعاقبة.

خامسًا : يتوجب التوقف عن التدابير المضادة المتّخذة فور ثبوت توقف الدولة المعتدية عن اعتدائها وتحقيقها لالتزاماتها الدولية(104)، مع ملاحظة أن الحق باللجوء للتدابير المضادّة يبقى مستمرًا إذا كانت محاولات إرجاع الوضع إلى ما كان عليه أو التعويض لا زالت قائمة.

سادسًا : يجب التوقّف عن التدابير المضادّة في حالة عرض النزاع على جهة قضائية دولية بصدد إصدار قرار ملزم على حيثياته، بل إنه يمكن تفسير الحق باتخاذ التدابير المضادّة، والذي يهدف إلى إرجاع شرعية العلاقات بين الدول، بإجبار الدول على الاتفاق على ردٍّ موضوع العلاقة إلى التحكيم أو القضاء الدولي عمومًا. ويكمن السبب في هذا بأن عنصر الضرورة للّجوء لتلك التدابير يتلاشى مع وجود جهة قضائية لها حق إصدار ما تراه مناسبًا من تدابير مؤقتة لحماية الدولة المعتدى عليها، أما إذا استحال هذا، بأن لا تمتلك الجهة القضائية هذه المُكنة، فإنه يبقى للدولة المتضررة الحق بالتدابير المضادّة(105).

سابعًا : ينبغي على الدولة المتضررة أن تطلب من الدولة المعتدية تصويب الإخلال قبل لجوئها للتدابير المضادّة. هذا الالتزام أقرّته محكمة التحكيم الدولية في قضية

(103) انظر في هذا الصدد: المادة 49(2) من مشروع مواد المسؤولية الدولية، المرجع 3 سابق الإشارة إليه؛ وأيضًا:

M. Kamto, The Time Factor in the Application of Countermeasures, in "the Law of International Responsibility", 1169, James Crawford et al. eds., 2010.

(104) المادة 53 من مشروع اتفاقية المسؤولية الدولية، المرجع 3 سابق الإشارة إليه.

(105) انظر في هذا الخصوص: قضية الخدمات، سابق الإشارة إليه، على الصفحة 59.

«ناوليلا»[106]، التي دارت حيثياتها بشأن اللجوء للانتقام في العلاقات الدولية، علاوة على قرار قضية «كابتشيكوفو ناجيمروس»، والذي قضى بأنه: «يتوجّب على الدولة المتضررة، قبل استخدامها حقّها باتخاذ تدابير مضادة، أن تقوم بالتواصل مع الدولة المتسببة بالضرر لتطلب منها وقف سلوكها الخاطئ وتعويضها إن لزم الأمر»[107].

المطلب الثاني
قيود اللجوء للتدابير المضادّة

لا بد لنا هنا من الإشارة إلى أن هناك شروطاً أوردها مشروع مواد المسؤولية الدولية تتعلّق باللجوء إلى التدابير المضادة، إذ إن على الدولة المضرورة أن تستنفد إجراءين ضروريين قبل استخدامها لحقها بالتدابير المضادّة: أولهما، أن تطلب من الدولة المسؤولة الوفاء بالتزاماتها؛ وثانيهما، أن تُخْطِر الدولةَ المسؤولة بأي قرار باتخاذ تدابير مضادة، وتعرض عليها التفاوض معها. ومما لا شك فيه بأن لهذه الشروط، وما يتمخّض عنها من نتائج، أثرًا خاصًّا وعلاقة مباشرة بالمسؤولية عن النشاطات الإلكترونية المعادية، إذ إنّها قد تصدر بغير علم من الدولة التي صدر من إقليمها النشاط المُعادي، أو أنّها كانت بذاتها ضحيّة لاستغلال قراصنة الإنترنت من على أراضيها، غير أنّه من الواجب التذكير هنا أن الطلب من الدولة المسؤولة الوفاء بالتزاماتها، أو ضرورة إخطارها المسبق بأي قرار باتخاذ تدابير مضادة، والتفاوض معها ما أمكن، لا يكون دائمًا متاحًا، فقد جاء في قرار محكمة التحكيم الدولية في قضية «الخدمات الجويّة» أنّه: «في ظل تعقيد العلاقات الدولية، فإنّه ليس من الممكن دائمًا تعطيل استخدام التدابير المضادّة خلال فترة التفاوض»، وخصوصًا إن كانت المفاوضات لا تجري بروح النيّة الحسنة، أو أن عدم الالتزام لا زال قائمًا. كما أنه يمكن طرح شروط اللجوء للتدابير جانبًا في الحالات التي تدل فيها المؤشرات على تعنّت الدولة المسؤولة، أو أن الدلائل توحي بتفاقم الضرر إن لم يتم اتخاذ إجراءات مضادة على وجه السرعة.

(106) انظر عمومًا في هذه الخصوص: في مذكرات كروفود التفسيرية: Y. Iwasawa & N. Iwatsuki, Procedural Conditions، المرجع سابق الإشارة إليه.

(107) قضية كابكيكوفو، سابق الإشارة إليه، على الصفحة 84؛ وأيضًا قضية الخدمات الجويّة، سابق الإشارة إليه، الصفحات 85 – 87. وانظر أيضًا: ذات المطلب في المواد 43(2) و 52 (1)(a) من مشروع مواد المسؤولية الدولية، المرجع 3 سابق الإشارة إليه.

وفي كل الأحوال، تلتزم الدولة المتضررة بعدد من الالتزامات الدولية عند اللجوء للتدابير المضادّة في مواجهة الاعتداء السيبراني، فقد جاءت المادّة (50) من مشروع المواد المتعلّقة بمسؤولية الدول عن الأعمال غير المشروعة دوليًا لتبيّن الالتزامات التي لا تتأثر بالتدابير المضادة على أنها تشمل:

أولًا : الالتزام المنصوص عليه في ميثاق الأمم المتحدة بالامتناع عن التهديد باستعمال القوة أو استعمالها فعلًا، وذلك كما ورد في نص المادة 2(4) من ميثاق الأمم المتحدة الذي يعكس عرفًا دوليًا قائمًا لا يجوز الإخلال به[108]. ويثار التساؤل هنا عمَّ إذا كان يمكن وصف بعض التدابير المضادة بأنّها ليست إلّا سبيلًا من سبل استعمال القوّة؟ والحقيقة أنه لا يمكننا هنا التفريق قطعًا بين ما يمكن اعتباره من قبيل التدبير المضاد أو استخدامًا للقوة، وقد جاء اختلاف واضعي مدوّنة تالين على هذا الأمر جليًا، إذ إن كل ما وصلوا إليه من اتفاق بهذا الشأن بعد ثلاث سنوات من المناقشات هو أن: «العمليات السيبرانية ترتقي لمصاف استخدام القوّة إذا امتد أثرها بطريقة مشابهة للأثر الذي يحدثه استخدام العمليات غير السيبرانية التي تصل إلى مصاف استخدام القوّة»[109].

ومع أنه من السهولة بمكان تصنيف النشاط السيبراني بأنه مكافئ لاستخدام القوة التقليدية إذا كان من نتائجه تدمير ملموس للبنية التحتية أو إزهاق للأرواح، إلّا أن استخدام القوّة قد يتحقّق أحيانا بالرغم من عدم وجود تدمير ملموس، وهذا ما قضت به محكمة العدل الدولية في قضية نيكاراجوا، إذ أشارت إلى أن مجرد تسليح وتدريب الميليشيات يجعل من هذا العمل استخدامًا غير مشروع للقوة[110]. إن قرار المحكمة هذا لم يكن نتيجة لإسناد عمليات الميليشيات إلى الولايات المتّحدة الأمريكية مباشرة، وإنّما لمجرّد قيامها بتسليح وتدريب تلك المليشيات، غير أننا لا نستطيع إسقاط نتائج هذا القرار بعموميّة على جميع النشاطات التي لا ترتقي نتائجها إلى تدمير أو إزهاق للأرواح، وبالتالي عدم إمكانية وصفها باستخدام القوّة المعروف تقليديًا.

(108) انظر بهذا الخصوص: المبدأ II لمؤتمر التعاون والأمن في أوروبا (I.L.M 197514)؛ وأيضًا: قضيتي كورفو ونيكاراجوا سابق الإشارة إليهما.

(109) المبدأ 11 من مبادئ كراسة تالين، المرجع 3 سابق الإشارة إليها.

(110) قضية نيكاراجوا، المرجع 1 سابق الإشارة إليه، الصفحة 228.

ونتيجة لصعوبة تحديد متى يكون الاعتداء السيبراني استخداما للقوة، عهد واضعو مدوّنة تالين إلى تبنّي عددٍ من العوامل التي يمكن للدول الاعتداد بها لتصنيف النشاط السيبراني كمكافئ لاستخدام القوة منها: وضوح الاعتداء السيبراني، الأثر المباشر للاعتداء السيبراني، الطبيعة الانتهاكية الظاهرة للاعتداء السيبراني، إمكانية وقابلية قياس الانتهاك، تطبّع الانتهاك السيبراني بطبيعة عسكرية، تدخّل الدولة المباشر في إحداثه وافتراض مشروعيته، نوع الهدف المعتدى عليه، والعلاقات السياسية السائدة وقت الاعتداء بين الدولة المعتدى عليها والدولة المسؤولة عن الاعتداء[111].

في ضوء ما سبق، ونتيجة لهذه الصعوبات والتأويل الذي يمكن أن يكون محلًا للخلاف، يمكننا القول إنه يمكن أن نكون إزاء حالة لا يمكن معها تحديد فيما إذا كان الرد على الاعتداء السيبراني يعد بمثابة استخدام للقوة وليس استخدامًا للحق في التدابير المضادّة. إن هذا بدوره يجعل من الجائز تصوّر استخدام لقوة مناسبة للتصدي لنشاط دولي غير مشروع ـ لدرء مخاطر سيبرانية معاديةً دون أن يفقد هذا السلوك تصنيفه ـ بأنّه من التدابير المضادّة، خصوصًا إذا لم يصل الصدام إلى مستوى نزاع مسلّح، بمعنى أن هناك مساحة فاصلة بين ما يمكن أن يكون استخدامًا للقوّة وبين النزاع العسكري المسلّح. إن هذا يعني أن هناك فرقًا بين الحالات التي يمكن فيها للدولة اللجوء لحقها باستخدام التدابير المضادّة وتلك التي تخوّلها اللجوء للدفاع الشرعي المسلّح. ومما قد ينتج عن هذا الاختلاف أنه يمكن للدفاع الشرعي أن يكون منفردًا أو جماعيًا، وذلك على خلاف التدابير المضادّة التي لا تستساغ إلّا أن تتّخذ بشكل منفرد من قبل الدولة المتضررة، ففي الحالة الأخيرة، يكون لتلك الدولة حق اللجوء لتدابير مضادّة اعتيادية أو قهرية (دفاع شرعي) حتى وإن لزم الأمر استخدام القوّة العسكرية، وهو كما وضّحه القاضي سيما في قضية «موانئ النفط» بقوله: «في الحالات التي لا تصل فيها المشاكسات الدولية حد الهجوم المسلّح بحسب ما ورد في نص الدفاع الشرعي في المادة 51 من ميثاق الأمم المتحدة، يكون للدولة فقط

(111) المبادئ 48 – 52 من مدوّنة تالين، المرجع 3 سابق الإشارة إليه.

الحق في الرد المناسب والمتناسب لا غير»[112].

ثانيًا : لا يجوز في اتخاذ التدابير المضادّة أن تؤدي تلك القواعد إلى الإخلال بالالتزامات المتعلقة بحماية حقوق الإنسان الأساسية[113]، وهنا يثور إشكال آخر يتعلّق بتحديد تلك الحقوق الأساسية، فمن ناحية، قد يُفهم من نص المادة 50 (1) من مشروع المواد المتعلّقة بمسؤولية الدول عن الأعمال غير المشروعة دوليًا بأن التدابير المضادّة يجب ألّا تمس الحقوق التي لا يجوز انتهاكها حتّى في وقت إعلان حالة الطوارئ أو وقت النزاعات المسلّحة، ومن ناحية أخرى، قد يتعدّى هذا المنع ليطال أيضًا الحقوق المتعلّقة بحماية سرّية المعلومات والاتصالات[114]، بل والحق في الخصوصية، باعتبارها من الحقوق الأساسية أيضًا. وفي هذا الإطار، لا بد من التذكير بالتعليق للذي أوردته لجنة الأمم المتحدة للحقوق الاقتصادية والاجتماعية بشأن نصوص المسؤولية الدولية، وتأكيدها على أنّه: «من الضروري التفرقة بين الأهداف المرجوّة من إيجاد نوع من الضغط السياسي أو الاقتصادي على حكومات الدول للامتثال لالتزامات دولية معيّنة، وبين الضرر الذي قد يحدثه هذا الضغط من أثر سلبي على الأفراد أو الجماعات في تلك الدول»[115]، وعليه، لا يجوز استخدام التدابير المضادّة إذا كان من شأنها الإضرار بالأفراد أو الجماعات التي ليس لها علاقة، لأن المقصود منها يجب أن لا يتعدى غاية إرغام الحكومات المخلّة بالتزاماتها بالعودة إلى جادّة الصواب واستمرار العلاقات الدولية المتّزنة.

ثالثًا : لا يجوز في استخدام التدابير المضادّة أن تمس بالالتزامات ذات الطابع الإنساني التي تمنع الأعمال الانتقامية[116]، وهذا بموجب اتفاقية جينيف لعام 1929

(112) انظر: قضية الأنشطة المسلّحة في الكونغو بين الولايات المتحدة الأمريكية والكونغو (I.C.J. 168, 147, 2005). وأيضًا: تمت التفرقة في قضية نيكاراجوا بين «النزاع المسلّح والحالة التي يكون فيها استخدام القوّة مفرطًا»، قضية نيكاراجوا، المرجع 1 سابق الإشارة إليه، الصفحة 191.

(113) المادة 50 (1) (b) من مشروع مواد المسؤولية الدولية.

(114) انظر مثلًا: المواد 7 و 8 من ميثاق الحقوق الأساسية للاتحاد الأوروبي لعام 2000 (O.J., C364)؛ وأيضًا: المادة 8 من معاهدة حماية الحقوق والحريات لعام 1950 (U.N.T.S. 221 213).

(115) انظر الملاحظة رقم 8 من:

The Relationship Between Economic Sanctions and Respect for Economic, Social and Cultural Rights, U.N. Doc. E/C.128/1997/ (Dec. 12, 1997), General Comment 8, 125, 4.

(116) المادة 50 (1) (b) من مشروع مواد المسؤولية الدولية، المرجع 3 سابق الإشارة إليه.

واتفاقيات جنيف الأربع لعام 1949 وبرتوكولها الإضافي الأول لعام 1977[117]، والتي تعكس عرفًا دوليًا بمنع الأعمال الانتقامية (وإن كانت بصورة تدابير مضادّة) بحق الجرحى والغرقى والأسرى وبمن يقومون بأعمال الإغاثة أو الأعمال الطبّية، فلا يجوز مثلًا القيام بهجوم إلكتروني سيبراني يمكن أن يؤدي إلى تعطيل الأجهزة الطبّية أو الكهربائية اللازمة لإسعاف المرضى والجرحى من قوات العدو كرد على قيامهم هم بمثل هذا النوع من العمليات العسكرية.

رابعًا : لا يجوز في استخدام التدابير المضادّة أن تمس بالالتزامات الأخرى القائمة بموجب قواعد قطعية من قواعد القانون الدولي العام[118]، فلا يجوز الإخلال مثلا بمبدأ عدم مشروعية الإبادة الجماعية كأن يكون من شأن اتخاذ التدابير المضادّة التحريض على تلك الجريمة، أو التلاعب بالمعلومات الإلكترونية أو التقارير بشأنها.

خامسًا : لا تُعفى الدولة التي تتخذ تدابير مضادة من الوفاء بالتزاماتها بموجب أي إجراء لتسوية المنازعات يكون ساريًا بينها وبين الدولة المسؤولة، أو فيما يتعلق بصون حرمة الممثلين الدبلوماسيين أو القنصليين أو الأماكن أو المحفوظات أو الوثائق الدبلوماسية أو القنصلية[119].

سادساً : لا بد في التدابير المضادّة من الانتباه لمبدأ التناسب في استخدامها حتى تكون مشروعة، وتجدر الإشارة هنا أنّه لا بد من التفريق بينها وبين مبدأ التناسب في قانون الحرب والذي يرتبط بقدر القوّة المستخدمة اللازمة لدولة ما للدفاع عن نفسها في نزاع مسلّح، ففي هذه الحالة الأخيرة، قد تتجاوز القوّة اللازمة مبدأ التناسب إذا كان من شأنها إيقاف الاعتداء المسلّح وكانت ضرورية لذلك، أمّا في التدابير المضادّة، فلا يجوز فيها تجاوز مبدأ التناسب. لذلك، يبقى على الدولة المتضررة أن تُبقي في

(117) انظر: المادة 2 من اتفاقية جنيف لعام 1929 (118 303 .L.N.T.S)؛ والمادة 64 من اتفاقية جنيف الأولى لعام 1949 (75 31 .U.N.T.S)، والمادة 47 من اتفاقية جنيف الثانية 1949 (75 85 .U.N.T.S)، والمادة 13 من اتفاقية جنيف الثالثة لعام 1949 (75 135 .U.N.T.S)؛ والمادة 33 من اتفاقية جنيف الرابعة لعام 1949 (75 .U.N.T.S 287)، وبروتوكولاتها الإضافية في المواد 20، 51(6)، 52(1)، 53(c)، 54 (4)، 55(2) 56(4).

(118) المادة 50 (1) (b) من مشروع مواد المسؤولية الدولية، المرجع 3 سابق الإشارة إليه.

(119) المادة 50 (2) (a) من مشروع مواد المسؤولية الدولية، المرجع السابق. وانظر بهذا الخصوص أيضًا: قضية الرهائن الدبلوماسيين في طهران، المرجع سبق الإشارة إليه، الصفحات 61، 62، 77 ، 86؛ والمواد 33 ، 35 من اتفاقية فيينا للحصانة القنصلية لعام 1963 (596 261 .U.N.T.S).

ذهنها أنه بلجوئها للتدابير المضادّة لا بد أن تتيقّن من أن يتناسب التدبير المضاد وحجم الضرر الواقع عليها وألَّا يتجاوز في أي حال من الأحوال جسامة الفعل المتسبب بالضرر.

ثم أيضًا وجب التفرقة بين مبدأ التناسب في التدابير المضادّة ومبدأ التناسب المعروف في القانون الدولي الإنساني، والذي يقصد به مراعاة التناسب ما بين الضرر الذي قد يلحق بالخصم والمزايا العسكرية الممكن تحقيقيها نتيجة لاستخدام القوة أثناء سير عملياتها العسكرية، بحيث يكون الهدف منه هو إقامة التوازن بين مصلحتين متعارضتين هما الإنسانية و»الضرورة الحربية»، بمعنى أن مبدأ التناسب في القانون الدولي الإنساني معنيٌّ بشكل مباشر بتناسب الضرر المتوقع حصوله مع المكاسب العسكرية المنشودة، أمّا مبدأ التناسب في التدابير المضادّة فهو معنيٌّ بتناسبه مع الضرر الذي وقع على الدولة المتضررة.

إذًا، لا بد للتدابير المضادّة أن تتناسب مع الضرر الذي ينتج عن العمل غير المشروع، وقد نصت المادة 51 من مشروع مواد المسؤولية الدولية عن ذلك بالنص على إنّه: «يجب أن تتناسب التدابير المضادة مع الضرر المتكبد، على أن توضع في الاعتبار جسامة الفعل غير المشروع دوليًا والحقوق المعنية». لقد جاء هذا المبدأ متوافقًا مع ما قرّرته محكمة التحكيم الدولية في قضية «ناوليلا» والتي نص حكمها على إنه: «حتى لو قبلنا جدلًا بأن القانون يجيز التدابير الانتقامية كأعمال مشروعة، إلّا أنه لا بد لنا مع ذلك ألَّا نغفل عن عدم شرعيتها إذا كانت مفرطةً أو أنّها لا تتناسب والفعل الدافع لها» [120].

(120) المرجع السابق الإشارة إليه.

الخـاتمـة :

هذه الدراسة جاءت لتلقي جانب الحق التقليدي في الدفاع الشرعي الوارد في المادة 51 من ميثاق الأمم المتحدة، ولتحدد فيما إذا كانت العمليات السيبرانية المعادية تُعطي حقًّا للدولة المعتدى عليها استخدام حقّها في اللجوء إلى التدابير المضادة في إطار مشروع مواد المسؤولية الدولية عن الأعمال غير المشروعة دوليًا. فمن المعلوم أنّه ينضوي تحت قواعد المسؤولية الدولية بندٌ خاصٌّ بالإجراءات المضادة التي يُمكن اللجوء إليها، ومفادها تمكين الدول المتضررة من مخالفة دولية ما بإتيان سلوك، أو الانتهاء عن سلوك واجب، ضد دولة تسببت بضرر ما، وإرغامها على الرضوخ والعدول عن مخالفتها لالتزاماتها الدولية.

وألقت هذه الدراسة الضوء على الشروط الواجب توافرها قبل نشوء حق الدول للّجوء لتلك التدابير المضادّة للهجمات السيبرانية، بغية إثبات أن اللجوء لهذه التدابير له فوائد جمّة يمكن التعويل عليه كرد مناسب للاعتداءات الدولية التي لا ترقى لأن تتصف بأنها اعتداء عسكري، بيد أنها لا تبدو كذلك من الناحية العمليّة لوجود عدد من الأسباب التي تحد من الاستخدام الأمثل لها وقت الحاجة.

ففي أكثر الحالات، لا ترقى الكثير من العمليات السيبرانية المعادية ـ بالرغم من أثرها المباشر على زعزعة الأمن الدولي ـ إلى مصاف العمليات «العسكرية» المعادية بوصفها المذكور في المادة 51 من ميثاق الأمم المتحدة، والسماح بالرد العسكري له محاذيره الخاصّة به أقلّها أن تتفاقم الاختلافات الدولية إلى مزيد من عدم الاستقرار، وإلى غياب السلم الدولي، أمّا التدابير المضادّة ففيها ميزة استدراك الوضع المتأزّم بين الدول والوصول إلى حالة أفضل من العلاقات الدولية، حيث إن هذه التدابير، وإن أتت كرد على فعل دولي غير مشروع، فإنّ المغزى منها هو تصويب الوضع القائم بحيث تقوم الدولة المتضررة بما يجب لضمان الكف عن هذا الفعل الضار، ثم جبر الضرر حيثما أمكن. لذلك، تعد التدابير المضادة نظامًا تحاول بواسطته الدول المتضررة إثبات حقوقها واستعادة العلاقة القانونية بالدولة المسؤولة، وهي علاقة قُطعت بسبب الفعل غير المشروع دوليًا.

وبيّنت هذه الدراسة أنّ للتدابير المضادّة شروطًا ومحاذير وحدود خاصّة بها، فلا يمكن اللجوء للتدابير المضادّة إلّا في مواجهة تصرف دولي خارجي غير قانوني،

ويجب في هذه التصرفات غير القانونية أن يتوافر بها مكوّنان أساسان: أولًا، خرق لالتزام دولي في حق دولة أخرى، وثانيًا، وجود رابطة واضحة بين التصرف غير القانوني والدولة التي يُزعم بأنه نشأ عنها، وهي الشروط ذاتها الخاصّة بنشوء المسؤولية الدولية بين دولة مسؤولة عن الضرر ودولة أخرى هي متضررة. لذلك، يأتي شرط الإسناد ماثلًا كي يقلّص من إمكانية اللجوء لهذه التدابير، فلا تدابير دون أن يتّسم أطراف النزاع بصفة الدولة، فلا تُسند جميع أعمال الشركات المملوكة للدولة لها بمجرّد ثبوت هذه الملكيّة، فعلى سبيل المثال، لا يكفي مجرّد ثبوت ملكية الدولة لشركة اتصالات ما أو مؤسسة معلومات تقنيّة أن تُسند جميع تصرفاتها للدولة ذاتها، وبالتالي ليس للدولة المتضررة من تصرفات هذه الشركات الحق للجوء إلى تدابير احترازية بحقّ الدولة إلّا إذا ثبت أن تلك الشركة تصرفت كمرفق حكومي أو كممثل للدولة، أو أنها قامت بتصرفاتها المخالفة برعاية، أو سيطرة، مباشرة من الدولة.

وينتج عن هذه الحدود نتائج لا بد من إدراكها، فلا يكون من قبيل التدابير المضادّة إذا كان اتخاذها سيفاقم المشكلة، وإلّا يكون اتخاذها بمثابة الانتقام، ولأن الهدف من التدابير المضادّة هو إرجاع العلاقات إلى المشروعية بين الدول، فإنّه لا يجوز اللجوء إليها استباقًا، ثم أنّه لا يجوز اللجوء إلى التدابير المضادّة كوسيلة من الوسائل الرادعة أو التأديبية، وبالتالي لا يجوز استخدامها في مواجهة ما تم وانتهى من أخطاء اقترفتها دولة أخرى ولا يُتوقّع تكرار الخطأ ذاته من جانبها، بل ويتوجب التوقف عن التدابير المضادة المتّخذة فور ثبوت توقف الدولة المعتدية عن اعتدائها وتحقيقها لالتزاماتها الدولية، ويجب التوقّف عن التدابير المضادّة في حالة عرض النزاع على جهة قضائية دولية.

كما بيّنت هذه الدراسة أن هناك شروطًا إجرائية يجب إتباعها في التدابير المضادّة منها أن يُطلب من الدولة المعتدية تصويب الإخلال قبل لجوئها للتدابير المضادّة، بل ويتوجّب على الدولة المتضررة، قبل استخدامها حقّها باتخاذ تدابير مضادة، أن تقوم بالتواصل مع الدولة المتسببة بالضرر لتطلب منها وقف سلوكها الخاطئ، فلا بد من أن يُطلب من الدولة المسؤولة الوفاء بالتزاماتها، ولا بد من إخطارها بأي قرار باتخاذ تدابير مضادة، ولا بد من أن يُعرض عليها التفاوض.

وأخيرًا بيّنت هذه الدراسة أنّه لا بد في التدابير المضادّة من الانتباه لمبدأ التناسب في استخدامها حتى تكون مشروعة، إذ يجب أن تتناسب التدابير المضادة مع الضرر المتكبد، على أن توضع في الاعتبار جسامة الفعل غير المشروع دوليًا والحقوق المعنية.

ومما تقدّم، يمكن التوصل للنتائج التالية:

1 – لا ترقى الكثير من العمليات السيبرانية المعادية إلى مصاف العمليات «العسكرية» المعادية بوصفها المذكور في المادة 51 من ميثاق الأمم المتحدة.

2 – السماح بالرد العسكري له محاذيره الخاصّة به أقلّها أن تتفاقم الاختلافات الدولية إلى مزيد من عدم الاستقرار، وإلى غياب السلم الدولي.

3 – التدابير المضادّة فيها ميزة استدراك الوضع المتأزّم بين الدول والوصول إلى حالة أفضل من العلاقات الدولية.

4 – هناك شروط إجرائية يجب إتباعها في التدابير المضادّة منها أن يُطلب من الدولة المعتدية تصويب الإخلال قبل لجوئها للتدابير المضادّة.

5 – ويتوجّب على الدولة المتضررة، قبل استخدامها حقّها باتخاذ تدابير مضادة، أن تقوم بالتواصل مع الدولة المتسببة بالضرر لتطلب منها وقف سلوكها الخاطئ، فلا بد من أن يُطلب من الدولة المسؤولة الوفاء بالتزاماتها، ولا بد من إخطارها بأي قرار باتخاذ تدابير مضادة، ولا بد من أن يُعرض عليها التفاوض.

6 – لا بد في التدابير المضادّة من الانتباه لمبدأ التناسب في استخدامها حتى تكون مشروعة، إذ يجب أن تتناسب التدابير المضادة مع الضرر المتكبد، على أن توضع في الاعتبار جسامة الفعل غير المشروع دوليًا والحقوق المعنية.

7 – ولأن الهدف من التدابير المضادّة هو إرجاع العلاقات إلى المشروعية بين الدول، فإنّه لا يجوز اللجوء إليها استباقًا.

8 – لا يجوز اللجوء إلى التدابير المضادّة كوسيلة من الوسائل الرادعة أو التأديبية، وبالتالي لا يجوز استخدامها في مواجهة ما تم وانتهى من أخطاء اقترفتها دولة أخرى، ولا يُتوقّع تكرار الخطأ ذاته من جانبها.

9 – يتوجب التوقف عن التدابير المضادة المتّخذة فور ثبوت توقف الدولة المعتدية عن اعتدائها وتحقيقها لالتزاماتها الدولية، ويجب التوقّف عن التدابير المضادّة في حالة عرض النزاع على جهة قضائية دولية.

10 – المغزى من التدابير ما هو الّا تصويب لوضع قائم بحيث تقوم الدولة المتضررة بما يجب فقط لضمان الكف عن هذا الفعل الضار، ثم جبر الضرر حيثما أمكن.

11 – تعد التدابير المضادة نظامًا تحاول بواسطته الدول المتضررة إثبات حقوقها واستعادة العلاقة القانونية بالدولة المسؤولة، وهي علاقة قُطعت بسبب الفعل غير المشروع دوليًا.

12 – لا بد أن يقوم المجتمع الدولي ولجنة القانون بالأمم المتحدة بدراسة ظاهرة الهجمات السيبرانية بشكل أكثر توسعاً ووضع قواعد قانونية لها أكثر وضوحاً وصرامة.

المراجـع:

المراجع باللغة الأجنبية:

1 - A. F. Lowenfeld, International Economic Law (Oxford, Oxford University Press, (2002).

2 - C. Bronk & E. Tikk-Rigas, The Cyber Attack on Saudi Aramco, SURVIVAL, Apr–May 2013.

3 - C. C Joyner, "Boycott", Max Planck Encyclopedia of Public International Law (Oxford University Press, 2011), available from: www.mpepil.com.

4 - D.E. Sanger & J. Markoff, After Google's Stand on China, U.S. Treads Lightly, N.Y. TIMES (Jan. 15, 2010), at: http://www.nytimes.com/201015/01//world/asia/15diplo.html?_r=0.

5 - D. E. Sanger, D. Barboza & N. Perlroth, Chinese Army Unit is Seen as Tied to Hacking Against U.S., N.Y. TIMES, Feb. 18, 2013, at: http://www.nytimes.com/201319/02//technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html?pagewanted=all.

6 - Diego Rafael Canabarro and Thiago Borne,"Reflection on the fog of Cyber War", National Center for Digital Government, Policy working Paper No. 13:001, March 1, 2013.

7 - Eshel, David,, "Israel adds cyber-attack to IDF", Aviation Week's DTI, 9 Feb. 2010: http://infosecisland.com/blogview/5160-Analysis-on-Defense-and-Cyber-Warfare.html.

8 - E. Tikk, K. Kaska & L. Vihul, International Cyber Incidents: Legal Consideration (2010).

9 - H. Tsukayama & P. Farhi, Syrian Hackers Claim Responsibility for Disrupting Twitter, available at: http://www.washingtonpost.com/lifestyle/style/syrian-hackers-claim-responsibility-for-hacking-twitter-new-york-times-website/201320500/27/08/f580-f5c-11e3-bdf6-e4fc677d94a1_story.html.

10 - Int'l L. Comm'n, Responsibility of International Organizations, U.N. Doc. A/CN.4/L.778.

11 - J. Boone, Mercenary Hacker Group 'Hidden Lynx' Emerges as World's Most Potent Cyber Threat, GLOBALPOST (Sept. 18, 2013,), available at: http://www.globalpost.com/dispatches/globalpost-blogs/the-grid/hacker-mercenary-group-china-hidden-lynx-worlds-most-potent-cyber-threat.

12 - J. Crawford, The International Law Commission's Articles on State Responsibility: Introduction, Text and Commentaries, 178–86 (2002).

13 - Jonathan A. Ophard, "Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield", DUKE Law & Technology Review, No. 3.

14 - Kenneth Grees, Darien Kindlind, Ned Moran, Rob Rachwald,"World War C: Understanding Nation-States Motives behind Today's Advanced Cyber Attaches". Fire Eyes report, at: https://www.fireeye.com/resources/pdfs/fireeye-wwc-report.pdf.

15 - K. Saalbach,»Cyber War, Methods and Practice», Version 9.0, University of Osnabruck, 17 Jun 2014.

16 - M. Ruffert, Reprisals, 8 Max Planck Encyclopedia of Public International Law, 927 (2012).

17 - M. P. Doxey, International Sanctions in Contemporary Perspective (Basingstoke, Palgrave Macmillan, 1996).

18 - M. Fisher, South Korea Under Cyber Attack: Is North Korea Secretly Awesome at Hacking?, at: http://www.washingtonpost.com/blogs/worldviews/wp/201320/03//south-korea-under-cyber-attack-is-north-korea-secretly-awesome-at-hacking/.

19 - M. C. Waxman, Self-defensive Force Against Cyber Attacks: Legal, Strategic and Political Dimensions, 89 INT'L L. STUD. 109 (2013).

20 - M. N. Schmitt, Cyber Operations and the Jus ad Bellum Revisited, 56 VILL. L. REV. 569, 586–603 (2011).

21 - M. J Gross, Enter the Cyber-Dragon, VANITY FAIR, Sept. 2011, at: http://www.vanityfair.com/culture/features/201109//chinese-hacking-201109.

22 - M. Kamto, The Time Factor in the Application of Countermeasures, in The law of International Responsibility, 1169 (James Crawford et al. eds., 2010).

23 - Michael Shmidt, "Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law, 3 Virginia Journal of International Law, vol. 54.

24 - N. Perlroth, Washington Post Joins List of News Media Hacked by the Chinese, N.Y. TIMES, Feb. 1, 2013, at: http://www.nytimes.com/201302/02//technology/washington-posts-joins-list-of-media-hacked-by-the-chinese.html

25 - Oona` A.Hathway , Rebecca Crootof , Philip Levtiz , aley Nix, Aileen Nowlan ,William Perdue and Julia Spiegel, «The Law of Cyber –Attack», California Law Review, 2012.

26 - S. Gorman & D. Yadron, Iran Hacks Energy Firms, U.S. Says, WALL ST. J., at: http://online.wsj.com/news/articles/SB10001424127887323336104578501601108021968

27 - S. Gorman, China Hackers Hit U.S. Chamber, WALL ST. J., Dec. 21, 2011, at: http://online.wsj.com/news/articles/SB10001424052970204058404577110541568535300

28 - T. G. Retorsion, 8 MAX PLANCK ENCYCLOPEDIA OF INTERNATIONAL LAW 976 (2012).

29 - W. Schwartau, Striking Back, Network World Fusion, at: http://www.networkworld.com/news/0111vigilante.html

30 - Y. Dinstein, Computer Network Attacks and Self-Defense, 76 INT'L L. STUD. 99 (2002).

31 - Y. Lee, South Korea Says North Korea Behind Computer Crash In March, HUFFINGTON POST (Apr. 10, 2013), at: http://www.huffingtonpost.com/201310/04//north-korea-cyberattack_n_3050992.html.

32 - Scott J. Shackelford, «Analogizing Cyber: from Nuclear War to Net War Attacks in International Law".

33 - Scoot Shckelford, ,» State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem», University of Cambridge, Department of politics and International Studies, Cambridge, UK, 2009.

34 - Shin, Beomchul,» The Cyber Warfare and the Right of Self –Defense: Legal Perspectives and the Case of the United States, IFANS, Vol.19, No1, June 2011.

35 - S. Stalinsky, China Isn't the Only Source of Cyberattacks, WALL ST. J. (May 21, 2013), at: http://online.wsj.com/news/articles/SB10001424127887324744104578475571183053736

36 - Thomas W. Smith,» The New Law of War: Legitimizing Hi-Tech and Infrastructural,» International Studies Quarterly, 2002, Vol. 46.

37 - Zach West, Young Fella, If You're Looking for Trouble I'll Accommodate You: Deputizing Private Companies for the Use of Hackback, 63 SYRACUSE L. REV. 119 (2012).

38 – أحمد عيسى نعمة الفتلاوي، الهجمات السيبرانية: مفهومها والمسئولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي ، كلية القانون ، جامعة بابل 2015.

39 – د. السيد أبو عطية، الجزاءات الدولية بين النظرية و التطبيق، مؤسسة الثقافة الجامعية، الإسكندرية 2001

المراجع الالكترونية المستخدمة:

1 – النسخة العربية من مشروع المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دوليًا، 2002، السجلات الرسمية للجمعية العامّة، الدورة السادسة والخمسون، الملحق رقم ١٠ (A/56/10)، الفصل الرابع، الفقرة 76:

http://www.un.org/arabic/documents/GADocs/56/A_56_589.pdf

2 – مدوّنة مبادئ تالين» الإرشادية الخاصّة بالقانون الدولي المستخدمة في الحروب السيبرانية:

https://www.usnwc.edu/getattachment/Departments---Colleges/International-Law/Tallinn-Manual/Tallinn.pdf.aspx

3 - http://www.aljazeera.net/programs/infocus/201517/5//

4 - http://www.al-sharq.com/news/details/383883#.VkNnnl_XeJJ

5 - https://blog.cyberkov.com/270.html

قائمة بالقضايا المشار إليها بالبحث:

1 – قضية البوسنة وصربيا لعام 2007 (I.C.J. 43, 403–05).

2 – قضية الأنشطة المسلّحة في الكونغو بين الولايات المتحدة الأمريكية والكونغو (I.C.J. 168, 147, 2005). فتوى محكمة العدل الدولية في قضية حائط الفصل العنصري (I.C.J. 136, 140, 2004).

3 – قضية موانئ البترول بين أمريكا وإيران

(Iran v. U.S., I.C.J. 161, 74, 6 Nov. 2003)

4 – قضية الادعاء العام ضد تادتش في محكمة يوغسلافيا

(Case No. IT-94-1-A, Appeals Chamber Judgment, 117, 131–40, 145) 1999 .

5 – قضية مشروع غابتشيكوفو– ناغيماروس بين هنجاريا وسلوفاكيا

Gabcikovo-Nagymaros Project (Hungary/Slovakia), ICJ 97 Judgment، of 25 September 1997

6 – فتوى محكمة العدل الدولية بخصوص مدى قانونية التهديد باستخدام السلاح النووي (ICJ Advisory Opinion, I.C.J. 226, 38, 41, 8 July 1996).

7 – قضية إيجر ضد إيران عام 1987 (Yeager v. Iran, 17 Iran-U.S. Cl. Trib. Rep).

8 – قرار محكمة العدل الدولية في قضية نيكاراجوا

(Nicaragua v. U.S., I.C.J. 14, 176, 27 June 1986).

9 – القضية الخاصّة باتفاقية الخدمات الجويّة 27 مارس 1946 بين الولايات المتحدة الأريكية وفرنسا، قرار تاريخ 9 ديسمبر

(UNRIAA, vol. XVIII - Sales No. E/F.80.V.7) 1978

10 – قضية الدبلوماسيين الأمريكيين في طهران (I.C.J. 3 1980).

11 – قضية كورفو والبانيا وبريطانيا (I.C.J. 4, 23 1949).

12 – قضية فوسفات المغرب

(Preliminary Objections, 1938 P.C.I.J., ser. A/B, No. 74).

13 – قضية Caire Claim بين فرنسا والمكسيك (, 19295 R.I.A.A. 516)

14 – قضية مستعمرات البرتغال، حادثة نوليلا (UNRIAA, vol. II, 1928).

15 – قضية جزيرة بالماس بين هولندا والولايات المتحد الأمريكية

(R.I.A.A. 829, 838 - Perm. Ct. Arb. 1928 2).

16 – قضية مصنع شورزو بين المانيا وبولندا (P.C.I.J, ser. A, No. 9 1927).

17 – قضية ويمبلدون بين بريطانيا وفرنسا (P.C.I.J, ser. A, No. 1 1923).

18 – قضية Massey claim عام 1927 (R.I.A.A. 155 4)

قائمة بالاتفاقيات المشار إليها بالبحث:

1 – ميثاق الحقوق الأساسية للاتحاد الأوروبي لعام 2000 (O.J., C364).

2 – اتفاقية الأمم المتحدة للبحار لعام 1982 (U.N.T.S. 397 1833).

3 – اتفاقية فينا لقانون المعاهدات (1969, U.N.T.S. 331 1155).

4 – اتفاقية فينا للحصانة القنصلية لعام 1963 (U.N.T.S. 261 596).

5 – معاهدة حماية الحقوق والحريات لعام 1950 (U.N.T.S. 221 213).

6 – اتفاقية جنيف الأولى لعام 1949 (U.N.T.S. 31 75).

7 – اتفاقية جنيف الثانية 1949 (U.N.T.S. 85 75).

8 – اتفاقية جنيف الثالثة لعام 1949 (U.N.T.S. 135 75).

9 – اتفاقية جنيف الرابعة لعام 1949 (U.N.T.S. 287 75).

10 – اتفاقية الملاحة الجويّة الدولية لعام 1944 (U.N.T.S. 295 15).

11 – اتفاقية جنيف لعام 1929 (L.N.T.S. 303 118).

المحتوى: