مجلة جامعة الشارقة للعلوم القانونية

**اسم المقال:** حق الدفاع عن النفس نتيجة الهجمات الإلكترونية في ضوء قواعد القانون الدولي العام
**اسم الكاتب:** رزق أحمد سمودي
**رابط ثابت:** https://political-encyclopedia.org/index.php/library/8312
**تاريخ الاسترداد:** 2026/11/02 06:19 +03

الموسوعة السياسيّة هي مبادرة أكاديمية غير هادفة للربح، تساعد الباحثين والطلاب على الوصول واستخدام وبناء مجموعات أوسع من المحتوى العلمي العربي في مجال علم السياسة واستخدامها في الأرشيف الرقمي الموثوق به لإغناء المحتوى العربي على الإنترنت.
لمزيد من المعلومات حول الموسوعة السياسيّة – Encyclopedia Political، يرجى التواصل على info@political-encyclopedia.org

استخدامكم لأرشيف مكتبة الموسوعة السياسيّة – Encyclopedia Political يعني موافقتك على شروط وأحكام الاستخدام المتاحة على الموقع https://political-encyclopedia.org/terms-of-use

تم الحصول على هذا المقال من موقع مجلة جامعة الشارقة للعلوم القانونية ورفده في مكتبة الموسوعة السياسيّة مستوفياً شروط حقوق الملكية الفكريّة ومتطلبات رخصة المشاع الإبداعي التي ينضوي المقال تحتها.

جامعة الشارقة
ملتقى الحضارات

# مجلة جامعة الشارقة

دورية علمية محكمة

## للعلوم القانونية




المجلد 15، العدد 2
ربيع الثاني 1440 هـ / ديسمبر 2018 م

الترقيم الدولي المعياري للدوريات 2616-6526

# حق الدفاع عن النفس نتيجة الهجمات الإلكترونية في ضوء قواعد القانون الدولي العام


## رزق أحمد سمودي

كلية الحقوق - الجامعة العربية الأمريكية

جنين - فلسطين



**تاريخ الاستلام: 12-02-2018** **تاريخ القبول: 27-03-2018**



## ملخص البحث:

من أبرز القضايا التي خلفتها القدرات التكنولوجية الحديثة أنها قد أفرزت أسئلة قانونية جديدة ومعقدة أكثر من إفرازها إجابات بخصوص العلاقة بين الدول، حيث كانت تلك الأسئلة غير مسبوقة وغير متصورة إلى عهد ليس ببعيد، وأبرز هذه الأسئلة يتمثل في السبل القانونية المتاحة أمام الدولة للتعامل مع الحالة التي تتعرض فيها إلى اعتداء إلكتروني (غير حركي) منشأه دولة أخرى. وبالتحديد تتمحور المسألة حول مدى ملاءمة القواعد القانونية التقليدية الخاصة باستخدام القوة وبالدفاع عن النفس واستيعابها لفكرة الاعتداءات الإلكترونية.فهل يمكن للهجمة الإلكترونية أن تحقق المؤهلات القانونية الخاصة بالدفاع عن النفس حسب ما تقضي به المادة 51 من ميثاق الأمم المتحدة؟ أم هي مجرد استخدام للقوة في إطار المادة 2(4) من الميثاق، وبالتالي تضع الدولة المعتدى عليها أمام خيارات قانونية ما دون الدفاع عن النفس؟ أم أن هنالك نهجا آخر للتعامل مع الهجمات الإلكترونية؟ تسعى هذه الورقة وراء إجابات قانونية لهذه الأسئلة المحورية، من خلال مراجعة لقواعد القانون الدولي العام المتعلقة باستخدام القوة عموما، والدفاع عن النفس خصوصا والربط بينهما، وأيضا تتطرق الورقة إلى الممارسات المعاصرة للدول سعيا لاستشراف العرف الدولي بهذا الخصوص.



**الكلمات الدالة:** الهجوم غير الحركي، الهجمات الإلكترونية، دليل تالين، الأسلوب الوظيفي، الأسلوب الدلالي.

## مقدمة:

لقد أفرز التطور التكنولوجي المتسارع العديد من الأسئلة القانونية الشائكة التي لابد للدول من مواجهتها والتعامل معها بطريقة ما، أبرز هذه المسائل تتمثل في القدرة المتنامية -غير المسبوقة- على استخدام الوسائل التكنولوجية الإلكترونية في التعرض للأنظمة الإلكترونية في الدول الأخرى، مما يتسبب بالضرر لهذه الأخيرة، دون أن تكون الدولة الأولى قد قامت بأي تصرف حركي «Kinetic»، والذي يعني عدم استخدامها لأي من القطع العسكرية للقيام بهذا الاعتداء.

على سبيل المثال في 27 ابريل من العام 2007 أفاقت دولة استونيا على هجوم إلكتروني شامل استهدف المواقع الإلكترونية الحكومية والبرلمانية، إضافةً إلى المواقع الإلكترونية التابعة للبنوك وتلك الخاصة بالصحف الأستونية، حيث تسبب هذا الهجوم بانقطاع الخدمة على تلك المواقع. وفي حادثة أخرى في حزيران من العام 2010 تم التعرف على برنامج فيروسي أطلق عليه اسم «Stuxnet»، وهو برنامج غاية في التعقيد يهدف إلى مهاجمة أنواع محددة من أجهزة الحاسوب ذات خصائص محددة، وبعد اكتشافها أصبح هناك شبه إجماع بين الخبراء على أن هذا البرنامج قد صمم من لدن إسرائيل والولايات المتحدة خصيصا لمهاجمة البرنامج النووي الإيراني، تحديدا لمهاجمة الحواسيب المرتبطة بعملية تخصيب اليورانيوم، بحيث يعمل البرنامج على إعطاء أوامر خاطئة لأجهزة الطرد المركزي بحيث تسرع وتبطئ من عملها بوتيرة لا منهجية، مما يؤثر سلبا في فعالية تلك الأجهزة. يضاف إلى هذه الأمثلة ما يدور من حديث حول تدخل روسيا في الانتخابات الأمريكية الأخيرة التي جرت في العام 2016 والتي كانت تهدف روسيا من خلالها إضعاف أحد مرشحي الرئاسة الأمريكية وهي هلري كلنتون لمصلحة مرشحين آخرين في الحزب الجمهوري ومنهم الرئيس الحالي للولايات المتحدة دونالد ترامب. وهذه أمثلة واقعية على القدرة على تنفيذ هجمات إلكترونية وقعت داخل الدول من أطراف خارجية. وأبعد من ذلك، يمكن لنا أن نتخيل أن تقدم دولة معينة على هجوم إلكتروني لتخترق من خلاله نظام الطيران لدى دولة أخرى وتعمل على تعطيله، أو تعطي أوامر خاطئة للطائرات، ويمكن لنا أن نتخيل اختراقا مماثلا لأنظمة السدود لدى دولة معينة، في هذين المثالين المتخيلين يمكن أن يتسبب كل واحد منهما بأضرار للدولة «المعتدى عليها» قد تكون خارجة عن نطاق التصور.

وإذا كانت حقيقة واقعة أن الدولة وبحكم التطور التكنولوجي تمتلك كل تلك الإمكانات، فإن السؤال الحتمي يتمحور حول ما تمتلكه الدولة «المعتدى عليها» بواسطة وسائل إلكترونية من خيارات قانونية للتعامل مع اعتداء من هذا النوع؟ وتنبع أهمية الإجابة على هذا التساؤل من حقيقة أن الاعتداء الإلكتروني بذاته ذو طبيعة مميزة ويتصف بعدم الحركية

«non kinetic»،وهو ما كان خارجا عن تصور الدول عند توقيعها على الاتفاقات الدولية التي تعالج-على سبيل المثال- الحق في الدفاع عن النفس، وعلى وجه التحديد ميثاق الأمم المتحدة في المادة 51، واتفاقية حلف شمال الأطلسي في المادة الخامسة[1].

لذلك سوف تحاول هذه الورقة البحثية تفحص الخيارات القانونية -إن وجدت- أمام «الدولة المعتدى عليها» بواسطة وسائل إلكترونية، وفي هذا الإطار سوف تقسم هذه الورقة إلى مجموعة من المباحث، كل منها سوف يقدم مساهمته الخاصة في الإجابة عن هذا السؤال المحوري. ففي المبحث الأول تتعرض الورقة إلى القواعد التقليدية في القانون الدولي العام التي تعالج فكرة الاعتداء و الدفاع عن النفس بالاستناد إلى المادة 51 من ميثاق الأمم المتحدة، وفي المبحث الثاني سيتم التعرض إلى فهم شامل لفكرة الهجمات الإلكترونية من خلال تعريف الهجمات الإلكترونية ومن ثم تمييزها عن مجموعة من النشاطات الإلكترونية التي يمكن أن تلتبس بها، مثل الجرائم الإلكترونية والحرب الإلكترونية، وبعد ذلك تتعرض هذه الورقة في المبحث الثالث إلى جوهر موضوعها والذي يتمثل في مدى ملاءمة القواعد التقليدية المصممة للدفاع عن النفس انطلاقا من المادة 51 في مواجهة الهجمات الإلكترونية، وكل ذلك سوف يتم من خلال مراجعة الاتفاقات الدولية ذات العلاقة باستخدام القوة والدفاع عن النفس، وكذلك لقواعد العرف الدولي ورأي محكمة العدل الدولية بهذا الخصوص، في هذا الإطار تتطرق الورقة إلى دليل تالين «Tallinn Manual»، والذي يمثل جهدا أكاديميا متميزا لمجموعة من الخبراء في مجال القانون الدولي والمسائل التكنولوجية المعاصرة، ومدى انطباق قواعد القانون الدولي عليها، في المبحث الرابع تعرج الورقة على ممارسات الدول بخصوص طريقة الرد على الهجمات الإلكترونية وأيضا ثم رأي الفقه الدولي في هذه المسألة وصولا إلى فهم شامل لهذه المسألة.

## اشكالية البحث:

تتمثل إشكالية هذا البحث في فهم معالم قواعد القانون الدولي العام المتعلقة بالدفاع عن النفس. وسيقوم البحث بمحاولة فهم فيما إذا كانت هذه القواعد تتسع لظاهرة الهجمات الإلكترونية تحديدا في ضوء غياب قواعد قانونية دولية ملزمة تعالج مسألة الهجمات الإلكترونية وأيضا في ضوء عدم بروز معالم واضحة لقواعد العرف الدولي حول هذه المسألة بالتحدد.

(1) انظر في الأقسام التالية من هذه المساهمة حيث سيتم التطرق إلى هاتين المادتين والنقاش الدائر حولهما.

## المنهجية:

سوف يتبع هذا البحث المنهج الوصفي التحليلي المقارن لما عليه الحال بشأن الهجمات الإلكترونية. في هذا الإطار سوف يتم إدراج مجموعة من النصوص القانونية الدولية الخاصة باستخدام القوة والدفاع عن النفس ومقاربتها مع فكرة الهجمات الإلكترونية. سيتطرق البحث أيضا إلى وثائق دولية ذات قيمة خاصة في مسألة الهجمات الإلكترونية أهمها «دليل تالين» بنسخته الأولى والثانية وفهم موقفها وتحليلها ومقارنتها مع القواعد القانونية الدولية المستقرة بخصوص الدفاع عن النفس وأيضا فقه محكمة العدل الدولية النابع من العديد من الأحكام سواء الملزمة أو الاستشارية الصادرة عن المحكمة متوخياً نتائجَ ذات قيمة قانونية مهمة في إطار الهجمات الإلكترونية.

## المبحث الأول:

## استخدام القوة والدفاع عن النفس في ضوء قواعد القانون الدولي العام/ الموقف التقليدي

يعتبر حظر استخدام القوة أو التهديد باستخدامها بين الدول الوارد في المادة 2(4) من ميثاق الأمم المتحدة مبدأ أساسيا من مبادئ القانون الدولي العام، وقد تطور هذا المبدأ ليصبح عرفا دوليا وفقا لما جاءت به محكمة العدل الدولية في حكمها في قضية «النشاطات العسكرية وشبه العسكرية في و ضد نيكاراغوا» لعام 1986[1]، حيث ينطلق فهم هذا المبدأ من المادة 2(4) من ميثاق الأمم المتحدة والتي تنص على أنه «على جميع الأعضاء في علاقاتهم أن يتخلصوا من التهديد باستخدام أو استخدام القوة ضد سلامة الإقليم أو الاستقلال السياسي لأي دولة، أو في أي حالة أخرى تتعارض مع مبادئ الأمم المتحدة»[2].

إن موقع هذه المادة من الميثاق - بمجيئها ضمن مبادئ الميثاق- والتركيبة اللغوية القوية التي جاءت بها تشير إلى مركزيتها في الميثاق لغايات الوصول إلى رؤية منظمة الأمم المتحدة في تحقيق الأمن والسلم الدوليين، من خلال عدم التهديد أو استخدام القوة. واستنادا إلى ذلك أصبحت وجهة النظر السائدة حول هذه المادة أنها قد خلقت «حظرا عاما» على استخدام القوة أو التهديد بها في سياق العلاقات بين الدول.

(1) Judgment of the International Court of Justice in Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States), 1986, I.C.J. 14, 96-97; See also, Malcolm Shaw, International Law, (7th edition, 2014), Cambridge University Press; Yoram Dinstein, War, Aggression and Self-defence (3ed edition 2011).

(2) ميثاق الأمم المتحدة، 1945، المادة 2(4) .

بالرغم من ذلك فإن هذا الحظر العام لاستخدام القوة أو التهديد بها ليس مطلقا، حيث إن بنود الميثاق أجازت استخدام القوة في حالتين استثنائيتين أوردهما الميثاق استنادا إلى ذيل المادة 2(4) والتي بمفهوم المخالفة تجيز استخدام القوة في الحالات التي لا تتعارض مع مبادئ الأمم المتحدة، وهذان الاستثناءان هما أولا: حالة الأمن الجماعي وفقا لقرار يصدر عن مجلس الأمن بالاستناد إلى المادة 42 من الميثاق،[1] وثانيا: حالة الدفاع الفردي أو الجماعي عن النفس وفقا للمادة 51 من الميثاق.

بعيدا عن الحالة الأولى يتمحور اهتمام هذا القسم من البحث حول فهم الحالة الثانية انطلاقا من المادة 51 والتي تبث في الدول قدرة قانونية لاستخدام القوة في سياق الدفاع عن نفسها ضمن ظروف معينة مستمدة من المادة ذاتها، ومن القواعد الدولية العرفية التي سيتناولها الجزء التالي بالتفصيل.

## المطلب الأول:

## الدفاع عن النفس وفق المادة 51 من ميثاق الأمم المتحدة

تنص المادة 51 على أنه «لا يوجد في هذا الميثاق ما ينقص أو يضعف الحق الطبيعي للدول، بشكل فردي أو جماعي، في الدفاع عن النفس في الحالة التي تتعرض بها إلى اعتداء مسلح...».[2]

إن أبرز الشروط التي أوردتها هذه المادة - في حدود غرض هذا البحث- يتمثل في وقوع «اعتداء مسلح» على دولة ما حتى تتمكن هذه الأخيرة من استخدام القوة كرد على هذا الاعتداء.[3] إن أول ما يجب أن يثار في هذا السياق يتمثل في الاختلاف حول المصطلح المستخدم في المادة 51، وهو شرط الاعتداء المسلح لتفعيل الحق في الدفاع عن النفس، ومصطلح استخدام القوة أو التهديد بها حسب المادة 2(4).

ويلاحظ أن هاتين المادتين استخدمتا مصطلحات مختلفة كل منها يؤدي إلى خيارات قانونية متباينة أمام الدولة المعتدى عليها، ف «الاعتداء المسلح» يضع الدولة المعتدى

(1) See, Kamal Ahmad Khan, Use of Force and Human Rights under International Law, Athens Institute for Education and Research, Conference Paper Series BLE 2017-2205.

(2) ميثاق الأمم المتحدة، 1945، المادة 51.

(3) تجدر الإشارة إلى أن هنالك شروط أخرى تضمنتها المادة من اجل مباشرة حق الدفاع عن النفس وفقا للمادة منها شرط الضرورة والتناسب والفورية. أكدت على هذه الشروط محكمة العدل الدولية في قرارها في قضية نيكاراغوا 1986 وأيضا في رأيها الاستشاري في قضية التهديد باستخدام أو استخدام الأسلحة النووية 1996.

عليها أمام خيار استخدام القوة، حيث يقرأ استخدام القوة هذا في سياق الدفاع عن النفس الذي قد يكون فرديا أو جماعيا حسب المادة 51، أما «استخدام القوة أو التهديد بها» والذي لا يرقى إلى كونه اعتداءً مسلحا، فيضع الدولة المعتدى عليها أمام خيارات قانونية أخرى أبرزها الإجراء المضاد والذي يعطي الدولة المتضررة القدرة للرد على الاعتداء بطرق ما دون استخدام القوة.[1] الجدير ذكره أن فكرة الإجراء المضاد كخيار أمام الدولة المعتدى عليها والتي جاء النص عليها في المادة 22 من مشروع مواد مسؤولية الدول عن الأفعال غير المشروعة 2001 قد جاء مقيدا بمجموعة من الشروط أهمها شرط التناسب بين الخرق والخرق المقابل وهذا ما أكدت عليه محكمة العدل الدولية في قضية كوبسكوفو للعام 1997 [2].

وقد جاءت هذه التفرقة على اعتبار أن القانون الدولي قد وفر بعض الحماية للدولة التي تستخدم القوة في مواجهة دولة أخرى، عندما لا يرقى استخدام للقوة هذا إلى مستوى الاعتداء المسلح الفعلي[3]، وبالرغم من وضوح هذا الفرق في التعبيرات ونتائجه القانونية يبرز التعقيد عند رسم الخط الفاصل بين استخدام القوة والاعتداء المسلح، والذي قد يكون في كثير من الحالات ضبابيا غير واضح المعالم، خاصة وأن ميثاق الأمم المتحدة ذاته قد خلا من أي نص يوضح هذه الفرق، وبالرغم من ذلك، يمكن الاستهداء إلى معالم هذا الخط الفاصل من خلال العودة إلى قرار محكمة العدل الدولية في قضية نيكاراغوا، حين وصفت «الاعتداء المسلح» بأنه اخطر شكل من أشكال استخدام القوة، وفي هذا الخصوص، بينت المحكمة في هذا القرار أن المناوشات المسلحة على الحدود -مثلا- لا ترقى إلى مرتبة الاعتداء المسلح الذي من شأنه تفعيل خيار الدفاع عن النفس وفقا للمادة 51.[4]

وكررت محكمة العدل الدولية هذا الموقف في عام 2003 في قضية منصات النفط بين إيران والولايات المتحدة، والتي تمحورت حول حادثة قيام الولايات المتحدة بتدمير مجموعة من منصات النفط الإيرانية في منطقة الخليج لعام 1987 وفيما إذا كانت الولايات المتحدة مسؤولة عن هذا التصرف في ضوء اتفاقية الصداقة الموقعة بين البلدين في العام

(1) See, Omer Elegab, The Legality of Non-forcible Counter-measures in International Law (Oxford Monographs in International Law), 1988.

(2) ICJ, Case Concerning Gabčíkovo–Nagymaros Project (HUNGARYISLOVAKIA), 1997, paragraph 71.

(3) A. Randelzhofer, Article 51, in The Charter of the United Nations: A Commentary 661, 664 (B. Simma ed.) 1995.

(4) ICJ, case concerning *Military and Paramilitary Activities in and Against Nicaragua* (Nicaragua v. United States), Reports 1986, para. 191.

1955.[1] وفي ضوء ذلك يمكن لنا أن نتصور أن استخدام للقوة من قبل دولة معينة لا يرقى إلى اعتداء مسلح، مثل إطلاق النار على الحدود من دولة باتجاه دولة أخرى أو الاعتداء على المناطق المائية لدولة معينة، حيث إن هذه الأعمال تنطوي على استخدام للقوة، ولكنها لا ترقى إلى حالة الهجوم المسلح الذي يجيز الدفاع عن النفس وفقا للمادة 51.

إلى جانب ذلك جاء قرار الجمعية العامة للأمم المتحدة رقم 3314 لعام 1974 الخاص بتعريف العدوان مشترطا «الخطورة الكافية» (Sufficient Gravity) كأحد متطلبات الهجوم العسكري[2]، أما الفقه الدولي فقد كانت له اليد الطولى في تحديد هذا الخط الفاصل، وذلك يتجلى في مساهمات الفقيه الدولي «Jean-Pictet» حين جاء بمجموعة من المعايير أو المتطلبات لاعتبار الاعتداء هجوم عسكريا وهي النطاق والشدة والمدة الزمنية[3]، ويلاحظ أن هنالك عاملا مشتركا بين مجمل هذه التعريفات للهجوم العسكري وهو - باعتقادي- الغموض، إذ من الصعوبة بمكان في كثير من الحالات بناء على هذه التعاريف تحديد ما إذا كان استخدام معين للقوة يرقى إلى حد الهجوم المسلح. ولكن بالرغم من هذا الغموض، إلا أن هذه التعاريف تقود إلى نتيجة مفادها أن كل اعتداء مسلح في ضوء المادة 51 يعد في الوقت ذاته استخداما للقوة ولكن العكس غير صحيح؛ فالهجوم بالأسلحة الفتاكة مثلا يعد استخداما للقوة وهجوما مسلحا في آن واحد، وبالتالي يجيز تفعيل المادة 51 لأنها قد حققت الشرط الوارد في المادة.

وتجدر الإشارة إلى أن تفعيل المادة 51 واللجوء إلى الدفاع عن النفس في مواجهة هجوم مسلح لا يعني بأية حال أن الدولة التي تدافع عن نفسها غير مقيدة في طريقة رد الهجوم، بل على العكس من ذلك، لقد تضمنت قواعد العرف الدولي، إلى جانب المادة 51 من ميثاق الأمم المتحدة مجموعة من الشروط الواجب توافرها حتى يبقى التصرف متوافقا مع أحكام المادة، وهذه الشروط هي أولا: الضرورة، وثانيا: التناسب، وثالثا: الفورية[4].

أما شرط الضرورة فيقصد به الحالة التي تجبر فيها الدولة على اللجوء للدفاع عن النفس باستخدام القوة، حيث لم يعد اللجوء إلى «الطرق السلمية» لفض النزاع بحسب

(1) ICJ, case concerning *Oil Platforms*, (Islamic Republic of Iran v. United States of America), Reports 2003, para. 51.

(2) UN General Assembly Res. 3314 (XXIX), Definition of Aggression, Adopted 14 December 1974.

(3) Cited in: Jeffry Car, Inside Cyber Warfare, O'Reilly Media, Inc., 2011, p.114.

(4) أكدت على هذه الشروط محكمة العدل الدولية في قرارها في قضية نيكاراغوا 1986 وأيضا في رأيها الاستشاري في قضية الأسلحة النووية 1996.

الفصل السادس من الميثاق[1] خيارا، أو أن هذه الطرق قد تم اللجوء إليها ولكنها أثبتت عدم فعاليتها في مواجهة الدولة الأخرى[2]، ويضاف إلى ذلك أن شرط الضرورة قد جاء كمساحة إضافية للتأكد من نية الدولة المهاجمة والظروف التي تحيط بالهجوم، إذ خلال هذه المساحة الزمنية تعطى الدولة المعتدية فرصة إضافية يمكن أن تثبت خلالها -مثلا- أن الاعتداء لم يكن مقصودا وأنها لا تسعى إلى حرب مع الدولة الأخرى.

وأما التناسب فإن معناه يتجسد في مصطلح «الدفاع»، والذي يعني اتخاذ الإجراءات اللازمة والضرورية لرد الاعتداء وعدم تجاوزها، وهذا يتحقق في شبه التماثل بين الاعتداء والإجراءات المتخذة لرده من لدن الدولة المعتدى عليها، أو أن لا تتجاوز الإجراءات المتخذة الهدف التي يجب أن تسعى وراءه الدولة المعتدى عليها، وهو تحقيق الأمن والسلم الدوليين[3]، أما شرط الفورية فيقصد به أساسا أن لا تفوت الدولة المعتدى عليها فترة زمنية طويلة على الاعتداء قبل أن تقوم باتخاذ إجراءات الدفاع عن النفس، لأنه في هذه الحالة سوف ينتفي المنطق من إعطاء الدولة الحق في الدفاع عن نفسها دون اللجوء إلى مجلس الأمن صاحب السلطة الأساسية في حفظ الأمن والسلم الدوليين[4]. بالرغم من ذلك يمكن لهذه الفترة الزمنية أن تمتد بصورة معقولة، وفي هذا تحقيق لشرط الضرورة آنف الذكر، والذي يوجب على الدولة المعتدى عليها التحقق من نية الدولة المعتدية، وتجدر الملاحظة أن شرط الفورية ينظر إليه بنوع من الخصوصية في سياق الهجمات الإلكترونية، حيث يمكن لهذه الفترة الزمنية أن تمتد، آخذين بعين الاعتبار خاصية جوهرية للهجمات الإلكترونية تتمثل في التعقيد الذي يكتنف عملية التحقق من مصدر الاعتداء.[5]

(1) تحديدا المادة 33 والتي حددت أن هذه الطرق تشمل المفاوضات والتحقيق والوساطة والتوفيق والتحكيم والوسائل القضائية بالإضافة إلى الوكالات الإقليمية.

(2) Lee Stuesser, Active Defense: State Military Response to International Terrorism, 17, California Western International Law Journal, 1987, p.31.

(3) Micheal Newton & Larry May, Proportionality in International Law, Oxford University Press, 2014; Arbitral Award in the Naulilaa Case 1928, 2 Reports of the International Arbitral Awards 1011-1028.

(4) Yoram Dinstein, Computer Network Attacks and Self-Defense, 76 U.S. Naval War College of International Law Studies (2002).

(5) انظر في ألأقسام الأخرى من هذه المساهمة حيث تم التعريج على هذه الخاصية والإفرازات القانونية الناتجة عنها.

## المبحث الثاني:

## الهجمات الإلكترونية - تقديم

جاءت مجموعة من الاتفاقات الدولية لكي تنظم حالة الحرب، سواء قواعد اللجوء إلى استخدام القوة «Jus ad Bellum» أو قواعد إدارة المعارك خلال حالة الحرب «Jus in Bello»، حيث تعاملت تلك الاتفاقات مع النطاق المكاني الذي يمكن أن تدار فيه حالة الحرب وهي الأرض، البحر، الجو، الفضاء[1]، إضافة إلى النطاق الزمني لهذه الحالة[2].

يرى بعضهم أن التقدم التكنولوجي والإنترنت قد أحدث ثورة أخرى في سياق نطاق المجال الذي تدار فيه المعارك حيث أضاف نطاق خامسا، لم يكن متصورا عند التوقيع على هذه الاتفاقات، يتمثل فيما أصبح معروفا بالمجال الإلكتروني أو الفضاء الإلكتروني «Cyber Space»، وهو مصطلح يعبر عن البيئة أو الوسط الذي يتم من خلاله التواصل بين أجهزة الكمبيوتر في أماكن مختلفة[3]، وإن أبرز ما يميز هذا المجال، في سياق هذا البحث، كوسيلة لاستخدام القوة أو إدارة المعارك هو أنه غير محسوس وغير حركي؛ حيث إن استخدام هذا الوسط من أجل إحداث خلل سواء بشكله الوظيفي أو التركيبي[4] لا يتطلب نقلا لقطع عسكرية من مكان إلى مكان آخر، إضافة إلى ذلك فإنه من غير الممكن التنبؤ بالفترة الزمنية التي سيستخدم فيها هذا الوسط من أجل إحداث ذلك الخلل[5]، وبالرغم من ذلك يرى البعض أن المجال أو الفضاء الإلكتروني لا يعتبر مجالا متميزا، بل يصنف على أنه أسلوب مستحدث للجوء إلى القوة أو إدارة المعارك -على غرار الأسلحة النووية- على اعتبار أنه ينطلق من واحدة من المجالات الأربعة آنفة الذكر ويحدث أثرا في واحدة منها، فهو بذلك يعد تطورا في الأسلوب[6].

---

(1) انظر اتفاقات لاهاي للعام 1899 و 1907 واتفاقات جنيف ألأربعة للعام 1949 التي نظمت حالة إدارة استخدام القوة استنادا إلى هذه المجالات المختلفة.

(2) انظر، على سبيل المثال، المادة 42 من اتفاقية لاهاي 1899 والتي تحدد الجانب الزماني لحالة الاحتلال العسكري، انظر أيضا المادة السادسة من اتفاقية جنيف الرابعة والتي تتحدث عن الفترة الزمنية التي ينتهي عندها تطبيق ألاتفاقية.

(3) Research Handbook on International Law and Cyberspace, (Nicholas Tsagourias & Russell Buchan Eds.) Elgar, 2015, pp. 14-24.

(4) لفهم الفرق بين هذين المصطلحين انظر 4.1 من هذا البحث.

(5) 'War as the Fifth Domain', The Economist 1.July.2010.

(6) See, Thomas Rid, Cyber War Will Not Take Place, Oxford University Press, 2013, pp. 165-166.

ومع تطور الإنترنت أصبح هنالك تطور مصاحب للأساليب التي يمكن من خلالها التأثير في المعلومات المستقرة في أجهزة الكمبيوتر، والتي تشكل اعتداء إلكترونيا، فبالنظر إلى العديد من الأمثلة الواقعية من الاعتداءات على المعلومات الإلكترونية، أصبح من الممكن لنا أن نميز بين نوعين من هذه الاعتداءات بالاعتماد على الأسلوب، وتمييز آخر لهذه الاعتداءات مبني على الباعث عليها، بالنسبة للنوع الأول يتمثل في الأسلوب التركيبي أو الوظيفي «Syntactic»، والثاني هو الأسلوب الدلالي «Semantic».

واستنادا إلى الباعث، يمكننا تقسيم العمليات الإلكترونية إلى جرائم إلكترونية «Cyber Crime»، واعتداء إلكتروني «Cyber Attack» وحرب إلكترونية «Cyber Warfare»، وسنقوم بعرض مختصر للفرق بين هذه الأنواع المختلفة تباعا.

**المطلب الاول:**

**الجرائم إلكترونية «Cyber Crime» والاعتداء الإلكتروني «Cyber Attack»**

**أولا: الجريمة الإلكترونية**

يتمحور الفرق بين الجريمة الإلكترونية وكل من الهجمة الإلكترونية والحرب الإلكترونية في الباعث «Intent»، الذي تستند إليه كل واحدة من هذه الأفعال وهدف كل منها والبيئة القانونية ذات العلاقة[1]، وبالرغم من عدم وجود تعريف موحد لمصطلح «الجريمة الإلكترونية» تبقى مجموعة من الخصائص لهذه العملية تبعدها كل البعد عن كل من الهجمات الإلكترونية ، فأول ما يميز الجريمة الإلكترونية هو كونها تصرف صادر عن جهة لا تمثل الدولة أو إحدى مؤسساتها، سواء كان شخصا عاديا أو اعتباريا، سعيا وراء هدف جرمي يتحقق عند اختراق أجهزة إلكترونية معينة لأغراض شخصية، وغني عن القول إن هذا التصرف لا يرقى إلى مستوى الجريمة الإلكترونية إلا إذا شكل جريمة وفقا للقانون الجنائي الداخلي استنادا إلى مبدأ «لا جريمة ولا عقوبة إلا بنص»، وهو أحد المبادئ الأساسية التي تقوم عليها أنظمة العدالة الجنائية.[2]

يضاف إلى ذلك أن الباعث على هذا العمل يبقى دائما باعثا جنائيا بحتا، إذ تجدر الإشارة أيضا إلى أن التصرف الذي يعد جريمة إلكترونية لا يهدف أساسا إلى إضعاف الوظيفة التي تقوم بها الأجهزة الإلكترونية المراد اختراقها، لأن هدف الفاعل من خلال

(1) Martin Roesler, When Do We Call a Cyber Attack an Act of Cyber War?, March, 2013.

(2) انظر، ذياب البداينة، الجرائم الإلكترونية: المفهوم والأسباب، ورقة عمل ضمن الملتقى العلمي حول الجرائم المستحدثة في ظل المتغيرات والتحولات الدولية، كلية العلوم الإستراتيجية، عمان 2 - 4/9/2014.

استخدام الشبكة المعلوماتية يكون لأغراض شخصية، واستخدامه يساهم في الإبقاء على وظيفة الشبكة الإلكترونية، علاوة على ذلك فإنه من مصلحة الجاني الإبقاء على النظام دون أي خلل حتى يحقق أكبر المكاسب التي تضاف إليه من خلال ارتكابه للجريمة وعدم لفت الأنظار إليه.

**ثانيا: الهجمة الإلكترونية**

تختلف الهجمة الإلكترونية بشكل جوهري عن الجريمة الإلكترونية في كون الهجمة الإلكترونية صادرة عن الدولة أو إحدى مؤسساتها بهدف إضعاف الوظيفة التي تقوم بها أجهزة الحاسوب المستهدفة[1]، يضاف إلى ذلك أن القواعد القانونية التي تقرأ من خلالها الهجمات الإلكترونية هي قواعد القانون الدولي العام، تحديدا قواعد اللجوء إلى استخدام القوة «Jus ad Bellum».[2]

وتجدر الإشارة إلى الفرق الجوهري الآخر بين الجريمة الإلكترونية والهجمة الإلكترونية والذي يتمثل في الباعث، حيث إن الباعث على الهجمة الإلكترونية يتمثل أساسا في إضعاف وظيفة شبكات الحاسوب في دولة أخرى لتحقيق هدف سياسي، ويضاف إلى ذلك أن الأضرار المحتملة لكل من الهجمة الإلكترونية والجريمة الإلكترونية تختلف بشكل كبير، على اعتبار أن الهجمة الإلكترونية تهدف إلى إلحاق ضرر شامل سواء للأشخاص أو الممتلكات في الدولة الأخرى، وهو ما يختلف جذريا عن الجريمة الإلكترونية والتي ينحصر ضررها عموما في مستخدمين معينين.[3]

(1) راجع قرار محكمة العدل الدولية بخصوص متى يكون العمل منسوبا للدولة
انظر على وجه التحديد Effective Control & Overall Control ICJ, case concerning *Application of the Convention on the prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro),* Judgment, I.C.J. Reports (2007), para. 400.

(2) أحمد عبيس نعمة الفتليوي، الهجمات السيبرانية: مفهومها و المسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، بحث مقبول للنشر في مجلة المحقق الحلي ، كلية القانون ، جامعة بابل 2015.

(3) Michael N. Schmitt (ed.), Tallinn Manual on the International Law Applicable to Cyber Warfare (Cambridge University Press, 2013) at 106.

## المبحث الثالث:

## موقف قواعد القانون الدولي العام من الهجمات الإلكترونية

سوف يعمد هذا الجزء من البحث، بشكل أساس، إلى المقاربة بين قواعد القانون الدولي القائمة، وتحديدا تلك المتعلقة باستخدام القوة والدفاع عن النفس ومحاولة إسقاطها على الهجمات الإلكترونية، إضافة إلى ذلك سيتم الاسترشاد بجهود المنظمات والمؤسسات الدولية والفقهاء في بذل جهد مستفيض سعيا وراء فهم ملامح قواعد القانون الدولي العام القائمة حيال هذه الظاهرة المتنامية[1].

لذلك سيتطرق هذا الجزء إلى ثلاثة مواضيع وهي أولا: مدى انطباق أحكام المادتين 2(4) و51 من ميثاق الأمم المتحدة على الهجمات الإلكترونية وثانيا: في طريقة أو مستوى الرد على الهجمات الإلكترونية وثالثا: في مستوى الدليل المطلوب من الدولة التي تدعي أنها قد تعرضت إلى هجوم إلكتروني.

### المطلب الأول:

### مدى انطباق أحكام المادتين 2(4) و 51 من ميثاق الأمم المتحدة على الهجمات الإلكترونية

في إطار مدى انطباق أحكام المادتين 2(4) و 51 من ميثاق الأمم المتحدة على الهجمات الإلكترونية يبرز تساؤلان جوهريان هما أولا: هل يمكن أن تشكل الهجمة الإلكترونية مخالفة للمادة 2(4) من ميثاق الأمم المتحدة والتي تحظر على الدول « استخدام القوة أو التهديد بها ضد سلامة الإقليم...»[2] التابع لدولة أخرى؟ تنبع أهمية هذا التساؤل تحديدا في ضوء عدم وضوح المعنى الدقيق لمصطلح «استخدام القوة» وفق هذه المادة ، وثانيا: هل يمكن أن تصل الهجمة الإلكترونية إلى مستوى «الهجوم المسلح» الوارد في المادة 51 حتى يثبت للدولة «المعتدى عليها إلكترونيا» حق الدفاع عن نفسها كما هو الحال بالنسبة للدولة المعتدى عليها عسكريا في سياق هذه المادة؟ في ظل خلو الاتفاقات الدولية أو العرف الدولي المستقر من إجابة واضحة عن هذه الأسئلة المركزية، وهو ما يعتبر إشكالية البحث الأساسية، لا بد من اللجوء إلى موقف محكمة العدل الدولية، وبالتحديد موقف المحكمة في قضية نيكاراغوا لعام 1986 وأيضا إلى دليل تالين «Tallinn Manual»، وتحديدا الجزء

(1) إضافة إلى دليل تالين انف الذكر فقد تم اختيار الهجمات الإلكترونية من قبل تجمع طلبة القانون الدولي (International Law Students Association) كموضوع لمسابقة هذا العام اعترافا من المجلس والخبراء العاملين فيه بمدى صعوبة هذا الموضوع والإشكالات المتمثلة في تفاصيله.

(2) United Nations Charter (1945), Article 2(4).

الأول الخاص بسيادة الدولة، والجزء الثاني المتعلق باستخدام القوة، بالإضافة إلى مجموعة من الآراء الفقهية لبلورة فهم لملامح قواعد القانون الدولي العام بخصوص هاتين المسألتين.

تصدت محكمة العدل الدولية في قضية نيكاراغوا Nicaragua Case[1] إلى المادة 2(4) من ميثاق الأمم المتحدة من زاويتين، الأولى عندما تعرضت المحكمة إلى طبيعة هذه المادة، حيث أكدت في الفقرة 187 من حكمها على تحول مبدأ حظر استخدام القوة أو التهديد بها إلى قاعدة عرفية دولية يقع على جميع الدول واجب الالتزام بها[2]. يشار إلى أن ذلك يأتي منسجما مع حقيقة أن معظم بنود ميثاق الأمم المتحدة قد وصلت إلى كونها مبادئ أساسية لا يجوز لأي دولة مخالفتها أو القفز عنها «Jus Cogens»[3]، أما الزاوية الثانية فتتمثل في الحالات التي يمكن أن تعتبر استخداما للقوة خلافا لهذه المادة، في هذا الصدد أقرت المحكمة بشمولية المادة وعدم اقتصارها على استخدام القوة بالمعنى التقليدي، والمتمثل في استخدام قوات عسكرية نظامية خارج حدود الدولة؛ حين أسهبت وأقرت أن « إرسال القوات من لدن الدولة أو بالنيابة عنها سواء كانت على شكل مجموعات نظامية أو غير نظامية أو أية أدوات أخرى» يعتبر مخالفة للمادة 2(4) من الميثاق، ويمكن لمثل هذا التصرف أن يعتبر هجوما مسلحا وفقا لأحكام المادة 51 من الميثاق بالاستناد إلى حجم وتأثير استخدام القوة[4].

بعيدا عن الفرق في التعبيرات المستخدمة من قبل المحكمة بين استخدام القوة والهجوم المسلح- والتي سيتم التعرض لها -لاحقا- هنالك نقطة جوهرية يجب الوقوف عندها هنا تتمثل في الخروج الواضح للمحكمة عن النهج التقليدي لفهم استخدام القوة؛ ذلك الاستخدام للأدوات التقليدية في الاعتداء، والذي كان يشترط قرارا مباشرا من الدولة باتجاه استخدام القوة في إقليم دولة أخرى[5]، وهذا الموقف للمحكمة جاء تأكيدا على النية الحقيقية للدول المشاركة في صياغة المادة 2(4) من الميثاق، حيث إن الأعمال التحضيرية لهذه المادة تشير وبوضوح إلى أن أي تهديد أو استخدام للقوة بين الدول الأعضاء سوف يشكل خرقا

(1) ICJ, Case concerning, *Military and Paramilitary Activities in and Against Nicaragua* (Nicaragua v. United States), 1986.

(2) *Id*. Para. 187.

(3) See, Kamrul Hossain, The Concept of Jus Cogens and the Obligation under the U.N. Charter, Santa Clara Journal of International Law, Vol.3, Issue 1, 2005.

(4) ICJ, Nicaragua Case. 1986, Para, 195.

(5) Milorad Petreski, The International Public Law and the Use of Force by States, Journal of Liberty and International Affairs | Vol. 1, No. 2, 2015.

لهذه المادة، شريطة أن يكون مخالفا لمبادئ الميثاق[1] . يشار إلى أن هذا الموقف للمحكمة يعد تأكيدا لفكرة مسؤولية الدولة عن الممارسات الخاطئة المباشرة وغير المباشرة، بما فيها تلك الناشئة عن تقصيرها بواجب عدم التسبب بأذى للآخرين خارج نطاق إقليمها، وهو ما يعرف «Due Diligence»، والذي بدوره تطور من خلال المحكمة في قضية قناة كورفو بين ألبانيا والمملكة المتحدة في العام 1949[2] .

في هذا السياق يمكن أن نصل إلى نتيجة محددة مفادها أن المحكمة من خلال حكمها في قضية نيكاراغوا قد كانت مهيأة لضم فئات أخرى غير الهجوم العسكري التقليدي في إطار التصرفات التي يمكن أن تشكل خرق للمادة 2(4) من الميثاق، ويجب أن نشير إلى أن موضوع النزاع أمام المحكمة في هذه القضية لم يكن في إطار الهجمات الإلكترونية، وإنما كان يتمحور حول الدعم العسكري غير المباشر الذي كانت تقدمه الولايات المتحدة لمجموعات مناهضة للحكومة في نيكاراغوا، وبسبب الاتصال بين هذه المجموعات وحكومة الولايات المتحدة أقرت المحكمة بالخرق من جانب الولايات المتحدة للمادة2(4) حيث حكمت المحكمة لصالح نيكاراغوا.

وانطلاقا من المعايير آنفة الذكر والتي استندت إليها المحكمة، فيمكن لنا أن نتخيل تصورا مشابها في حالة ادعاء دولة معينة على أخرى بشأن هجمة إلكترونية عندما تحقق هذه الهجمة معيار الحجم والتأثير على الدولة التي تتعرض للهجوم، بشرط اتصالها بالدولة المدعى عليها، إلى جانب ذلك، جاءت النسخة الأولى من دليل تالين للعام 2011 لكي تدعم هذه النتيجة حين جاءت القاعدة 11 منه لتؤكد على أن «العمليات الإلكترونية تعتبر استخداما للقوة عندما يكون مستواها وتأثيرها متقاربا مع العمليات غير الإلكترونية»[3]، ففي سياق هذا النص أقرت مجموعة من الخبراء أعدت هذا الدليل أنها قد استندت إلى معيار الحجم والتأثير «Scale and Effect» في سياق تحديد فيما إذا كانت الهجمة الإلكترونية ترقى إلى استخدام غير مشروع للقوة خلافا للمادة 2(4) من ميثاق الأمم المتحدة، وأيضا فيما إذا كان هجوما عسكريا يبرر الدفاع عن النفس وفقا للمادة 51، وهما المعياران -ذاتهما- اللذان استندت إليهما محكمة العدل الدولية في قضية نيكاراغوا آنفة الذكر.

(1) Doc. 784 1/1/27, 6 U.N.C.I.O Docs. (1945).

(2) ICJ, *Corfu Channel Case* (UK. v. Albania), Judgment, 1949 I.C.J. Rep. 4, 22 (Apr. 9); See also Rorbert P. Barnidge, The Due Diligence Principle under International Law, International Law Community Law Review, Vol.81, Issue 8, (2006).

(3) Michael N. Schmitt (ed.), Tallinn Manual on the International Law Applicable to Cyber Warfare (Cambridge University Press, 2013) at paragraph 11.

ويبقى السؤال حول المعنى الدقيق لمصطلحي الحجم والتأثير الخاص بالهجمة الإلكترونية، لكي نقرر فيما إذا كان هذا الحجم والتأثير يجيز للدولة «المعتدى عليها» أن تستند إلى المادة 51 من الميثاق للدفاع عن نفسها أم لا؟

في هذا السياق يجب العودة مرة أخرى إلى ما قررته محكمة العدل الدولية في قضية نيكاراغوا، حيث فرقت المحكمة بين الأشكال «الأكثر خطورة» لاستخدام القوة والتي تصل إلى الهجوم المسلح عن تلك «الأقل خطورة» والتي بالتالي لا تجيز تفعيل المادة[1]، حيث رأت المحكمة من خلال هذا الحكم أن الأعمال «الأكثر خطورة» فقط هي التي تفعل حق الدولة في الدفاع عن نفسها وفقا للمادة 51 من الميثاق، أما الأفعال «الأقل خطورة» فلا تفعل هذا الحق، وإنما يمكن أن تفعل حقوق أخرى مصممة للرد على الدولة المرتكبة لمثل تلك ألأفعال، كالإجراء المضاد مثلا أو أي إجراء آخر من تلك المنصوص عليها في مشروع مواد مسؤولية الدول عن الأفعال غير المشروعة 2001 ما دون الدفاع عن النفس وفقا للمادة 51 من الميثاق[2].

واللافت للنظر هو أن المحكمة لم تقم بخطوة ضرورية أخرى تتمثل في رسم الخط الفاصل بين الأفعال «الأقل خطورة» وتلك «الأكثر خطورة»، حيث تركت الباب مفتوحا في هذا الإطار حين أقرت من خلال تعابير مرسلة أن تفعيل المادة 51 يكون مثلا في الحالة ترسل دولة معينة قوات عسكرية خارج حدودها إلى دولة أخرى، أما مجرد الحوادث الحدودية البسيطة فلا ترقى- بحسب المحكمة- إلى مستوى الهجوم المسلح[3]، أما في سياق الهجمات الإلكترونية فلم يكن هذا هو النهج الذي تبنته مجموعة الخبراء التي أعدت دليل تالين.

بالاستناد إلى أهمية هذا المعيار الذي جاء به دليل تالين سيقوم الجزء التالي من هذا البحث بالتفصيل بشأنه.

(1) ICJ, Nicaragua Case, Para. 191.

(2) البعض يرى أن مثل هذه الإجراءات يمكن أن تتضمن ما نصت عليه بنود مشروع مواد مسؤولية الدول عن الأفعال غير المشروعة لعام 2001. على وجه التحديد فإن هذا الفريق يرى أن الرد المناسب للهجمات الإلكترونية التي لا تصل إلى مستوى «الهجوم المسلح» وبالتالي لا تجيز الدفاع عن النفس وفقا للمادة 51 من الميثاق يتمثل في الإجراء المضاد (Countermeasure) والذي يعني «أجراء كان يمكن أن يعتبر مخالفا لالتزام دولي من قبل الدولة المتضررة في مواجهة الدولة المسؤولة عن الضرر إن لم يكن قد اتخذ من الأولى لمواجهة تصرف مخالف لالتزام دولي من قبل الدولة ألأخيرة...»

Draft Article on Responsibility of States for Wrongful Acts (2001), International Law Commission, Fifty Third session, General Assembly resolution 56/83 of 12 December 2001; See also, Oona A. Hathaway, The Law of Cyber-Attack, Yale Law School Legal Scholarship Repository, 2012, page 857.

(3) ICJ, Nicaragua Case, Para. 195.

**المطلب الثاني:**

**المعيار المعتمد وفقا لدليل تالين**

بالرغم من هذا الاختلاف التفصيلي بين فقه محكمة العدل الدولية وموقف مجموعة الخبراء لدليل تالين، نجد أن هنالك قاسما مشتركا بينهما يتلخص في الحجم والتأثير كمعيارين يستند إليهما لتفعيل الدفاع عن النفس وفقا لأحكام المادة 51 من ميثاق الأمم المتحدة، حيث إن كلا من المحكمة ولجنة الخبراء تريان بأن الاعتداء على الدولة -بأي شكل كان بما في ذلك الهجمات الإلكترونية- يشكل انتهاكا لسيادتها ما يعطي الحق للدولة المعتدى عليها رد هذا الاعتداء ضمن شرط جوهري وحيد وهو أن يكون حجم وتأثير هذا الهجوم على الدولة المعتدى عليها ضمن مستوى معين، وهو ما عملت اللجنة جهدا استثنائيا لتحديده من خلال مجموعة من الصفات التي يجب أن تتسم بها الهجمات الإلكترونية حتى ترقى إلى عتبة الهجوم المسلح، وبالتالي تعطي الدولة المعتدى عليها فرصة تفعيل المادة 51 من الميثاق وهذه الشروط هي:

**أولا:الحدة «Severity»**

اعتبرت اللجنة أن أهم المعايير التي يجب الاستناد إليها في تحديد المستوى المطلوب لوصول العمليات الإلكترونية إلى عتبة الهجوم المسلح يتمثل في جسامة هذا التصرف أو حدته، ومدى تأثيره على الدولة المعتدى عليها، ولكن العقدة الأبرز في هذا الشرط كانت -مرة أخرى- تتمثل في مستوى هذه الحدة، أو الحد المطلوب لتصنف العملية الإلكترونية على أنها جسيمة، وهو ما خلق فجوة في قرار محكمة العدل الدولية في حكمها بقضية نيكاراغوا، لذلك رأت اللجنة ضرورة وضع معيار دقيق يستند إليه لسد هذه الفجوة.

في هذا السياق أقرت اللجنة أن جوهر المعيار يتمثل في الضرر المادي على الأفراد أوالممتلكات في الدولة المعتدى عليها بهجوم إلكتروني، حيث إن العمليات الإلكترونية ترقى إلى مستوى الهجوم المسلح الوارد في المادة 51 فقط في الحالة التي تعكس فيها هذه العمليات ضررا ماديا حالا[1]على الأفراد أو على الممتلكات في الدولة المعتدى عليها، وفي سبيل ذلك قامت اللجنة بالمقاربة بين أثر الهجمات العسكرية التقليدية والهجمات الإلكترونية استنادا إلى قياس نتائج الأخيرة وفيما إذا كانت منتجة لأضرار مماثلة للهجمات العسكرية التقليدية أم لا.

(1) انظر في الشروط ألأخرى تحديدا «شرط الآنية» حيث يجب في هذا الضرر أن يكون واضحا وحالا وليس متوقعا.

غني عن القول إن الهجمات الإلكترونية يمكن لها أن تنتج مثل هذا الضرر المماثل المتصور في الهجمات العسكرية التقليدية أو يزيد، ولكن التساؤل الفرعي على هذا الضابط يتمثل في المستوى المطلوب في حدة الضرر الذي يجب أن تعكسه مثل تلك الهجمات،إذ تتبادر هذه المسألة إلى الأذهان بسبب قدرتنا أن نتصور نتائج متباينة للهجمات الإلكترونية، والتي في بعض الحالات تختلف جذريا عن الهجمات العسكرية التقليدية بأنها قد لا تنتج ضررا ماديا على الأفراد أو الممتلكات، فيمكن لنا -على سبيل المثال- أن نتصور اعتداءً إلكترونيا على إحدى الدوائر الإدارية الفرعية في دولة أخرى ما أدى إلى إرباك العمل في هذه الدائرة بشكل جزئي دون أي ضرر مادي، وأيضا لنا أن نتصور اعتداء إلكترونيا آخر على شبكات الكمبيوتر الخاصة بمطار العاصمة في الدولة ما أدى إلى مقتل الآلاف بسبب الخلل الذي أحدثته الهجمة ما أدى إلى تصادم الطائرات هبوطا وصعودا، والسؤال في هذا الصدد هو هل أن كلا التصرفين يشكلان هجوم إلكترونيا من شأنه أن يفعل الدفاع عن النفس وفقا للجنة؟

في محاولة الإجابة عن هذا التساؤل قامت اللجنة بوضع معيار أساس يستند إلى الضرر المادي سواء قد وقع على الأفراد أو على الممتلكات، ففي مثل هذه الحالة تعتبر العملية الإلكترونية هجوما عسكريا، أما تلك التصرفات التي لا تلحق مثل هذا النوع من الضرر فتخرج حسب اللجنة من دائرة الهجوم العسكري، إلا في الحالة التي تضر فيها هذه العمليات الإلكترونية بمصلحة وطنية حساسة للدولة المعتدى عليها دون أن تتصل بضرر مادي محسوس.

في هذا السياق قامت اللجنة بإخراج مجموعة من العمليات الإلكترونية من دائرة كونها تشكل هجوما مسلحا مثل تلك المؤدية إلى خلق «حالة من الانزعاج» في الدولة المتضررة، دون أن تقترن بضرر في مصلحة أساسية من مصالح الدولة، فحالة الانزعاج التي خلفها الاعتداء على الدائرة الإدارية لا يرقى إلى كونه هجوما يستدعي تطبيق المادة 51، ولكن العملية الإلكترونية التي تؤثر مباشرة في حركة الطائرات أو في سير العملية الانتخابية في دولة ما فإنها تضيف إلى انزعاج الدولة المعتدى عليها ضررا بمصلحة وطنية للدولة، وبالتالي تشكل وفقا لهذا المعيار هجوما عسكريا يبيح اللجوء إلى الدفاع عن النفس وفقا للمادة 51 من الميثاق.

وبالعودة إلى الضرر المادي على الممتلكات أو الأفراد والذي اعتبرته اللجنة محققا لمعيار الجسامة؛ يلاحظ أن هذا التوجه جاء متوافقا أيضا مع موقف محكمة العدل الدولية في قضية نيكاراغوا عندما فرقت بين الأعمال الأكثر خطورة والأقل خطورة، وفي هذا الشأن قررت اللجنة بأن الأضرار غير الجسيمة على الأفراد أو الممتلكات لا تشكل هجمة عسكرية، وهو ما عبرت عنه المحكمة بمصطلح «الأعمال الأقل خطورة»، مثل المناوشات

الحدودية إذ لا يمكن أن تعتبر شكلا من أشكال استخدام القوة، ومع ذلك تبقى الحاجة قائمة إلى وضع معيار لتحديد ما يعتبر جسيما وما يعتبر أقل جسامة بهذا الصدد.

**ثانيا: الضرر «الحال» أو «الآني» (Immediacy)**

يعتبر شرط وقوع الضرر من بين الشروط الجوهرية للهجمات الإلكترونية والذي اعتدت به اللجنة حتى يرتقي بالعملية الإلكترونية إلى مستوى الهجوم المسلح، وهو شرط متباين -عموما- عن فكرة المسؤولية الدولية التي تبنى على خرق الالتزام بغض النظر عما إذا كان هذا الخرق مصاحبا لضرر أم لا[1]، ويتحقق هذا الشرط في حالتين: الأولى، عندما يقع الضرر فعلا على الدولة المعتدى عليها، والحالة الثانية -وهي الأكثر تعقيدا- عندما لا يكون الضرر قد وقع فعلا وإنما هو ضرر وشيك الوقوع، وهو أيضا - بحسب اللجنة- منتج للحق في الدفاع عن النفس، وفي هذه الحالة الأخيرة يبرز السؤال حول المعنى الدقيق لمصطلح الآنية، والفرق- إن وجد- بين الضرر الآني والضرر غير الآني في سياق العمليات الإلكترونية.

في هذا الإطار استندت اللجنة إلى معيار «الفترة الزمنية الكافية» التي يمكن تستغلها الدولة «المعتدى عليها» لتجنب وقوع الضرر من خلال تواصلها بالدولة منشأ الاعتداء للتراجع عن هذا التصرف، فلا يمكن للتصرف وفقا لهذا المعيار أن يرقى إلى كونه استخداما للقوة إذا أثبت أن الدولة المستهدفة في هذا الهجوم قد فرطت بأي نافذة زمنية كان يمكن لها استغلالها لدرء الضرر، بكلمات أخرى فإن الخطر الآني أو الحال هو الذي سوف يقع لا محالة دون أي قدرة للدولة المعتدى ولا بأي طريق على درءه.[2]

إن شرط الآنية هذا يعيد إلى الأذهان اختبار كارولاين «Caroline Test» والذي يعد ترجمة حقيقية لفكرة الآنية، والذي يقرأ في سياق الدفاع عن النفس ضد خطر محتمل في القانون الدولي، ومفاده أن للدولة الحق في أن تدافع عن نفسها حيال هجوم عسكري لم يقع بعد ولكنه «فوري ولا يترك أي خيار أو أي لحظة للمداولات»[3]، وتجدر الإشارة إلى

(1) هذا ما أكدت عليه المادة الثانية مشروع مواد مسؤولية الدول عن الأفعال غير المشروعة للعام 2001 والتي بنت مسؤولية الدولة على الخرق أو المخالفة دون أن تتطلب الضرر.

(2) See, Daniel Bethlehem, Principles Relevent to the Scope of Self-Defence Against Imminent or Actual Armed Attack by Nonstate Actors, American Journal of International Law, Vol. 106, 769, 2012.

(3) يشار إلى أن هذا المبدأ والمستمد من حادثة كارولاين بين المملكة المتحدة والولايات المتحدة قد أصبح عرفا دوليا بشأن الدفاع عن النفس ضد خطر محتمل. ,
Larry May, War Crimes and Just War, Cambridge University Press, (2007), p. 206;

أن دليل تالين لم يتطرق إلى الحالة التي يمكن فيها للدولة «المستهدفة» من هذا الهجوم أن تمنع حدوث هذا الضرر، أو أن تحد من أثره لوحدها، أو دون الحاجة للتواصل مع الدولة منشأ الاعتداء، وبالرغم من ذلك يمكن لنا أن نبني اعتقادا مفاده أن عدم ذكر هذه الحالة جاء انطلاقا من كونها حالة مفترضة، على اعتبار أن إمكانية درء الضرر- بأي وسيلة كانت- تمثل جوهر هذا المعيار.

**ثالثا: أن يكون أثر الهجوم مباشرا «Ddirectness»**

يجب أن يكون واضحا ابتداءً أن واحدا من أهم الفروقات بين الهجمات التقليدية بالأسلحة التقليدية والهجمات الإلكترونية يتمثل في أن نتائج الأخيرة قد لا تكون واضحة، أي بمعنى عدم القدرة على تحديد العلاقة السببية بين الفعل والضرر، وذلك نتيجة لما يطلق عليه الانفصال الزمني بين التصرف الأساس الذي يعد مخالفة والنتائج التي يمكن يرتبها هذا التصرف، وهذه صفة ملازمة للهجمات الإلكترونية.(1)

فيمكن لنا أن نتخيل مثلا أن عمليات إلكترونية قد وجهت إلى سوق الأسهم في دولة، مما يؤثر سلبا - ولكن ببطء شديد- في أداء الأسواق بشكل عام، وبالتالي ترتب عليه انكماش اقتصادي في تلك الدولة، ففي هذه الحالة يمكن لهذه العمليات الإلكترونية أن تقرأ في إطارين، الأول: أن الانكماش الاقتصادي كان نتيجة مباشرة للعملية الإلكترونية، ولكنه خرج بشكله النهائي بعد فترة طويلة من الزمن. أما الإطار الثاني: أن اقتصاد تلك الدولة كان أصلا ضعيفا ومتهالكا، وأن العملية الإلكترونية لم تكن هي السبب الجوهري وراء هذا الانكماش، بل كانت كاشفة له، وبالتالي لا يوجد علاقة مباشرة بين التصرف والنتيجة.

استنادا إلى شرط «الاتصال المباشر» الوارد في دليل تالين، فإن هذا الإطار الأخير لا يمكن أن يرتقي بالتصرف إلى عتبة الهجوم المسلح استنادا إلى عدم القدرة على تحديد العلاقة السببية بين الفعل والضرر، ولذلك يجب عدم الخلط بين الآنية والمباشرة كشرطين متميزين جاء بهما الدليل، حيث إن الأول يتمثل في خروج الضرر إلى حيز الوجود والثاني يرتبط بالعلاقة بين التصرف والضرر.

ويشار إلا أنه وبالرغم من كون هذين الشرطين متمايزين، إلا أنهما في أغلب الأحيان متلازمان بحيث من الصعوبة بمكان تصور هجمة إلكترونية غير حالة ومباشرة في ذات الوقت، فالهجوم الحال غير المباشر كأن تعتقد دولة ما -مثلا- أن هجوم إلكترونيا حالا

(1) See, Haitao Du and Shanchieh Jay Yang, Temporal and Spatial Analyses for Large-Scale Cyber Attacks, Handbook of Computational Approaches to Counterterrorism, pp. 559-578, 2012.

على شبكة معلوماتية مدمرة أصلا سيحدث بحيث لا يمكن لهذه الهجمة أن تحدث ضررا إضافيا، لا يرقى بهذا التصرف إلى عتبة الهجوم العسكري بسبب عدم الاتصال بين الفعل والنتيجة، ويبقى لنا أن نتصور الحالة التي يمكن فيها أن تكون الهجمة الإلكترونية مباشرة ولكنها ليست حالة وتتمثل عموما في الأضرار الاقتصادية بعيدة المدى التي يمكن أن تقع على الدولة «المعتدى عليها».

**رابعا: العدائية**

يعد شرط العدائية أحد الشروط المتصلة بشكل كبير بحالة الدفاع عن النفس، وفي ذلك تطابق مع ما جاء به نص المادة 51 من ميثاق الأمم المتحدة، والتي اعتبرت أن «الاعتداء» من دولة باتجاه دولة أخرى هو المحرك الأساس لتفعيل حالة الدفاع عن النفس بالنسبة للدولة المعتدى عليها، والمعنى الدقيق لهذا المصطلح هو الاتصال المباشر بين السلوك والنية العدائية المتمثلة في إحداث ضرر في الدولة الأخرى أو إحدى مصالحها[1].

على هذا الأساس جاء دليل تالين متضمنا شرط العدائية، والذي يتمثل في النية خلف العملية الإلكترونية، فبحسب هذا الشرط ترتقي العملية الإلكترونية إلى عتبة الهجوم المسلح كلما كانت الدولة المعتدى عليها قادرة على إثبات أن هذا التصرف يسعى إلى تحقيق أهداف عدائية في الدولة الأخرى، كإضعاف القدرة العسكرية من خلال التأثير على برامجها الإلكترونية العسكرية، ولكن التساؤل الأبرز حول هذا الشرط يكمن في كيفية تقدير فيما إذا كانت النية خلف الهجوم هي نية عدائية أم لا؟

يستمد هذا التساؤل والنقاش برمته أصوله من حقيقة مفادها أن هنالك أنواعا مختلفة للعدوان من شأن بعضها فقط أن يفعل الدفاع عن النفس وفقا للمادة 51 انطلاقا من حكم محكمة العدل الدولية في قضية نيكاراغوا، حين فرقت بين الأعمال الأكثر خطورة وتلك الأقل خطورة، على اعتبار أن الفئة الأولى من هذه الأعمال فيه تصميم من قبل الدولة المعتدية على إلحاق أشد الضرر على الدولة المعتدى عليها، وهذا ما دعا المحكمة إلى التفرقة بين الأعمال الأكثر خطورة وتلك الأقل خطورة، والفئة الأخيرة من هذه الأعمال - بحسب المحكمة- لا ترتقي إلى كونها اعتداء يفعل الحق في الدفاع عن النفس وفقا للمادة 51.

مرة أخرى، كيف لنا أن نفرق بين هاتين الفئتين من التصرفات في سياق العمليات الإلكترونية؟ يستمد هذا التساؤل قيمته من حقيقة مفادها أن إثبات النية وراء القيام بتصرف معين هي عملية معقدة، والوصول إليها لا يتم إلا من خلال عملية قضائية وبقرار قضائي،

(1) ICJ, *Oil Platforms Case*, (Islamic Republic of Iran v. United States of America), Reports 2003, p. 161, para. 64..

ويشار إلى أن هذه العملية القضائية غير متصورة في حالة الهجمات الإلكترونية خصوصا والدفاع عن النفس بشكل عام لسببين هما أولا: عدم وجود اختصاص قضائي دولي إلزامي، وثانيا: حتى في الحالة التي تتفق فيها الدول على اللجوء إلى القضاء يتنافى هذا الشرط مع شرط السرعة في رد الهجوم والذي يعتبر أساساً لمباشرة الدولة لحقها في الدفاع عن النفس[1].

ومن أجل التقريب بين هاتين الكرتين المغناطيسيتين: السرعة في الدفاع عن النفس من جهة، والكشف عن العدائية من جهة أخرى، اعتمد دليل تالين على نهج مفاده أن شرط العدائية والوارد في المادة 51 من الميثاق يمكن أن يتبين من خلال استهداف الدولة مصدر الهجوم شبكات إلكترونية محمية ومؤمنة في مواجهة خروقات إلكترونية مستقبلية من جهات أخرى، بسبب كونها تعمل في ميدان إستراتيجي للدولة المعتدى عليها.

فالاعتداء-على سبيل المثال-على الشبكات الخاصة بوزارة الدفاع في دولة ما لا يمكن من حيث المبدأ أن يقرأ إلا في إطار العدائية حسب المادة 51، حيث إن هذه الشبكات في طبيعة الحال من أكثر الشبكات الإلكترونية حماية في أي دولة، ولذا يمكن لنا أن نخرج بنتيجة مفادها أنه وبحسب دليل تالين هنالك علاقة طردية بين درجة الحماية للشبكة الإلكترونية موضع الهجوم وشرط العدائية وبالتالي النية وراء هذا الهجوم.

**خامسا:اتصال التصرف بالدولة**

يعد شرط اتصال التصرف بالدولة من أهم وأبرز الشروط لنهوض المسؤولية الدولية عموما، حيث يتضمن هذا الشرط ضرورة أن يكون التصرف صادرا عن من يمثل الدولة، سواء السلطة التشريعية أو التنفيذية أو القضائية أو أي جهة أخرى يعهد إليها مهمة القيام بعمل معين بالنيابة عن الدولة[2]، وبالرغم من السهولة في فهم ما يرمي إليه هذا الشرط والمنطق من وراءه إلا أنه يبقى- باعتقادي- من أكثر الشروط تعقيدا وصعوبة للفهم بالتحديد في سياق العمليات الإلكترونية وذلك لسببين جوهريين، الأول: يتمثل في صعوبة تحديد ما إذا كان هذا العمل منسوبا للدولة فعلا، وهذا مرتبط بالقدرة التكنولوجية المتنامية، والتي يمكن أن تمكن الدولة منشأ التصرف أن تطمس هوية الفاعل الحقيقي، إضافة إلى ذلك فإن عملية نسبة العمل للدولة تزداد تعقيدا في الحالة التي لا تكون الشبكات الإلكترونية هي الوسط الذي تمت من خلاله هذه الهجمات، كإرسال فيروسات توضع مباشرة في أجهزة الحاسوب الخاصة بالدولة المستهدفة، أو في الحالة التي يستخدم فيها إقليم دولة أخرى لتنفيذ

(1) انظر الجزء الأول من هذه المساهمة والخاص بشروط الحق في الدفاع عن النفس.

(2) هذا ما أقرته المادة الرابعة من مشروع مواد مسؤولية الدول عن الأفعال غير المشروعة.

هـذه الهجمـات، فلنـا أن نتخيـل مثـلا أن الدولـة (أ) قـد اسـتخدمت إقليـم الدولـة (ب) مـن خـلال عمـلاء لهـا لتنفيـذ هجمـة إلكترونيـة فـي الدولـة (ج) دون علـم الدولـة (ب).

أمـا السـبب الثانـي للإشـكالية الخاصـة بنسـبة العمليـات الإلكترونيـة للدولـة فيتمثـل فـي الحالـة التـي ينسـب فيهـا التصـرف إلـى مجموعـات خارجـة عـن سـلطات الدولـة[1]، ولكـن هـذه المجموعـات اسـتخدمت إقليـم الدولـة لتنفيـذ العمليـة، حيـث أثـارت هـذه الحالـة نقاشـا مسـتفيضا بيـن لجنـة الخبـراء حـول دليـل تاليـن، حيـث- فـي نهايـة المطـاف- أقـرت اللجنـة بشـكل ضمنـي فـي الفقـرة الثانيـة مـن القاعـدة 13 أن التحكـم الفعـال هـو فقـط مـا ينهـض بالمسـؤولية فـي مواجهـة الدولـة مصـدر الاعتـداء، وهـو موقـف متوافـق مـع قـرار محكمـة العـدل الدوليـة فـي قضيـة نيكاراغـوا[2].

إضافـة إلـى الشـروط أنفـة الذكـر، قامـت اللجنـة بوضـع شـروط أخـرى تتمثـل فـي وضـوح نتائـج الهجمـات أو القـدرة علـى قياسـها، بمعنـى قـدرة الدولـة المعتـدى عليهـا تحديـد الضـرر الـذي تسـببت بـه الهجمـة الإلكترونيـة، إضافـة إلـى شـرط الطابـع العسـكري للعمليـة الإلكترونيـة وهـو شـرط مسـتمد مـن مجمـل مـواد ميثـاق الأمـم المتحـدة الخاصـة باسـتخدام القـوة والتـي تربـط بيـن اسـتخدام القـوة وبيـن الطبيعـة العسـكرية لهـذه النشـاطات[3].

لكـن فـي هـذا الصـدد يتحتـم علينـا أن نشـير إلـى الخطـأ الـذي وقـع بـه الخبـراء علـى اعتبـار أن العمليـات الإلكترونيـة تتميـز جذريـا عـن الاسـتخدام التقليـدي للقـوة، وهـو مـا دفـع أساسـا إلـى خلـق هـذا النقـاش المسـتفيض حـول هـذا النـوع المسـتحدث مـن «اسـتخدام القـوة»، ويظهـر مـن خـلال هـذا التوجـه للخبـراء تأثرهـم بالفكـرة التقليديـة لاسـتخدام القـوة علـى اعتبـار أنهـا مكافئـة للقـوة العسـكرية، متأثريـن بذلـك مـن موقـف الميثـاق والنظـرة النمطيـة للـدول حـول مدلـول اسـتخدام القـوة.

مـن جانـب آخـر نـرى أن هـذا الاتصـال الـذي أقامـه الخبـراء متناقـض - مـن حيـث المبـدأ- مـع معيـار الحجـم والتأثيـر الـذي تبنتـه محكمـة العـدل الدوليـة، وأيضـا اللجنـة فـي موضـع آخـر

(1) تجدر ملاحظة الفرق بين كون هذه المجموعات تعمل خارج إطار الدولة أو أنها جزء من الدولة ولكنها قد تجاوزت السلطة أو أنها قد خالفت التعليمات. في الحالتين الأخيرتين يبقى هذا التصرف منسوبا للدولة استنادا إلى قواعد المسؤولية الدولية وبالتحديد ما جاءت به المادة السابعة من مشروع مواد مسؤولية الدول عن الأفعال غير المشروعة للعام 2001.

(2) ICJ, *Nicaragua Case*, Para. (115).

(3) انظر على سبيل المثال ديباجة ميثاق الأمم المتحدة والتي تفرض على الدول واجب « عدم استخدام القوة العسكرية إلا لتحقيق مصالح مشتركة» وأيضا المادة 44 والتي تشير بشكل ضمني إلى القوة العسكرية في سياق استخدام القوة بناء على السلطة الممنوحة لمجلس الأمن التابع للأمم المتحدة.

من الدليل، ودليلنا على هذا التناقض ينبع من قدرتنا على أن نتخيل عملية إلكترونية ذات أثر مدمر في الدولة المهاجمة، دون أن يكون مصدر هذه الهجمة وزارة الدفاع في الدولة المهاجمة أو/ و أيضا دون أن يكون الهدف عسكريا.

لذلك نرى أنه كان يتوجب على اللجنة أن تفرق بين حالتين: الأولى، هي الاتصال بين التصرف والوسيلة، والثانية الاتصال بين التصرف والغاية أو النية، وذلك حتى تكون اللجنة منسجمة مع نفسها ومع فقه محكمة العدل الدولية، كما كان يجب على اللجنة أن تعطي الأولوية للربط بين التصرف والغايات المكافئة للغايات العسكرية، ويمكن لنا أن نبرر هذا الموقف ليس فقط على أساس الوسائل المستحدثة لتنفيذ الهجوم - بما فيها الوسائل الإلكترونية - بل أيضا على أساس الغايات المستحدثة، والتي أصبحت الدولة ترى فيها تفوقا خارج إطار التفوق التقليدي «العسكري»، كما هو الحال في التفوق الاقتصادي أو حتى البيئي، والذي يمكن أن يعد مقاربا للتفوق العسكري بل في بعض الحالات يزيد[1].

فعلى الصعيد الزراعي الاقتصادي - مثلا- يمكن لنا أن نتصور عملية إلكترونية تهدف إلى تدمير أجهزة الكمبيوتر الخاصة بري المزروعات في دولة أخرى، ما قد يقضي على هذه المزروعات والتي تعتبر عنصراً مهما في اقتصاد الدولة، وفي الجانب البيئي يمكن لنا أن نتخيل استهدافا لأجهزة الكمبيوتر الخاصة بتنقية المياه الجوفية لغايات إحداث تلوث في هذه المياه، ما ينتج كارثة بيئية محتمة على هذه الدولة، ويمكن لهذين المثالين العمليين أن يبرزا أهمية و تفوق الغاية على الوسيلة التي جاء بها دليل تالين في سياق الهجمات الإلكترونية.

## النتائج:

أفرزت مسألة الهجمات الإلكترونية مجموعة من الأسئلة القانونية المعقدة في العلاقات بين الدول والتي بقيت تكتنف إجاباتها، حتى هذه اللحظة، درجة عالية من الغموض حيث سعت هذه الورقة لفهم معالم الإجابات أو على الأقل تحديد مواطن الغموض. أبرز هذه الأسئلة- وهو موضوع هذه الورقة- يتمحور حول الخيارات المتاحة أمام الدولة المعتدى عليها بهجوم إلكتروني في مواجهة الدولة مصدر الهجوم. على وجه التحديد عالجت هذه الورقة مسألة مدى انطباق توافق القواعد التقليدية الخاصة في الدفاع عن النفس ضمن ما تسمح به قواعد القانون الدولي مع فكرة الهجمات الإلكترونية. في هذا السياق تم التعرض إلى فهم عميق لقواعد القانون الدولي العام لاخاصة بالدفاع عن النفس سواء تلك الواردة في ميثاق الأمم المتحدة وفقه محكمة العدل الدولية لاستشراق العرف الدولي بخصوص

(1) وذلك حسب المادة 38 من النظام الأساسي لمحكمة العدل الدولية.

المسألة. إضافة إلى ذلك تمت العودة والتعمق في دليل تالين كجهد متميز بخصوص المواءمة بين قواعد القانون الدولي العام الخاصة بإستخدام القوة والدفاع عن النفس وبين الهجمات الإلكترونية كظاهرة متنامية في العلاقات بين الدول.

خلصت هذه المساهمة البحثية إلى أن الاستناد إلى القواعد العامة في القانون الدولي العام وتحديدا المادة 51 من ميثاق الأمم المتحدة والخاصة بالدفاع عن النفس وانطباقها على حالة الهجمات الإلكترونية له ما يدعمه في فقه القانون الدولي. جاء ذلك تحديدا بالاستناد إلى فقه محكمة العدل الدولية والتي كانت مهيأة في العديد من القضايا التي عرضت أمامها (في قضية «النشاطات العسكرية وشبه العسكرية في و ضد نيكاراغوا» 1986 وأيضا قضية منصات النفط بين إيران والولايات المتحدة 2003) إلى ضم فئات أخرى غير الهجوم الحركي لكي يعطي الحق للدولة التي تتعرض إلى هجوم الارتكاز إلى المادة 51 والدفاع عن نفسها ولكن ضمن شروط أبرزها الحجم والتأثير (Scale and Effect). في هذا الصدد يمكن القول: إن محكمة العدل الدولية قد ركزت على نتائج الهجوم أكثر من تركيزها على الوسائل المستخدمة في تنفيذ الهجوم ما يفيد أن المحكمة مهيأة لإدخال الهجمات الإلكترونية ضمن فئة الهجمات التقليدية لما لها من حجم وتأثير في الدول محل الهجوم الإلكتروني. ذات النهج تم اتباعه من لدن الخبراء القائمين على دليل تالين بفوارق بسيطة وهي أولاً: أن الدليل كان قد تعامل بشكل مباشر مع الهجمات الإلكترونية وثانيا: الخبراء القائمون على هذا الدليل قد قاموا بتحديد ضوابط لمعيار الحجم والتأثير الذي جاءت به المحكمة حتى ترقى الهجمة الإلكترونية إلى عتبة الهجوم المسلح الوارد في المادة 51. بالرغم من ذلك تبقى مسألة المقاربة بين الهجوم المسلح الحركي والهجوم الإلكتروني غير عملية وذلك بسبب الفوارق الجوهرية بين هاتين الفئتين من الهجمات وعدم إمكانية إسقاط بعض الشروط الواجب توافرها من أجل تفعيل المادة 51 على الهجمات الإلكترونية. على وجه التحديد فإنه من الصعوبة بمكان إسقاط شرط السرعة أو الفورية في رد الهجوم -والذي يقصد به أساساً أن لا تفوت الدولة المعتدى عليها مدة زمنية طويلة على الاعتداء قبل أن تقوم الدولة المعتدى عليها باتخاذ إجراءات الدفاع عن النفس- وذلك بسبب الصعوبة التي تصاحب عملية تحديد الجهة مصدر الهجوم إلا بعد مدة زمنية طويلة والتي يمكن عندها أن ينتفي المنطق من إعطاء الدولة الحق في الدفاع عن نفسها دون اللجوء إلى مجلس الأمن صاحب السلطة الأساسية في حفظ الأمن والسلم الدوليين. كذلك من الصعوبة بمكان التحقق من شرط الضرورة والذي يعني التثبت من النية العدائية للدولة مصدر الهجوم. يضاف إلى ذلك تعقيد آخر بشأن الهجمات الإلكترونية وهو مرتبط بالحالة التي يكون فيها مصدر الهجوم الإلكتروني جماعات معينية تعمل من إقليم الدول دون علم هذه الأخيرة. فهذه الحالة تفرز إشكالية أخرى تتمحور حول مسؤولية الدولة عن التصرفات ضمن نطاق إقليمها، فهل في هذه الحالة يتم الاستناد إلى معيار التحكم الفعال أم معيار التحكم العام؟ سؤال تخلو حتى هذه اللحظة قواعد القانون الدولي العام من إجابة واضحة بشأنه.

تبقى هذه المسائل مشكلةً العقبة الأبرز في طريق إيجاد تنظيم دولي دقيق ليحكم مسألة الهجمات الإلكترونية. حيث يرى الباحث أن الوصول إلى هذا التنظيم القانوني بعيد المنال وذلك لسببين جوهريين ألأول: القدرة التكنولوجية المتنامية والتي أصبحت تؤثر في إخفاء الجهة مصدر الاعتداء أكثر من أي وقت مضى والثاني: أن الكثير من الدول ترى في الإبقاء على حالة الغموض طريقا للإضرار بدول معينة من خلال هجمات إلكترونية دون تمكن الأخيرة من الاستناد إلى الدفاع عن النفس ضمن إطار قواعد القانون الدولي والعام وتحديدا المادة 51 من ميثاق الأمم المتحدة.

## قائمة المصادر و المراجع:


### الاتفاقات والوثائق الدولية:

النظام الأساسي لمحكمة العدل الدولية 1945.

مشروع مواد مسؤولية الدول عن الأفعال غير المشروعة للعام 2001.

الاتفاقية الخاصة باحترام قوانين وأعراف الحرب البرية 1907.

اتفاقات جنيف 1949 وبروتوكولاتها الإضافية.

United Nations Charter (1945).

UN General Assembly Res. 3314 (XXIX), Definition of Aggression, Adopted 14 December 1974.

### الأحكام القضائية:

ICJ, Oil Platforms Case, (Islamic Republic of Iran v. United States of America), Reports 2003.

ICJ, Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States), 1986.

ICJ, Corfu Channel Case (UK. v. Albania), 1949.

ICJ, Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro) 1996.

ICJ, Case Concerning Gabčíkovo–Nagymaros Project (HUNGARYISLOVAKIA), 1997.

Arbitral Award in the Naulilaa Case 1928, 2 Reports of the International Arbitral Awards 1011-1028.

**الكتب:**

B. Rorbert P., The Due Diligence Principle under International Law, International Law Community Law Review, Vol.81, Issue 8, (2006).

D. Yoram, War, Aggression and Self-defence (3ed edition 2011).

M. Larry, War Crimes and Just War, Cambridge University Press, (2007).

N. Micheal & M. Larry, Proportionality in International Law, Oxford University Press, 2014.

R. Thomas, Cyber War Will Not Take Place, Oxford University Press, 2013.

S. Malcolm, International Law, (7th edition, 2014), Cambridge University Press.

S. Michael N. (ed.), Tallinn Manual on the International Law Applicable to Cyber Warfare (Cambridge University Press, 2013).

T. Nicholas & B. Russell (Eds.), Research Handbook on International Law and Cyberspace, Elgar, 2015.

**المقالات:**

B. Daniel, Principles Relevent to the Scope of Self-Defence Against Imminent or Actual Armed Attack by Nonstate Actors, American Journal of International Law, Vol. 106, 769, 2012.

H. Oona A., The Law of Cyber-Attack, Yale Law School Legal Scholarship Repository, 2012.

H. Kamrul, The Concept of Jus Cogens and the Obligation under the U.N. Charter, Santa Clara Journal of International Law, Vol.3, Issue 1, 2005.

P. Milorad, The International Public Law and the Use of Force by States, Journal of Liberty and International Affairs | Vol. 1, No. 2, 2015.

S. Lee, Active Defense: State Military Response to International Terrorism, 17, California Western International Law Journal, 1987.

**مراجع أخرى:**

البداينـة، ذيـاب ، الجرائـم الإلكترونيـة: المفهـوم والأسـباب، ورقة عمل ضمـن الملتقى العلمي حول الجرائم المسـتحدثة فـي ظـل المتغيـرات والتحولات الدولية، كلية العلوم الإسـتراتيجية، عمـان 2014/9/4-2.

D. Yoram, Computer Network Attacks and Self-Defense, 76 U.S. Naval War College of International Law Studies (2002).

E. Omer, The Legality of Non-forcible Counter-measures in International Law (Oxford Monographs in International Law), 1988.

# The Right to Self-Defense in Response to Cyber-Attacks in Light of International Law

**Rezeq Ahmad Samoudi**

Faculty of Law - Arab American University

Jenin - Palestine

**Abstract:**

One of the most important issues brought about by modern technological capabilities is that they have produced new and more complex legal questions than answers regarding the relationship between states. These questions were unprecedented and inconceivable not long ago. One of the most current complicated questions concerns the availability of legal means to the state to deal with situations where it is subjected to electronic (non-kinetic) aggression by another State. More specifically, the question is whether or not traditional legal rules on the use of force and self-defense are consistent with the notion of cyber attacks. Is a cyber attack legally entitled to self-defense as required by Article 51 of the Charter of the United Nations? Or is it merely a use of force under Article 2 (4) Charter that leaves the aggressor state with no legal option to defend itself? Or else, is there another distinct approach particularly designed to deal with cyber attacks? This paper handles these important legal questions through a comprehensive review of the rules of international law on the use of force in general and self-defense in particular and the relation between them. In addition, the paper looks at the current state of practice of states in an attempt to forecast any emerging customary international law in this regard.

**Keywords:** Non Kinetic Attack, Cyber Attacks, Tallinn Manual, Syntactic, Semanti.