مجلة العلوم الشرعية
جامعة القصيم، العدد (١)، *المجلد* (١٢)، ص ص ٧٦٧ -٧٨٩ (ذو الحجة ١٤٣٩ هـ / سبتمبر ٢٠١٨م)

الحرب المعلوماتية وإمكانية تطبيق قواعد حقوق الإنسان

الدكتور علي عبد المعطي الحمدان
أستاذ مساعد في قسم القانون الدولي بكلية الحقوق، جامعة دمشق

ملخص البحث: تناول الكثير من فقهاء القانون الجانب القانوني للحرب المعلوماتية وخاصة مسألة القانون واجب التطبيق على هذا النوع من الحروب. ولقد انقسم هؤلاء الفقهاء إلى قسمين: نادى القسم الأول بوجوب تطبيق القواعد التقليدية للقانون الدولي العام والقانون الدولي الإنساني على عمليات الحرب المعلوماتية ولكن مع تكييف هذه القواعد مع هذا النوع من الحروب. أما القسم الثاني فطالب بوجوب إيجاد قواعد قانونية خاصة بالحرب المعلوماتية. وقد برروا ذلك بأن القواعد التقليدية التي تطبق عادة على الحروب الكلاسيكية لا يمكن تطبيقها في حالة الحرب المعلوماتية لاختلاف طبيعة كل منهما حيث أن الأخيرة تتكون عادة من مجموعة عمليات غير متجانسة فيما بينها. وفي هذه الدراسة تم اقتراح إيجاد حل آخر وهو تطبيق قواعد القانون الدولي لحقوق الإنسان لأسباب سوف نشرحها في صلب الدراسة. وبالتالي استعرضنا في هذا البحث الحلول التقليدية بشكل عام والحل الذي اقترحناه بشكل خاص.

الكلمات المفتاحية: الحرب المعلوماتية، الهجمات الإلكترونية، حقوق الإنسان، القانون الدولي العام، القانون الدولي الإنساني.

مجلة العلوم الشرعية
جامعة القصيم، العدد (١)، *المجلد* (١٢)، ص ص ٧٦٧ -٧٨٩ (ذو الحجة ١٤٣٩ هـ / سبتمبر ٢٠١٨م)

مقدمة

يعتقد نائب مدير الشؤون الاستراتيجية في وزارة الدفاع الفرنسية، بأن خلل ما بمفتاح (USB)[١] أو ما يسمى (الناقل التَّسَلْسُلي العام)، يمكن أن يؤدي إلى أضرار أكثر من قنبلة بحجم (٢٥٠) كيلو غرام. ويضيف بأن التهديد الإلكتروني لا يقف عند حد زعزعة وجه الصراع التقليدي، بل يشكل خطراً حقيقياً على الدول فضلاً عن تهديده للأفراد[٢].

إن الحرب المعلوماتية[٣] هي ظاهرة جديدة نسبياً، برزت نتيجة اعتماد الإنسان على تقنية المعلومات، بالإضافة إلى انخفاض تكلفتها نسبياً والتي جعل منها سلاحاً غير مادي مع إمكانات هجومية قوية.

انتشرت هذه الظاهرة في الآونة الأخيرة بشكل كبير جداً في العلاقات الدولية، خاصة في الولايات المتحدة الأمريكية والصين وروسيا. حيث أصبحت تشكل نسخة جديدة من التوترات الدولية وتحدياً واضحاً للقانون الدولي. وقد أثارت هذه الظاهرة منذ فترة قصيرة اهتمام القانونيين الدوليين[٤]، وخاصة فيما يتعلق بالتغييرات التي يمكن أن تطرأ بسببها على قانون الحرب وعلى نظرية

---

[١] Universal Serial Bus

[٢] مقابلة أجرتها معه الصحفية الفرنسية (Dorthée Moisan) بتاريخ ٢٨ يناير كانون الثاني ٢٠١٣ ومنشورة على الموقع التالي:
http://www.roubaix.maville.com/actu/actudet_-Les-cyberattaques-ont-fait-evoluer-les-questions-de-defense-General-Eric-Bonnemaison-_fil-٢٢٨٣٩٦٢_actu.Htm

[٣] حبذنا استعمال مصطلح (المعلوماتية) للدلالة على علوم الحاسوب بشكل عام وعلى النشاطات التي تتم عن طريق الشبكة العنكبوتية بشكل خاص، علماً أن هناك بعض الكتّاب العرب يستعمل مصطلح (السايبر) وهو مصطلح أكثر دقة ولكنه أجنبي. انظر الدكتور طارق المجذوب، السَّايْبِر ساحة خَفِيَّة لحربٍ ناعِمَة قادِمة! منشور على الموقع الرسمي للجيش اللبناني:
http://www.lebarmy.gov.lb/ar/news/?٤٠٩١٥
وقد يقول قائل لماذا لا نستعمل مصطلح "الحرب الإلكترونية"، والجواب على ذلك أن مصطلح "الحرب الإلكترونية" يستعمل للدلالة على استخدام وسائل إلكترونية حديثة في الحرب كاستعمال الرادارات والصواريخ الموجهة والطائرات بدون طيار، الخ، وليس المقصود منه استعمال الشبكة العنكبوتية في الحرب، إلا إننا قد نضطر لاستعمال هذه المصطلحات وفق السياق المقصود إذا رأينا أنه مناسب أكثر من غيره.

[٤] يمكن أن نذكر هنا على سبيل المثال:
M.N. Schmidt, «Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework», *Columbia Journal of Transnational Law*, ١٩٩٩, pp. ٨٨٥-٩٣٧.

مجلة العلوم الشرعية
جامعة القصيم، العدد (١)، المجلد (١٢)، ص ص ٧٦٧ -٧٨٩ (ذو الحجة ١٤٣٩ هـ / سبتمبر ٢٠١٨م)

الحرب العادلة. وقد أصبحت مسألة وجود المعاهدات الدولية التي تضع القواعد الناظمة للحرب المعلوماتية ضرورة حتمية. ولكن يبدو من المرجح أن ذلك يحتاج إلى المزيد من الوقت لإتاحة الفرصة أمام النقاشات الجادة التي يمكن أن تغني هذا الموضوع الحساس وتطرح الحلول المناسبة لبعض إشكالاته(٥).

ومن هنا يبدو من المناسب التساؤل عن مدى قدرة القواعد الدولية الموجودة حالياً على استيعاب ومواجهة جميع الإشكالات القانونية التي تثيرها الحرب المعلوماتية. من هذا المنطلق، ركزت دراستنا على تلك الأعمال الهجومية التي تُرتكَب من خلال الحاسوب وتشترك فيها الدول كفاعل أو كضحية أو يُشكل مواطنوها ضحية لهذه الأعمال. أما أعمال القرصنة العادية التي يرتكبها الأفراد العاديون بشكل فردي معزول من خلال الشبكة العنكبوتية فهي خارج نطاق هذه الدراسة.

ولابد من الإشارة إلى أن الصعوبة هنا لا تظهر فقط في الدلالة وبل أيضاً في المفاهيم؛ لأن ما يسمى الحرب المعلوماتية هي عبارة عن أفعال متعددة الأوجه، لذلك يجب أولاً تحديد مفهوم الحرب المعلوماتية (المبحث الأول)؛ ومن ثم تحديد قواعد القانون الدولي القادرة على مواجهة هذه الأعمال وبالتالي حماية ضحاياها سواءً أكانوا أفراداً أم دولاً (المبحث الثاني).

إشكالية البحث:

لقد انقسم الفقهاء الدوليون إلى قسمين فيما يتعلق بمسألة القانون واجب التطبيق على عمليات الحرب المعلوماتية:

- نادى القسم الأول بوجوب تطبيق القواعد التقليدية للقانون الدولي العام والقانون الدولي الإنساني؛
- أما القسم الثاني فيرى وجوب إيجاد قواعد قانونية خاصة بعمليات الحرب المعلوماتية. وقد برّر فقهاء هذا الاتجاه رأيهم بأن طبيعة الحرب المعلوماتية تختلف عن طبيعة الحرب التقليدية.

M. Hecker et T. Rid, «Les armées doivent-elles craindre les réseaux sociaux ?», Politique étrangère, vol. ٧٧, été ٢٠١٢, n°٢, pp. ٣١٧-٣٢٨.

(٥) حول هذه المسألة، انظر:

D. Brown, « A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict », *Harvard International Law Journal*, ٢٠٠٦, pp. ١٧٩-٢٢١; Ch. Dodge, « United States Cyber Command: International Restrictions vs. Manifest Destiny », North Carolina Journal of Law & Technology Online Edition, ٢٠١٠, pp. ١-٢٧.

مجلة العلوم الشرعية
جامعة القصيم، العدد (١)، *المجلد* (١٢)، ص ص ٧٦٧ -٧٨٩ (ذو الحجة ١٤٣٩ هـ / سبتمبر ٢٠١٨م)

والسؤال المطروح هنا: هل من الممكن تطبيق قواعد أخرى تكون أكثر مرونة من القواعد التقليدية للقانون الدولي العام؟ هذه الدراسة هي عبارة عن محاولة للإجابة على هذا التساؤل المثير للجدل من خلال اقتراح تطبيق قواعد القانون الدولي لحقوق الإنسان على الحرب المعلوماتية.

المبحث الأول: مفهوم حرب المعلوماتية

عملنا في هذا المبحث على محاولة إيجاد تعريف لمصطلح الحرب المعلوماتية (المطلب الأول)، ومن ثم حاولنا الوصول إلى فهم قانوني واضح ومحدد لهذا المصطلح (المطلب الثاني).

المطلب الأول: محاولة إيجاد تعريف لمصطلح الحرب المعلوماتية

الحرب المعلوماتية بالمعنى الدقيق للكلمة، لا ينبغي أن تكون إلا افتراضية فقط، تدور رحاها في العالم الافتراضي، وتستخدم أسلحة إلكترونية[٦]، غير موجودة إلا في المجال غير المادي[٧].

---

[٦] تحصي (سونسون) ثلاثة أنواع من الأسلحة الالكترونية، وهي حسب قولها:

١) «Syntactic weapons, which target a computer's operating system, include malicious code, such as viruses, worms, Trojan Horses, Dodos, and spyware»;

٢) «semantic weapons which consist of altering information that enters the computer's system»;

٣) « mixed or blended weapons which combine syntactic and semantic weapons to attack both information and the computer's operating system, resulting in a more sophisticated attack».

Lesley Swanson, « The Era of Cyber Warfare: Applying International Humanitarian Law to the ٢٠٠٨ Russian-Georgian Cyber Conflict », Loyola of Los Angeles International and Comparative Law Review, ٢٠١٠, p. ٣١٠-٣١١.

[٧] أنظر:

M. Baud, « La cyberguerre n'aura pas lieu, mais il faut s'y préparer », *Politique étrangère*, ٢٠١٢, vol. ٢, p. ٣٠٥-٣١٦.

مجلة العلوم الشرعية
جامعة القصيم، العدد (١)، المجلد (١٢)، ص ص ٧٦٧ -٧٨٩ (ذو الحجة ١٤٣٩ هـ / سبتمبر ٢٠١٨م)

والحقيقة أن السؤال المطروح هنا: ماهي الأعمال التي يمكن أن تُشكل ما يسمى "الأعمال الحربية" في الفضاء المعلوماتي؟
كما بينا سابقاً، فإن مصطلح "الحرب المعلوماتية" تم استخدامه للإشارة إلى حقائق متباينة جداً، من الصعوبة جمعها في وصف واحد؛ وبالتالي فهي تفتقد إلى مضمون قانوني واضح، مما أدى إلى استخدام تعابير جديدة أصبحت تُشكل المرجعية عند دراسة هذا النوع من الأفعال.
هذه التعابير يُفهم منها بأن: الحرب المعلوماتية هي في الواقع مجموعة من الأفعال والتصرفات تتم عن طريق الحاسوب، وتُستخدم من أجل خلق ضرر ما في المجال الدولي دون اللجوء بالضرورة إلى العنف[٨].
هذه الأفعال التي تُستخدم كجزء من الصراع أو الأعمال العدائية في سياق العلاقات الدولية، وأحيانا داخل إقليم دولة ما، قد تأخذ أشكالاً وتراكيباً مختلفة:
– قد يُشكل فعلٌ من أفعال الحرب المعلوماتية على سبيل المثال، أحد جوانب عملية عسكرية تجري في سياق نزاع مسلح، سواءً كان دولياً أم محلياً. وهكذا فقد سُجلت عدة هجمات إلكترونية روسية ضد جورجيا عام ٢٠٠٨ في سياق حرب أوسيتيا الجنوبية.
– وفي كثير من الأحيان، فإن أفعال الحرب المعلوماتية يمكن القيام بها خارج أي صراع مسلح، في وقت لا يعد من أوقات الحرب ولا السلام، ولكن "في وقت ما بين وبين". أي في وقت التوترات التي لا ترقى إلى وصف الحرب المعروف في القانون الدولي.

---

[٨] يوجد العديد من التعاريف، من أهمها: تعريف الكاتب رماح الدلقموني (الحرب الإلكترونية (Cyberwar) هي صراع ميدانه شبكة الإنترنت وينطوي على هجمات ذات دوافع سياسية على المعلومات ونظمها، حيث يمكنها تعطيل مواقع الويب الرسمية والشبكات وتعطيل الخدمات الأساسية أو سرقة وتعديل البيانات السرية، وتخريب الأنظمة المالية، وذلك من بين العديد من الاحتمالات الأخرى.) انظر مقال الكاتب على الجزيرة نت:

http://www.aljazeera.net/home/print/f٦٤٥١٦٠٣-٤dff-٤ca١-٩c١٠-١٢٢٧٤١d١٧٤٣٢/٠cd٢٣e٢b-d٠٥f-٤٣ec-a٢d٣-de٨٦٦٣٩d٤fd٦

أما عباس بدران فإنه لا يعرّف الحرب المعلوماتية ولكنه لجأ الى تقسيمها الى عدة مجالات منها مجال الدفاع الإلكتروني والهجوم الإلكتروني واخيراً مجال التجسس الرقمي، للمزيد انظر عباس بدران، الحرب الإلكترونية: الاشتباك في عالم المعلومات، مركز دراسات الحكومة الالكترونية، بيروت لبنان ٢٠١٠،.صفحة ٣٠.

مجلة العلوم الشرعية
جامعة القصيم، العدد (١)، *المجلد* (١٢)، ص ص ٧٦٧ -٧٨٩ (ذو الحجة ١٤٣٩ هـ / سبتمبر ٢٠١٨م)

– وكما ذكرنا أعلاه، فإن الهجوم الإلكتروني يمكن أن يتم في إطار العلاقات الدولية المتوترة؛ ويكون عبارة عن أعمال عدائية ضد دولة أخرى، مثل الهجمات الإلكترونية التي شنتها الحكومة التايوانية ضد المواقع الحكومية الصينية في عام ١٩٩٩. أو الهجمات الإلكترونية التي شنتها في العام نفسه، الحكومة الصينية ضد الولايات المتحدة الأمريكية، وذلك رداً على التفجير الذي تعرضت له السفارة الصينية في بلغراد.

أيضاً من الأمثلة الحية، والتي تأتي ضمن السياسات الأمريكية والإسرائيلية تجاه إيران، العملية التي سميت ستكسنيت (Stuxnet) ضد المنشآت النووية التي تم من خلالها نشر فيروس ستوكسنيت الحاسوبي عام ٢٠١٠، والذي دمّر أجهزة الطرد المركزي لتخصيب اليورانيوم[٩]. ويمكن اعتبار الهجوم الإلكتروني الذي يتم برعاية سلطات دولة معينة لتقويض مصالح دولة أجنبية، كعمل من أعمال الحرب المعلوماتية. وهذا النوع من الحرب المعلوماتية هو الأكثر شيوعاً. وعلى سبيل المثال، فإن استونيا كانت ضحية لعمليات واسعة النطاق عام ٢٠٠٧، والتي ضربت المواقع الحكومية والبنوك ووسائل الإعلام والأحزاب السياسية إلى درجة شل الحكومة بشكل شبه كامل.

– كذلك فإن مصطلح "الحرب المعلوماتية" يمكن أن يستعمل في اللغة المتداولة للدلالة على العمليات التي تتم من قبل دولة ضد كيان غير حكومي خارج أراضيها؛ ولاسيما في سياق إجراءات مكافحة الإرهاب أو العكس، فيمكن أن تكون هذه العمليات عبارة عن هجوم إرهابي تقوم به مجموعات غير حكومية ضد مصالح دولة ما أو ضد شعب هذه الدولة[١٠].

– كذلك يمكن أيضاً أن تدرج ضمن ما يسمى بأعمال "الحرب المعلوماتية"، الإجراءات المتخذة من قبل سلطات الدولة ضد مجموعة معادية تقع في أراضيها تطالب على سبيل المثال بالاستقلال.

– وأخيراً، وفقاً للتفسير العريض لمصطلح "الحرب المعلوماتية"، أصبح هناك ما يسمى "الثورات الحاسوبية أو الإلكترونية" التي تقودها الشبكات الاجتماعية والتي قد تحرّض على العنف أو على تغيير النظام، كما حصل في الثورة التونسية عام ٢٠١١ التي استفادت من المساعدات "الإلكترونية" التي قدمتها بعض الجهات.

---

[٩] ستكسنت عبارة عن برنامج كومبيوتر خبيث يهاجم أنظمة التحكم الصناعية المستخدمة على نطاق واسع في مراقبة الوحدات التي تعمل آلياً.

[١٠] حول دور الانترنت في العمليات الإرهابية، انظر:

W. Adhami, « The Strategic Importance of the Internet for Armed Insurgent Groups in Modern Warfare », RICR, vol. ٨٩, n°٨٦٨, ٢٠٠٧, p. ٨٦٤.

مجلة العلوم الشرعية
جامعة القصيم، العدد (١)، المجلد (١٢)، ص ص ٧٦٧ -٧٨٩ (ذو الحجة ١٤٣٩ هـ / سبتمبر ٢٠١٨م)

من خلال هذه الأمثلة، نلاحظ أن ما يسمى أعمال الحرب المعلوماتية هي مجموعة من الظواهر المتنوعة وغير المتجانسة، وبالتالي من الصعب إيجاد تعريف شامل وافٍ لهذه الأعمال.

المطلب الثاني: محاولة الوصول إلى توصيف قانوني للحرب المعلوماتية

هذه المجموعة المتنوعة من الحالات تكشف لنا حجم الصعوبات، وخاصة في ظل العدد المحدود من الظواهر المدروسة التي من خلالها يمكن أن نتوصل عادة إلى فرضيات معينة، يمكن فهمها من خلال القانون الدولي الإنساني.

وكما رأينا في الفقرة السابقة، فإن مصطلح "حرب الإنترنت أو الحرب المعلوماتية" يشير بشكل عام إلى مجموعة من الأعمال غير الودية تمارس ضد دولة ما، وتسبب لها أضراراً مباشرةً تصيبها أو تصيب رعاياها[١١]. ومن أجل محاولة الوصول إلى توصيف قانوني لظاهرة الحرب المعلوماتية، يمكن أن نلجأ إلى بعض المصطلحات التي قد تساعد في الوصول إلى الهدف المنشود:

بداية يمكن دراسة مصطلح "النزاع المسلح"، على أنه لابد من التنويه إلى أن هذا المصطلح لا يشكل سياقاً ضرورياً لفهم كل الحقائق التي شملتها الدراسة، ولكن من خلال هذا السياق يمكن فهم التركيب الذي يتكون منه مصطلح "الحرب المعلوماتية" لقياس قدرة عنصر "العدائية" على تحديد بعض الأمور بشكل قانوني. وكما هو معروف، فإن التعريف القانوني للنزاع المسلح لا يخلو من إثارة عدد من الصعوبات؛ إلا أن الاستعانة به يعد بالفعل أمراً ضرورياً للوصول إلى فهم مبدئي للكثير من الظواهر التي يتألف منها مفهوم الحرب. وبالتالي نستطيع القول بوجود حرب[١٢] كما برز في قضية "تاديتش"، في كل حالة يتم فيها اللجوء إلى القوة المسلحة بين الدول أو بين السلطات الحكومية والجماعات المسلحة المنظمة أو بين هذه الجماعات داخل الدولة[١٣].

---

[١١] يَعتبر الأستاذ (Joshua E. Kasterberg) أن الهجمات التي تمت ضد جورجيا عام ٢٠٠٨ التي عادة ما توصف بأنها من أعمال الحرب المعلوماتية، يمكن أن تعد جرائم وفقا لاتفاقية مجلس أوربا حول الجرائم الإلكترونية. أنظر:

E. Kastenberg, « Non-Intervention and Neutrality in Cyberspace, An Emerging Principle in the National Practice of International Law », Air Force Law Review, ٢٠٠٩, vol. ٦٤, p. ٥٨.

[١٢] أنظر: M. Bettati, *Droit humanitaire*, Précis Dalloz, ٢٠١٢, p. ٢٩.

[١٣] المحكمة الجنائية الدولية ليوغسلافيا السابقة، النائب العام ضد تاديتش، حكم الاستئناف التبعي، ١٩٩٥/١٠/٢، خاصة فقرة رقم ١٠.

ولكن هل نستطيع في ظل انتشار ظاهرة الإرهاب والجريمة المنظمة[١٤]، أن نقول بأن مرونة مصطلح "الحرب"، يمكن أن يشمل أيضاً "الحرب المعلوماتية"، سواء من حيث تحديد مجال تطبيق القواعد القانونية في الحرب أم من حيث ما يسمى بالحرب العادلة! في الحقيقة، لا يوجد في القانون الوضعي ما يسمح بتوسيع مصطلح "الحرب" بما فيه الكفاية ليشمل جميع وقائع الأفعال "التكنولوجية". والأسوأ من ذلك، أن استخدام مصطلح "الحرب" في عمليات الفضاء الإلكتروني يحجب حقيقة الحرب المعلوماتية التي لا تتناسب من حيث الإطار القانوني مع مصطلح "الحرب" و"استخدام القوة" في القانون الوضعي[١٥]. وإذا كان مصطلح "الحرب" يؤكد على خطورة الأفعال المعنية وعواقبها، فإنه لا يمكننا بمعناه المعتاد تحديد في معظم الأحيان حالات الهجمات الإلكترونية التي تدخل ضمن هذا المصطلح. فهدف هذه الهجمات إحداث أضرار متفاوتة الخطورة تترك آثاراً في الجوانب الاقتصادية أو السياسية أو العسكرية أو حتى الإنسانية. علاوةً على ذلك، فإنه من خلال رصد بعض الحقائق تبين أن هجمات الحاسوب تشكل غالباً تصرفاً معزولاً[١٦]؛ وبالتالي مع وجود هكذا صعوبات، تبدو الفرصة سانحة للبحث عن مصطلح آخر ذو نطاق عام قد يكون أقل إثارة للجدل. وقد قام مركز الدراسات الأمنية (CSS) في زيوريخ بتمييز بعض الحالات من مثل حالات القرصنة أو ما يسمى "الهكر" "cyberhacktivisme" أو التخريب الإلكتروني"cybervandalisme" والتي تعد قرصنة للمواقع مع تدمير البيانات الحاسوبية عن حالات "الإرهاب الإلكتروني" أو "الجرائم الإلكترونية" أو حتى "التجسس

---

[١٤] حول هذا الموضوع، انظر:

S. Vité, «La lutte contre la criminalité organisée : peut-on parler de conflit armé au sens où l'entend le droit international humanitaire ? », Conflits armés, parties aux conflits armés et droit international humanitaire : les catégories juridiques face aux réalités contemporaines, Actes du colloque de Bruges, ٢٢-٢٣ octobre ٢٠٠٩, Collegium, n°٤٠, ٢٠١٠, pp. ٦٩-٧٧.

[١٥] أنظر: فيدا أنتولين جينكينز:

V.M. Antolin-Jenkins, « Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places? », Naval Law Review, ٢٠٠٥, p. ١٣٤.

[١٦] أنظر: فيدا أنتولين جينكينز، مرجع سابق، ص.١٢٧.

مجلة العلوم الشرعية
جامعة القصيم، العدد (١)، المجلد (١٢)، ص ص ٧٦٧ -٧٨٩ (ذو الحجة ١٤٣٩ هـ / سبتمبر ٢٠١٨م)

الإلكتروني"[١٧]. وبالتالي في خضم هذه المصطلحات، يبدو أن مصطلح "النزاع المسلح" هو أقرب المصطلحات التي تستطيع تحديد مفهوم "الحرب المعلوماتية". أما بقية المصطلحات فيمكن أن تؤدي إلى مفاهيم غامضة وقد لا تفي بالغرض المطلوب.

وهناك رأي يدعو لوضع مصطلح يسمح بوصف جميع أنواع التصرفات الضارة عبر شبكة الإنترنت، سواءً أكانت هذه التصرفات موجهه ضد دولة ما أو ضد مصالح هذه الدولة أو أن تكون هذه التصرفات مرتكبة من قبل دولة أخرى.

فحالات القرصنة والتخريب الإلكتروني والإرهاب الإلكتروني والتجسس الإلكتروني، وما ورد في إطار الاتفاقية المتعلقة بجرائم الإنترنت[١٨]، يمكن أن يضمها تعريف عام واحد. وبالتالي يمكن أن يكون مصطلح "الهجوم الإلكتروني" هو المصطلح الأنسب والأصح لوصف أي واحدة من هذه الممارسات عندما تحدث بشكل معزول ولا تصل إلى درجة "النزاع المسلح". لذا هذا المصطلح يشير إلى حدث أو تصرف بشكل أكثر دقة من مصلح "الحرب المعلوماتية"، وليس بالضرورة أن يشكل هذا الحدث "عدواناً" بموجب القانون الدولي وبالتالي يعكس بدقة أكبر مجموعة من الحقائق ذات الصلة. وإذا كانت العمليات الإلكترونية هي التي يمكن وصفها على نطاق واسع، بأنها مجموعة عمليات موجهة ضد جهاز حاسوب أو شبكة معلوماتية أو من خلال تدفق البيانات بين هذه الأجهزة والشبكات[١٩]؛ فإن الهجوم الإلكتروني هو أحد مشتقاتها، فهو يقع في حال كون الدولة هي أصل العمل العدواني الموجه ضد الأهداف السياسية أو العسكرية أو الاقتصادية أو التجارية أو الاجتماعية لدولة أخرى.

---

[١٧] أنظر:

M. Dunn Cavelty, « Cyberwar: Concept, Status Quo, and Limitations », CSS Analysis in Security Policy, n° ٧١, avril ٢٠١٠.

[١٨] الاتفاقية المتعلقة بجرائم الإنترنت، بودابست، حزيران يونيو ٢٠٠١.

[١٩] اللجنة الدولية للصليب الأحمر:

Comité international de la Croix-Rouge, Le droit international humanitaire et les défis posés par les conflits armés contemporains. Rapport, XXXIème Conférence internationale de la Croix-Rouge et du Croissant-Rouge, Genève, Suisse, ٢٨ novembre-١er décembre ٢٠١١, ٣١IC/١١/٥,١,٢, p. ٤٢.

مجلة العلوم الشرعية
جامعة القصيم، العدد (١)، *المجلد* (١٢)، ص ص ٧٦٧ -٧٨٩ (ذو الحجة ١٤٣٩ هـ / سبتمبر ٢٠١٨م)

نستنتج هنا أن غياب تعريف دقيق لمفهوم الحرب المعلوماتية أدى إلى غياب الوصف القانوني المناسب لهذه الأعمال التي تشكل هذا النوع من الحروب. ولكن يمكن استعمال بعض المصطلحات التي يمكن من خلالها الوصول إلى فهم جزئي لمفهوم الحرب المعلوماتية، مثل مصطلح "نزاع مسلح" ومصطلح "الهجمات الإلكترونية"... الخ.

المبحث الثاني: تحديد القواعد القانونية واجبة التطبيق

بالنظر إلى اختلاف وتنوع هذه الممارسات التي يمكن أن تشكل ما يسمى بالحرب المعلوماتية، فإن رجل القانون يقع عليه واجب البحث عن قانون واجب التطبيق على هذه الظواهر المتنوعة. في هذا البحث تطرقنا إلى إمكانية تطبيق القواعد التقليدية للقانون الإنساني الدولي والقانون الدولي العام (المطلب الأول)؛ ثم عرجنا على إمكانية تطبيق قواعد أخرى تساعد في فهم هذه الظواهر وتتمثل هذه القواعد في القانون الدولي لحقوق الإنسان (المطلب الثاني).

المطلب الأول: الحرب المعلوماتية وإمكانية تطبيق القواعد التقليدية

تتحدى الحرب المعلوماتية القواعد التقليدية للقانون وذلك بسبب خصائصها المميزة لها كما رأينا أعلاه. وبالتالي فإن ظهور الشبكة العنكبوتية وما رافقها من عمليات أتمتة، أثار على الفور تساؤل القانونيين[٢٠]. وإذا كانت شبكة الإنترنت تثير تساؤلات جديدة فيما يتعلق بالقواعد القانونية القابلة للتطبيق، فإنها تتطلب أيضاً إيجاد قواعد خاصة بها. وكذلك فإن الهجمات الإلكترونية التي تتميز بتنوعها تحتاج إلى قواعد خاصة تطبق على واقع متغير جداً. فبالإضافة إلى القواعد العامة الموجودة مسبقاً، فإن الهجمات الإلكترونية تحتاج إلى معالجة خاصة تتكيف مع الخصوصية التي تنتج عن استخدام شبكة الإنترنت وعمليات الأتمتة التي تتصف بالفورية والآنية بالإضافة إلى الصعوبات التي تواجه تحديد مكان وزمان هذه التصرفات[٢١]. ولكن في غياب مثل

---

[٢٠] انظر على سبيل المثال:

A.-T. Norodom, «Propos introductifs. Internet et le droit international : défi ou opportunité ? », dans: Colloque de la S.F.D.I., Rouen, *Internet et le droit international*, Paris, Pedone, ٢٠١٤, pp. ١١ et suiv.

[٢١] أنظر:

M.N. Schmidt (dir.), Tallinn Manual on the International Law Applicable to Cyber Warfare. Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defense Centre of Excellence, Cambridge UP, ٢٠١٣, p. ١٥.

مجلة العلوم الشرعية
جامعة القصيم، العدد (١)، المجلد (١٢)، ص ص ٧٦٧ -٧٨٩ (ذو الحجة ١٤٣٩ هـ / سبتمبر ٢٠١٨م)

هذه القواعد الخاصة، فإن القواعد التي يمكن تطبيقها الآن هي في معظمها مستمدة من القانون الدولي العام والقانون الدولي الإنساني. وفي مواجهة ما يعنيه مصطلح الحرب المعلوماتية، فإن الفقه القانوني مثله مثل الفقه العسكري، عادة ما يتبنى منطق التقليد الأعمى لحالة النزاعات المسلحة التقليدية؛ وبالتالي فإن هذا المنطق يؤدي إلى تطبيق قواعد القانون الدولي الإنساني التقليدي. وإذا أجرينا إحصاء سريع للفرضيات التي ينطوي عليها مدلول الحرب المعلوماتية، فإننا سنخلص إلى نتيجة مفادها عدم كفاية المقاربات التي تنادي بتطبيق قواعد الحرب التقليدية.

عندما ينطوي الهجوم الإلكتروني على تورط سلطات الدولة التي تتحمل المسؤولية عن هذه الأعمال أو يؤدي هذا الهجوم إلى الإضرار بمصالح إحدى الدول، فإن القواعد الأساسية تعتمد على سياق الوقائع المحددة لكل حالة على حدة. وعندما يكون النزاع المسلح موجود بالفعل، فإن القانون الدولي الإنساني يسعى إلى تطبيق قواعد هذا النزاع على الهجوم الإلكتروني نفسه[٢٢]؛ أي يصبح هذا الهجوم الإلكتروني مسألة فرعية أو جزء من كل. ولكن باعتبار أن الحرب تتضمن "قيام أفعال" كشرط لتطبيق قواعد لاهاي وجنيف[٢٣]، فإن الحرب المعلوماتية فقط هي التي يمكن أن يطبق عليها القانون الدولي الإنساني دون بقية الحالات أو الممارسات الإلكترونية. وكذلك فإن الحرب المعلوماتية يجب أن تحترم القواعد الآمرة في قانون الحرب، وخاصة فيما يتعلق بمبدأ الضرورة العسكرية ومبدأ التناسب ومبدأ الحياد[٢٤]. وعلاوة على ذلك، فإن قواعد الحرب عندما تكون قابلة للتطبيق، فإنها تواجه صعوبات جمة منها: عدم وجود قواعد محددة خاصة بالحرب المعلوماتية، وصعوبة تحديد مكان الهجوم، بالإضافة إلى تجنب السلطات الحكومية توريط نفسها بشكل مباشر في هذه الأعمال. وهكذا على الرغم من أن القواعد التقليدية للقانون الدولي الإنساني قد تكون مفيدة في فهم الهجمات الإلكترونية، إلا أنها تبدو غير كافية.

---

[٢٢] انظر:

K. Dörmann, « Applicability of the Additional Protocols to Computer Network Attacks», International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law, Stockholm, ١٧-١٩ novembre ٢٠٠٤, http://www.icrc.org/eng/resources/documents/misc/٦٨lg٩٢.htm

[٢٣] انظر:

E. David, *Principes de droit des conflits armés*, ٥ème éd., Bruxelles, Bruylant, ٢٠١٢, p.٧٨.

[٢٤] كثيراً ما يتم اختراق مبدأ الحياد في الحرب المعلوماتية بسبب ان الفاعلين قد يستخدمون أراضي الدول المحايدة.

مجلة العلوم الشرعية
جامعة القصيم، العدد (١)، *المجلد* (١٢)، ص ص ٧٦٧ -٧٨٩ (ذو الحجة ١٤٣٩ هـ / سبتمبر ٢٠١٨م)

من ناحيته، فإن القانون الدولي العام يقدم أيضاً بعض الحلول، ولكنه لم يستطع الإجابة على كثير من الأسئلة. فالهجوم الإلكتروني يجب أن يحتوي على استخدام القوة بموجب القانون الدولي، وتحديداً وفق ميثاق الأمم المتحدة؛ وبالتالي فإنه يمكن جزئيا على الأقل أن يوصف على هذا الأساس، بأنه عدوان[٢٥]. كذلك فإن الهجوم الإلكتروني عندما يأتي كإجراء انتقامي أو كإجراء مضاد، فإنه يمكن أن يخضع للنظام القانوني ذي الصلة؛ وبالتالي عندما يكون الهجوم الإلكتروني نوعاً من الإجراءات الانتقامية، فإنه يجب ألا يسبب إلا أضراراً محدودةً، لأنه يخضع لمبدأ التناسب وهو السبيل الوحيد لرد العدوان[٢٦]. كذلك يستطيع مجلس الأمن وفقاً للفصل السابع من ميثاق الأمم المتحدة اتخاذ التدابير الضرورية في حالات تهديد السلم والإخلال به ووقوع العدوان؛ وبالتالي للمجلس أن يقرر ما إذا كان قد وقع تهديد للسلم أو إخلال به أو عمل من أعمال العدوان؛ ولديه كامل الصلاحيات بأن يقدم توصيات أو يلجأ إلى القيام بعمل عسكري أو غير عسكري لحفظ السلم والأمن الدوليين. ولكن من شروط الفعل المجرّم هنا تهديده للسلم والأمن الدوليين، أي أن العبرة للنتيجة وليس للوسائل المستخدمة[٢٧]. وبالتالي نستطيع الاستنتاج بأن العمليات الإلكترونية إذا أدت إلى تهديد السلم والأمن الدوليين فإن مجلس الأمن يستطيع التدخل وفقاً للفصل السابع من الميثاق.

---

[٢٥] انظر على سبيل المثال:

M.N. Schmitt, « Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework », *Columbia Journal of Transnational Law*, ١٩٩٩, pp. ٨٨٥-٩٣٦; M. Roscini, «World Wide Warfare – *Jus ad bellum* and the Use of Cyber Force», *Max Planck UNYB*, ٢٠١٠, pp. ٨٥-١٣٠.

[٢٦] انظر:

Tribunal arbitral germano-portugais, *Affaire de Lysne (Responsabilité de l'Allemagne à raison des actes commis postérieurement au ٣١ juillet ١٩١٤ et avant que le Portugal ne participât à la guerre*), *RSA* II, p. ١٠٥٦.

[٢٧] مصطفى نعوس، حقوق والتزامات الدول في الحرب المعلوماتية، مجلة علوم الشريعة والقانون، المجلد ٤٠، الملحق الأول، ٢٠١٣، ص ٧٨٦.

مجلة العلوم الشرعية
جامعة القصيم، العدد (١)، المجلد (١٢)، ص ص ٧٦٧ -٧٨٩ (ذو الحجة ١٤٣٩ هـ / سبتمبر ٢٠١٨م)

بالمقابل، فإن تطبيق قواعد للقانون الدولي بالمعنى المعتاد على جميع الهجمات الإلكترونية، يعد أمراً غير متفق عليه. لأن هناك العديد من الحالات التي هي عبارة عن أفعال أو ممارسات معزولة أو على الأقل لا تشكل جزءاً من صراع مسلح، وبالتالي من الصعب اعتبارها عدواناً بموجب ميثاق الأمم المتحدة.

ويجب التنويه أيضاً إلى أنه في كثير من الأحيان يتم اللجوء إلى مبدأي الإقليمية والشخصية بالنسبة للقوانين[٢٨]، والتي تسمح عادةً بتحديد اختصاصات الدولة، وذلك لتطبيق القواعد القانونية المناسبة على جرائم الشبكة العنكبوتية[٢٩].وقد تكون معايير إسناد المسؤولية مفيدة أيضاً في هذا المجال، مثل معيار مدى تورط أجهزة الدولة في ارتكاب أعمال الحرب المعلوماتية. مما يسمح بإسناد المسؤولية الدولية للدولة بسبب تصرفات مسؤوليها عندما تسبب هذه التصرفات ضرراً ما. ولكن الإشكالية تقع عندما يرتكب الأفراد العاديون هذه الأعمال، لأن أعمال الهجمات الإلكترونية يرتكبها في كثير من الأحيان مواطنو دولة موجودون خارج حدود دولتهم. أي أن هذه التصرفات تتم في أراضي دولة أجنبية أخرى. ولهذا فإن هذه المعايير تبدو غير كافية للتعامل مع قضية تكنولوجيا المعلومات. وهكذا، فإن القانون الدولي العام لا يعطينا إلا الحلول الجزئية لمسألة الحرب المعلوماتية ويترك الكثير من المناطق الرمادية إلى أن يحين الوقت المناسب لفهم هذه الظاهرة الجديدة التي تثير المزيد من الصعوبات والتي تتميز ببعدها غير المادي وبصفتها الآنية.

من جانبه، فإن القانون الدولي لحقوق الإنسان، يمكن أن يحتوي على بعض الأدوات التي تساعد في البحث عن القواعد ذات الصلة بالهجمات الإلكترونية.

---

[٢٨] يعني مبدأ إقليمية القوانين أن يسري قانون الدولة على كل من يوجد في اقليمها من وطنيين وأجانب، وعدم سريان هذا القانون على كل من يقع خارج حدود اقليمها، فلا يسري قانون الدولة حتى على رعايا هذه الدولة المقيمين خارج اقليمها، (اي المقيمين في دولة اجنبية). أما مبدأ شخصية القوانين فيعني سريان قانون دولة معينة على الاشخاص التابعين لها حتى لو كانوا مقيمين خارج حدود اقليمها، وعدم سريان ذلك القانون على الاجانب حتى ولو كانوا مقيمين في اقليمها.

[٢٩] انظر على سبيل المثال:

Ph. Lagrange, « Internet et l'évolution normative du droit international : d'un droit international applicable à l'Internet à un droit international du cyberespace ? », dans: Colloque de la S.F.D.I., Rouen, *Internet et le droit international*, Paris, Pedone, ٢٠١٤, p. ٢٨.

مجلة العلوم الشرعية
جامعة القصيم، العدد (١)، المجلد (١٢)، ص ص ٧٦٧ -٧٨٩ (ذو الحجة ١٤٣٩ هـ / سبتمبر ٢٠١٨م)

المطلب الثاني: إمكانية تطبيق القانون الدولي لحقوق الإنسان

بما أن قواعد كل من القانون الدولي الإنساني والقانون الدولي العام لا تشمل جميع الفرضيات، فإن اللجوء إلى مصادر إضافية بما فيها القانون الدولي لحقوق الإنسان، يعد أمراً مرغوباً به لفهم ظواهر الحرب المعلوماتية وعواقبها ضد الافراد. فبفضل صفة العمومية التي يتمتع بها هذا القانون وشموليته وقدرته على الدوام والاستمرار فهو يعد أعم واشمل من القانون الدولي الإنساني؛ وكذلك يتميز بالدوام[٣٠] مما يجعله شبه قادر على احتواء وفهم أغلب ظواهر الحرب الإلكترونية وعواقبها ضد الأفراد. خاصة أن الحالات التي يعالجها القانون الدولي لحقوق الإنسان ليس من الضروري أن تكون محكومة بقواعد القانون الدولي الإنساني. وبالتالي فإن قواعد القانون الدولي لحقوق الإنسان يمكن أن تكون قابلة للتطبيق على الهجمات الإلكترونية.

إن قواعد القانون الدولي لحقوق الإنسان هي قواعد ثمينة لأنها تقدم الحلول القانونية الأكثر شمولية واتساقاً نظراً لعدم التجانس الفعلي للحالات التي ينظر فيها؛ من خلال ذلك، فإنه يمكن أن يكون لدينا بعض الحلول القانونية الشاملة والمنطقية التي تساعد في فهم هذه الأوضاع الجديدة. وبالتالي، فإن القانون الدولي لحقوق الإنسان يقدم إطاراً جديداً قد يساعد على حل اثنتين من الصعوبات القانونية الرئيسة التي تثيرها الحرب المعلوماتية: إسناد الهجوم الإلكتروني إلى دولة معينة، وتحديد قواعد القانون التي يجوز أن تحكم آثار هذا الهجوم على الأفراد.

إن إسناد الهجوم الإلكتروني إلى دولة معينة من أجل تحديد مسؤوليتها هو أحد التحديات التي يمكن أن تُحل من خلال قواعد القانون الدولي لحقوق الإنسان. والواقع أن مسألة "الآنية" لأي عمل من شأنه التسبب في ضرر وبالتالي تحريك مسؤولية الدولة، أُثيرت ضمن مجال الحماية الدولية لحقوق الإنسان. فمن المتعارف عليه، أن تشمل اختصاصات الهيئات القضائية أراضي الدول التابعة لها؛ وأن تصدر هذه الهيئات قرارات وأحكام تتعلق بقضايا وقعت أحداثها في داخل هذه الدول وعلى أراضيها. ولكن لم تمنع هذه القاعدة القانونية المحكمة الأوروبية لحقوق الإنسان من النظر في عدد من القضايا التي تتعلق بانتهاكات لأحكام الاتفاقية الأوروبية لحقوق الإنسان[٣١] من قبل دول أطراف في هذه الاتفاقية؛ ولكن بخصوص أحداث وقعت على أراضي دول غير أطراف في الاتفاقية ارتكب فيها عدد من المواطنين الخاضعين لقضاء الدول الأطراف هذه الانتهاكات.

---

[٣٠] من المعروف أن القانون الدولي لحقوق الإنسان يطبق في جميع الاوقات (السلم والحرب)، بعكس القانون الدولي الإنساني أو ما يسمى (بقانون الحرب) الذي لا يطبق إلا في وقت الحرب.

[٣١] انظر ترجمة هذه الاتفاقية في: الاتفاقيات الأوروبية لحماية حقوق الإنسان، تقديم وترجمة الدكتور محمد أمين الميداني، الدكتور نزيه كسيبي،

مجلة العلوم الشرعية
جامعة القصيم، العدد (١)، المجلد (١٢)، ص ص ٧٦٧ -٧٨٩ (ذو الحجة ١٤٣٩ هـ / سبتمبر ٢٠١٨م)

ففي قضية العراقيين الذين قتلتهم القوات البريطانية والتي عُرضت على المحكمة الأوروبية لحقوق الإنسان عام ٢٠٠٧، المتعلقة بانتهاكات حقوق الإنسان، أثيرت عدة نقاشات حول إمكانية الولاية القضائية خارج الحدود دون وجود أي علاقة بين الأفعال المجرّمة وبين هذا القضاء الأجنبي. وتتلخص وقائع هذه القضية[٣٢] بتقديم مجموعة من المواطنين العراقيين شكاوى فردية إلى المحكمة الأوروبية لحقوق الإنسان بخصوص مقتل أقاربهم من قبل القوات البريطانية في مدينة البصرة. وقد دفعوا بأن أقاربهم قُتلوا وهم خاضعين لقضاء المملكة المتحدة وولايتها، حسب ما تنص عليه المادة الأولى من الاتفاقية الأوروبية لحقوق الإنسان[٣٣]. كما تشملهم حماية حق الحياة التي تقررها المادة الثانية من هذه الاتفاقية، وحظر التعذيب والعقوبات والمعاملات غير الإنسانية أو المهينة التي تنص عليها المادة الثالثة من الاتفاقية. وقد بينت المحكمة الأوروبية أن المملكة المتحدة كانت تملك الولاية القضائية التي تنص عليها المادة الأولى من الاتفاقية الأوروبية لحقوق الإنسان فيما يخص المدنيين الذين قُتلوا خلال الأعمال الأمنية التي قامت بها القوات البريطانية في البصرة وذلك أثناء الظروف الاستثنائية المرتبطة بمسؤولية المملكة المتحدة المكلفة بسلامة جنوب شرق العراق خلال الفترة ما بين الأول من الشهر الخامس من عام ٢٠٠٣ وحتى ٢٠٠٤/٦/٢٨. وحكمت المحكمة الأوروبية بمقتضى المادة (٤١) من الاتفاقية الأوروبية[٣٤]، بترضية عادلة للمدعين، وطلبت من حكومة المملكة المتحدة أن تدفع لكل مدعٍ مبلغ (١٧) ألف يورو كتعويض معنوي، ومبلغ (٥٠) ألف يورو بالتضامن بينهم كنفقات دعوى[٣٥].

إن لجنة البلدان الأمريكية لحقوق الإنسان كانت قد تبنت أيضاً نفس المنطق في قرارها الصادر في ٢٠١٠/١٠/٢١. وتتلخص هذه القضية بأن الإكوادور طلبت الاعتراف بالمسؤولية المحتملة لكولومبيا لتسببها بالضرر لمواطنها "ايسالا مولينا"، الذي تعرض

الطبعة الأولى، منشورات مركز القاهرة لدراسات حقوق الإنسان، سلسلة تعليم حقوق الإنسان ٢٢، القاهرة، ٢٠١٠، ص ٣٣ وما بعدها.

[٣٢] للمزيد من التفاصيل حول هذه القضية، راجع الدكتور محمد أمين الميداني، دراسات في الحماية الإقليمية لحقوق الإنسان، مركز المعلومات والتأهيل لحقوق الإنسان، تعز، طبعة ثانية معدّلة ومزيدة، ٢٠١٢، صفحة ٣٧٠ وما بعدها.

[٣٣] تنص المادة الأولى من الاتفاقية الأوروبية لحقوق الإنسان على أن "تعترف كل الأطراف السامية المتعاقدة لجميع الأشخاص الخاضعين لولايتها القانونية بالحقوق والحريات الواردة في القسم الأول".

[٣٤] تنص المادة ٤١ من هذه الاتفاقية الأوروبية، وعنوانها ترضية عادلة، على ما يلي: "إذا قررت المحكمة بأن هناك مخالفة للاتفاقية أو لبروتوكولاتها، وإذا كان القانون الداخلي للطرف السامي المتعاقد لا يسمح بإزالة نتائج هذه المخالفة بشكل تام، تمنح المحكمة للطرف المتضرر، إذا استدعى الأمر، ترضية عادلة".

[٣٥] الدكتور محمد أمين الميداني، مرجع سابق، ص. ص. ٣٧٢-٣٧٣.

للإعدام خارج نطاق القضاء على يد قوات الأمن الكولومبية في سياق عملية "فيونيكس"[٣٦] التي قادتها هذه القوات في شهر مارس آذار عام ٢٠٠٨ في الأراضي الأكوادورية. وقد سعت اللجنة إلى إيجاد علاقة سببية بين الضرر المتعلق بحقوق الإنسان وبين سلوك الدولة خارج حدودها. وراء هذا الامتداد السببي للالتزام بالمسؤوليةٍ المقبول جزئيا في نطاق الحماية الدولية لحقوق الإنسان، فإن الاعتراف بالطابع الفوري للسيطرة اللازمة لإثارة مسؤولية الدولة، يبدو أكثر سهولة.

في الواقع، فإن قرارات أجهزة الحماية الدولية لحقوق الإنسان تسمح في غياب وجود فعلي يمتد لفترة طويلة، بإثارة مسؤولية الدولة التي تسيطر بشكل فعال في الأحداث الجارية في إقليم دولة أخرى. إن نظرية "السيطرة الكاملة" التي تشير بصفة عامة إلى السلطة والسيطرة للدولة غير الإقليمية، تعد حاسمة لتحديد الاختصاص القضائي وبالتالي القدرة على إثارة المسؤولية. وبشكل أكثر تحديداً، في قضية "ستوكيه Stocké"[٣٧]، فإن "السلطة الفعلية والمسؤولية" هي المعايير التي أُعتبرت حاسمة. والرقابة المطلوبة يمكن أن تكون مجرد وقتية، فالنقطة الأساسية تكمن في أن السلطة التي تمارسها الدولة يجب أن تكون فعالة في لحظة معينة. كما أشارت اللجنة الأمريكية لحقوق الإنسان إلى أن وصف "الخاضعين لولايتها" الوارد في المادة الأولى من الاتفاقية الأمريكية لحقوق الإنسان، لا يشير إلى مكان حدوث الانتهاك بل إلى علاقة الفرد بالدولة المعنية[٣٨]. وبالتالي، وفقاً لنهج غير

---

[٣٦] Opération Phoenix.

[٣٧] تتلخص وقائع هذه القضية بأن السيد "ستوكيه Stocké" كان متهما بالتهرب الضريبي ولذلك قرر الهروب من المانيا الى سويسرا ومن ثم الى فرنسا إلى أن استطاع أحد مخبري الشرطة الألمانية استدراجه إلى المانيا حيث تم القبض عليه واعتقاله. احتج السيد ستوكيه بالاعتقال غير القانوني والمحاكمة غير العادلة، رفضت اللجنة الاوربية لحقوق الانسان الطلب واعتبرت ذلك كله تم في إطار القانون، إلا أنها اكدت على أنه وفق المادة الأولى من الاتفاقية الأوربية لحقوق الإنسان، يتعين على الأطراف السامية أن تعترف بحقوق محددة وفقاً للاتفاقية، وهذا الالتزام لا يقتصر على التراب الوطني للأطراف المتعاقدة بل يمتد الى جميع الأشخاص الخاضعين لسلطتها سواء أكانوا متواجدين على ارضها او في الخارج. للمزيد انظر:

Commission européenne des droits de l'homme, Stocké v. Allemagne, ١٢ octobre ١٩٨٩, Série A, vol. ١٩٩. P. ٢٤, § ١٦٦.

[٣٨] Commission IADH, Affaire ١٠,٦٧٥ c. Etats-Unis (Haitian Interdiction Case), ١٣ mars ١٩٩٧, § ١٤١.

مجلة العلوم الشرعية
جامعة القصيم، العدد (١)، المجلد (١٢)، ص ص ٧٦٧ -٧٨٩ (ذو الحجة ١٤٣٩ هـ / سبتمبر ٢٠١٨م)

إقليمي، فإن مقاربة تسلط الضوء على العلاقة البشرية، يمكن أن تكون أكثر فائدة لإثارة مسؤولية الدولة نتيجة لهجوم عبر الإنترنت يطال المدنيين ويقوض حقوق الإنسان.

إن الفكرة القائلة بأن الممارسة الآنية للسيادة من قبل الدولة على الأفراد، تكفي لإثارة مسؤولية الدولة عن انتهاكات حقوق الإنسان، تبدو مفيدة بشكل خاص وذلك لمعالجة حالات الهجمات الإلكترونية. ففي الواقع يتم الجمع بين الطابع الآني لهذه الظاهرة وبين افتقارها إلى جذور إقليمية حقيقية لإظهار أوجه الشبه مع فرضية الهجمات الإلكترونية التي تمت ضد دولة ما والتي تؤثر على الأرجح على الأفراد الموجودين في إقليمها وحقوقهم. على سبيل المثال: الحق في الحياة الخاصة والحقوق الاجتماعية وما إلى ذلك ...الخ.

وأخيراً، فمن الواضح أن حقوق الإنسان نفسها كما هو معترف بها من قبل النصوص الدولية، يمكن أن تشكل عوناً كبيراً لفهم الهجمات الإلكترونية. فالحق في الحياة والحق في الخصوصية والسلامة البدنية، والكثير من الحقوق التي تُمنح حماية دائمة من قبل النصوص الدولية، يمكن أن تكون عرضة للهجمات الإلكترونية. وبالتالي لدى ضحايا الانتهاكات الإلكترونية كل المصلحة، في حالة وقوع ضرر ما، في استدعاء قواعد القانون الدولي لحقوق الإنسان وأجهزته بدلاً من الانتظار للحصول على الحماية المقررة في القانون الإنساني. في الواقع هذا الأخير لا يطبق إلا في وقت النزاع المسلح، ومن المرجح ألا يثير مسؤولية الدول إلا في هذه الحالات فقط؛ ولا يثير مسؤولية الأفراد إلا في حالة ارتكاب جرائم تتصف بالخطورة الكافية ويجب أن يكون منصوص عليها في القانون الجنائي الدولي. في هذا السياق، فإن أجهزة الحماية الدولية لحقوق الإنسان من مصلحتها تبني قضايا الهجمات الإلكترونية وتحديد التقنيات اللازمة لتسهيل الوصول إلى مرتكبيها وبالتالي الاعتراف بمسؤولية الدول الراعية لمثل هذه الأعمال.

خاتمة وتوصيات:

لقد رأينا خلال البحث بأن خبراء القانون انقسموا إلى قسمين بالنسبة للقانون واجب التطبيق على الهجمات الإلكترونية: فمنهم من أوصى بتطبيق القواعد التقليدية للقانون الدولي العام والقانون الدولي الإنساني؛ ومنهم من أوصى بتطبيق قواعد خاصة بالهجمات الإلكترونية. ومع أننا نميل إلى الرأي الثاني لاحترامه لخصوصية الحرب المعلوماتية وبالتالي وجوب إيجاد قواعد قانونية خاصة بها، ولكن المشكلة أنه حتى الآن لم يتم سن هكذا قواعد. وبالتالي فمن الممكن اللجوء إلى قواعد تكميلية أخرى للوصول إلى إدراك وفهم الإشكالات القانونية المرتبطة بالحرب المعلوماتية.

هذه القواعد التكميلية هي قواعد القانون الدولي لحقوق الإنسان، وذلك لتميزها بعدة ميزات منها: الديمومة: حيث أنها دائمة التطبيق في حالة السلم والحرب بعكس قواعد القانون الدولي الإنساني التي تطبق في حالة الحرب فقط. كذلك تتصف هذه القواعد بصفة العمومية: حيث أنها أعم وأشمل من قواعد القانون الدولي الإنساني، وكذلك هي أشمل من قواعد القانون الدولي الجنائي التي تتعلق بالجرائم الكبرى فقط. وقد رأينا أنها قد تساعد في حل مشكلة الإسناد أيضاً، أي إسناد الفعل إلى دولة معينة. وقد ساعد على ذلك أحكام عدة هيئات ومحاكم دولية تم فيها إسناد انتهاكات حقوق الإنسان إلى دولة معينة دون ان يكون هناك رابط إقليمي معين بربط هذه الدولة بمكان وقوع الانتهاك. وبالتالي نوصي يتبني هذه القواعد بانتظار سن قواعد خاصة تطبق في حالة الحرب المعلوماتية.

أخيراً، أرجو أن تساهم هذه الدراسة بصورة فعالة في إغناء المكتبة القانونية العربية والله ولي التوفيق.

مجلة العلوم الشرعية
جامعة القصيم، العدد (١)، المجلد (١٢)، ص ص ٧٦٧ -٧٨٩ (ذو الحجة ١٤٣٩ هـ / سبتمبر ٢٠١٨م)

د. علي عبد المعطي الحمدان

Cyberwar and the possibility of application of human rights rules

Dr. Ali Alhamdan
Assistant Professor International Law Department, Faculty of Law

Damascus University

Many jurists have addressed the legal aspects of cyberwar focusing on the question of the international law that can be applied to this type of war. These jurists were divided into two categories: The first one has proposed the application of conventional rules of public international law as well as international humanitarian law on the operations of cyberwar with the adjustment of these rules to cyberwar. The second has suggested finding special legal rules for cyberwar. They supposed that the classic rules usually govern conventional wars cannot be applied to this war due to its heterogeneous nature usually consists of a set of operations. In the present study, we have proposed a new solution consisting mainly by the rules of international law of human rights for reasons explained in f the study. In this circumstance, we have discussed in details these solutions.

Keywords: cyberwar, cyber-attacks, human rights, public international law, international humanitarian law.

المراجع

المراجع العربية

١- الاتفاقيات الأوروبية لحماية حقوق الإنسان، محمد أمين الميداني، نزيه كسيبي، منشورات مركز القاهرة لدراسات حقوق الإنسان، سلسلة تعليم حقوق الإنسان ٢٢، القاهرة، الطبعة الأولى، ٢٠١٠.

٢- الحرب الإلكترونية، رماح الدلقموني، الجزيرة نت:

http://www.aljazeera.net/home/print/f٦٤٥١٦٠٣-٤dff-٤ca١-٩c١٠-١٢٢٧٤١d١٧٤٣٢/٠cd٢٣e٢b-d٠٥f-٤٣ec-a٢d٣-de٨٦٦٣٩d٤fd٦

٣- الحرب الإلكترونية: الاشتباك في عالم المعلومات، عباس بدران، مركز دراسات الحكومة الإلكترونية، بيروت لبنان ٢٠١٠.

٤- حقوق والتزامات الدول في الحرب المعلوماتية، مصطفى نعوس، مجلة علوم الشريعة والقانون، المجلد ٤٠، الملحق الأول، ٢٠١٣.

٥- دراسات في الحماية الإقليمية لحقوق الإنسان، محمد أمين الميداني، مركز المعلومات والتأهيل لحقوق الإنسان، تعز، طبعة ثانية معدّلة ومزيدة، ٢٠١٢.

٦- السَّايْبِر ساحة خَفِيَّة لحربٍ ناعِمَة قادِمة! طارق المجذوب، منشور على الموقع الرسمي للجيش اللبناني: http://www.lebarmy.gov.lb/ar/news/?٤٠٩١٥.

المراجع الأجنبية

٧- Anne-Thida Norodom, «Propos introductifs. Internet et le droit international : défi ou opportunité ? », dans : Colloque de la S.F.D.I., Rouen, *Internet et le droit international*, Paris, Pedone, ٢٠١٤.

٨- Commission européenne des droits de l'homme, Stocké v. Allemagne, ١٢ octobre ١٩٨٩, Série A, vol. ١٩٩. P. ٢٤, § ١٦٦.

مجلة العلوم الشرعية
جامعة القصيم، العدد (١)، المجلد (١٢)، ص ص ٧٦٧ -٧٨٩ (ذو الحجة ١٤٣٩ هـ / سبتمبر ٢٠١٨م)

٩- Commission IADH, Affaire ١٠,٦٧٥ c. Etats-Unis (Haitian Interdiction Case), ١٣ mars ١٩٩٧, § ١٤١.

١٠- Comité international de la Croix-Rouge, Le droit international humanitaire et les défis posés par les conflits armés contemporains. Rapport, XXXIème Conférence internationale de la Croix-Rouge et du Croissant-Rouge, Genève, Suisse, ٢٨ novembre-١er décembre ٢٠١١, ٣١IC/١١/٥,١,٢

١١- Christopher Dodge, « United States Cyber Command: International Restrictions vs. Manifest Destiny », North Carolina Journal of Law & Technology Online Edition, ٢٠١٠.

١٢- Davis Brown, «A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict», *Harvard International Law Journal*, ٢٠٠٦.

١٣- Éric David, *Principes de droit des conflits armés*, ٥ème éd., Bruxelles, Bruylant, ٢٠١٢.

١٤- Joshua E. Kastenberg, « Non-Intervention and Neutrality in Cyberspace, An Emerging Principle in the National Practice of International Law », Air Force Law Review, ٢٠٠٩, vol. ٦٤.

١٥- Knut Dörmann, « Applicability of the Additional Protocols to Computer Network Attacks», International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law, Stockholm, ١٧-١٩ November ٢٠٠٤, http://www.icrc.org/eng/resources/documents/misc/٦٨lg٩٢.htm.

١٦- Lesley Swanson, « The Era of Cyber Warfare: Applying International Humanitarian Law to the ٢٠٠٨ Russian-Georgian Cyber Conflict », Loyola of Los Angeles International and Comparative Law Review, ٢٠١٠.

١٧- Marc Hecker et Thomas. Rid, «Les armées doivent-elles craindre les réseaux sociaux?», Politique étrangère, vol. ٧٧, été ٢٠١٢.

١٨- Marco Roscini, «World Wide Warfare – *Jus ad bellum* and the Use of Cyber Force», *Max Planck UNYB*, ٢٠١٠.

١٩- Mario Bettati, *Droit humanitaire*, Précis Dalloz, ٢٠١٢.

٢٠- Michael N. Schmidt, «Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework», Columbia Journal of Transnational Law, ١٩٩٩.

٢١- Michael N. Schmidt (dir.), Tallinn Manual on the International Law Applicable to Cyber Warfare. Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defense Centre of Excellence, Cambridge UP, ٢٠١٣.

٢٢- Michel Baud, «La cyberguerre n'aura pas lieu, mais il faut s'y préparer», *Politique étrangère*, ٢٠١٢, vol. ٢.

٢٣- Myriam Dunn Cavelty, «Cyberwar: Concept, Status Quo, and Limitations», CSS Analysis in Security Policy, n° ٧١, Avril ٢٠١٠.

٢٤- Philippe Lagrange, « Internet et l'évolution normative du droit international : d'un droit international applicable à l'Internet à un droit international du cyberespace ? », dans: Colloque de la S.F.D.I., Rouen, *Internet et le droit international*, Paris, Pedone, ٢٠١٤.

مجلة العلوم الشرعية
جامعة القصيم، العدد (١)، المجلد (١٢)، ص ص ٧٦٧ -٧٨٩ (ذو الحجة ١٤٣٩ هـ / سبتمبر ٢٠١٨م)

٢٥- Sylvain Vité, «La lutte contre la criminalité organisée : peut-on parler de conflit armé au sens où l'entend le droit international humanitaire ? », Conflits armés, parties aux conflits armés et droit international humanitaire : les catégories juridiques face aux réalités contemporaines, Actes du colloque de Bruges, ٢٢-٢٣ octobre ٢٠٠٩, Collegium, n°٤٠, ٢٠١٠.

٢٦- Wael Adhami, « The Strategic Importance of the Internet for Armed Insurgent Groups in Modern Warfare », RICR, vol. ٨٩, n°٨٦٨, ٢٠٠٧.

٢٧- Vida M. Antolin-Jenkins, « Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places? », Naval Law Review, ٢٠٠٥.