تحديات تطبيق القانون الدولي الإنساني على النزاعات السيبرانية
(دراسة تحليلية)

الدكتورة/ إعتصام العبد صالح الوهيبي*

الملخص:

تهدف الدراسة إلى بيان التحديات التي تواجه القانون الدولي الإنساني في ظل تزايد النزاعات السيبرانية، باعتبارها أصبحت تهدد السلم والأمن الدوليين، وكذلك تسلط الضوء على أهم قواعد ومبادئ هذا القانون التي من الممكن تطبيقهاعلى النزاعات السيبرانية، خاصة أن استخدام الفضاء السيبراني في الحرب أدى إلى قلب قوانين النزاع المسلح رأساً على عقب، حيث إن الأهداف في أي نزاع سيبراني ستكون على الأرجح مدنية لا عسكريه، وستؤثر على السكان المدنيين لا على القوات العسكرية. كما تتطرق الدراسة إلى بيان الطبيعة القانونية للهجمات السيبرانية من حيث اعتبارها نزاعاً مسلحاً أم لا.

وتركز الدراسة على ضرورة شمول الهجمات السيبرانية بما يسري على الهجمات المسلحة وضرورة استعمال حق الدفاع الشرعي للدول التي تتعرض لهذه الهجمات بناء على نصوص ميثاق الأمم المتحدة والقانون الدولي العام، وأن كان لا يوجد فعلياً أي سند قانوني يبرر استخدام حق الدفاع الشرعي ضد هذا النوع من الهجمات، إلا أنه يمكن إرادها تحت بند العدوان غير المسلح وغير المباشر.

الكلمات المفتاحية: النزاعات السيبرانية – الحرب السيبرانية – الهجمات السيبرانية – القانون الدولي الإنساني – المسؤولية الدولية.

---

* أستاذ القانون الدولي العام المساعد بكلية إدارة الأعمال – جامعة الحدود الشمالية – المملكة العربية السعودية، أستاذ القانون الدولي العام المساعد بكلية الحقوق – جامعة عدن – الجمهورية اليمنية.

Challenges of Applying International Humanitarian Law to Cyber Conflicts (An Analytical Study)

Dr. Etesam Al-Abd Saleh Al-Wheebe *

Abstract :

The study aims to clarify the role of international humanitarian law in cyber conflicts, as it has become a threat to international peace and security, as well as shedding light on the most important rules and principles of this law that can be applied to cyber conflicts, especially that the use of cyberspace in war led to the upside down of the laws of armed conflict After that, the targets in any cyber conflict are likely to be civilian rather than military, and will affect the civilian population rather than the military. The study also addresses the legal nature of cyber attacks in terms of whether they are considered an armed conflict or not.

The study focuses on the need to include cyber attacks with what applies to armed attacks and the need to use the right of legitimate defense for countries that are exposed to these attacks based on the provisions of the Charter of the United Nations and public international law, although there is virtually no legal basis justifying the use of the right of legitimate defense against this type of attacks. However, it can be willed under the category of unarmed and indirect aggression.

Keywords: Cyber Conflicts - Cyber Warfare - Cyber Attacks - International Humanitarian Law - International Responsibility.

---

*Assistant Professor of Public International Law, College of Business Administration, Northern Border University, Kingdom of Saudi Arabia; Assistant Professor of Public International Law, College of Law, Aden University, Republic of Yemen.

في الحقيقة أن الحرب السيبرانية (Cyber warfare) 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. فلم تعد الحروب تقتصر على استخدام الأسلحة الفتاكة التي تحملها الطائرات أو المدرعات أو الجنود، فهذه توشك أن تتوارى في المستقبل وراء ظل حروب ربما تكون أكثر فتكا وهي الحروب السيبرانية.

ولا جدال أنه أصبح من الضروري البحث في مجال الفضاء السيبراني بوصفه بعداً جديداً للصراع الذي لا يتوفر في القانون الدولي العام، ونتيجة لهذه الأهمية وكما هو معروف لدينا المبرر الوحيد لحالة الدفاع الشرعي هو حصول هجوم مسلح من إحدى الدول على دولة أخرى عضو في الأمم المتحدة، وبما أن الرأي قد اختلف حول العدوان غير المسلح غير المباشر مثل العدوان الاقتصادي والأيديولوجي، حيث ذهب البعض إلى أن حق الدفاع الشرعي يسري في مواجهة هذا النوع من العدوان.

وبالتالي يمكن إدراج هذا النوع من العدوان تحت العدوان غير المسلح غير المباشر قياساً على ما سبق وبما أن العمليات الإلكترونية تتجاوز الهجوم المسلح في بعض الأحيان يسمح ذلك للدول بالدفاع عن نفسها بالقوة بما فيها القوة الإلكترونية حسب المادة (51) من ميثاق الأمم المتحدة والقانون الدولي المتعارف عليه؛ لأن مفهوم الهجمات المسلحة على الأقل يشمل عمليات إلكترونية ممكن أن تدمر منشآت استراتيجية وخدماتية ودمارها قد يؤدي إلى الأضرار الجسمية أو الموت أحياناً.

بالرغم من أن الهجوم السيبراني الذي أصبح بلا شك يسبب دمارًا هائلاً لا يقل عن الهجوم المسلح، إلا انه مازال خارج دائرة الهجمات المسلحة مما زاد الأمر تعقيداً كون موقف ميثاق الأمم المتحدة والقانون الدولي ليس واضحاً بشأن الهجمات السيبرانية بوصفها وليدة التطورات الحديثة للتكنولوجيا. لذا أصبحت بعض الدول تستغل هذه الإشكالية؛ لتحقيق أهدافها عبر الفضاء السيبراني دون رادع، وفي بعض الاحيان هناك صعوبة في تحديد هوية المهاجم؛ وكذلك غياب التشريعات التي تخص الهجمات السيبرانية مما يخلق ثغرة تساعد بشكل كبير على شن الهجمات السيبرانية؛ وهذا سيؤدي بلا شك إلى عدم القدرة على ملاحقة المهاجم قانونياً بخلاف الحرب التقليدية.

وينطبق القانون الدولي الإنساني على أي وضع يدخل في أعمال القتال أو يترتب عليها، وقد اهتمت اتفاقيات جنيف الأربع لعام 1949 م والملحقا ن الإضافيان لعام 1977 بإقرار جملة من القواعد التي تهدف لإضفاء طابع إنساني على أي نزاع مسلح، بحيث لم يعد يقتصر انطباق أحكام القانون الدولي الإنساني حكراً على النزاعات المسلحة فقط في ظل التطورات الحالية وتعدد أشكال النزاعات، بل أضيف اعتبار آخر لا يقل عنه أهمية وهو حماية ضحايا النزاعات، وبذلك يعد الإنسان القيمة العليا التي يتوجب الحفاظ عليها وحمايتها وهو ما أدى لتوسع النطاق الموضوعي لتطبيق القانون الدولي الإنساني. وتطبيقا لذلك، فقد تضمنت قواعد القانون الدولي الإنساني واتفاقيات جنيف مجموعة من الإجراءات الاحترازية وقواعد الحظر الشخصية والمادية التي يتوجب على أطراف النزاع اتخاذها قبل وأثناء وقوع النزاع لتجنب الانتهاكات الواقعة على الفئات والأعيان المحمية، وفقاً للقانون الدولي والحد من استمرارها استنادًا لمبدأ التمييز والتناسب.

أهمية الدراسة:

يُعد موضوع النزاعات السيبرانية من الموضوعاتِ الحديثة والبالغة الأهمية في الفكر الاستراتيجي الحديث التي يمكن أن تمثلَ المظهر الجديد لحروب المستقبل. واختصت الدراسة بالوقوف على ماهية هذه النزاعات، وما الخصائص والسمات التي تتميز بها وما السبل والإمكانيات المتاحة لمواجهتها؟

ونظرًا لتزايد الهجمات السيبرانية في الآونة الأخيرة وصعوبة تحديد الجهة التي صدرت عنها هذه الهجمات وعدم وجود أساس قانوني ينظمها، فإن أهمية الدراسة تكمن في كونها تعالج موضوع حديث لا يزال في طور التبلور وتسلط الضوء على مفهوم هذه النزاعات وطبيعتها الاستثنائية. فضلاً عن أنها تحلل قواعد ومبادئ القانون الدولي الإنساني لبحث إمكانية انطباقها على الهجمات السيبرانية.

أهداف الدراسة:

تهدف الدراسة إلى التأكيد على:

1- بيان ماهية النزاعات السيبرانية وما يميزها عن النزاعات التقليدية.

2- التأكيد على انطباق القانون الدولي الإنساني على النزاعات السيبرانية.

3- إبراز المسؤولية الدولية عن النزاعات السيبرانية.

مشكلة الدراسة:

من المعلوم أن الهجمات السيبرانية تُشن في ميدان افتراضي على شبكة الإنترنت مما تتميز به من استخدام مزدوج عسكري–مدني، وذلك على عكس الهجمات العسكرية التقليدية التي تتم في الميدان المادي، وعلى اعتبار أن قواعد ومبادئ القانون الدولي الإنساني، ومنذ صياغة اتفاقيات جنيف الأربع لعام 1949 وبروتوكوليها الملحقين لعام 1977، واجبة التطبيق على كافة الأنشطة التي تقوم بها الأطراف أثناء النزاع المسلح، تثور الإشكالية حول مدى إنطباق قواعد ومبادئ هذا القانون على النزاعات السيبرانية.

وتظهر مشكلة هذه الدراسة أيضاً في مناقشة مسألة ما مدى جواز الدفاع الشرعي في مواجهة الهجمات السيبرانية في القانون الدولي العام.

وبناء على ذلك فإن الدراسة تنطوي على السؤال الرئيسي التالي: هل بالإمكان تطبيق القانون الدولي الإنساني على النزاعات السيبرانية؟ كما تُمثل الدراسة إجابة للأسئلة الآتية:

- ماهي النزاعات السيبرانية؟
- ما الطبيعة القانونية للنزاعات السيبرانية؟
- ما هي قواعد ومبادئ القانون الدولي الإنساني التي يمكن تطبيقها على النزاعات السيبرانية؟
- ماهي المسؤولية الدولية المترتبة عن هذا النوع من النزاعات؟

منهجية الدراسة:

بالنظر لأهمية موضوع الدراسة وحداثته فقد تم الأعتماد على المنهج التحليلي والمنهج الوصفي لأحكام ميثاق الأمم المتحدة والاتفاقيات الدولية ذات العلاقة في سبيل تقييم إمكانية إنطباقها على النزاعات السيبرانية، وكذلك من أجل الوصول إلى حلول مناسبة للإشكالات المطروحة.

خطة الدراسة:

سيتم تناول موضوع الدراسة من خلال الثلاثة المباحث الآتية:

المبحث الأول: ماهية النزاعات السيبرانية وطبيعتها القانونية.

المبحث الثاني: مدى ملاءمة تطبيق القانون الدولي الإنساني على النزاعات السيبرانية.

المبحث الثالث: المسؤولية الدولية الناشئة عن النزاعات السيبرانية.

الفصل الأول

ماهية النزاعات السيبرانية وطبيعتها القانونية

أدت الطفرة الإلكترونية خلال السنوات الأخيرة، إلى تطور برامج الحاسوب وظهور متخصصين في استخدام تقنيات الحاسوب الحديثة، مما أدى الى ظهور العديد من الظواهر الجديدة منها الهجوم السيبراني (Cyber-Attack) والجريمة السيبرانية (Cyber-Crime) التي كثيراً ما يتم الخلط بينهما، اذ أن مصطلح الهجوم السيبراني يختلف تماماً من حيث المفهوم عن مصطلح الجريمة السيبرانية، أن كل واحد منهما تكون الغاية والهدف منه مختلفة عن الآخر[١]، كما أن الانتشار الواسع في استعمال شبكات الإنترنت والتحكم في سوق الأسهم رفع من تحديات أمن المعلومات بشكل متسارع في الفضاء السيبراني مما يستوجب وضع أنظمة معقدة من أجل عدم اختراقها[٢].

والسيبرانية مصطلح مشتق من الكلمة اليونانية (kybernetes) وتعنى القيادة والتحكم عن بعد[٣]، وأصبح الفضاء السيبراني اليوم[٤] ميداناً لخوض الحروب مثله مثل الجو، والفضاء، والبر، والبحر بواسطة أسلحة لها القدرة على الحاق أضرار مادية واسعة، كما أن هذه التكنولوجيا تستخدم الشبكة الإلكترونية كوسيلة يمكن الانطلاق منها وعبرها لتنفيذ العمليات العسكرية.

---

[١] أوليفا، لورنس، (2011)، أمن تقنية المعلومات، المنظمة العربية للترجمة، ترجمة محمد مراياتي، بيروت، ص 9.

[٢] حسن، كاميران عزيز، (2021)، الجهود الدولية في مواجهة الجرائم السيبرانية، ط1، منشورات الحلبي الحقوقية، بيروت، لبنان، ص 7.

[٣] سعود، يحيى ياسين، (2018)، الحرب السيبرانية في ضوء قواعد القانون الدول الانساني، المجلة القانونية، المجلد 4، العدد4 ، كلية الحقوق، جامعة القاهرة، فرع الخرطوم، ص 83.

[٤] يقصد بالفضاء الإلكتروني "البيئة أو الفضاء المصنوع من قبل الإنسان حيث يشكل المكان الذي تحدث فيه الاتصالات الإلكتر ونية عبر الشبكات المترابطة للبنية التحتية للمعلومات والاتصالات، بما في ذلك الإنترنت وشبكات الاتصالات وأنظمة الكمبيوتر":

-Kittichaisaree, K. (2017). Public International Law of Cyberspace, Law, Governanceand Technology, Series 32, P. 2.

وتُعد الهجمات السيبرانية من أهم التحديات التي يواجهها المختصون في القانون الدولي العام؛ وذلك لصعوبة تحديد طبيعتها وعناصرها، وما يترتب على هذه الهجمات من تبعات المسؤولية الجنائية أو المدنية الدولية، خاصة وأن تلك الهجمات قد تلجأ إليها بعض الدول؛ لأجل تحقيق مكاسب: كالهيمنة على واقع النزاع المسلح، أو توجيه تهديدات سياسية أو عسكرية لدول أخرى، فضلًا عن النتائج السلبية من التهديدات الإجرامية والإرهابية، التي قد تنتجها تلك الهجمات في حال لجأت إلى ارتكابها مجموعات فرديّة؛ من أجل الحصول على مزايا سياسية أو اقتصادية.

وسنُبيّن ماهية النزاعات السيبرانية وطبيعتها القانونية، من خلال مطلبين، الأول نتناول فيه مفهوم النزاعات السيبرانية في ضوء أحكام القانون الدولي الإنساني، أما الثاني نتطرق فيه للطبيعة القانونية للنزاعات السيبرانية.

المطلب الأول
مفهوم النزاعات السيبرانية في ضوء أحكام القانون الدولي الإنساني

ظهر الفضاء السيبراني على الساحة الدولية في الحرب بين جورجيا وروسيا في أغسطس عام 2008 وفي التوتر ما بين استونيا وروسيا في مايو عام 2007 على نحو مباشر وعلني، فقد كشفت الهجمات التي تعرضت لها استونيا وجورجيا بأنها كانت غير تمييزية – أي لم تحترم مبدأ التمييز المنصوص عليه في اتفاقيات جنيف – حيث إنها هاجمت خطوط الاتصالات عن طريق توجيه المئات من قنابل"الميجابايت"، وهذا الهجوم لم يتعرض له فقط السكان بل أثر على توقف أرقام الطوارئ التي تستخدم في استدعاء الإسعاف وخدمات المطافئ لما يزيد على ساعة والتي تقع ضمن المنشآت المحمية وفقا للقانون الدولي[٥].

[٥] صدوق، عمر، (١٩٩٥)، محاضرات في القانون الدولي العام، ديوان المطبوعات، بدون طبعة، الجزائر، ص 20.

ولم يكن لدى المجتمع الدولي أية مشكلة في اعتبار استخدام الأسلحة البيولوجية أو الكيميائية يقع تماماً ضمن تعريف الهجوم المسلح، على الرغم من كون هذه الأسلحة غير قابلة للكشف عنها بواسطة الحواس البشرية المجردة، كما أنها لا تعد من الأسلحة الحركية، وبالتالي فإن نوع الأسلحة المستخدمة في أي نزاع مسلح ليس له أهمية تذكر، وعليه وجب اعتبار الهجوم بالأسلحة المعلوماتية هجوماً مسلحاً تبعاً لنتائجه المحتمة، وينظم القانون الدولي الإنساني العمليات السيبرانية التي تُنفذ في سياق نزاع مسلح غير دولي قائم وتتصل به. والسؤال الذي يثار، على الرغم من أنه قد يبدو سابقًا لأوانه في هذه المرحلة، هو ما إذا كان مستوى الشدة المطلوب لتحقيق نزاع مسلح غير دولي يمكن الوصول إليه في حالة استخدام الوسائل الإلكترونية فقط على افتراض أن هناك طرفين أو أكثر في النزاع.

وأضحى استخدام العمليات السيبرانية أثناء النزاع المسلح سمة واقعية من سمات النزاعات المسلحة ومن المرجح أن يكون محلاً لتسليط مزيد الضوء عليه في المستقبل.

وأقرت بعض الدول علناً بأنها أجرت عمليات سيبرانية في نزاعات مسلحة جارية، وكشفت الولايات المتحدة والمملكة المتحدة وأستراليا على وجه الخصوص أنها لجأت إلى العمليات السيبرانية في نزاعها ضد تنظيم الدولة الإسلامية. وتم نشر أيضا تقارير عامة تشير إلى أن إسرائيل استخدمت عمليات سيبرانية ضد حماس–ومزاعم بأن حماس استخدمت عمليات سيبرانية ضد إسرائيل. وأثرت العمليات السيبرانية على بلدان أخرى مشاركة في نزاعات مسلحة مثل جورجيا في عام 2008، وأوكرانيا في الفترة 2015–2017، والمملكة السعودية العربية في عام 2017، وإن كان منفذو هذه الهجمات لا يزالون مجهولي الهوية وثمة تنازع على عزو المسؤولية[٦].

[6]Geisel, Laurent, Rodenhauser, Tilman and Dormann, Knut. (2020). Twenty Years Later: International Humanitarian Law and the Protection of Civilians from the Effects of Cyber Operations during Armed Conflicts, International Review of the Red Cross, 102 (913), pp. 289-290.

ويشير تعبير النزاع في الفضاء السيبراني إلى الأفعال التي يتخذها أطراف نزاع ما، لتحقيق ميزة على خصومهم في الفضاء السيبراني باستخدام أدوات تقنية مختلفة وتقنيات تعتمد على البشر. ومن الناحية النظرية، يمكن تحقيق المزايا عن طريق إتلاف أو تدمير أو إعطاب أو نهب أنظمة الحاسوب لدى الخصم) الهجوم السيبراني)، أو بالحصول على معلومات يُفضِّل الخصم أن تبقى سرية (التجسس السيبراني أو الاستغلال السيبراني). ويُتاح لطائفة متنوعة من الفاعلين الحصول على هذه الأدوات والتقنيات، ومنهم الدول القومية، والأفراد، ومجموعات الجريمة المنظمة، والمجموعات الإرهابية، وتتباين بشدة الدوافع إلى استخدام الهجمات السيبرانية أو التجسس السيبراني، ويشمل ذلك التجسس أغراضًا مالية، وعسكرية، وسياسية، وشخصية، ويختلف النزاع في الفضاء السيبراني عن النزاع في الفضاء المادي في كثير من النواحي، وقد تصعب نسبة العمليات السيبرانية المعادية إلى طرف مسؤول.

وما زالت مشاكل الحماية من العمليات السيبرانية المعادية وردعها بلا حل من الناحية الفكرية، ولميثاق الأمم المتحدة واتفاقيات جنيف صلة وثيقة بالعمليات السيبرانية لكن سمات هذه الصلة غير واضحة اليوم؛ لأن الفضاء السيبراني شيء جديد بالمقارنة بهذه الصكوك. والمصطلح الشائع في التعبير عن تكنولوجيا المعلومات من خلال شبكات الاتصال هو« الفضاء السيبراني »والذي تُعرِّفه وزارة الدفاع الأمريكية بأنه:» مجال يتسم باستخدام الإلكترونيات–أي تكنولوجيا المعلومات–والطيف الكهرومغناطيسي في تخزين البيانات وتعديلها وتبادلها عن طريق أنظمة شبكات الاتصال والبنية التحتية المادية المرتبطة بها »[٧]، وبناء على هذا التعريف، تعمل الكيانات المدنية والعسكرية والإرهابية في الفضاء السيبراني لتنفيذ أنشطتها وعملياتها.

[٧] وزارة الدفاع الأمريكية، (2006)، الاستراتيجية العسكرية الوطنية لعمليات الفضاء السيبراني، متاح في الرابط التالي:

http:// www.dod.mil/pubs/foi/joint_staff/jointStaff_jointOperations/07-F-2105doc1.pdf

وهناك العديد من المصطلحات والمفاهيم التي أُطلقت على الهجمات السيبرانية، فقد أطلق مصطلح الحرب الافتراضية، أو الحرب الإلكترونية، أو الحرب السيبرانية، على الهجمات السيبرانية التي يتم من خلالها قيام القراصنة (Hackers) بمهاجمة الملفات والمواقع التي تخص الآخرين، كمهاجمة المواقع الإلكترونية للمنشآت المهمّة، أو مهاجمة الحواسيب التابعة للوحدات العسكرية أو الوحدات الاقتصادية لدول معيّنة، بقصد تدميرها، والسيطرة عليها، والإضرار بها[٨]، وتتميز عملية استخدام الأسلحة عبر الفضاء السيبراني بسهولة الانتشار، والقدرة على التأثير على الأهداف الجاهزة الكترونياً كالبنية التحتية الحيوية ومؤسسات اقتصادية ومالية وسياسية وعسكرية، وقد تنشأ الحروب السيبرانية بالوساطة، كأن تبيع المنظمات المتخصصة في الأعمال العسكرية خدماتها المعلوماتية والأمنية لبعض الجهات[٩].

ومن المسلّم به، أن وسائل الحرب وأساليبها قد تطورت منذ اعتماد اتفاقيات جنيف الأربع عام 1949م.

ولكن لا يزال القانون الدولي الإنساني منطبقًا على كافة الأنشطة التي تقوم بها الأطراف أثناء النزاع المسلح وينبغي احترامه، ومع ذلك لا يمكن استبعاد حقيقة مؤداها أن هناك حاجة إلى تطوير القانون لضمان توفير الحماية الكافية للسكان المدنيين، تماشيًا مع تطور التكنولوجيا السيبرانية وفهم تأثيرها الإنساني بشكل أفضل، وهذا الأمر تقرره الدول بنفسها، وتختلف الحرب السيبرانية عن الحرب التقليدية، إذ تنطوي الأخيرة على استخدام الجيوش النظامية مع إعلان مسبق للحرب وميدان قتال محدد، بينما تكون الأولى غامضة وغير محددة الأهداف كونها تتحرك عبر شبكة المعلومات الإلكترونية[١٠].

---

[٨] إيهاب، خليفة، (2014)، القوة الإلكترونية وأبعاد التحول في خصائص القوة، مكتبة الإسكندرية، الإسكندرية، مصر، ص 15.

[9] Libicki, M. (2007). Conquest in Cyberspace: National Security and Information Warfare, Cambridge University Press, New York, P. 13-323.

[10] Hathaway, Oona A, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue & Julia Spiegel Levitz, Philip. (2012). The Law of Cyber-Attack, CALIFORNIA LAW REVIEW, vol. 100 (817), p. 880.

وقبل توضيح الهجمات السيبرانية، لا بد من تناول معنى الهجوم في العمليات السيبرانية إذا استُخدمت لأغراضٍ عسكرية، وقد عرّف البروتوكول الإضافي الأول لعام 1977الملحق باتفاقيات جنيف الأربع لعام1949 في المادة (1/49) بأن: «الهجوم هو أعمال العنف الهجومية أو الدفاعية ضد الخصم»، وقد كان هذا التعريف كافيًا في عصر كانت فيه الهجمات تُنفّذ بالوسائل التقليدية؛ لأن هذه الوسائل عنيفة بطبيعتها، أما العمليات السيبرانية معقّدة كونها تفي بالغاية العسكرية المطلوبة من دون التسبب بآثارٍ مدمرة أو ضارة أحيانًا، وبعد نقاش طويل في تعريف الهجوم في سياق العمليات السيبرانية، انقسم خبراء القانون الدولي الإنساني بين مؤيد لنهجٍ يقصر نطاق الهجمات على العمليات العسكرية التي تؤدي إلى أضرار وإصابة[١١]، إذ يركّز هؤلاء على المعنى الواضح للنص، وبين مؤيد لمفهوم أوسع للهجمات لبعض العمليات غير المدمرة أو غير الضارة[١٢].

إن كلا النهجَين لهما نقاط قوة ونقاط ضعف، ولم يستطع أي منهما الحصول على الدعم الكلي أو الإجماع من قبل الخبراء الدوليين، لكن تم التوصل بين الفريقَين إلى قاعدة مفادها: «إن العملية السيبرانية، سواء في الهجوم أو في الدفاع، التي يُتوقع منها أن تسبب إصابة، أو وفاة للأشخاص، أو إلحاق الضرر، أو تدمير الأشياء، تعد بمثابة هجوم». طبعًا الحد الأدنى من الضرر أو التدمير لا يفي بهذا المفهوم. ويعطي دليل تالين الحق للدولة التي تتعرض لهجوم سيبراني شن حرب هجومية الكترونية مضادة على الدولة الأخرى، كما ذكر دليل تالين إنه يمكن استخدام القوة العسكرية الحقيقية في حالة تم شن هجوم إلكتروني على دولة وأدى هذا الهجوم لخسائر بالأرواح البشرية [١٣].

---

(11) The lead article advocating this view is Schmitt, M. N. (2002). Wired Warfare : Computer Network Attack and International Law, note 73, p. 392. The author has since moderated his views to accord with the functionality approach set forth in the Tallinn Manual.).

(12) The lead article advocating this view is Dörmann, Knut. (2004). Applicability of the Additional Protocols to Computer Network Attacks, INT'L COMM. OF THE RED CROSS, Nov. 19. [Online] Available at : http://www.icrc.org/eng/resources/documents/misc/68lg92.htm.

(13) See the Tallinn Manual. (2013). North Atlantic Treaty Organization, Tallinn Manual on the Jnternatonal Law applicable to Cyber Warfare, NATO Cooperative Cyber Defence Centre of Excellence, Cambridge University Press, UK, rule (14).

ويقدم دليل تالين المطبّق على الحرب السيبرانية، تعريف للهجمات السيبرانية بأنها: «عملية الكترونية سواء هجومية أو دفاعية يتوقع أن تتسبب في إصابة أو قتل أشخاص أو الأضرار بأعيان أو تدميرها كما يعدّ توقف أحد الأعيان عن العمل قد يشكل ضرراً مادياً»[١٤]، ووفق هذا التعريف فقد اتفق معظم الفقهاء القانونيين على أنه قد يتحقق الضرر أيضًا بتوقف أحد الأعيان عن العمل، علاوة على الضرر المادي، وليس من المهم كيف يحدث ذلك، كما تعرف الهجمات السيبرانية بأنها: «كل فعل يقوض من قدرات ووظائف شبكة الكمبيوتر لغرض قومي أو سياسي، من خلال استغلال نقطة ضعف معينة تُمكن المهاجم من التلاعب بالنظام» [١٥]، وتُعرف أيضاً بأنها: «مجموعة من الإجراءات التي تتخذها الدولة للهجوم على نُظم المعلومات المعادية بهدف التأثير والإضرار بها، وفي الوقت نفسه للدفاع عن نُظم المعلومات الخاصة بالدولة المهاجمة»[١٦].

إن اندفاع دولة في الهجوم على دولة أخرى يمكن أن يدفع الدولة المعتدَى عليها للردّ بهجمات مضادة دفاعًا عن النفس، وتلك الهجمات لم يتمّ تحديدها قانونًا في حق الدفاع الشرعي عن النفس، كما يواجَه الهجوم في الفضاء الإلكتروني بتحديات تتعلق بخصائص هذا الهجوم، الذي يتميز بان المهاجمين يتسببون في سلسلة من الاضرار عن طريق الدخول إلى نظم المعلومات، وطبيعة تلك الهجمات تجعل من الصعوبة بمكان إن لم يكن مستحيلاً تحديد مركز الهجوم المباشر، بما يؤثر على فاعلية الردّ الدفاعي، ولا توجد دولة يمكنها أن تصل إلى درجة عالية من المنعة ضد تلك الهجمات[١٧]، فالعمليات السيبرانية تُستخدم اليوم في النزاعات المسلحة كوسيلة من وسائل الحرب أو سبلها، حتى إن بضع دول أقرت علنًا باستخدامها، ويتزايد عدد الدول التي تُطور قدراتها العسكرية السيبرانية، سواء لأغراض هجومية أو دفاعية.

---

(14) Tallinn Manual, op, cit, rule (30).
(15) Matthew, C. Waxman. (2011). Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4), e Yale Journal of International, vol. 36, P.423.
(16) Schmitt, M. N. (1999). Computer network attack and the Use of Force in International Law : Thoughts on a Normative Framework, Columbia journal of Transnational law, vol 37. No (885). P. 890.
(17) Hathway, Oona, al at, op. cit, P. 873.

ويمكن تعريف الحرب السيبرانية بأنها عبارة عن هجمات تتم بواسطة استخدام الحاسوب أو الشبكات أو الأنظمة ذات الصلة، وتهدف إلى تعطيل، أو تدمير أنظمة الإنترنت، أو الممتلكات، أو الوظائف الحاسوبية الخاصة بالخصم[١٨]، كما يستخدم هذا المصطلح للإشارة إلى وسائل وأساليب القتال التي تتألف من عمليات في الفضاء السيبراني ترقى إلى مستوى النزاع المسلح، أو تجري في سياقه ضمن المعنى المقصود في القانون الدولي الإنساني[١٩]، أما الهجوم السيبراني فيُعرف على أنه "أي تصرف دفاعياً كان أم هجومياً، يتوقع منه وعلى نحو معقول التسبب بجرح أو قتل شخص أو الحاق أضرار مادية أو دمار بالهدف المهاجم، ويشكل تهديدا أو استخداما للقوة ضد سلامة الأراضي أو الاستقلال السياسي لأية دولة، أو التي لا تتفق بأي وجه مع مقاصد الأمم المتحدة" [٢٠].

وتتميز الهجمات السيبرانية بأنها تتم بواسطة شخص أو أكثر باستخدام جهاز حاسوب مزوّد بعددٍ كبير من الفيروسات، ويتم إرسالها إلى الهدف المراد إلحاق الضرر به، ويمكن أن يكون الضرر ماديًا أو معنويًا. وعليه، فإن الهجمات السيبرانية ليست سلاحًا تقليديًا، ولا ترقى لأن تكون سلاح دمار شامل؛ وذلك نظرًا للأضرار الناتجة عنها.

---

(18) Kittichaisaree, op. cit, P.154.

(١٩) اللجنة الدولية للصليب الأحمر، (2013)، ما هي القيود التي يفرضها قانون الحرب على الهجمات السيبرانية؟، 28 يونيو، متاح على الرابط التالي:
https://www.icrc.org/ar/doc/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm

(20) Schmitt, M. N. (2013). Tallinn Manual on the International Law Applicable to Cyber Warfare, (1st Edition) Cambridge University press, first publishes, p.92.

ونظرًا لأهميتها في النزاعات المسلحة، والأضرار المتوقعة من جرائها، عُقدت مباحثات بين أميركا وروسيا لوضع قيود لاستخدام هذا النوع من الأسلحة، إذ نادت أميركا بتقييده، بينما كانت روسيا مع حظره، وبالنهاية لم يتم التوصل إلى قواعد مشتركة، أما من منظور القانون الدولي الإنساني فتثير الهجمات السيبرانية التساؤل الآتي: «هل هي وسيلة أم أسلوب قتال؟».

وفي الإطار ذاته، رأى بعض الخبراء أنه نظرًا لعدم وجود ممارسات دولية بشأن الاعتماد على تعريف موحد «للهجوم» في العمليات السيبرانية، فإن القانون الحالي يقصر المصطلح على الأذى الجسدي الذي يلحق بالأشخاص والضرر الذي يلحق بالأشياء المادية. فبالنسبة لهم، تُعد العملية السيبرانية بمنزلة هجوم تتطلب إصلاحًا للبنية السيبرانية المستهدفة بهذه العملية[٢١].

ومن خلال قراءة التعاريف السابقة، وللتمييز سواء أكانت الهجمات السيبرانية وسيلة أم أسلوب قتال، يجب معرفة الهدف من استخدامها. ففي العام 2007، قامت إسرائيل بواسطة سلاحه الجوي بهجومٍ على موقع سوري يُشتبه بأنه مفاعل نووي والذي تزامن معه قيامها أيضاً بهجمات سيبرانية على أجهزة الرادار الاتصال في وزارة الدفاع وباقي منظومات الاتصال في المطارات العسكرية والمدنية، أدت إلى تعطيلها عن العمل بالكامل.

ففي هذه الحالة، يُعد الهجوم السيبراني أسلوب قتال؛ لأنه يدخل ضمن الخطط العسكرية، وساعدت في تحسين أداء العمليات العسكرية التقليدية وتوفر الدعم اللازم في إنجازها[٢٢] في المقابل قد تكون الهجمات السيبرانية وسيلة قتال من خلال استخدامها بذاتها، للتسلل إلى أنظمة إلكترونية معدّة لحماية سير عمل منشآت حيوية أو لتنظيمها كمحطات توليد الطاقة النووية أو السدود أو وسائل نقل كالمطارات، بهدف تطويعها والسيطرة عليها، لتدمير ذاتها بذاتها من خلال تغذيتها بمعلوماتٍ خاطئة لأجهزة التحكم والحماية الإلكترونية والمثال على ذلك ما تعرضت له محطة نطانز لتوليد الطاقة النووية الإيرانية من هجوم سيبراني من قبل الولايات المتحدة الأميركية في عام 2011، باستخدام برنامج (Stuxnet) الذي عطّل العمليات الحساسة وألحق أضرارًا جزئية في عمليات تخصيب اليورانيوم[٢٣].

---

(21) Schmitt, Mi. N. (2014). The Law of Cyber Warfare: Quo Vadis? STANFORD LAW & POLICY REVIEW, Vol 25. No (269), P. 295.

(22) Thomas Rid & Peter Mcburney. (2012). Cyber – Weapons, Routledge publisher, The RUSI Journal, February, p. 6.

(23) Gervais, Micheal. (2012). "Cyber Attacks and the law of warfare'', Berkeley Journal of international law, vol : 30Issue. 2 articles 6, p 46.

إن ما يميز الهجوم السيبراني عن الأنشطة الأخرى، هو الأضرار والتأثيرات التي يؤدي فيها الهجوم السيبراني إلى عدم إمكانية الوصول إلى النظام المستهدف أو تعريض سلامة أنشطته للخطر، والسؤال المهم الذي يمكن طرحه هنا هو ما إذا كانت هذه الآثار وحدها تجعل حق الدفاع عن النفس قائماً حتى في ظل غياب الأضرار البشرية والمادية؟ علماً بإن الحالات الواردة في المادة (51) من الميثاق، والعرف الدولي وأكدوا على حق الدفاع عن النفس، ويبدو أن كلا فرعي القانون يتفقان في هذه الحالة على أن ما يخلق حق الدفاع عن النفس هو الاعتداء المسلح.

وعلى الرغم من عدم وجود أي تعريف حول ما يُشكل هجوم مسلح في الميثاق، ولكن ما هو مقبول أن الهجوم السيبراني يتم تعريفه من خلال استخدام القوة، وازدادت في الآونة الأخيرة الدراسات القانونية المتخصصة للبحث في إمكانية توجيه المسؤولية الدولية على اساس استخدام القوة والتأثيرات الناتجة، وليس على أساس الأداة المستخدمة[٢٤]، وأن كان الهجوم المسلح هو أشد أشكال استخدام القوة من حيث الحجم وآثاره، فإن الهجوم السيبراني يُسبب دماراً جوهرياً وقد يحدث خسائر في الأرواح البشرية أو دمار مادي كبير، ويعد اعتداءً مسلحاً ويؤدي إلى قيام حق الدفاع عن النفس– على سبيل المثال– عند حدوث هجوم عبر الإنترنت على أنظمة مراقبة الحركة الجوية أو المفاعلات النووية ويسبب أضراراً بشرية ومالية هائلة كالتي يُحدثها الهجوم المسلح، والتمييز بين أن تكون الهجمات السيبرانية وسيلة أو أسلوب قتال، يعتمد على الهدف من استخدامها والنتيجة المتوقعة منها، فإذا تسببت بشكلٍ مباشر، أو غير مباشر بقتلٍ، أو جرح، أو تدمير، أو تعطيل كلي، أو جزئي، تعد وسيلة قتال، أما إذا استُخدمت كجزءٍ من مخطط عسكري فتعد أسلوب قتال، ومن كل ذلك يتبيّن أنها وسيلة وأسلوب قتال في الوقت نفسه، وفق الهدف من استعمالها.

وفي الواقع يتم إطلاق الهجمات السيبرانية بعيدًا عن ساحات القتال، ما يثير مخاوف عن الحدود العملية والمعيارية لتصنيف نزاع على أنه نزاع مسلح، فالقدرة على إخفاء نقطة انطلاق أو أصل الهجمة السيبرانية يعقد خيارات الرد لأولئك المستهدفين، فضلًا عن أنها يمكن أن تؤدي إلى آثار مدمرة أو ضارة بالسكان المدنيين.

وبالتالي، فإن رسم خط واضح يفصل بين الحالات التي تمثّل نزاعًا مسلحًا والحالات التي لا تمثّله لم تكن بالمهمة اليسيرة على الإطلاق في الحروب التقليدية، فكيف يمكن أن تكون

(24) Tsagourias, Nicholas. (2012). Cyber Attacks, Self Defense and the Problem of Attribution, Journal of Conflict and Security Law, Oxford University Press, Vol.17, No.2, pp.230-233.

عليه في هذا النوع الجديد من الحروب وبخاصةٍ في استعمال الهجمات السيبرانية؛ لأن هذه المسائل تؤثّر تأثيرًا كبيرًا على إمكانية تطبيق القانون الدولي الإنساني، وتؤدي إلى مزيد من الصعوبة في تصنيف النزاعات، وتخضع العمليات السيبرانية المستخدمة خلال النزاع المسلح إلى القانون المطبّق على النزاعات المسلحة الدولية أو غير الدولية[٢٥]، وهذا يطرح السؤال الآتي: هل يمكن في أي نوع من النزاعات المسلحة أن تقتصر العمليات على التبادل السيبراني فقط؟

إن النزاع المسلح الدولي هو نزاع مسلح بين دولتَين أو أكثر، إذ يتطلب اللجوء إلى القوة المسلحة بين الدول[٢٦]، فقد اقترحت المحكمة الجنائية الدولية ليوغوسلافيا السابقة تعريفًا عامًا للنزاعات المسلحة الدولية في قضية تاديتش، وقالت المحكمة إن «النزاع المسلح يوجد حيثما يكون هناك لجوء للقوة المسلحة بين الدول»، من دون الإشارة إلى متطلبات أخرى لتصنيف النزاع[٢٧]. وقد وجد هذا الرأي تأييداً من بعض الفقهاء[٢٨]، ولا يوجد أساس منطقي أو قانوني لوجوب تمييز العمليات التقليدية والعمليات السيبرانية، فيما يتعلق ببدء نزاع مسلح دولي، في الحالة التي تتسبب الأخيرة فيها بعواقب مماثلة للنزاع المسلح، من الواضح أن العمليات

---

(25) See discussion of the subject of characterization of cyber warfare in Schmitt, M. N. (2013). Classification of Cyber Conflict, 89 INT'L L. STUD. 233, Vol. 89.

(26) Prosecutor v. Tadić, Case No. IT-94-1-I, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, 70 (Int'l Crim. Trib. for the Former Yugoslavia Oct. 2, 1995).

(27) Prosecutor v. Tadić, Case No. IT-94-1-A, Appeals Chamber Judgment 131-40, 145 (Intl'l Crim. Trib. For the Former Yugoslavia July 15, 1999). See also Application of theConvention on the Prevention and Punishment of the Crime of Genocide (Bosn. &Herz. v.Serb. & Montenegro.), 2007 I.C.J. 108, 404 (Feb. 26) ; Prosecutor v. Lubanga, Case No.ICC-01/0401/06, Decision on Confirmation of Charges, 211 (Jan. 29, 2007), http://www.icccpi.int/iccdocs/doc/doc266175.pdf. On the internationalization of a noninternationalarmed conflict, see Tadić, Decision on Defence Motion, supra note 77, 76.

(٢٨) وقد أيد هذا الرأي الفقهيه جان بكتيه قائلاً: «إن أي خلاف ينشب بين دولتَين ويُفضي إلى تدخّل القوات المسلحة هو نزاع مسلح بالمعنى المقصود، حتى لو لم يعترف أحد الطرفَين بحالة الحرب. ولا يعوّل في هذا الصدد على المدة التي تستمر خلالها النزاعات أو عدد القتلى».

- See J. Pictet. (1952). Commentary on the Geneva Convention for the Amelioration of the condition of the wounded and Sick in Armed Forces in the field, ICRC, Geneva, p, 3.

السيبرانية لن تشكّل جميعها حالة من اللجوء إلى القوة المسلحة، ولكي تكون هناك قوة مسلحة، يجب أن تكون هناك أعمال قتالية[٢٩].

وتكمن المشكلة الأساسية في الوضع الذي لا تؤدي فيه الأنشطة السيبرانية إلى أضرار جسيمة غير مدمرة وغير ضارة، فقد أثار ذلك جدلًا واسعًا، إلا أنه يبدو، وفق تعريف الهجوم في القانون الدولي الإنساني، أن أي عملية سيبرانية ترقى لمستوى الهجوم، تعد تجاوزًا للأعمال العدائية، ولم يتوصل الخبراء الدوليون حتى اليوم إلى اتفاق بشأن مقدار الضرر أو الإصابة المطلوبَين من الهجمات السيبرانية لبدء نزاع مسلح دولي، ووفق اتفاقيات جنيف الأربع المؤرخة في 12 /أغسطس 1949 م، النزاع المسلح الدولي هو «أي خلاف نشأ بين دولتَين ويؤدي إلى تدخّل القوات المسلحة فهو نزاع مسلح لا يهم كم من الوقت يستمر النزاع أو حدة العنف»، ومع ذلك، هناك بعض الخبراء تبنوا موقفًا أكثر تقييدًا يستلزم نطاقًا أوسع، أو مدة أطول أو حدة أشد.

ومن الصعب التكهن أي المقاربات سوف تحدد العمليات السيبرانية المطلوبة لتصنيف النزاع على أنه نزاع مسلح دولي، فمن جهة إن الخيار الأول مفضّل من قبل الدول، لتوسيع حماية القانون الدولي الإنساني للأشخاص والأشياء التي يُحتمل أن تتأثر بالنزاع السيبراني. ومن جهة أخرى، فإن الموقف الأخير له فائدة الحد من الحالات التي توصف فيها العمليات السيبرانية بأنها نزاع مسلح دولي، وبالتالي تُجنّب عدم الاستقرار بين الدول، الذي يصاحب هذه التوصيفات. أما بالنسبة إلى إنطلاق العمليات السيبرانية في النزاع المسلح غير الدولي، بين جماعة مسلحة من غير الدول والقوات النظامية التابعة لدولةٍ ما، فهو أمر في غاية التعقيد، على عكس النزاع المسلح الدولي، هناك عاملان واقعيان لتصنيف حالة عنف على أنها نزاع مسلح غير دولي وفق المادة الثالثة المشتركة:

أولًا: أن تظهر الأطراف المشاركة مستوىً معيّنًا من التنظيم.

ثانيًا: أن يصل العنف إلى مستوى معيّن من الحدة[٣٠].

---

(29) Tallinn Manual, supra note 2, at 74.

(30) See ICTY, The prosecutor V. DuskoTadic. See also, SassoliM. (2006), " Transnational Armed Groups and International Humanitarian Law", program on Humanitarian policy and conflict Research, Harvard University, Occasional paper Series, Winter, number 6, p. 9.

في الواقع توجد عوامل عدة يمكن على أساسها تقييم معيار التنظيم، وفق ما أعلنته المحكمة الجنائية الدولية ليوغوسلافيا السابقة، إذ تتضمن هذه العوامل الإرشادية وجود هيكل للقيادة وقواعد وآليات تأديبية داخل الجماعة؛ وقدرة الجماعة على الحصول على الأسلحة والمعدات العسكرية والمجندين والتدريب العسكري؛ وقدرتها على تخطيط العمليات العسكرية وتنسيقها وتنفيذها، بما في ذلك تحركات القوات وتوفر الدعم اللوجستي لها؛ وقدرتها على وضع استراتيجية عسكرية موحدة والتفاوض وإبرام الاتفاقات مثل اتفاقات وقف إطلاق النار أو اتفاقات السلام[٣١].

أما المعيار الثاني فيتمثل في تحديد وجود نزاع مسلح دولي في حدة أعمال العنف، ولتقييمه يجب دراسة الأحداث الدائرة على أرض الواقع، فقدّمت المحكمة الجنائية ليوغوسلافيا السابقة أيضًا عوامل إرشادية لتقييم هذا المعيار منها: «عدد المواجهات الفردية ومدتها وحدّتها، نوع الأسلحة والمعدات العسكرية الأخرى المستخدمة وعدد الذخائر التي أُطلقت وعيارها، عدد الأفراد وأنواع القوات المشاركة في القتال، حجم الخسائر البشرية، حجم الدمار المادي وعدد المدنيين الفارين من منطقة القتال».

فالمجموعة المسلحة من غير الدول التي هي طرف من أطراف النزاع المسلح غير الدولي، يمكن أن تنخرط مستقبلًا في الأعمال العدائية التي تتكون بالكامل من العمليات السيبرانية التي تفي بمعيار الشدة، لكن لتصنيفها بأنها نزاع مسلح غير دولي يتعيّن على هذه المجموعة تلبية المعيار الثاني وهو التنظيم.

وكانت محكمة يوغوسلافيا السابقة قد أعلنت في قضية تاديتش وهي قضية في النزاع، على أن النزاع المسلح لكي يصنف غير دولي يجب توفر معيارَي العنف وهيكل القيادة لهذه المجموعة؛ لذلك فإن العمليات السيبرانية الفردية أو التي تنفّذها مجموعة غير منظمة من المقرصنين لا يمكن أن تُعد نزاعًا مسلحًا غير دولي، فقد ارتأى الخبراء الدوليون أن فشل أعضاء المجموعة من الاجتماع جسديًا، لا يعني أن هذه المجموعة غير منظمة، ففيالواقع يجب أن يعمل أعضاء الجماعة جنبًا إلى جنب، من خلال استهداف أهداف معينة يتم تحديدها على موقع المجموعة على الشبكة الإلكترونية، لكن في رأيهم هذا لا يكفي لتلبية متطلبات التنظيم، فيجب أن تعمل الجماعة بشكلٍ تعاوني لغرض مشترك، وأن تخضع لتعليمات قيادة موحدة، وتحترم أحكام القانون الدولي الإنساني[٣٢].

---

(31) Prosecutor v RamushHaradinaj, IdrizBalajBrahimaj, (Trial judgment), IT-04-84-T, 3 April 2008, para 49.

(32) See Schmitt, Classification of Cyber Conflict, op, cit, P. 246.

ومع ظهور الهجمات السيبرانية سواء كوسيلةٍ أو كأسلوبٍ جديد في ساحات القتال، يبرز تحدٍّ جديد يتمثل في معرفة حدود استعمال وسائل القتال وأساليبه الذي وضعه القانون الدولي الإنساني، سواء في القانون الدولي الاتفاقي أو القانون الدولي العرفي، فضلًا عن أن الهجمات السيبرانية العابرة للحدود وغير العابرة لها، إذا ما نُفّذت في أثناء نزاع مسلح يجب أن تتفق مع مبادئ القانون الدولي الإنساني في الحرب، ما أثار جدلًا قانونيًا بشأن شرعية الهجمات السيبرانية بموجب القانون السالف الذكر.

وأزداد لجوء الدول إلى استخدام الهجمات السيبرانية؛ نظراً لما توفره هذه الأخيرة من جهد ومال، كالتقليل من تكلفة الحروب والنزاعات المسلحة، نتيجة سهولة استخدام الأسلحة السيبرانية مثل الفيروسات وبرامج التجسس، وقرصنة المعلومات العسكرية والإستراتيجية، فضلا على تح قيق الأهداف المسطرة في ظرف وجيز، وكذا حجم الدمار الهائل الذي يمكن أن تسببه تلك الأسلحة، حيث يرى البعض أن حجم الدمار الذي تلحقه الأسلحة السيبرانية يضاهي الدمار الذي تحدثه أسلحة الدمار الشامل المعروفة، عن طريق استهداف المنشآ ت الحيوية للدول، وشل كل مظاهر الحياة فيها، كمحطات الكهرباء والسدود والبنوك... الخ[٣٣].

وجدير بالإشارة أن الفقرة الرابعة من المادة (2) من الميثاق حظرت استخدام القوة في العلاقات الدولية إلا في حالات معينة ومنها الإجراءات المتخذة في جزء منها عمليات الأمن الجماعي والفردي، وأن هذه الإجراءات هي وسيلة الدفاع عن النفس في حال حصول أي اعتداء على الدول.

ومن الواضح أن الإجراءات والمبادئ القانونية في الهجوم السيبراني يجب أن تمنع الدول في علاقاتهم الدولية من استخدام القوة ضد السلامة الإقليمية والاستقلال السياسي أو في أي حالة أخرى تتنافى وتختلف عن أهداف ومبادئ الأمم المتحدة.

---

[٣٣] درويش، سعيد، (2016)، ماهية الحرب الإلكترونية في ضوء قواعد القانون الدولي"، حوليات جامعة الجزائر-1، المجلد 29، العدد 2، ص 118.

وجديراً بالذكر أن نص المادة (39) من الميثاق لم يضع تعريفاً محدداً للعدوان، بل تركها دائرة موسعة حتى يستطيع مجلس الأمن تكييف أي تصرف من شأنه أن يعرض سلامة الدول للخطر، وبذلك يكون من الممكن أن ندرج الهجمات السيبرانية تحت هذا البند، وبالنظر إلى نص المادة (39) يلاحظ أنها منحت لمجلس الأمن سلطات واسعة لتحديد وجود أي تهديد أو خرق لشروط السلام أو أي تصرف عدواني وتقديمها على شكل توصيات للأمم المتحدة على توضيح الإجراءات التي يجب اتباعها في حالة حصول هذا الخطر وبذلك فإن القانون يدعم وجوب أخذ إجراءات في هذه الحالة فالهجمات السيبرانية التي تهدد وتخرق الشروط الأمنية[٣٤].

وعليه فإن الدفاع الشرعي ضد الهجمات السيبرانية يُعد استثناء من قاعدة عدم اللجوء إلى القوة؛ لأنه يهدف إلى الوقاية وليس الانتقام من المعتدي، إذ يعد سبباً للإباحة في القانون الدولي بشرط أن يسبقه هجوم سيبراني غير مشروع حال على أحد الحقوق الجوهرية التي يحميها القانون، ولا شك أن ما يهدد استقرار الدولة في أي مجال يجب اعتباره هجوم مسلح، وبذلك فإن الهجمات السيبرانية تهدد حماية واستقرار دول العالم كافة، كما أنه عند حدوث الهجمات السيبرانية على أحد الدول الأعضاء في الأمم المتحدة وتتبناها جهة دولية معترف بها، فيجب على مجلس الأمن أن يتخذ التدابير المناسبة والإجراءات الفعّالة لردع هذه الهجمات. ونرى ضرورة أن يتم تعديل ميثاق الأمم المتحدة لاستيعاب النزاعات السيبرانية وتحديد مفهوم هذا النوع من النزاعات وحالات الدفاع عن النفس ضد الهجمات السيبرانية، وبخاصةٍ تعديل المادة (42) من الميثاق بما يسمح لمجلس الأمن باتخاذ التدابير اللازمة من خلال الوسائل السيبرانية، ويمكن استخدام أسلحة الفضاء السيبراني في الصراع بين الدول بشكل متواز أو غير متواز مع حرب عسكرية تقليدية، ويمثل كلا النمطين خطراً متصاعداً في العالم مما ينذر بتحوله إلى أكبر تهديد أمني دولي[٣٥].

---

[٣٤] انظر: المادة (39) من ميثاق الأمم المتحدة.

[٣٥] عبد الصادق، عادل، (2009)، الإرهاب الإلكتروني القوة في العلاقات الدولية، نمط جديد وتحديات مختلفة، مركز الدراسات السياسية والاستراتيجية بالأهرام، القاهرة، ص 130 –140.

ورصدت اللجنة الدولية للصليب الأحمر التطورات التكنولوجية التي يمكن استخدامها كوسائل أو سبل للحرب، وتقيم المخاطر والتحديات التي التي تتولد عنها من منظور تقني وإنساني وعسكري وقانوني ودعت اللجنة الدولية في عام 2018 عدداً من الخبراء من جميع أنحاء العام للاجتماع لوضع تقييم واقعي للتكلفة البشرية المحتملة من جرَّاء العمليات السيبرانية[٣٦]، وإمعانًا فيما سبق فإن الهجمات السيبرانية تُعد من قبيل أفعال العدوان التي يعاقب عليها القانون الدولي العام بتفعيل دور مجلس الأمن الذي يكيف فعل العدوان على أي تصرف غير شرعي يرتكب في حق دولة عضو في هيئة الأمم المتحدة في حال أنه ارتكب من خلال دولة تبنت هذا الهجوم أو جماعة معينة تتبع لدولة.

المطلب الثاني

الطبيعة القانونية للنزاعات السيبرانية

أن تحديد طبيعة الهجمات السيبرانية خلق مشاكل عملية وجدلاً بين الخبراء القانونيين، كما أنه بسبب التطور التقني الحاصل أدى ذالك إلى ظهور العديد من المصطلحات والمفاهيم المتشابهة مع بعضها البعض في المجالات التقنية والمعلوماتية ولا سيما في إطار المصطلحات المشتقة من السايبر، فالحرب السيبرانية كإطار عام للمفهوم فإنها تُشَنّ ضد كيانات محددة بهدف تعطيلها والحفاظ على مجال المعلومات من أي اعتداء سيبراني من طرف الخصم باستخدام الوسائل التكنلوجية والمعلوماتية المتطورة[٣٧].

ومن المعلوم أن القانون الدولي الإنساني هو قانون وُلد مقترناً بالحروب، فهو على موعد مع التطوّر كلما تطوّرت وسائل القتال وأساليبه، لذا ترتب عن الفجوة التكنولوجية والتقنية المتزايدة يومًا بعد يوم بين دول العالم تحديات على مختلف الأصعده وبخاصةٍ على صعيد القانون الدولي الإنساني، من حيث الطبيعة القانونية للهجمات السيبرانية، ومدى إمكانية تطبيق مبادئ وقواعد القانون الدولي الإنساني على هذا الشكل الجديد من الحروب، وبعبارةٍ أخرى، في ظل وجود فراغ قانوني وعدم وجود قواعد قانونية محددة تُنظّم الهجمات السيبرانية، يُثار التساؤل عن القواعد الواجبة التطبيق.

---

(36) Geisel, Laurent, et al, op, cit, p. 294.

(37) Michael Robinson, Kevin jones, helge janicke. (2015). War Cyber Fare : Issues and Challenges Article in Computer and Security, Elsevier, vol. 49, march united kingdom, p, 24.

واللجوء المتزايد للدول في استخدام الفضاء السيبراني لشن هجمات سيبرانية في أثناء النزاعات المسلحة، جعل مبادئ القانون الدولي الإنساني وقواعده أمام اختبار حقيقي ومعقد حول إمكانية تطبيق قواعده على هذا النوع الجديد من الحروب؛ ذلك لأن الفترة التي جرى فيها تقنين قواعد قانونية ذات الصلة بوسائل القتال وأساليبه، لا سيما اتفاقيات لاهاي لعام 1899–1907م، واتفاقيات جنيف الأربع لعام 1949 والبروتوكولان الإضافيان لعام 1977، حينها لم يكن للهجمات السيبرانية عند إبرامها أي وجود يُذكر ما يعني أنها لم تُقنّن بأحكام خاصة تنظم استعمالها من الناحية القانونية.

وفي ضوء أحكام قانون الحرب، كان تطوير وسائل وأساليب قتال جديدة متوقعًا. فالمادة (36) من البروتوكول الإضافي الأول الملحق باتفاقيات جنيف نصت على أنه: «يلتزم أي طرف سامٍ متعاقد، عند دراسة سلاح جديد، أو تطويره، أو اقتنائه، أو أداة حرب، أو اتّباع أسلوب للحرب، بأن يتحقق مما إذا كان ذلك محظورًا في الأحوال كافة أو في بعضها بمقتضى هذا الملحق البروتوكول أو أي قاعدة أخرى من قواعد القانون الدولي التي يلتزم بها ذلك الطرف السامي المتعاقد». وبالتالي، تضع هذه المادة الإطار العام الناظم لاستخدام وسائل وأساليب قتال جديدة في النزاعات المسلحة، وتبيّن أحكام هذه المادة أنه على ضوء قانون الحرب، يتعيّن على الدول التي تقتني أسلحة حديثة أو تطوّرها تتبّع أسلوب قتال جديد، وأن تحدد مشروعية استعمالها، كما يفيد هذا النص ضمنيًا أن كل قواعد قانون الحرب تكون قابلة للتطبيق على وسائل القتال الحديثة وأساليبها، ففي حال غياب النص الخاص يطبّق النص العام، هذا من حيث المبدأ.

وباستقراء المادة (36) من البروتوكول الإضافي الأول نجد أنها لا تحرّم تطوير، أو اقتناء أسلحة حديثة أو حتى حيازة أسلحة أو اعتماد أساليب جديدة غير منظمة بقواعد القانون الدولي الإنساني، ومن هذا المنطلق فإن أحكام هذه المادة لا توقف حق الدول في ذلك، وإنما تنص على ضرورة المراجعة القانونية عند اقتناء أسلحة من نوع جديد أو تطويرها أو أسلوب حديث أو ما يعرف بالمطابقة القانونية مع قواعد القانون الدولي وذلك قبل استعمالها، ومن ثم لا يعد هذا النص قانونًا جديدًا ولكنه يقنّن القاعدة القانونية العرفية في التزام الدول بتطبيق معاهدة أو قاعدة عرفية بنيّةٍ حسنة، والمقصود هنا بصفةٍ خاصة القواعد الدولية لتنظيم العمليات العدائية.

وتطرح وسائل القتال الجديدة وأساليبه تحديات قانونية وعملية فيما يخص ضمان استخدامها على نحو يمتثل لقواعد القانون الدولي الإنساني القائمة وإيلاء الاعتبار الواجب للتداعيات الإنسانية المتوقعة جراء استخدامها. فحق الأطراف في اختيار وسائل الحرب وأساليبها حق مقيد باحترام مبادئ النزاعات المسلحة وقوانينها وأعرافها، ويحظّر القانون الدولي الإنساني استخدام وسائل الحرب وأساليبها التي تعد عشوائية الأثر أو تسبب ضررًا زائدًا أو آلامًا لا لزوم لها.

وعليه، فإن هذه المنظومة القانونية السابقة الذكر تشكّل القيود والحدود لاستعمال وسائل الحرب المنظومة وأساليبها[٣٨].

ومع دخولنا في عصر هذا النوع الجديد من الحروب، فإن الخطورة المتعلقة بوسائل القتال الجديدة وأساليبه تكمن في انتفاء عنصر المواجهة المباشرة والتقدير البشري الذي يصاحبها، ويجب أن تبقى الأعمال العدائية ضمن الغرض المطلوب من الحرب ألا وهو قهر قوات العدو وإجبارها على التسليم، وبذلك فإن الوسائل والأساليب المستعملة يجب ألا تتعدى هذا الغرض فتصل إلى الأعمال الوحشية، ويمكن أن تستهدف الهجمات السيبرانية القطاعات الاقتصادية، الأمنية، الزراعية، الصناعية وغيرها من القطاعات... في إطار نزاع مسلح، ونجحت عدة هجمات في السابق، في قطع إمدادات خدمات أساسية للسكان المدنيين، إذ طالت هذه الهجمات السيبرانية قطاع الخدمات الصحية المحمي بموجب القانون الدولي الإنساني، فضلًا عن الأعيان المدنية مثل الأعيان التي لا غنى عنها لبقاء السكان المدنيين على قيد الحياة، والأعيان التي تضم قوى خطرة وغيرها المحمية أيضًا بموجب قانون الحرب.

ولا جدال أن مصطلح الهجوم السيبراني يتميز عن الجريمة السيبرانية الذي كثيراً ما يتم الخلط بينهما من قبل المهتمين في هذا المجال، فأن الخلط بين المصطلحين يؤدي بالنتيجة الى خلق مشكلة جديدة قد تؤدي إلى خرق القانون الدولي فيما لو ان الدولة المعتدى عليها قد تصرفت بغض النظر عن تحديد نوع الاعتداء هل هو هجوم سيبراني أم جريمة سيبرانية، إذ إن حق الدولة المعتدى عليها في الهجوم السيبراني يكون مختلف عن حقها في الرد عن الجريمة السيبرانية، كما أن الهجوم السيبراني هو فعل يقوض من قدرات ووظائف شبكات الحاسوب من أجل هدف قومي أو سياسي، من خلال استغلال نقاط الضعف لتمكن المهاجم من خرق الانظمة والعبث بها[٣٩].

---

[٣٨] بيتر ماورير، (2014) القانون الدولي الإنساني، إجابات على أسئلتك، حقوق الطبع محفوظة للجنة الدولية للصليب الأحمر، كانون الأول، ص 50.

[39] Ian Traynor. (2007). Russia Accused of Unleashing Cyber War to Disable

وفي الواقع يكون للهجوم السيبراني القدرة على إغلاق أجهزة الطرد المركزي النووية وأنظمة الدفاع الجوية والشبكات الكهربائية الذي يعد تهديداً خطيراً للأمن القومي، لذا ينبغي التعامل مع الهجمات السيبرانية بوصفها أعمال حرب؛ لأنها تشبه الهجمات المسلحة التي ينظمها قانون الحرب.

في حين أن تعريف الجريمة السيبرانية هي عبارة عن مخالفة ترتكب ضد الأشخاص أو الجماعات بدافع إجرامي كالدخول غير المصرح به وإتلاف البيانات المخزونة في النظم أو الاعتراض غير القانوني لها عن طريق نقلها من جهاز حاسوب لآخر كإدخال بيانات خاطئة او العبث بها، كما عرف ت بأنها "سلوك غير مشروع معاقب عليه قانوناً صادر عن إرادة إجرمية محله معطيات الحاسوب"[٤٠]، وقد عرف الفقيه الألماني (Ulrich Sieber) الجرائم السيبرانية بأنها "الاعتداءات القانونية التي يمكن أن ترتكب بواسطة المعلوماتية بغرض تحقيق الربح". علاوة على ذلك، يبدو أن الهدف من الجريمة السيبرانية يكون مختلف تماماً عن الهدف من الهجوم السيبراني؛ لأن نتيجة الهجوم هي من تحدد من يقف وراءه، حيث إن الهجوم السيبراني تقوم به دولة أو منظمات إرهابية من أجل مقتضيات الأمن القومي، بينما الجريمة السيبرانية تكون بعيدة عن سياسة الدولة ويستبعد أن تكون الدولة هي المهاجم، بل يكون أشخاص أو مجاميع قرصنة من يقوم بتنفيذ الجريمة السيبرانية[٤١].

ويمكننا القول إن الهجوم السيبراني على البنية التحتية الحيوية وأدى إلى شل الإدارات الحكومية أو إحداث دمار واسع النطاق فيها، ينبغي اعتباره هجوماً مسلحاً، حتى لو لم يتسبب ذلك في أضرار مادية أو وفاة البشر على الفور. على سبيل المثال، هجوم على المالية الحكومية يجب أن يكون من خلال تغيير أو تدمير المعلومات التي تسبب خطرا على الحياة الاقتصادية للدولة وبالتالي يعد هجوماً مسلحاً وهذا ليس بسبب الدمار المادي، ولكن لكون

Estonia, Guardian London, May 17. [Online] Available at: http://www.theguardian.com/world/2007/may/17/topstories3.russia

[٤٠] صالح، نائل عبد الرحمن، (2004)، واقع جرائم الحاسب في التشريع الإردني، مؤتمر القانون والكمبيوتر والانترنيت، كلية الشريعة والقانون، جامعة الإما رات العربية المتحدة، ط3، المجلد الأول، ص 192.

[٤١] كامل، سعيد، (1993)، جرائم الكمبيوتر والجرائم الأخرى في مجال التكنولوجيا، بحث مقدم إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، ص 516.

الهجمات تسببت في أن تصبح البنية التحتية للدولة غير قادرة على الوصول إلى الأهداف التي تم إنشاؤها لتحقيقها، ولذلك ينبغي اعتبار مثل هذه الهجمات بمنزلة هجوم مسلح[٤٢].

لذا فان الهجوم السيبراني يكون من اختصاص القانون الدولي العام؛ لأنه يمثل خرق لسيادة الدولة، بينما تكون الجريمة السيبرانية ضمن اختصاص القانون الوطن ي وفقاً لمبدأ اقليمية القانون. بالتالي أن ما يميز الهجوم السيبراني عن الجريمة السيبرانية هو أن الهجوم السيبراني يهدف إلى إضعاف أو تدمير قدرات الدولة من خلال شبكات الإنترنت لغرض سياسي أو لمقتضيات الأمن القومي، وهذا لا نجده في الجريمة السيبرانية حيث يكون هدفها مقتصراً على السرقة من أجل الحصول على منافع مالية أو نقدية[٤٣]، في كلتا الحالتين تكون الدولة مسؤولة مسؤولية دولية عن أعمال مواطنيها التي تسبب ضرراً بمصالح الدول الأخرى، وهذا يؤدي الى الحد من الهجمات السيبرانية.

وتصاعد خطر الهجمات عبر الفضاء السيبراني بالتزامن مع النمو ذاته فيما يتعلق بأسلحة الدمار الشامل. كما أن هناك دولاً عدة تعمل على نمو قدراتها في مجال حرب المعلومات وأسلحة الفضاء السيبراني. وأخذت هجمات الكمبيوتر والإرهاب الإلكتروني (Cyber Attacks) المزيد من الاهتمام إلى الحدِّ الذي وضعته الدول في إطار استراتيجيتها العسكرية، وما يثيره ذلك من تساؤلات حول حدود استخدام القوة في الفضاء السيبراني للردّ على الهجمات في إطار الدفاع الشرعي أو في استخدامها باعتبارها نمطًا من أنماط استخدام القوة في العلاقات الدولية أو فيما يتعلق بالهجمات الوقائية؛ حيث فرضت هواجس التعرُّض للخطر في أي وقت انتهاج شتى الطرق للحماية، والتي تأخذ شكلا وقائيًّا أو إستباقيا على مصدر التهديد المحتمل، أو العمل على تقوية نظم الحماية والمنعة ضد التعرُّض لمثل تلك الهجمات[٤٤].

---

(42) Nazanin Baradaran & Homayoun Habibi. (2017). Cyber Warfare and Self - Defense from the Perspective of International Law, Journal of Politics and Law (JPL), August, 10 No (4). P. 42.

(٤٣) بن يونس، عمر محمد أبو بكر، (2004)، الجرائم الناشئة عن الأنترنيت، دار النهضة العربية للنشر والتوزيع، القاهرة، ص 158.

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

المبحث الثاني

مدى ملاءمة تطبيق القانون الدولي الإنساني على النزاعات السيبرانية

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

ويتميز الفضاء السيبراني بالترابط وهو يتألف من عدد كبير من أنظمة الحاسوب المتعلقة مع بعضها البعض في جميع أنحاء العالم، وتكون أنظمة الحاسوب عسكرية في كثير من الأحيان مترابطة مع الأنظمة المدنية، لذلك فإنه ليس من السهل إطلاق هجوم سيبراني ضد البنية التحتية العسكرية، والحد من آثاره دون تقوض البنية التحتية المدنية والذي من شأنه أن يكون مثالًا لانتهاك القانون الدولي الإنساني من خلال ضرب الأهداف العسكرية والمدنية والمدنيين على حد سواء.

وهناك مبادئ تتعلق بالنزاعات المسلحة تتمتع بالطبيعة العرفية العامة الآمرة، وتسري في مواجهة جميع الأطراف المتحاربة بغض النظر عن كونهم أطرافًا في الاتفاقيات الدولية المتضمنة لهذه المبادئ أو ليسوا كذلك[٤٥].

ومن هذه المبادئ التي يمكن الاسترشاد بها: مبدأ حق المتحارب في استخدام وسائل القتال وأساليبه، وما يرتبط بها من حظر استخدام الأسلحة التي تسبب آلاما مفرطة، ومبدأ التمييز بين المقاتل والمدني، وبين الأهداف العسكرية والمنشآت المدنية والمنشآت ذات الطبيعة الخطرة [٤٦].

إن القانون الدولي الإنساني ينطبق بمبادئه وقواعده بصفة عامة على أي نزاع مسلح، ويشمل ذلك وسائل الحرب المستخدمة ومكان النزاع أو الصراع المسلح، ولكن في حالة كون مكان النزاع هو الفضاء السيبراني، والأجهزة المستخدمه ذات خواص حديثة ومتطورة فهل ينطبق عليها؟ وسنحاول الاجابة عن عذا التساؤل من خلال ما سيأتي من هذه الدراسة.

---

[٤٥] عبد الصادق، عادل، (2016)، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، وحدة الدراسات المستقبلية، مكتبة الإسكندرية، العدد، 23، ص 82.

[46] Shulman, Mark Russell. (1999). Legal Constraints on Information Warfare. Occasional Paper No. 7 Center for Strategy and Technology Air War College Air University Maxwell Air Force Base. P. 11.

وسنوضح مدى ملاءمة تطبيق القانون الدولي الإنساني على النزاعات السيبرانية، من خلال مطلبين، الأول نتناول فيه تطبيق قواعد القانون الدولي الإنساني على النزاعات السيبرانية، فيما نتطرق في الثاني إلى تطبيق مبادئ القانون الدولي الإنساني على النزاعات السيبرانية.

المطلب الأول

تطبيق قواعد القانون الدولي الإنساني على النزاعات السيبرانية

لا جدال أن الهدف والغرض من القانون الدولي الإنساني هو تنظيم النزاعات المقبلة، أي التي تقع بعد اعتماد معاهدة من معاهدات القانون الدولي الإنساني، وأدرجت الدول، لدى اعتماد معاهدات القانون الدولي الإنساني، القواعد التي تستشرف تطوير وسائل وأساليب جديدة للحرب وافترضت أن القانون الدولي الإنساني سينطبق عليه.

وإن كان هناك من يرى أن استخدام الفضاء السيبراني في الحرب قلب قوانين النزاع المسلح رأساً على عقب؛ لأن الأهداف في أي نزاع سيبراني ستكون على الأرجح مدنية لا عسكريه، وستؤثر على السكان المدنيين لا على القوات العسكرية[٤٧]، كما أن شبكة الإنترنت لا تعترف بالحدود التقليدية، فالفضاء السيبراني جعل الحدود الوطنية وهمية؛ لأن التداخلات بين الشبكات جعلت الحدود غير ملموسة، ويعمل عموماً خارج سيطرة الدول ويمثل ذلك شكلاً جديداً من أشكال الأسلحة التي تعرض المدنيين لأخطار جسيمة، لذا فإنه ليس من المستغرب أن تفقد الدولة سيطرتها عندما يتعلق الأمر بالأمور التنظيمية في الفضاء السيبراني.

وعلى امتداد التاريخ الحديث تم تحديث القوانين الدولية للنزاع المسلح، استجابة لفظائع الحروب والوسائل الجديدة لخوضها، وثمة حاجة ملحة للقيام بذلك؛ لأن أعمال الحرب السيبرانية ستسفر على الأرجح عن خرق أحكام عديدة في القوانين الحالية للنزاعات المسلحة، أو أنها ستكون خارج نطاق هذه القوانين تماماً.

إن استخدام العمليات السيبرانية خلال النزاعات المسلحة حقيقة واقعة، فبينما أقر عدد ضئيل من الدول علانية بإجراء مثل هذه العمليات، يعمل عدد متزايد منها على تطوير قدرات سيبرانية لأغراض عسكرية، ومن المرجح أن يزداد استخدامها في المستقبل، وأظهرت أحداث السنوات الأخيرة أن العمليات السيبرانية يمكن أن تؤثر بشكل خطير على البنية التحتية المدنية، وقد تتسبب في إلحاق أضرار بشرية[٤٨].

---

[٤٧] انظر: وستبي، جودي ر.، (2011)، دعوة إلى الاستقرار الجيوسيبراني، البحث عن السلام السيبراني، الاتحاد الدولي للاتصالات والاتحاد العالمي للعلماء، ص 68.

[٤٨]– اللجنة الدولية للصليب الأحمر، (2019)، القانون الدولي الإنساني والعمليات السيبرانية خلال النزاعات

والدول اليوم معنيه بتحديد القانون الواجب التطبيق على الحرب السيبرانية، فقد تبنت عدة دول مبادرات على المستوى الوطني والدولي، فعلى سبيل المثال، الاتحاد الأوروبي ركز جهوده على جرائم الإنترنت عندما تبنى في عام 2013، "استراتيجية الأمن السيبراني ومشروع التوجيه الذي ركز على البُعد الخاص للأمن السيبراني".

والمبادرة الأكثر نجاحاً هو ما ورد في دليل تالين الذي يشير إلى أن القانون الدولي الإنساني ينطبق على الحرب السيبرانية، ويحدد الدور الذي ستلعبه قواعد القانون الدولي الإنساني في هذا المجال[٤٩].

ويقسم هذا الدليل إلى قسمين: الأول يعالج قانون الأمن السيبراني والثاني قانون النزاعات السيبرانية، ويقر قانون تالين بأن العمليات السيبرانية قد تشكل نزاعات مسلحة تبعاً للظروف، لا سيما الأثار المدمرة لتلك العمليات[٥٠].

وكان للاختلافات بين النزاع الحركي التقليدي والنزاع السيبراني آثار واسعة من حيث تصوراتنا للنزاع، فقانون النزاعات المسلحة والقوانين المنظمة لاستخدام القوة في العلاقات الدولية والتي يتضمنها ميثاق الأمم المتحدة وُضِعَت لتتماشى مع النزاع الحركي التقليدي،

ولكن على الرغم من أن المبادئ الرئيسية لهذه القوانين ما زالت صالحة، فإن كيفية تطبيقها على النزاع السيبراني في أي حالة مُعيَّنة أمر يشوبه–على أحسن تقدير–الغموض اليوم، فالمعتقدات البديهية للقادة (ومستشاريهم القانونيين) صُقِلت في بيئات النزاع الحركي التقليدي، وما عدا قلة من المتخصصين، لا يوجد على نطاق واسع فهم للنزاع السيبراني داخل أوساط قادة القوات المسلحة اليوم.

المسلحة، ورقة موقف مقدمة من اللجنة الدولية للصليب الأحمر إلى فريق العمل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، وإلى فريق الخبراء الحكوميين المعني بالارتقاء بسلوك الدول المسؤول في ميدان الفضاء السيبراني في سياق الأمن الدولي، 28 نوفمبر، ص 2.

[٤٩] نشر حلف شمال الأطلسي الناتو في عام 2013 دليلًا باسم تالين مكون من 282 صفحة، ويحتوي على (95) مادة للقوانين الدولية المطبقة في حال نشوب حروب السيبرانية وتنظيم قواعد الاشتباك عبر الإنترنت.

[50] Barrett, E. (2017). On the Relationship between the Ethics and the Law of War: Cyber Operations and Sublethal Harm, Ethics & International Affairs, 31(4). Pp. 467-477.

ويواجه انطباق القانون الدولي الإنساني على الهجمات السيبرانية تحديات عدة، فلا يتضمن القانون الدولي الإنساني على أي قواعد صريحة بشأن الهجمات السيبرانية في الفضاء السيبرانية، والسبب في ذالك هو أنها لا تكون هذه الهجمات حركية، أي ليست هجمات مسلحة بالمعنى التقليدي، إلا أنه وبالنظر إلى الهدف الأساسي للقانون الدولي الإنساني المتمثل بحماية المدنيين من ويلات الحرب، يصبح القانون الدولي الإنساني منطبقاً، وتندرج تلك الهجمات ضمن قواعده إذا كان هدف الهجمات السيبرانية هو تعريض الأشخاص المحميين وممتلكاتهم للخطر أو المخاطرة بحدوث ذالك، ولكن يبقى التحدي في مقدرة القانون الدولي الإنساني على تنظيم أساليب ووسائل الحرب الجديدة، ويسعى القانون الدولي الإنساني منذ نشوئه لتنظيم القواعد والضوابط التي تحكم سير العمليات العسكرية خلال النزاعات المسلحة بنوعيها الدولي وغير الدولي، وعلى الرغم من عدم قدرة هذا القانون على منع الحرب، إلا أنه يسعى للحد من آثار النزاع المسلح فيما بين الأطراف المتنازعة وبشكل خاص لحماية المدنيين الذين لا يشاركون في القتال، والأشخاص الذين أصبحوا عاجزين عن المشاركة في القتال والسعي لتحييد الأعيان المدنية عن سير الأعمال العدائية خلال سير العمليات القتالية التقليدية، ظهرت هذه المبادئ في ضوء الحروب التقليدية ومع التطور التقني ودخول مفهوم الحرب السيبرانية إلى النزاعات المسلحة كان من المفترض وجود ضوابط لحماية الفئات المحمية في سياق هذه النزاعات.

ولم تشر أحكام القانون الدولي الإنساني على وجه التحديد إلى الهجمات السيبرانية، ولهذا السبب، ولما كان استغلال التكنولوجيا الإلكترونية ظاهرة جديدة نسبيًا ويبدو أنها تؤدي في بعض الأحيان إلى استحداث تغيير نوعي كامل في وسائل وأساليب القتال، يدفع البعض من حين لآخر إلى القول بأن القانون الدولي الإنساني غير متوائم مع العالم السيبراني ولا يمكن تطبيقه على الحرب السيبرانية[٥١].

وبالرغم من ذلك، فإن عدم وجود إشارات محددة في القانون الدولي الإنساني إلى الهجمات السيبرانية لا يعني أن هذه الجمات غير خاضعة لقواعد القانون الدولي الإنساني، فالتكنولوجيات الجديدة من جميع الأنواع في حالة تطور باستمرار والقانون الدولي الإنساني يتسع بصورة كفاية لاستيعاب هذه التطورات الجديدة.

---

(51) Dunlap. op, cit, p. 81.

وتجدر الإشار إلى أن أي سلاح لم يتم ذكره في أي اتفاقية لا يعني بالضرورة إباحة استخدامه، ويعد المثال الواضح للحظر الوقائي الوحيد هو ما ورد في البروتوكول الرابع لاتفاقية الأسلحة التقليدية لعهام 1980 الخاص بحظر استخدام أسلحة الليزر المعمية والذي ألحق باتفاقية عام 1995، فهذا السلاح تم تحريمه بمجرد بدء التجارب عليه، وقبل وضعه موضع الاستخدام العسكري الفعلي، لكن هذا المثال لا يمكن تعميمه؛ لأن معظم التجارب على الأسلحة الجديدة تعد أسراراً عسكرية، وبالتالي من النادر التعرف على آثار تلك الأسلحة، ومن ثم يأخذ تحريم استخدام سلاح معين حيزاً من الجهد والوقت والنيات الحسنة، وهذا ما قد لا يتوفر، ولا شك أن الحرب السيبرانية تشكل تحديات خطيرة أمام المبادئ الأساسية التي يستند إليها القانون الدولي الإنساني، ولا سيما التمييز –وهو القدرة المحتملة على التمييز– بين الأهداف العسكرية والأعيان المدنية. وبالتالي، فإن السؤال المطروح لا يتعلق كثيراً بما إذا كانت القواعد التي تحكم سير العمليات العدائية تنطبق على الحرب السيبرانية، بل بالأحرى كيف ستُطبق؛ أي كيف يمكن ترجمتها بحيث يكون لها مدلول منطقي في هذا العالم الجديد، ما الأفعال التي تخضع لقواعد القانون الدولي الإنساني التي تحكم سير العمليات العدائية؟ والسبب الذي يؤدي إلى إثارة هذه المناقشة هو أن الفضاء الإلكتروني يختلف عن مسارح الحروب التقليدية في أن وسائل وأساليب الهجوم لا تتضمن استخدام القوة الحركية التقليدية، أو ما يفهم عمومًا على أنه عنف.

وبالتالي، يمكن لعدد من العمليات الإلكترونية أن تلحق تأثيرًا شديدًا على العين المستهدفة من خلال تعطيلها عن العمل، ولكن دون إلحاق الأضرار المادية بالعين التي تحدث في الحرب التقليدية.

وقد وقع اختلاف في آراء المختصين القانونيين، ما بين من يرى أن المبادئ والقواعد التي أرساها القانون الدولي الإنساني تنطبق على تلك الهجمات، ومن يذهب إلى أن المُدة التي جرى فيها تقنين القواعد القانونية ذات الصلة باستخدام وسائل وطرائق القتال، لم يكن لاستخدام الأنظمة الالكترونية للأغراض العسكرية الهجومية وجود يذكر، ما يعني أنها غير مقننة، وغير منظمة وفقاً للقواعد الدولية؛ أي أنها خارج التنظيم القانوني الدولي، وهي بحاجة لقوانين جديدة صريحة تنص على تنظيمها بشكل لا يدع أي مجال للاجتهاد والتأويل[٥٢].

(52) Haslam, Emily. (2000). Information Warfare: Technological Changes and International Law. Journal of Conflict and Security Law. Vol (5). No (2). P, 157-175.

ولعل أهم المبادئ القانونية الذي فتح مجالاً أمام القياس وإنزال حالة الحروب الإلكترونية عليه هو مبدأ الامتناع عن استخدام القوة عموما من قبل أي دولة ضد أي دولة أخرى، والذي جاء النص عليه في الفقرة الرابعة من المادة الثانية من الميثاق[٥٣]. وهنا ظهر الجدل حول إمكانية اعتبار الهجمات السيبرانية بمنزلة خرق واضح لحكم هذه الفقرة. ما بين اعتبار أنها تقتصر على التهديد أو الاستخدام الفعلي للقوات المسلحة فحسب، حيث تحبذ هذا التفسير الدول المتفوقة في مجال الحرب السيبرانية، أما الدول الأخرى فتميل إلى توسعة نطاق مدلول كلمة "القوة" في الفقرة، لتشمل السيبرانية أيضاً.

وذهب كُلاً من "شين"، و"روسيني" إلى أنه من الممكن أن تُعد الهجمات السيبرانية بمنزلة خرق واضح لأحكام الفقرة الرابعة من المادة الثانية من ميثاق الأمم المتحدة، شريطة أن تتسبب في تعطيل أو دمار واسع للبنى التحتية الضرورية في حياة الناس[٥٤]، ووفقاً لهما، فإنه وأن تم ذلك فإن للدولة المعتدى عليها الحق في اللجوء إلى إستخدام القوة وفقاً للمادة (51) من الميثاق[٥٥]، والتي تتيح الحق في الدفاع عن النفس، يمكن للقواعد العرفية الدولية أن تؤدي دوراً متميزاً في تكييف تلك الهجمات، ولا سيما في ظل عدم وجود اتفاقيات دولية تنظم الهجمات السيبرانية.

ووفقاً لهذا الاجتهاد فإن للدولة الحق في الدفاع عن نفسها إزاء أي هجوم، بغض النظر عن شكله ووسيلته، وقد جاء إعلان وزارة الدفاع الأمريكية "البنتاغون" في عام 2011 ليؤكد على هذا الاعتبار، إذ جاء فيه بأن توجيه هجمات سيبرانية ضد الولايات المتحدة الأمريكية، وما ينجم عنها من أضرار، يعني تبرير استخدام القوة العسكرية اللازمة، للرد على هذا الاعتداء، باعتبار ذلك حرباً مبررة وعادلة[٥٦].

---

[٥٣]– تنص المادة (2/4) على أنه: «يمتنع أعضاء الهيئة جميعاً في علاقاتهم الدولية عن التهديد باستعمال القوة أو استخدامها ضد سلامة الأ راضي أو الاستقلال السياسي لأية دولة أو على أي وجه آخر لا يتفق ومقاصد الأمم المتحدة».

[54] Roscini, Marco. (2010). Worldwide Warfare: Jus ad bellum and the Use of Cyber Force. Max Planck Yearbook of United Nations Law, Vol, (14). No (1). pp: 85-130.

[٥٥] نصت المادة (51) من الميثاق على أنه: «ليس في هذا الميثاق ما يضعف أو ينتقص الحق الطبيعي للدول، فرادى أو جماعات، في الدفاع عن أنفسهم إذا اعتدت قوة مسلحة على أحد أعضاء الأمم المتحدة».

[56] Gorman, S., & Barnes, J. E. (2011). Cyber combat: Act of war. The Wall Street Journal. Y. No. (31).

وبينما يستمر الجدل حول مسألة ما إذا كان القانون الدولي الإنساني ينطبق على العمليات السيبرانية أثناء النزاع المسلح، وبالتالي يقيدها، وكان اللجنة الدولية موقفاً إيجابياً واضحاً منذ البداية جيث ترى اللجنة الدولية أنه ليس هناك شك في أن القانون الدولي الإنساني ينظم العمليات السيبرانية أثناء النزاعات المسلحة أو الحرب السيبرانية– شأن أي سلاح أو أساليب ووسائل القتال التي يلجأ إليها أي طرف من الأطراف المتحاربة في النزاع، سواء كانت قديمة أو حديثة، واعتماد العمليات السيبرانية على تقنية جديدة ومتطورة باستمرار لا يحول دون تطبيق القانون الدولي الإنساني على استخدام هذه التقنيات باعتبارها من وسائل أو أساليب القتال، ويصح ذلك سواء كان الفضاء السيبراني يعد ميداناً جديداً للحرب على غرار الجو والأرض والبحر والفضاء الخارجي أو يعد نوعاً مختلفاً من الميادين؛ لأنه من صنع الإنسان في حين أن الأول طبيعي؛ أو لا يعد ميداناً على هذا النحو[٥٧]، وهناك تأييداً قوياً لهذا الرأي في معاهدات القانون الدولي الإنساني، وفي الاجتهاد القضائي لمحكمة العدل الدولية، وفي الآراء التي أعرب عنها عدد من الدول والمنظامت الدولية[٥٨].

وأكدت اللجنة الدولية على أن "قواعد القانون الدولي الإنساني لا تنطبق فقط على العمليات الحركية ضد الأجسام الفضائية، –بل أيضاً –على العمليات غير الحركية التي من شأنها أن تعطل الأجسام الفضائية دون أن تلحق بها ضرر مادياً بالضرورة، وعند تقييم مشروعية هذه الهجمات، يجب النظر في جميع حالات الضرر والأذى العرضية المباشرة وغير المباشرة التي من المتوقع أن تلحق بالأعيان المدنية، بما في ذلك عند استهداف جسم موجود في الفضاء ذي استخدام مزدوج. وينبغي –أيضًا– عند تطبيق هذه القواعد، مراعاة خطر إحداث الحطام وآثاره غير المباشرة[٥٩]، كما أكدت –أيضًا– على أن القانون الدولي الإنساني يحظر الأسلحة التي من شأنها أن تسبب إصابات مفرطة أو آلاماً لا مبرر لها، والتي تكون عشوائية بطبيعتها بالإضافة إلى عدد من الأنواع المحددة من الأسلحة[٦٠].

---

(57) Geisel, Laurent, et al, op, cit, p. 297-298.

(58) Ibid, p. 298.

[٥٩] اللجنة الدولية للصليب الأحمر، (2019)، القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة، اللجنة الدولية، جنيف، ص 27.

[٦٠] اللجنة الدولية للصليب الأحمر، (2021)، التكلفة البشرية المحتملة لاستخدام الأسلحة في الفضاء الخارجي والحماية التي يوفرها القانون الدولي الإنساني، ورقة موقف مقدمة من اللجنة الدولية للصليب الأحمر إلى الأمين العام للأمم المتحدة، بشأن المسائل المحددة في قرار الجمعية العامة رقم 36/75، 7 أبريل، ص4.

ويحظر القانون الدولي الإنساني أو يقيد استخدام أسلحة معينة على وجه التحديد (الأسلحة الكيماوية أو البيولوجية أو الألغام المضادة للأفراد على سبيل المثال)، وهو كذلك ينظم، من خلال قواعده العامة، جميع وسائل وأساليب القتال، بما في ذلك استعمال جميع الأسلحة، وعلى وجه التحديد تنص المادة (36) من البروتوكول الأول لاتفاقيات جنيف على ما يلي:"يلتزم أي طرف سام متعاقد، عند دراسة، أو تطوير، أو اقتناء سلاح جديد، أو أداة للحرب، أو اتباع أسلوب للحرب، بأن يتحقق مما إذا كان ذلك محظورًا في جميع الأحوال أو في بعضها بمقتضى هذا الملحق «البروتوكول» أو أية قاعدة أخرى من قواعد القانون الدولي التي يلتزم بها الطرف السامي المتعاقد"[٦١].

وتبين هذه القاعدة أن قواعد القانون الدولي الإنساني تنطبق على التكنولوجيا الجديدة، بخلاف الالتزام المحدد الذي يفرضه على الدول الأطراف في البروتوكول الإضافي الأول، وهناك منطلق قانوني آخر يدفع باتجاه ضرورة تحديد الوضع القانوني للهجمات السيبرانية يتمثل فيما جاء بالمادة (31) من البروتوكول الإضافي الأول الملحق باتفاقيات جنيف، والتي نصت على أنه: "يلتزم أي طرف سامٍ متعاقد، عند دراسة سلاح جديد، أو تطويره، أو اقتنائه، أو أداة حرب، أو اتباع أسلوب للحرب، بأن يتحقق مما إذا كان ذلك محظوراً في الأحوال كافة أو في بعضها بمقتضى هذا الملحق البروتوكول أو أي قاعدة أخرى من قواعد القانون الدولي التي يلتزم بها ذلك الطرف السامي المتعاقد"[٦٢]، وبالتالي، فإن هذه المادة تنص على ضرورة التنظيم القانوني لوسائل وأساليب القتال الجديدة، ومن بينها بالطبع الوسائل الإلكترونية المستخدمة في شن الهجمات السيبرانية، وتعقيباً على ما سبق يُلاحظ بأن التكييف القانوني للهجمات السيبرانية لازال ضمن مستوى القياس والاجتهاد، ولم يصل بعد إلى مرحلة إبرام اتفاقيات دولية صريحة خاصة به، بحيث تكون متعددة الأطراف، وتنظم الهجمات الإلكترونية وفق نصوص وقواعد قانونية صريحة، وهو ما يُعزى إلى أسباب عدة، يأتي في مقدمتها وجود عقبات تضعها الدول المهيمنة في مجال حروب الفضاء الإلكتروني، مثل الولايات المتحدة الأمريكية، وروسيا، والصين.

---

[٦١] انظر: نص المادة (36) من البرتوكول الإضافي الأول.

[٦٢] انظر: نص المادة (31) من البروتوكول الإضافي الأول.

إذ إن هذه الدول لا تفضل طرح موضوع التنظيم على المنابر الدولية حتى لا تفقد موقعها المهم بين الدول المهيمنة، وهو ما يضر بأمنها القومي، فضلاً على أن بقاء الموضوع خارج حدود القضايا القانونية، يتيح للدول مساحة واسعة لكي تتحرك في توظيف أسلحتها الإلكترونية لتحقيق أهدافها، وهي بذلك تبقى خارج نطاق المساءلة القانونية يترتب على ذلك كله مسألة أخرى أخرى تتعلق بطبيعة المواجهات في الفضاء الإلكتروني، إذ أن من الصعوبة بمكان إثبات المسؤولية عن الهجمات، والتي تتخذ من الفضاء الإلكتروني مجالها الرحب، لكونها تصرفات غير مادية، ولا يمكن إثباتها بالطرق العادية، وما يزيد من الصعوبة في التنظيم أيضا هو استخدام هذه التقنيات لا من الدول فقط، بل من مجموعات من غير الدول.

أيضاً، بالرغم من ذلك، فقد برزت بعض المحاولات لبلورة اتفاقيات دولية بهذا الشأن، إلا أنها لم ترقَ إلى مستوى تنظيم الحروب والهجمات السيبرانية، بقدر ما كانت أقرب لإقرار أطُر لما بات يُعرف بالجرائم الإلكترونية، ذات الطابع الجنائي، وذلك تحديداً على المستويات الوطنية، ومن أبرز هذه المساعي اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، المقرة في تشرين الثاني/نوفمبرعام2001، والتي تعرف أيضا باسم "معاهدة بودابست لمكافحة جرائم الفضاء المعلوماتي". وقد بُنيَ عليها لاحقاً تشريعات وطنية استندت إليها، سواء في أوروبا أو غيرها من الدول حول العالم[٦٣].

وبالتالي فإن مفهوم الجريمة السيبرانية، وفقاً لهذه الاتفاقية، قد اقتصر على هذه الحالات، ولم يتطرق إلى مستوى الهجمات والحروب السبيرانية التي تكون أطرافها من الدول أو من المنظمات المرتبطة بها، ومن ثم جاء قرار الجمعية العامة للأمم المتحدة رقم (56/121) الصادر في 23/ كانون الثاني/يناير2002 م، والموسوم بـ "مكافحة إساءة استعمال تكنولوجيا المعلومات" والذي جاء فيه: " دعوة الدول الأعضاء، لوضع قوانين وسياسات وممارسات وطنية لمكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية"[٦٤].

---

[٦٣] محمد، لينا جمال، (2016)، الجرائم الإلكترونية، (ماهيتها – طرق مكافحتها) ، ط1، عمّان، الأردن، دار خالد اللحياني للنشر والتوزيع، ص 94.

[64] See GA/RES 56/121(23 January 2002).

وجاء في دليل تالين الإشارة في القاعدة (33) منه إلى أنه: "لا يجوز أن تكون الأعيان المدنية هدفاً للهجمات السيبرانية، فلا يجوز على سبيل المثال توجيه الهجمات السيبرانية التي من شأنها تدمير الأنظمة المدنية والبنية التحتية، ما لم تعد هذه الأنظمة من قبيل الأهداف العسكرية التي يجوز استهدافها وفق الظروف السائدة"[٦٥].

وفي الحقيقة أن التحدي الأكبر الذي يواجه تنظيم الهجمات السيبرانية قانونياً هو عدم وجود إرادة دولية على صعيد المفاوضات أو على صعيد قرارات مجلس الأمن، حيث تغيب الإرادة الدولية اللازمة للدفع باتجاه ذلك، وخصوصاً من قبل الدول المهيمنة في هذا المجال، كما أن القانون الدولي الإنساني يذهب إلى تنظيم استخدام الأسلحة بصورتها التقليدية وغير التقليدية، في حين لا يبدو أن الهجمات السيبرانية، حتى الآن، تصنف على هذا النحو، باعتبارها أسلحة مادية، وذلك باعتبار بقاء النظر لها باعتبارها تعمل في الحيز السيبراني غير المادي، كما في عمليات الاستحواذ على ملفات رقمية أو تعطيل مواقع إلكترونية، ومع ذلك، فإن الحرب السيبرانية تتحدى بعضًا من أكثر الافتراضات الأساسية للقانون الدولي الإنساني منها:

أولاً: يفترض القانون الدولي الإنساني أن أطراف النزاع معلومة ومحددة، ولا يمكن التسليم بهذا الأمر دائمًا حتى في النزاعات المسلحة التقليدية، ولا سيما النزاعات المسلحة غير الدولية، ومع ذلك، في العمليات السيبرانية التيتحدث يوميًا، فإن عدم الكشف عن الهوية هو القاعدة وليس الاستثناء، ويبدو من المستحيل في بعض الحالات تتبع مصدر هذه العمليات، وحتى عندما يكون هذا ممكنًا، فإنه يستغرق وقتًا طويلاً في معظم الحالات، ولما كان القانون كله قائمًا على إسناد المسؤولية (في القانون الدولي الإنساني إلى طرف في النزاع أو إلى فرد)، تنشأ صعوبات رئيسية على وجه الخصوص، إذا لم يكن من الممكن تحديد هوية مرتكب عملية معينة ومن ثم لا يمكن تحديد علاقة العملية بنزاع مسلح معين، فسيكون من الصعب للغاية تحديد ما إذا كان القانون الدولي الإنساني ينطبق حتى على العملية، ومن ثم على سبيل المثال، إذا تعرضت البنية الأساسية لحكومة ما لهجوم، ولكن لم يكن من الواضح من يقف وراء الهجوم، فمن الصعب تحديد من هي أطراف النزاع المسلح، ومن ثم تحديد ما إذا كان هناك نزاع مسلح أصلاً، وبالمثل، حتى إذا كانت أطراف النزاع معلومة، قد يكون من الصعب إسناد الفعل إلى طرف واحد معين.

ثانيًا: يستند القانون الدولي الإنساني إلى افتراض أن وسائل وأساليب القتال سيكون لها آثار عنيفة في العالم المادي، ومن المرجح أن يكون للكثير من الهجمات السيبرانية آثار تخريبية، ولكنها ليست مدمرة من الناحية المادية بشكل مباشر، ثالثًا، يتأسس هيكل القواعد التي تحكم

(65) Tallinn Manual, op. cit, rule (33).

سير العمليات العدائية بأسره –ولا سيما مبدأ التمييز– على افتراض أن معظم الأعيان المدنية والأهداف العسكرية يمكن تمييزها، وفي مسرح عمليات الحرب السيبرانية، من المرجح أن يكون هذا هو الاستثناء وليس القاعدة؛ لأن أغلب البنية الأساسية الإلكترونية حول العالم (الكابلات الممتدة تحت البحر، وأجهزة التوجيه، والخوادم، والأقمار الصناعية) تخدم الاتصالات المدنية والعسكرية على حد سواء.

ومن القواعد التي تحكم سير العمليات العدائية والمصاغة في صورة قيود على الهجمات بشكل أكثر تحديدًا المادة (51) من البروتوكول الإضافي الأول على سبيل المثال، بعد أن تبين في فقرتها الأولى أن «السكان المدنيين والأشخاص المدنيين يتمتعون بحماية عامة ضد الأخطار الناجمة عن العمليات العسكرية»، تستطرد لتنص على أنه «لا يجوز أن يكون السكان المدنيون بوصفهم هذا، وكذا الأشخاص المدنيون، محلًا للهجوم وأن «الهجمات العشوائية محظورة»[٦٦]، ويعرف الهجوم المخالف لمبدأ التناسب في المادة (5/51/ ب) من البروتوكول الإضافي الأول على أنه «الهجوم الذي يمكن أن يتوقع منه أن يسبب خسارة في أرواح المدنيين أو إصابة بهم أو أضرارًا بالأعيان المدنية، أو أن يُحدث مزيجًا من هذه الخسائر والأضرار، يفرط في تجاوز ما ينتظر أن يسفر عنه ذلك الهجوم من ميزة عسكرية ملموسة ومباشرة». وتحظر المادة (6/51) هجمات الردع ضد السكان المدنيين أو الأشخاص المدنيين»، وتنص المادة (52) على أن «تقصر الهجمات على الأهداف العسكرية فحسب». وينص مبدأ الاحتياط في المادة (57) على أن «يتخذ عدد من الاحتياطات فيما يتعلق بالهجمات». وهناك كثير من المواد التي تستخدم مصطلح «الهجوم» عند تقييد حقوق الأطراف المتحاربة[٦٧].

إن عدم وجود ضوابط خاصة بنشاط عسكري معين لا يعني أنه يمكن ممارسة هذا النشاط بدون قيود. فوسائل وأساليب الحرب المستندة إلى التكنولوجيا السيبرانية تخضع لأحكام القانون الدولي الإنساني تمامًا كما يخضع لها أي سلاح جديد عندما يستخدم في نزاع مسلح[٦٨]، اعتمادًا على معيار النتائج غير الإنسانية التي تحدثها هذه الأسلحة، فإذا استخدمت العمليات

---

[٦٦] أنظر: نص المادة (51) البروتوكول الإضافي الأول.

[٦٧] انظر: على سبيل المثال المواد (12 و54 و55 و56) من البروتوكول الإضافي الأول.

[٦٨] اللجنة الدولية للصليب الأحمر، (2011)، تقرير عن القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة، المؤتمر الدولي الحادي والثلاثون للصليب الأحمر والهلال الحمر، جنيف، ص 43– 42.

السيبرانية ضد عدو معين في نزاع مسلح لإلحاق الضرر به عن طريق التلاعب، على سبيل المثال، بنظام المراقبة الجوية بطريقة تؤدي إلى سقوط طائرة مدنية، أو بنظم أنابيب نقل النفط أو منشآت نووية عن طريق العبث بالنظم الحاسوبية المستخدمة بها. فمن الصعب في هذه الحالة نفي كون هذا الهجوم في واقع الأمر وسيلة من وسائل الحرب المحظورة بموجب القانون الدولي الإنساني، كما أنه عندما تتعرض الحواسيب أو الشبكات التابعة لدولة ما لهجوم أو اختراق أو إعاقة، قد يجعل المدنيين عرضة لخطر الحرمان من الاحتياجات الأساسية مثل مياه الشرب والرعاية الطبية الكهرباء، وإذا تعطلت أنظمة عن العمل، قد تحدث إصابات في صفوف المدنيين من خلال تعطيل عمليات إقلاع GPS تحديد المواقع مروحيات الإنقاذ على سبيل المثال، ويمكن أن تتعرض السدود والمحطات النووية وأنظمة التحكم في الطائرات لهجمات سيبرانية؛ نظراً لاعتمادها على الحواسيب، وتكون الشبكات مترابطة إلى حد يجعل من الصعب الحد من آثار هجوم سيبراني ضد جزء من المنظومة دون الإضرار بأجزاء أخرى أو تعطيل المنظومة بأكملها[٦٩]، فمن خلال السلاح الإلكتروني يستطيع العدو أن يخرب شبكة الاتصالات العسكرية، وأن يشل الدورة الاقتصادية والمالية والتجارية والصناعية ... الخ، كل ذلك دون أن يطلق رصاصة واحدة[٧٠].

فالحروب لها قواعد وحدود تنطبق على اللجوء إلى الحرب السيبرانية بنفس القدر الذي تنطبق به على استخدام البنادق والمدفعية والصواريخ وباقي الأسلحة الأخرى[٧١]، ومن الإحصائيات التي يمكن أن تدل على فعالية الهجمات السيبرانية تلك الهجمات التي تم شنها على العراق خلال حرب الخليج الثانية، حيث تشير مصادر كلية الحرب الأمريكية إلى أن ضرب مولدات الطاقة الكهربائية العراقية أدى بشكل غير مباشر إلى موت ما بين (70 إلى

---

[٦٩] اللجنة الدولية للصليب الأحمر، (2013)، ما هي القيود التي يفرضها قانون الحرب على الهجمات السيبرانية؟، أسئلة وإجابات، 28 يونيو، متاح على الرابط التالي:
https://www.icrc.org/ar/doc/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm

[٧٠] نعوس، مصطفى، (2014)، حق الدولة في استخدام القوة في الفضاء الالكتروني للدفاع عن النفس، مجلة الحقوق، العدد الأول، جامعة الكويت، ص 57.

[٧١] اللجنة الدولية للصليب الأحمر، ما هي القيود التي يفرضها قانون الحرب على الهجمات السيبرانية، المرجع السابق.

90) ألف مواطن عراقي كنتيجة مباشرة لعدم توفر الطاقة الكهربائية[٧٢].

المطلب الثاني

تطبيق مبادئ القانون الدولي الإنساني على النزاعات السيبرانية

أفرد القانون الدولي الإنساني مجموعة من القواعد التي تهدف إلى الحد من آثار النزاعات المسلحة سواء أكانت دولية أم غير دولية، إذ تضمن مبادئ وقواعد أساسية تحكم اختيار وسائل القتال وأساليبه؛ إذ انبثقت مبادئ القانون الدولي الإنساني من فكرة مفادها أن هذه المبادئ لا تمنع الأعمال القتالية في النزاعات المسلحة، إنما أفرد القانون الدولي الإنساني مجموعة من القواعد التي تهدف إلى الحد من آثار النزاعات المسلحة سواء أكانت دولية أم غير دولية، إذ تضمن مبادئ وقواعد أساسية تحكم اختيار وسائل القتال وأساليبه؛ إذ انبثقت مبادئ القانون الدولي الإنساني من فكرة مفادها أن هذه المبادئ لا تمنع الأعمال القتالية في النزاعات المسلحة، إنما وُجدت لتقييد وسائل القتال وأساليبه في هذه النزاعات، ولهذه الأسباب هناك إقرار بضرورة قبول مستوى معيّن من العنف والخسارة في الأرواح والدمار من جانب الأطراف المتحاربة كافة كنتيجةٍ طبيعية لمباشرة الأعمال العدائية، وهي تمثّل أبسط الأسس الإنسانية التي تنطبق في كل زمان ومكان، كما أنها تقدّم الحل باستقراء الحالات غير المتوقعة وتسهم في سد ثغرات القانون.

وأكدت محكمة العدل الدولية على أن مبادئ القانون الدولي الإنساني وقواعده الراسخة المنطبقة في النزاعات المسلحة تنطبق "على كافة أشكال الحرب وكافة أنواع الأسلحة، ما كان منها في الماضي، وما هو في الحاضر، وما سيكون في المستقبل[٧٣].

وعليه، يقوم القانون الدولي الإنساني على المبادئ التي تحكم سير العمليات العدائية وهي التمييز، التناسب في استخدام القوة، ومبدأ الضرورات العسكرية، وسنوجزهم على النحو الآتي:

---

[٧٢] عبد الصادق، الإرهاب الإلكتروني القوة في العلاقات الدولية، مرجع سابق، ص 180-181.

[٧٣] قالت المحكمة:

"International humanitarian law has evolved to meet contemporary circumstances, and is not limited in its application to weaponry of an earlier time."I.C.J. Reports 1996, Legality of the reat or Use of Nuclear Weapons Advisory Opinion of 8July 1996, p.38, par.86.

الفرع الأول

مبدأ التمييز

إن مبدأ التميز من المبادئ الأساسية في القانون الدولي الإنساني، وقد أكدت عليه محكمة العدل الدولية، بقولها لا يجوز توجيه الهجمات إلا نحو المقاتلين والأهداف العسكريةٌ فقط، وهذا يعني أنه عند تخطيط وتنفيذ العمليات الإلكترونيةٌ فالأهداف التي تكون مسموح بها هي الأهداف العسكرية، كاجهزة الحاسوب أو الأنظمة الحاسوبية التي تسهم بشكل فاعل في العمليات العسكرية، فلا يجوز توجية الهجمات عبر الفضاء الإلكتروني نحو نظم حاسوبية مستخدمة في منشآت مدنية بحتة، وجاء في المادة (48) من البروتوكول الإضافي الأول أنه: «تعمل أطراف النزاع على لتمييز بين السكان المدنيين والمقاتلين وبين الأعيان المدنية والأهداف العسكرية، ومن ثم توجه عملياتها ضد الاهداف العسكرية دون غيرها، وذلك من أجل تأمين احترام وحماية السكان المدنيين والأعيان المدنية»[٧٤]. وبالاستناد على نص هذه المادة، فإن مبدأ التمييز يتطلب أن تميز أطراف النزاع المسلح في الأوقات كافة بين الأشخاص المدنيين والأعيان المدنية من جهة، والمقاتلين والأهداف العسكرية من جهة أخرى، فضلًا عما نصت عليه المادة (2/51) من البروتوكول نفسه: «لا يجوز أن يكون السكان المدنيون بوصفهم هذا، وكذلك الأشخاص المدنيون محلًا للهجوم وتُحظّر أعمال العنف أو التهديد به الرامية أساسًا إلى بث الذعر في صفوف السكان المدنيين»[٧٥]، كما ورد في المادة (52) من البروتوكول: «لا تكون الأعيان المدنية محلًا للهجوم أو لهجمات الردع»[٧٦]، فضلًا عن المادة (55) من البروتوكول الأول أيضًا الذي يُحظّر استخدام وسائل القتال وأساليبه التي يُقصد بها أو يُتوقع منها أن تسبب أضرارًا بالغة واسعة الانتشار وطويلة الأمد بالبيئة الطبيعية ومن ثم تضر بصحة السكان أو بقائهم، وتُحظّر هجمات الردع ضد البيئة الطبيعية، كما توفر المادة (56) منه الحماية للأشغال الهندسية والمنشآت التي تضم قوى خطرة. ونصت الفقرة الثانية من المادة (50) من البروتوكول على أنه: «لا يجوز أن يكون السكان المدنيون بوصفهم هذا، وكذا الأشخاص المدنيون، محلاً للهجوم، وتحظر أعمال العنف أو التهديد الرامية إلى بث الذعر بين المدنيين»[٧٧].

---

[٧٤]– انظر نص المادة (48) من البرتوكول الإضافي الأول.

[٧٥]– انظر نص المادة (2/51) من البورتوكول الإضافي الأول.

[٧٦]– انظر نص المادة (52) من البورتوكول الإضافي الأول.

[٧٧]– أنظر نص المادة (2/50) من البروتوكول الإضافي الأول.

أما الفقرة الرابعة من المادة (50) فقد نصت على: «عدم جواز استعمال وسائل وطرق قتال من شأنها أن تؤدي إلى هجمات عشوائية، وحددتها بأنها: تلك التي لا توجه إلى هدف عسكري محدد، أو تلك التي تستخدم طريقة أو وسيلة للقتال لا يمكن أن توجه إلى هدف عسكري محدد، أو تلك التي تستخدم طريقة أو وسيلة للقتال لا يمكن حصر آثارها على النحو الذي يتطلبه هذا الملحق، ومن ثم فإن من شأنها أن تصيب في كل حالة كهذه الأهداف العسكرية والأشخاص المدنيين أو الأعيان المدنية دون تمييز» [٧٨].

ونصت الفقرة الخامسة من المادة (50) من البروتوكول على أنه: "يحظر الهجوم الذي يتوقع منه أن يسبب بصورة عارضة خسائر في أرواح المدنيين أو اصابات بينهم، أو أضرا ر بالأعيان المدنية. ويكون مفرطاً في تجاوز ما ينتظر أن يسفر عنه من ميزة عسكرية ملموسة ومباشرة"[٧٩].

وتضمنت العديد من أحكام القانون الدولي الإنساني والقانون الدولي العرفي، اللذين يوفران إرشادات حول كيفية شن الهجمات، مبدأ التمييز، بالإضافة إلى مبدأَي الضرورة والتناسب.

وجاء الرأي الاستشاري لمحكمة العدل الدولية في في العام 1996 ليؤكد على أن القانون الدولي الإنساني يقوم على مبدأَين جوهريَين، يقضي الأول بأنه يجب على الدول ألا تجعل من المدنيين هدفًا للهجوم، أما المبدأ الثاني فيقضي بتحريم استعمال الأسلحة التي من شأنها أن تسبب آلامًا لا مبرر لها، وهذا المبدأ قد نصت عليه أيضًا لائحة لاهاي المتعلقة بقوانين الحرب البرية وأعرافها لعام 1907م «على أن حق الأطراف المتحاربين في اختيار وسائل القتال وأساليبه ليس بالحق غير المحدود»[٨٠]. ونظرًا لكون هذه القواعد مُلزمة، فيكون تنطبقها بالكامل على الهجمات السيبرانية، أمراً ضرورياً.

---

[٧٨]– انظر نص المادة (4/50) من البروتوكول الإضافي الأول.

[٧٩]– أنظر نص المادة (5/50) من البروتوكول الإضافي الأول.

[٨٠]– الرأي الاستشاري لمحكمة العدل الدولية لعام 1996 والخاص بشأن شرعية التهديد أو استخدام الأسلحة النووية.

وربطاً بمبدأ التمييز هناك فضاء سيبراني واحد فقط تتقاسمه القوات المسلحة مع المستخدمين المدنيين وكل شيء متشابك ومترابط، وتبرز التحديات في ضمان توجيه هذا النوع من الهجمات السيبرانية ضد المقاتلين والأهداف العسكرية، وبالتالي تحييد المدنيين أو الأعيان المدنية المحميين بموجب القانون الدولي الإنساني، كما يجب على الدول المشاركة في النزاع المسلح أن تكون حذرة عند استخدام الهجمات السيبرانية، مع العلم أن الخصائص التقنية التي تتمتع بها الهجمات السيبرانية تمنحها القدرة على أن تُضبط بدقةٍ كبيرة لتصيب أهدافًا عسكرية بعينها فقط[٨١]، أن القاعدة هي أنه لا يجوز مهاجمة السكان المدنيين إلا في حال مشاركتهم مشاركة مباشرة في الأعمال العدائية وعلى مدى الوقت الذي يقومون خلاله بهذا الدور، أي أن المدنيين يشاركون مشاركة مباشرة في الأعمال العدائية عندما يقومون بأعمالٍ محددة كجزءٍ من سير الأعمال العدائية بين الأطراف في نزاع مسلح، فالقراصنة يظلون مشمولين بالحماية بموجب القانون الدولي الإنساني ما لم يقوموا بدورٍ مباشر في العمليات العدائية. شمولهم بالحماية لا يعني إعفاءهم من المساءلة الجنائية عما قد ارتكبوه، أما في حال شارك هؤلاء القراصنة مباشرة في الأعمال العدائية، وقاموا بهجمات سيبرانية دعمًا لطرفٍ في النزاع على حساب طرف آخر، فإنهم يخسرون هذه الحماية المكفولة لهم ضد الهجوم المباشر في أثناء تنفيذ الهجوم السيبراني[٨٢].

وبالنظر إلى القضاء الدولي يُعد الرأي الذي ذهبت إليه محكمة العدل الدولية بشأن شرعية التهديد باستعمال أو استعمال الأسلحة النووية عام 1996 الجانب التطبيقي الأكثر تأكيدا إلى مبدأ التمييز والذي جاء فيه" : يهدف إلى حماية السكان المدنيين والأعيان المدنية ويؤسس التمايز بين المقاتلين وغير المقاتلين، وينبغي على الدول، ألا تجعل المدنيين هدفاً للهجوم، ويجب بالتالي ألا تستخدم الأسلحة التي لا تميز بين الأهداف المدنية والعسكرية[٨٣].

---

[٨١] اللجنة الدولية للصليب الأحمر، (2019)، الحرب السيبرانية، القانون الدولي الإنساني يوفر طبقة إضافية من الحماية، 10 سبتمبر.

[٨٢] اللجنة الدولية للصليب الأحمر، الحرب السيبرانية، المرجع السابق.

[83] ICJ Report 1996," Legality of the threat or use of nuclearWeapons", Para 78, p.257.

وبالتالي، فإنه ووفقا لمبدأ "التمييز بين المدنيين والعسكريين" يتوجب على أطراف النزاع المسلح التمييز بين المقاتلين والمدنيين في الهجمات وهو ما لا يتحقق في جانب كبير من الهجمات السيبرانية، والتي تؤدي إلى تدميرمنشآت حيوية مدن ية محمية وفقا للقانون الدولي، وبالتالي يمكن اعتبار بأن هذه الهجمات محظورة ومُدانة وفقا لما تقرره المبادئ الدولية التي تحظر ذلك، وعليه فإنه بالإمكان تكييف الهجمات الإلكترونية وفقا لمبدأ وجوب التمييز بين المدنيين والمقاتلين، وخاصةً إن جانب كبير من الهجمات السيبرانية يستهدف القطاعات الاقتصادية، والأمنية، والزراعية، والصناعية وغيرها من القطاعات المدنية التي لا غنى عنها لبقاء السكان المدنيين على قيد الحياة، ولا تقتصر في أهدافها على المنشآت والأهداف العسكرية، وفي إطار تطبيق مبدأ التمييز على الهجمات السيبرانية فقد أشار دليل تالين، على الرغم من عدم إلزامية قواعده، بأنه لا يجوز أن تكون الأعيان المدنية هدفًا للهجمات السيبرانية، فلا يجوز على سبيل المثال توجيه الهجمات السيبرانية التي من شأنها تدمير الأنظمة المدنية والبنية التحتية، ما لم تعد هذه الأنظمة من قبيل الأهداف العسكرية التي يجوز استهدافها وفق الظروف السائدة[٨٤]، وبناءً على ما تقدّم من معطيات، فإن تطبيق مبدأ التمييز بين المقاتلين والمدنيين على الهجمات السيبرانية هو أمر في غاية التعقيد، إذ إن المهاجم في الأغلب يكون بعيدًا عن مكان الهجوم ولمسافةٍ تتجاوز المئات من الكيلومترات، ما يجعل التأكد من الالتزام به أمرًا غاية في الصعوبة.

(84)See The Tallinn Manual, Op. Cit.

الفرع الثاني

مبدأ الضرورة العسكرية

يعّد هذا المبدأ من المبادئ المهمة في القانون الدولي الإنساني، إذ يقوم أساساً على الموازنة بين متطلبات الضرورة العسكريةّ والإعتبارات الإنسانية، فتلك الضرورة تتطلب إستخدأماً للقوة العسكريةّ المتاحة لتحقيقّ تفوق أو ميزة عسكرية، بينما الإعتبارات الإنسانيةّ تقتضي تقييد إستخدام هذه القوة لتحقيقّ ميزة عسكرية المبتغاة بأقل الخسائر في الأرواح والاعيان وبوسائل وأساليب قتالية إنسانية، ولإهمية هذا المبدأ يمكن تعريفه بإنه: تلك التدابير التي لا غنى عنها لتحقيق غايات الحرب، على أن تكون هذه التدابير مشروعة وفقاً لاعراف وقوانين الحرب، وبتعبير آخر أن الضرورة العسكريةّ هي الملإذ الأخير الذي يبرر كل التدابير التي لا غنى عنها لضمان التقدم على العدو، بشرط ألا تّعارض مع قانون النزاعات المسلحة[٨٥].

بالرغم من غموض فكرة الضرورة، فإنها بالغة الأهمية في مجال القانون بصفةٍ عامة وفي مجال القانون الدولي الإنساني بصفةٍ خاصة، وغاية ما في الأمر أنه يجب أن تقدّر هذه الضرورة بقدرها، وبالتالي لا يجوز بأي حال من الأحوال أن تُتخذ كستارٍ لخرق قوانين الحرب وأعرافها، فهي بهذا تخرج من إطار القدر المقدّر لها، فلا يجوز مهاجمة الأهداف المدنية كانت مدنًا مأهولة بالسكان أو أعيانًا مدنية، فلا يوجد ضرورة ملحّة إلى ذلك، كما أن فكرة الضرورة المقصودة يُعنى بها عدم تجاوز مقتضيات الحرب، وهي تحقيق النصر وإضعاف قدرة العدو بالطرق والأساليب التي لا تخالف حكمًا في قوانين الحرب، سواء كان هذا الحكم بمقتضى قاعدة عرفية أو قاعدة تعاهدية، وفي إطار قيام الدولة بردّ العدوان أو المحافظة على كيانها، وتم النص على هذا المبدأ في صكوك دولية عدة، ومنها إعلان سان بترسبورغ عام 1868، بالقول (ضرورات الحرب يجب أن تخضع للمتطلبات الإنسانية)، كذلك جاء في اتفاقية لاهاي الخاصة بالحرب البرية لعام 1907م التي نصت على أنه: «يُمنع...تدير ممتلكات العدو أو حجزها، إلا إذا كانت ضرورات الحرب تقتض هذا التدمير» [٨٦].

---

[٨٥] مروة إبراهيم محمد، (2015)، مبدأ الضرورة العسكريةّ في القانون الدولي الإنساني، رسالة ماجستير، كلية القانون، جامعة بغداد، ص 19.

[٨٦] المادة (3/ 2/ز) من اتفاقية لاهاي للحرب البريةّ لعام 1907م.

كما نص البرتوكول الاضاف الأول على أن: «تقتصر الهجمات على الأهداف العسكرية فحسب، وتنحصر الأهداف العسكرية فيما تعلق بالأعيان على تلك التي تسهم مساهمة فاعلة في العمل العسكري، سواء كان ذلك بطبيعتها أم بموقعها أم بغايتها أم باستخدامها، والتي يحقق تدميرها التام أو الجزئي أو الإستيلاء عليها أو تعطيلها، في الظروف السائدة حينذاك، ميزةعسكرية أكيدة»[٨٧]. ومن خلال هذه النصوص تبيّن مدى أهمية هذا المبدأ فهو يطبق في حال الهجمات التقليدية، أما بالنسبة إلى الهجمات السبرانية فقال"ركس هوجيس" (أن الهجمات السيبرانية تنشئ تحدياً أمام تطبيق مبدأ الضرورة العسكرية لذلك لابد من تضافر جهود خبراء القانون الدولي ومهندسي الصناعات الإلكترونية لتحديد ما يمكن أن يوصف بإنه هدف عسكري...)[٨٨]، فإن عدم تحديد أو وضع معايير منظمة لاستخدام تكنولوجيا المعلومات لإغراض عسكرية، هذا يعني امكانية اللجوء في استخدامها بداع الضرورة العسكرية.

وهذا يعني أن هجوم سبيراني يمكن أن يكون الرد عليه بهجوم مادي على الدولة القائمة به، ومن ذلك تبين أن مبدأ الضرورة العسكرية هو مبدأ حاضر في النزاعات السيبرانية[٨٩]، ومن المعلوم أن الجيوش تقاتل وفق خطط مدروسة وموافق عليها من القيادات العسكرية الأعلى، لكن في بعض الظروف الطارئة في أثناء النزاع المسلح، يضطر فيها القائد إلى اتخاذ قرار مباشر وفي وقت ضيق، كما أنه قد تواجهه ضرورات عسكرية حربية تكون مؤثّرة في قراره، وتلك ضرورات عسكرية قد تمليها على القائد ظروف القتال ومتطلبات تحقيق مهمته، فهل يُقدِم على تنفيذ قراره أم يحجم عنه؟.

---

[٨٧] المادة (52/ 2/) من البرتوكول الإضافي الأول لعام1977 م.

[٨٨] الفتلاوي، أحمد عبيس نعمة، (2016)، الهجمات السيبرانية، مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية والسياسية، جامعة بابل، كلية القانون العدد 4، السنة 8، ص 635.

[٨٩] وهذا مانجده في التصريحات المتبادلة بين روسيا والولايات المتحدة الأمريكية، عندما اصدرت وزارة الدفاع الأمريكية بياناً بإن خبراء روسيين نشروا دراسة قانونيةً تقول (أن لروسيا الحق في استخدام الاسلحة النووية إذا تعرضت لهجوم سيبران) ، أما روسيا فقد اعلنت من جانبها (أن توجية هجمة سيبرانية ضد منشآت الاتصال الإلكترونية الأمريكية، هذا يعني وقوع نتائج كارثية توازي استخدام أسلحة الدمار الشامل) . الفتلاوي، الهجمات السيبرانية، المرجع السابق، ص 635.

وقد سلّمت اتفاقيات جنيف ذات صلة بوجود مثل هذه الضرورات الحربية التي قد تمليها ظروف القتال، وجعلت منها مبرراً لبعض الانتهاكات لأحكامها، فقد نصت المواد (17،51،50) من الاتفاقيات الأولى والثانية والثالثة على التوالي على أن تدمير الممتلكات أو الاستيلاء عليها على نطاق واسع يعد انتهاكًا جسيمًا لهذه الاتفاقيات ما لم تبرره الضرورات الحربية[٩٠].

ترتيباًعلى ما تقدّم، يُفهم أن مبدأ الضرورة العسكرية يتيح مهاجمة الأهداف العسكرية كخيارٍ ضروري بالمرتبة الأولى، إلا أن ذلك لا يمنع كضرورةٍ من مهاجمة الأعيان المدنية إذا كانت تُسهم بطريقةٍ مباشرة في تحقيق ميزة عسكرية أكيدة، وعدم تحديد معايير منظمة لاستخدام تكنولوجيا المعلومات للأغراض العسكرية الهجومية، سيعني إمكانية اللجوء إلى استخدامها بداعي الضرورة العسكرية، وهو ما نجده جليًا في تصريحات متبادلة بين الولايات المتحدة الأميركية وروسيا، وأشار دليل تالين، وفيما يتعلق بمبدأ الضرورة العسكرية، إلى أنه في الحالات التي يكون فيها الخيار ممكنًاً بين عدة أهداف عسكرية للحصول على ميزة عسكرية مماثلة، فالهدف الذي يتم اختياره للهجوم السيبراني، هو ذلك الهدف الذي يُتوقع منه أن يسبب أقل خطر على المدنيين والأعيان المدنية[٩١].

الفرع الثالث

مبدأ التناسب في استخدام القوة

يُعد هذا المبدأ من المبادئ الجوهرية المطبّقةٌ في إطار النازعات المسلحة بكافة انواعها الداخليةٌ والدوليةٌ، فهو يرّمي إلى الإقلال من الخسائر أو أوجه المعناة التي تترتب على العمليٌات العسكرية، سواء أكان بالنسبة لاشخاص أو الأشياء، ومن ثم فإذا كانت وسائل القتال المستخدمة لاتتناسب مع الميزة العسكرية المرجوة من العملية العسكرية فلا يجوز استخدامها، ومثال ذلك الهجوم العشوائي الذي يتوقع أن يسبب خسائر كبيرة للمدنيين أو المنشآت المدنية، تتجاوز بكثير الميزة العسكرية المترتبة عليها[٩٢].

---

(90) See The Geneva Conventions 1949, Articles (50, 51, 17) of the first, second and third conventions, respectively.

(91) Schmitt, Wired warfare op cit. P, 397.

(٩٢)– محمد، مروة إبراهيم،(2015) ، مبدأ الضرورة العسكريةٌ في القانون الدولي الإنساني، رسالة ماجستير، كلية القانون، جامعة بغداد، ص 95.

ومبدأ التناسب، ذو طابع ميداني، ومفاده أنه من المحظور شن هجوم من المحتمل أن يسبب خسائر عرضية في أرواح المدنيين أو إلحاق الضرر بهم، و/أو الإضرار بالأعيان المدنية والتي يمكن أن تكون مفرطة فيما يتعلق بالميزة العسكرية الملموسة والمباشرة المتوقعة.

ويرى شين (Shin) «أن مبدأ التناسب في استخدام القوة السيبرانية لا يزال غامضاً ويحتاج إلى أجوبة أهمها كيف يمكن ضمان مبدأ التناسب في الرد على الهجمات السيبرانية»[٩٣].

ففي حال كان الهجوم السيبراني موجهًا إلى هدف عسكري بحت، يكون هدفًا مشروعًا. ولكن القلق الذي يراود الخبراء جميعًا في هذا المجال يكمن في أن الفضاء السيبراني يتميز بالارتباط بين نُظم الحواسيب. ويتألف هذا الفضاء من عدد لا يحصى من نُظم الحواسيب المتصلة بعضها ببعض في أرجاء العالم. وغالبًا ما يبدو أن نُظم الحواسيب العسكرية تتصل بالنُظم التجارية والمدنية وتعتمد عليها كليًا أو جزئيًا. وبالتالي، قد يكون من المستحيل شن هجوم سيبراني على بنية تحتية عسكرية وجعل الآثار تقتصر على هدف عسكري فحسب. وهذا ما أكده الخبيران في القانون الدولي الإنساني ركس (Rex) وشين (Shin) بقولهما: «إذا تم توجيه هجمات سيبرانية ضد بنى تحتية تُستخدم للاستعمال المزدوج المدني–العسكري وعن بُعد، فلا يبدو أن الميزة العسكرية الملموسة والمباشرة ستكون واضحة، ما يجعل تطبيق مبدأ التناسب في أثناء الهجمات السيبرانية أمرًا معقدًا عمليًا»[٩٤].

ومن المسلّم به، أن أيًا من الأعيان المدنية التي تُستخدم لأغراضٍ عسكرية تصبح هدفًا عسكريًا، وبالتالي لا تتوافر لها الحماية بموجب القانون الدولي الإنساني. وتبرز المشكلة بوجود العديد من البنى التحتية الإلكترونية الحالية ذات استخدام مزدوج بطبيعتها، ولن يتغير هذا في المستقبل. على سبيل المثال، يمكن مد شبكة الاتصالات العسكرية جزئيًا عبر الكابلات مع وسائط أخرى تُستخدم أيضًا لحركة المرور المدنية.

---

(93)-Beomchul, Shin, (2011), "The Cyber Warfare and the Right of Self –Defense: Legal Perspectives and the Case of the United States, IFANS, Vol.19, No1, June, p.118.

(94)-HUGES, Rwx, (2010)."Atreaty for Cyberspace", International Affairs journal, Vol.86.No.2, p. 538. and Beomchul, Shin, op, cit, p.118.

وغالبًا ما تعتمد الأسلحة على البيانات الناتجة عن نظام تحديد المواقع العالمي GPS، والذي يخدم أغراضًا مدنية مثل الملاحة. كما أنه تم استخدام وسائل التواصل الاجتماعي مثل Facebook وTwitter على نطاق واسع خلال النزاعات الأخيرة لنقل معلومات مهمة عسكريًا. كما تتجه الجيوش بشكلٍ متزايد إلى المعدات الجاهزة مثل أنظمة الحاسوب التجارية لقواتها، ما يجعل من المصانع التي تنتجها أهدافًا عسكرية.

وكانت هذه الحقيقة مصدر دراسة مكثفة من قبل فريق الخبراء الدولي، الذي خلص إلى أن «الأشياء والمنشآت كافة ذات الاستخدام المزدوج هي أهداف عسكرية، من دون قيد أو شرط». تتبع أي حماية للجوانب المدنية للبنية التحتية الإلكترونية ثنائية الاستخدام المستهدفة من تطبيق مبدأ التناسب وشرط اتخاذ الاحتياطات في أثناء الهجوم. وأشار الخبراء على وجه الخصوص، إلى أن الهجوم على منشأة إلكترونية أو على أجزاء كبيرة منها، قد يتعارض بالقدر نفسه مع مبدأ التناسب.

ويتزايد الاعتماد العسكري على البنية التحتية الإلكترونية المدنية، وذلك للحفاظ على القوات التابعة لدولةٍ ما وقدراتها العسكرية في مواجهة تراجع الميزانيات. سيكون من الصعب تمويل صيانة شبكات إلكترونية منفصلة أو شراء منتجات مصممة خصيصًا للأغراض العسكرية. هذا الواقع سيضع الدول أمام معضلة. فمن ناحية، سيرغبون في حرمان أعدائهم من استخدام البنية التحتية الإلكترونية ذات الاستخدام المزدوج، ومن ناحية أخرى، سترغب الدول في تحصين البنية التحتية الإلكترونية التي يعتمد عليها سكانها المدنيون وأنشطتها[٩٥].

ويثير تطبيق مبدأ التناسب في استخدام القوة في الهجمات السيبرانية عدة صعوبات، بسبب عدم وجود فاصل في الكثير من الأحيان بين الفضاء السيبراني الذي يستخدمه المدنيين وبين الفضاء الذي تستخدمه القوات المسلحة المشاركة في العمل العدائي، وعلى الرغم من هذه الصعوبة، إلا أن دليل تالين أوجب الإلتزام بهذا المبدأ، إذ حظر الهجمات السيبرانية التي قد تسبب خسائر في ارواح المدنيين أو اضرار في الاعيان المدنية التي قد تكون مفرطة مقارنة

[95]-Schmitt, Michael N., (2014) "The Law of Cyber Warfare: Quo Vadis?", STANFORD LAW & POLICY REVIEW, No. 25, P. 269-299.

مع الميزة العسكرية التي يُحققها ذلك الهجوم[٩٦]، كما من الممكن أن يكون تحقيق هذا المبدأ مستحلاً في احيان أخرى، لان تكنولوجيا المعلومات والاتصالات غير متساوية بين الدول، فقد تكون الدولة غير متطورة تكنولوجياً لرد الهجوم السيبراني الموجه ضدها[٩٧]، ومن ثم يمكن تطبيق مبدأ الضرورة العسكرية والتناسب بدلالة القاعدة (14) من دليل تالين التي جاء فيها (أن استخدام القوة الذي تنطوي على عمليات سيبرانية تقوم بها دولة في ممارسة حقها ف الدفاع الشرعي أن تكون ضرورة ومتناسبة)[٩٨].

الفرع الثالث

مبدأ مارتينز

يُنسب مبدأ مارتينز إلى "فريدريك مارتينز"، المندوب الروسي في مؤتمر السلام المنعقد في لاهاي عام 1899 م، ويعتبر بمثابة شرط إضافي يؤكد على ضرورة تصويب وتحديد الوضع القانوني للهجمات السيبرانية، إذ ينص على: "في الحالة التي لا تنطبق فيها معاهدة أو قانون عرفي، فإن المدنيين والعسكريين يتمتعون بحماية مبادئ القانون الدولي المشتقة من العرف المستقر، ومن المبادئ الإنسانية، وما يمليه الضمير العام"[٩٩].

إن غياب أي إشارات في القانون الدولي الإنساني على الاستهداف المباشر للأشخاص المدنيين والأعيان المدنية للعمليات السيبرانية، لا يعني أن قواعد القانون الدولي الإنساني لا تغطي وسائل وأساليب الحرب السيبرانية ما دامت هذه الوسائل تنتج نفس الآثار الذي يمكن أن ينتج عن الأسلحة التقليدية من دمار وانقطاع الخدمات الحيوية والضرر أو الإصابة أو الوفاة.

---

[٩٦]– سعود، يحيي ياسين، (2018)، الحرب السيبرانية في ضوء قواعد القانون الدول الانساني، المجلة القانونية، المجلد 4، العدد4 ، كلية الحقوق، جامعة القاهرة، مصر، ص 94.

[٩٧]– الفتلاوي، أحمد عبيس نعمة، محمد، زهراء عماد، (2020)، تكييف الهجمات السيبرانية في ضوء القانون الدولي، مجلة الكوفة للعلوم القانونية والسياسية، المجلد 44، العدد1 ، كلية القانون والعلوم السياسية، جامعة الكوفة، ص 63.

[98]-See The Tallinn Manual, op, cit, rule (14).

[99]-Gessese, Antonio (2000). The Martens Clause: Half a loaf or simply pie in the sky? European Journal of International Law. Vol., (11). No (1). Pp: 187-216.

ويخضع استخدام هذه الوسائل لنفس قواعد الأسلحة التقليدية، باعتبار أن القانون الدولي الإنساني واسع بما فيه الكفاية لاحتضان التقدم الحاصل في التكنولوجيا، بالإضافة إلى أنه يمكن الرجوع إلى شرط مارتينز كأساس لتفسير معاهدات القانون الدولي الإنساني كلما وجدت الشكوك حول معنى بعض الأحكام الواردة فيه[١٠٠].

واستناداً إلى هذه القاعدة، فإن كل ما يقع أثناء المنازعات يخضع لمبادئ القانون الدولي الإنساني، مما يعني عدم خلو الهجوم على شبكات الحاسوب من القانون أثناء النزاع المسلح. ويوضح الرأي الاستشاري لمحكمة العدل الدولية في مشروعية التهديد الأسلحة النووية أو استخدامها.

إن المادة (4/2) والمادة (51) من ميثاق الأمم المتحدة تحظر استخدام القوة بغض النظر عن الأسلحة المستخدمة، فالمبادئ والقواعد الإنسانية قد وضعت قبل الأسلحة النووية، ومع ذلك فإنه لا يوجد شك بانطباق القانون الدولي الإنساني على الأسلحة النووية، وليس هناك ما يدعو للتمييز بين الأسلحة النووية وأسلحة الحاسوب، من حيث الزمن الذي استحدثت فيه مما يعني إمكانية تطبيق القانون الدولي الإنساني عليها [١٠١].

---

[100]- Roscini, M., (2014), Cyber Operations and the Use of Force in International Law, Oxford University Press, p. 22.

[101]- International Court of Justice. Reports, 1996. Legality of the threat or use of nuclear weapons p. 226 at para. 39.

ويلحق بمبادئ القانون الدولي الإنساني، مبدأ حظر الهجمات العشوائية، إذ نصت الفقرة الرابعة المادة (51) من البروتوكول الإضافي الأول، على أن «الهجمات العشوائية هي تلك الهجمات التي لا توجه إلى هدف عسكري محدد، أو التي تستخدم طريقة أو وسيلة للقتال لا يمكن أن توجه إلى هدف عسكري محدد، أو التي تستخدم طريقة أو وسيلة للقتال تترتب عليها آثار لا يمكن أن تقتصر على النحو المطلوب بموجب القانون الإنساني الدولي. وبالتالي، من شأنها أن تصيب الأهداف العسكرية والأشخاص المدنيين أو المنشآت المدنية من دون تمييز»[١٠٢]. أن التأكيد على أن القانون الدولي الإنساني ينطبق على العمليات السيبرانية أثناء النزاع المسلح لا يشجع على عسكرة الفضاء السيبراني ولا ينبغي، بأي حال من الأحوال، أن يُفهم على أنه يضفي الشرعية على الحرب السيبرانية[١٠٣].

كما أن أي لجوء من جانب الدول إلى القوة، سواء كان ذو طابع سيبراني أو حركي، يظل دائماً خاضعاً لميثاق الأمم المتحدة والقانون الدولي العرفي، ولا سيما حظر استخدام القوة[١٠٤].

المبحث الثالث

المسؤولية الدولية الناشئة عن الهجمات السيبرانية

تطورت منظومة القانون الدولي المعنية بتنظيم الحروب قانونياً بالتزامن مع تطور الحروب وأدوات وأساليب القتال والسلاح المستخدم فيها، ويُفترض أن يكون التطور مستمراً باستمرار تطور أساليب القتال وأدواته.

ومع تزايد الاعتماد على الشبكات وتكنولوجيا المعلومات في النواحي العسكرية وفي إدارة مختلف مناحي وشؤون الحياة، بدأ نوع جديد من المواجهات بالظهور، يتخذ من الفضاء الإلكتروني ميداناً له، ما فرض تحدياً جديدا في ميدان القانون الدولي حول التنظيم والتأطير القانوني لهذه الهجمات، وذلك من حيث إدانة الأطراف الضالعة بها، وما يترتب عليها من مسؤولية دولية جراء ذلك.

---

[١٠٢]– المادة (4/51) من البروتوكول الإضافي الأول.

[١٠٣] جاء هذا الرأي في مجموعة من الوثائق ومنها الإفادات المقدمة من أستراليا، والبرازيل، والدانمرك، وشيلي، والمملكة المتحدة في المسودة الأولية لتقرير الفريق العامل المفتوح العضوية، متاحة على الرابط التالي:

https://disarmament.unoda.org/open-ended-working-group/

[١٠٤]انظر: المادة (4/2) من الميثاق.

تطورت منظومة القانون الدولي المعنية بتنظيم الحروب قانونياً بالتزامن مع تطور الحروب وأدوات وأساليب القتال والسلاح المستخدم فيها، ويُفترض أن يكون التطور مستمراً باستمرار تطور أساليب القتال وأدواته، ومع تزايد الاعتماد على الشبكات وتكنولوجيا المعلومات في النواحي العسكرية وفي إدارة مختلف مناحي وشؤون الحياة، بدأ نوع جديد من المواجهات بالظهور، يتخذ من الفضاء الإلكتروني ميداناً له، ما فرض تحدياً جديدا في ميدان القانون الدولي حول التنظيم والتأطير القانوني لهذه الهجمات، وذلك من حيث إدانة الأطراف الضالعة بها، وما يترتب عليها من مسؤولية دولية جراء ذلك.

ومن أجل الوقوف على أبعاد المسؤولية الدولية الناشئة عن النزاعات السيبرانية وما ينتج عنها من أضرار، سنتطرق لذلك في مطلبين، الأول نتناول فيه قيام المسؤولية الدولية عن الهجمات السيبرانية وتوفر شروطها، أما الثاني نتناول فيه مسؤولية الدول عن الأضرار المترتبة عن الهجمات السيبرانية.

المطلب الأول

قيام المسؤولية الدولية عن الهجمات السيبرانية وتوفر شروطها

في الحقيقة إن المسؤولية الدولية تعد من أهم موضوعات القانون الدولي في الوقت الحاضر، فعند النظر إلى التطورات العلمية الحديثة التي أثرت تأثيراً بالغاً على العلاقات الدولية، نجد أنه ظهرت مشكلات جديدة لم تتناولها قواعد القانون الدولي بالتنظيم، مما أدى إلى ضرورة معالجة هذه المشكلات بطريقة جديدة تتلاءم مع طبيعتها، إضافة إلى ذلك فإن قواعد المسؤولية الدولية يكتنفها الغموض وعدم الوضوح بشكل عام[١٠٥].

وازدادت في الآونة الأخيرة الدراسات القانونية المتخصصة[١٠٦] للبحث في إمكانية توجيه المسؤولية الدولية إلى دولة أُسندت إليها تُهم بارتكاب هجمات سيبرانية، ضد دولة أو مجموعة من غير الدول.

ومع تزايد الهجمات السيبرانية وبروزها منذ العقد الأول من الألفية الثالثة، بدأت تبرز بالتزامن مع ذلك معضلة التكييف القانوني لهذه الهجمات، وبرز بالتحديد التساؤل حول مدى

---

[١٠٥]– بوادي، حسنين المحمدي، (2008)، إرهاب الإنترنت الخطر القادم، ط1، دار الفكر الجامعي، الإسكندرية، مصر، ص 29.

[106]- Jonathan A. OPHARD, "Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield ", DUKE Law & Technology Review, No.3,para 12-18.

إمكانية تطبيق مبادئ وقواعد القانون الدولي الإنساني على هذا الشكل الجديد من الحروب، وجاءت المعضلة بسبب توقيت إبرام الاتفاقيات التي صاغت مبادئ وقواعد القانون الدولي، إذ أنها تعود إلى فترات تبدأ منذ منتصف القرن الثامن عشر وما بعدها.

وبالنظر إلى تواريخ أهم الاتفاقيات نجد اتفاقية لاهاي الأولى لعام 1899، والثانية لعام1907، ومن ثم اتفاقيات جنيف لعام 1949، والبروتوكولان الإضافيان لعام1977، إذ لم يكن للهجمات السيبرانية خلال إبرامها جميعاً أي وجود[١٠٧]، وبالتالي، لم يقع تنظيمها بشكلٍ صريح، ما استدعى الحاجة للاجتهاد بعد ظهورها، إلا إن إشكاليات عدة سرعان ما ظهرت إزاء ذلك، وتمثلت بشكل أساسي في صعوبة القدرة على تحديد طبيعتها وعناصرها، إضافة إلى كون أغلب الهجمات السيبرانية لا تعلن الدول رسمياً عن تبنيها لها، عدا عن إشكالية عدم القدرة على إثبات الدليل المادي على استخدام الهجمات الالكترونية، على عكس طرق القتال الأخرى المعروفة، إذ في بعض الهجمات لا يكون حتى هناك دمار لمنشآت وانما فقط تلاعب وتعطيل لأنظمة، خلافا للهجمات بالأسلحة التقليد ية وغير التقليدية التي تخلف دماراً ملموسا جزئياً أو كلياً، كل ذلك شكل تحدياً أمام المختصين في القانون الدولي، وعن صعوبة في تحديد نطاقها ضمن القانون الدولي الإنساني، وما يترتب عليها من تبعات المسؤولية الدولية.

وأن الدولة التي تقوم بأي فعل من شأنه إحداث ضرر يصيب دولة أخرى أو عدة دول، فتتحمل الدولة التي أحدثت ذلك الضرر، أو تسببت في إحداثه، تبعات المسؤولية الدولية عن ذلك الفعل، فالهجمات السيبرانية يقوم بها أشخاص يخضعون للقانون الدولي، وتؤدي إلى أضرار، وبذلك تكون الهجمات السيبرانية مستوفية شروط قيام المسؤولية الدولية، لكن لنقص القواعد القانونية، وصعوبة إثبات مصدر تلك الجهات، فإنه يتعذر ذلك[١٠٨].

---

[١٠٧] الفتلاوي، أحمد عبيس نعمة، (2018)، الهجمات السيبرانية، دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر، منشورات زين الحقوقية، ط1، بيروت، لبنان، ص 39.

[١٠٨] شفيق، نوران، (2016)، أثر التهديدات الإلكترونية على العلاقات الدولية، دراسة في أبعاد الأمن الإلكتروني، المكتب العربي للمعارف، القاهرة، ص 12.

وبالنظر إلى نص المادة (51) من الميثاق نجدها تنص على أنه: "ليس في الميثاق ما يضعف أو ينتقص الحق الطبيعي للدول فرادى أو جماعات في الدفاع عن أنفسهم إذا اعتدت قوة مسلحة على أحد أعضاء (الأمم المتحدة) وذلك إلى أن يتخذ مجلس الأمن التدابير اللازمة لحفظ السلم والأمن الدولي والتدابير التي اتخذها الأعضاء استعمالاً لحق الدفاع عن النفس تبلغ المجلس فوراً ولا تؤثر تلك التدابير بأي حال فيها للمجلس– بمقتضى سلطته ومسؤولياته المستمرة من أحكام هذا الميثاق، من الحق في أن يتخذ في أي وقت ما يرى ضرورة لاتخاذه من الأعمال لحفظ السلم والأمن الدولي أو إعادته إلى نصابه"[١٠٩].

وقد أجمع الفقه الدولي على أن الحرب السيبرانية تعدّ حرب بالمعنى الصحيح عندما تكون أثارها على العالم المادي أثار مدمرة [١١٠]، وفي حال وقوع هجمات السيبرانية من دولة فإن للدولة المعتدى عليها الحق في الدفاع عن نفسها استناداً لنص المادة (51) من الميثاق سواء كان ذلك ناتج عن عدوان مسلح في العالم الحقيقي أو في الفضاء الإلكتروني وهنا يكون الرد فردي أو جماعي ويكون من حق الدولة الضحية اتخاذ تدابير للدفاع عن النفس في الفضاء السيبراني وفي العالم الحقيقي، ولكنها يجب أن تكون ضرورية ومتناسبة لمواجهة الهجوم المفاجئ[١١١].

وهنالك تشابه بين النظام القانوني الداخلي والنظام القانوني الدولي، فإذا كان شخص النظام القانوني الداخلي الفرد، فإن النظام القانوني الدولي له أشخاصه الخاصون ومنهم الدول، فيفرض النظام القانوني الدولي التزامات على أشخاصه، كما يرتب لهم حقوقاً، فالدولة التي

---

[١٠٩] انظر: المادة (51) من الميثاق.

[١١٠] وضع مايكل سميث عدة معايير لاعتبار العمليات السيبرانية بمثابة استخدام للقوة ومنها شدة الإصابة والفورية وتقييم الأثار وتورط الدولة والقرينة القانونية:

See Schmitt, M.N. (2012). Classification of Cyber Conflict. Journal of Conflict & Security Law, 17(2), P. 245–260.

– كذلك اعتبر بومتشول أن الهجمات السيبرانية الناتج عنها أثار مادية ملموسة في الأعيان المدنية أو العسكرية هي استخدام للقوة وفقاً للمادة (4/2) من ميثاق الأمم المتحدة:

See Shi, Beomchul. (2011). The Cyber and The Right of Self – Defense: Legal Perspectives and the Case of the United States, IFANS, Vol, 19. 1, June, p.111.

وفي نفس الاتجاه:

See Roscini, Marco. Worldwide Warfare, op, cit. p. 130.

[111] Schmitt, M. N. (2012). International Law in Cyberspace: The Koh Speech and. Tallinn Manual Juxtaposed. Harvard International Law Journal, December, Volume 54. P. 16.

تقوم بأي فعل من شأنه إحداث ضرر يصيب دولة أخرى أو عدة دول، فتتحمل الدولة التي أحدثت ذلك الضرر، أو تسببت في إحداثه، تبعات المسؤولية الدولية عن ذلك الفعل، فالهجمات السيبرانية يقوم بها أشخاص يخضعون للقانون الدولي، وتؤدي إلى أضرار، وبذلك تكون الهجمات السيبرانية مستوفية شروط قيام المسؤولية الدولية، لكن لنقص القواعد القانونية، وصعوبة إثبات مصدر تلك الجهات، فإنه يتعذر ذلك[١١٢].

واتفق وفقهاء القانون الدولي الحديث، على أن قيام مسؤولية الدولة عن الهجمات السيبرانية تتطلب لإثباتها توفر العناصر التالية والتي تشكل أركان هذه الجريمة في نطاق القواعد والمبادئ الثابتة في القانون الدولي العام.

أولاً– أن يكون الفعل غير مشروع دولياً: أجمع الفقه الدولي على أن الفعل غير المشروع، هو ذلك الفعل الذي يُعد انتهاك الأحكام القانون الدولي، إذ هو الفعل الذي يتضمّن مخالفة لقواعد القانون الدولي، أو مخالفة مبادئ القانون العامة، فالفعل غير المشروع دولياً هو السلوك المنسوب إلى الدولة وفقاً للقانون، والذي يتمثل في القيام بفعل، أو امتناع عن القيام بفعل، يشكّل مخالفة لأحد التزاماتها الدولية، فمعيار عدم المشروعية هو معيار دولي موضوعي، لا عبرة فيه لمنشأ الالتزام؛ لأن مخالفة أي التزام دولي أيا كان مصدره، تولد المسؤولية الدولية دون النظر لوصف الفعل في القانون الداخلي، كما لا يعتد بالوسيلة التي يتحقق بها انتهاك القانون الدولي، سواء أكان ذلك بفعل أم امتناع عن فعل، أم إهمال[١١٣].

وعند تطبيق هذا الركن على الهجمات السيبرانية، نجد أنها مخالفة لقواعد القانون الدولي؛ نظراً لما ينتج عنها من اضرار ومخلفات مدمرة فيها مخالفة واضحة وصريحة لمقاصد ومبادئ جوهرية أشارت إليها الاتفاقيات والمواثيق الدولية وألزمت الدول باحترامها، وعلى راسها ميثاق الأمم المتحدة.

---

[١١٢] البداينة، ذياب، (2002)، الأمن وحرب المعلومات، دار الشروق للنشر والتوزيع، الأردن، ص 82.

[١١٣] الطائي، صلاح، (2009)، حق الاسترداد في القانون الدولي، مكتبة الجامعة الحديث، القاهرة، ص53.

ثانياً– نسبة الفعل إلى الدولة: في الواقع أن القول بوجود مسؤولية نتيجة وقوع فعل ضار، أو غير مشروع بموجب القانون الدولي، لا يكفي، بل يجب أن يتم اسناد هذا الفعل إلى دولة معينة، فلا مسؤولية دون تحديد الفاعل الأصلي للفعل الذي يشكل جريمة، ويشترط بهذا الصدد ان تكون الدولة ذات سيادة تامة كشرط أساسي لقيام مسؤوليتها عن تصرفاتها الضارة، بمعنى ان تتمتع بكامل الاستقلالية، وبالتالي يمكن مساءلتها عن سلطاتها التنفيذية والتشريعية والقضائية، وعليه فان الدول المنظمة في ظل دولة اتحادية لا يمكن مساءلتها عما ارتكبته من سلوك مجرم قانونا، لانتفاء صفة الدولة عنها وبالتالي لم تعد من أشخاص القانون الدولي العام[١١٤].

وتُسأل الدولة في بعض الأحيان عن أعمال الأفراد العاديين، أو الموظفين الرسميين، وبهذا فإن الدولة المنضمّة إلى دولة اتحادية لا تسأل عن أعمالها؛ لأنه لم تعد من أشخاص القانون الدولي العام، كما أن الدولة المنقوصة لا تُسأل عن أعمالها، لأنها لا تمارس حقوق الدولة التامة الأهلية[١١٥].

وفي حالة الهجمات السيبرانية، نجد أن الضرر يتحقق في مثل هذا النوع من الهجمات بمجرد تنفيذها، خاصةً وإنها تستهدف البنية التحتية للدول في الغالب، مخلفة وراءها آثاراً ضارة قد تفوق احياناً ما ينتج عن الاسلحة التقليدية من أضرار؛ نظراً لاتساع نطاق العمليات السيبرانية وسرعة انتشارها في عدد من الانظمة المخترقة في ظل ثوان معدودة، وبغض النظر عما إذا كانت الجهة صاحبة الاعتداء الدولة ذاتها أم منظمات حكومية أو اشخاص عاديين أو مجاميع إرهابية، ففي جميع الحالات السابقة يتوفر الركن الأول، وهو صفة الدولة، وبالتالي قيام مسؤولية الدولة عن هذه الأفعال، استنادا لمسؤولية الدولة عن أفعال رعاياها في حالة التقصي[١١٦].

---

[114] Donnb Parker, (1983). fighting computer crime, Charles Scribner Son, New York, p, 273.

[١١٥] أبو بكر، محمد عبد الله،(2006) ، جرائم الكمبيوتر والإنترنت، منشأة المعارف، الإسكندرية، ص121.

[١١٦] عبابنة، محمود، الرازقي، محمد معمر، (2005)، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للتوزيع والشر، عمّان، ص 381.

أن من يقوم بهذه الهجمات هي الدول المتقدمة التي تمتلك قوة سيبرانية كبيرة، وقد تقوم بهذه الهجمات أطراف عديدة خاصة في ظل الانتشار الإلكتروني وسهولة الوصول إليه، وزيادة الاعتماد الدولي على الفضاء السيبراني، فقد تقوم بهذا الهجمات الدول القومية، أو المنظمات الحكومية سواء أكانت عالمية أم إقليمية، أو بعض الأفراد ممن تهيأت لهم دون غيرهم إمكانية التحرك على قاعدة واسعة نسبياً من الاتصالات الدولية أو الجماعات الإرهابية والمتمردون، وحركات التحرر الوطني، وفي المجمل نجد أن هؤلاء الفاعلين ينطبق عليهم الركن الأول، وهو نسبة الفعل إلى الدولة؛ وذلك لأن الدول تسأل عن أفعال رعاياها في حالة التقصير[١١٧].

ثالثاً–الضرر: في الحقيقة لا يكفي القول بوجود مسؤولية نتيجة وقوع فعل ضار، أو غير مشروع بموجب القانون الدولي، بل يجب، بالإضافة إلى ذلك أن يترتب ضرر. ويشكل عنصر الضرر أحد أبرز عناصر وأركان تحقق المسؤولية، أن لم يكن اهمها على الاطلاق؛ نظراً لأن انعدام هذا الركن يهدم قيام المسؤولية ويلغي أي مبرر لوجودها. وللضرر عدة صور وأنواع، منها ما يقسم نظراً لمصلحة المعتدى عليه، ومنها ما يقسم وفقا للجهة المتضررة ممن لحقها الضرر،(كالضرر المباشر، أو غير المباشر)[١١٨].

فمن حيث المصلحة محل الاعتداء يقسم الضرر إلى ضرر مادي وهو كل ما يمس بحق مادي للدولة، أو رعاياها، الأمر الذي يترتب عليه اثراً مباشرة ظاهراً للعيان، في حين يتمثل الضرر المعنوي بكل مساس بالشخصية الاعتبارية للدولة، أو أحد رعاياها، فهو كل اعتداء ينصب على أحد الحقوق المعنوية للأشخاص مما يرتب آثاراً غير ملموسة، إلا إنها تشكل قيمة ادبية للمعتدى عليه[١١٩].

---

[١١٧] البداينة، مرجع سابق، ص 88.

[١١٨] الألوسي، محمود، (2006)، جرائم الحاسب الآلي ورقة عمل مقدمة من الأمانة العامة لمجلس التعاون الخليجي لاجتماع اللجنة الفنية المتخصصة بدراسة سبل مكافحة الجرائم الإلكترونية" الإنترنت "الأول والذي أنعقد بمقر الأمانة العامة بالرياض، ص 2.

[١١٩] خليفة، إيهاب، (2014)، القوة الإلكترونية وأبعاد التحول في خصائص القوة، مكتبة الإسكندرية للطباعة والنشر، الإسكندرية، مصر، ص 17.

وعند مقارنة ما سبق على حالة الهجمات السيبرانية نجد أن الضرر في الأخيرة يتحقق بكافة اشكاله، سواء كان الفاعل دولة، أم هيئات، أم أشخاص عاديين، فإن ركن الضرر يتحقق بمجرد وقوع الفعل الضار على الدولة والذي يمس سيادتها وامنها القومي، إلا أنه بالرغم من ذلك تبقى مسألة تتبع الفاعلين وتقديمهم إلى العدالة مهمة مصحوبة بالمخاطر لما يتمتع به الفضاء السيبراني من خصوصية وسهولة إخفاء معلومات وبيانات الفاعلين، ومن ثم التخفي للحيلولة دون الكشف عن هويته، مما يعقد من عملية مساءلة القائمين على هذه الهجمات(١٢٠).

المطلب الثاني
مسؤولية الدول عن الأضرار المترتبة عن الهجمات السيبرانية

يتيح الفضاء السيبراني للجهات الفاعلة إمكانيات تقنية متنوعة لإخفاء هويتهم أو تزوي رها، مما يزيد من تعقيد إسناد التصرف ويخلق صعوبات كبيرة، فعلى سبيل المثال، ينطبق القانون الدولي الإنساني، حتى أثناء النزاع المسلح، على العمليات المرتبطة بالنزاع فحسب، وإذا تعذر تحديد منفذ العملية السيبرانية – وبالتالي تعذر تحديد الصلة بين العملية والنزاع المسلح المعني–فقد يكون من الصعب تحديد ما إذا كان القانون الدولي الإنساني ينطبق على العملية أم لا، ويُعد إسناد التصرف في العمليات السبرانية مهمًا أيضًا لضمان مساءلة الجهات الفاعلة

التي تنتهك القانون الدولي، بما في ذلك القانون الدولي الإنساني، وقد يؤدي التصور بأنه من الأسهل إنكار المسؤولية عن هذه الهجمات أيضًا إلى إضعاف الحظر المفروض على استخدامها، وقد يجعل الجهات الفاعلة أقل تدقيقًا بشأن مخالفة القانون الدولي باستخدامها(١٢١)، وبذلك، لا يُسبب إسناد التصرف أي مشكلة للجهات الفاعلة التي تنفذ العمليات السيبرانية أو تديرها أو تتحكم فيها: فهي تملك كل الوقائع المتاحة لتحديد الإطار القانوني الدولي ولالتزامات التي يجب أن تحترمها.

(120) Clay, Wilson. (2009). Cyber power and National Security, Potomac Book, p. 143.

(١٢١) اللجنة الدولية، (2019)، القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة، ص 20.

ولا جدال أن الفاعل الرئيسي في الحرب السيبرانية هي الدول، إذ بدأت بعض الدول الاستعداد لهذا النوع من الحروب بإنشاء جيوش سيبرانية داخل صفوف القوات المسلحة للدول عن طريق إبرام الاتفاقات السياسية والعسكرية، إذ توصلت الولايات المتحدة الأمريكية والصين في عام 2015 لاتفاق خاص بالحروب السيبرانية بعدم شن أي هجمة سيبرانية، وأعلن الاتحاد الأوروبي في عام 2017 من أن شن أي هجمة سيبرانية من دولة عدائية على الاتحاد الأوروبي يعد (تصرف حرب) يجب التصدي له، رغم الهجمات السيبرانية بين الحين والآخر وإنكار كل طرف ذلك[١٢٢].

ويجب تسوية المنازعات الدولية بالطرق السلمية، وهذا المبدأ ينطبق في الفضاء السيبراني كما ينطبق في جميع المجالات الأخرى. بالإضافة إلى مقتضيات ميثاق الأمم المتحدة–وكذلك بمعزل عنها–يوفر القانون الدولي الإنساني قيوداً على سير الأعمال العدائية متى قررت الدول أو الأطراف من غير الدول اللجوء إلى العمليات السيبرانية أثناء النزاع المسلح، وعلى وجه الخصوص، يحمي القانون الدولي الإنساني المدنيين والأعيان المدنية من آثار الأعمال العدائية من خلال تقييد اختيار المتحاربين لوسائل وأساليب القتال، بغض النظر عن مشروعية أو عدم مشروعية استخدام القوة، وهذا يعني أن القانون الدولي الإنساني –قانون الحرب– بدلاً من إضفاء الشرعية على العمليات السيبرانية (أو أي عمليةً عسكرية أخرى) أثناء النزاع المسلح، فإنه يفرض قيوداً بالإضافة إلى القيود التي ينص عليها ميثاق الأمم المتحدة والقانون الدولي العرفي.

كما يفرض القانون الدولي الإنساني أيضاً بعض القيود على عسكرة الفضاء السيبراني؛ حيث يحظر على سبيل المثال تطوير قدرات سيبرانية يمكن اعتبارها أسلحة وتكون عشوائية بطبيعتها أو من شأنها أن تسبب إصابات غير مبررة أو معاناة غيري ضرورية[١٢٣].

---

[١٢٢] إيهاب خليفة، (2019)، مجتمع ما بعد المعلومات: تأثير الثورة الصناعية الرابعة على الأمن القومي، ط1، العربي للنشر والتوزيع، القاهرة، ص 114.

[123] Henckaerts, Jean-Marie, & Doswald-Beck, Louise. (2005). Customary International Humanitarian Law Volume I : Rules, International Committee of the Red Cross (ICRC), CAMBRIDGE NIVERSITY PRESS, p. 237-244.

وجدير بالذكر إن أهداف الحرب السيبرانية ليس لأضرارها حدود، فبإمكانها التسبب بانفجارات في مخازن الوقود والمحطات النووية وكافة المراكز الحيوية أو تعطيل وسائل النقل براً وبحراً وجواً أو تغيير مسار الرحلات، فضلاً عن تعطيل أنظمة الطاقة وقطع الكهرباء عن مدن بأكملها[١٢٤].

والدولة مسؤولة بموجب القانون الدولي عن التصرفات المسندة إليها بما في ذلك انتهاكات القانون الدولي الإنساني، والتي تشمل:

– تصرف من قبل أجهزة الدولة، بما في ذلك قواتها المسلحة أو أجهزتها الاستخباراتية.

– تصرف من قبل أشخاص أو كيانات فوّضتها الدولة للقيام بقدر من السلطة الحكومية، مثل الشركات الخاصة.

– تصرف من قبل أشخاص أو مجموعات تعمل في الواقع بناء على تعليمات الدولة أو تحت إشرافها أو سيطرتها، مثل الميليشيات أو مجموعات من المتسللين.

– تصرف من قبل أشخاص أو مجموعات خاصة، والتي تعترف بها الدولة وتتبناها كتصرفات صادرة عنها[١٢٥].

---

[١٢٤] غيث علاو، (2020)، الهجمات السيبرانية أكبر من حروب نووية بوسائل الكترونية، 5 يوليو، متاح على الرابط التالي:

https://aljadah.media/archives/16835

[١٢٥] القاعدة (149)، دراسة القانون الدولي الإنساني العرفي الصادرة عن اللجنة الدولية. انظر ايضًا لجنة القانون الدولي، مسؤولية الدول عن الأفعال غير المشروعة دولّياً، (2001)، لاسيما المواد (4–11).

والجدير بالذكر أن الهجمات السيبرانية في عالم متغير ومتسارع وفي السباق التقني الدولي سينحي جانباً الخلافات الاقتصادية والعسكرية مقابل خطورة ودقة الفضاء السيبراني وما يحصل فيه من مناورات وصراعات قوية وسوف تكون مثاراً للجدل الدائم مما لا يسمح ولا يدع مجالاً للشك في حدوث مثل هذه الهجمات وواقعية حصولها وحتى أحياناً دراسة خطورة نتائجها؛ لأنها سوف تقع فجأة ودون سابق إنذار؛ لأن الحرب الفضائية خدعة أيضاً كالحرب التقليدية، وتظهر عن الهجمات السيبرانية وتأثيرها على الدول المسؤولية الدولية التي تكون بالالتزام الذي تتحمله الدول أو المنظمة الدولية بحكم القانون الدولي المنسوب إليها بارتكاب أفعال أو امتناع مخالف لالتزاماتها الدولية بتعويض للمجني عليها في شخصها أو في رعاياها، وقيام المسؤولية الدولية يقوم على عنصرين أهمهما أن يكون منسوباً إلى دولة أو منظمة (شخص من أشخاص القانون الدولي العام)، أو يكون مخالفاً لمقتضيات قاعدة قانونية دولية، وبذلك تنحصر لدينا شروط المسؤولية الدولية بداية في حصول فعل أو امتناع عن فعل من شخص قانوني دولي ويكون أيضاً بإلحاق ضرر بشخص قانوني دولي بأي شكل وأن يكون هذا الفعل أو التصرف غير المشروع بالاستناد إلى الشرعية الدولية[١٢٦].

وبهذا الالتزام المفروض على الدولة أو المنظمة الدولية نجد أن حصول هجوم سيبراني يأخذ طابعاً دولياً بمعنى أن القائم عليه دولة أو منظمة دولية واستهدفت دولة أو منظمة دولية فإن ذلك واستناداً إلى مبدأ المسؤولية الدولية يحمل هذه الجهة القائمة على الهجوم السيبراني أن تقوم بتعويض الجهة المجني عليها استناداً إلى مبدأ هذه المسؤولية الدولية التي ترتب عنها هذا الإخلال، وعند قياس فعل الهجمات السيبرانية على عناصر المسؤولية الدولية فإننا نجد أن المقياس الأول أن تخضع هذه الهجمات إلى الصفة الدولية، أي أنه يجب أن تتبناها جهة دولية أو منظمة دولية حتى يتم الحاقها بالمسؤولية الدولية أما المقياس الثاني فأن يكون هذا الهجوم السيبراني الدولي يخرق معاهدة أو عرف أو ميثاق دولي وبتوضيح أكثر لهذا العنصر يجب أن يترتب على هذا الهجوم الإضرار بمصالح الدولة المعتدى عليها الاقتصادية والسياسية والإستراتيجية، أو أنه يخل بمبدأ من مبادئ الأمم المتحدة والتي كان من أهم مقاصدها هو حفظ السلم والأمن الدوليين والمحافظة عليهما من أي اختراق أو تدخل يضر بمصالح الدول الأساسية التي لا يجوز انتهاكها، ونستنتج من المسؤولية الدولية مبرر آخر يورد لدينا أحقية فعل الدفاع الشرعي في حال حصول هجمات سيبرانية دولية.

---

[١٢٦] صدوق، مرجع سابق، ص 21.

وللربط بين شروط قيام المسؤولية الدولية والهجمات السيبرانية نجد أن شرط أن الفعل غير المشروع الذي يعد انتهاكاً لأحكام القانون الدولي العام أو مخالفة لقواعد القانون الدولي أو المبادئ العامة للقانون وبذلك أن فعل الهجمات السيبرانية هو غير مشروع ابتداء، وهو بحد ذاته ينتهك أحكام وقواعد القانون الدولي؛ لأنه يخترق أسرار ووثائق الدول ويستهدف مصالحها الكبرى ويختلق مشاكل وقضايا دولية معاصرة لم تكن موجودة في السابق في عهد الحروب التقليدية ولا حتى الحرب الباردة، فهذا التسابق في التسلح التقني الجديد نعده في غاية الخطورة والدقة والأهمية. وأما الشرط الثاني فأن حصول الهجمة من شخص قانوني دولي وذلك بالرجوع للشرط الأول فهذا يعني حصولها من جهة غير دولية لا يبرر قيام المسؤولية الدولية وعند البحث بالشرط الأخير وهو الحاق الضرر فهذا أمر جوهري وفي غاية الأهمية، فإن الهجمات السيبرانية تلحق خطورة الكبيرة في حالة استهداف مصالح استراتيجية دولية وحساسة، في الوقت نفسه فعنصر الضرر شيء واقع لا محال عندما تقع بشكل كبير وعدواني، وكذلك أن هذا الموضوع –الضرر– ليس بحاجة إلى التبرير؛ لأنه مبرر أساسي لحصول المسؤولية الدولية، لأنه على الأغلب يكون الهجوم السيبراني الدولي باستهداف مصالح ذات قيمة وأهمية، وليست بمصالح فردية بسيطة، وبذلك لا نستطيع إبعاد عنصر الضرر عن الهجمة الدولية.

إن أهم عناصر وشروط المسؤولية الدولية أن الإخلال بالالتزام الدولي ينتج المسؤولية الدولية التي بحد ذاتها تخترق وتخل بقواعد القانون الدولي الذي يوجب التعويض، وبحصول الضرر من الفعل المخالف لأحكام القانون الدولي أما إذا لم يحصل ضرر فإن المسؤولية الدولية لا تقوم إذاً الضرر هو الأساس في قيام المسؤولية ولزوم التعويض.

والمسؤولية عن الجرائم الدولية تكون على الإخلال بالتزام دولي على درجة كبيرة من الأهمية، وضروري لحماية المصالح الأساسية للمجتمع الدولي، ويعد الإخلال به جريمة في نظر المجتمع الدولي بأسره، ويندرج تحت الجريمة الدولية الإخلال الجسيم بالالتزام له أهمية في المحافظة على السلم والأمن الدوليين، مثل تحريم الاعتداء على سيادة الدول واستقلالها، وكذلك الإخلال بالتزام يهدف إلى حماية حق تقرير المصير مثل تحريم الاستعمار، وكذلك الإخلال الجسيم بالتزام يهدف إلى حماية الإنسان مثل تحريم العبودية وجرائم الإبادة الجماعية، وأخيراً الإخلال الجسيم في الالتزام يهدف إلى حماية بيئة الإنسان التي يعيش فيها مثل حماية الهواء من التلوث وحماية البيئة البحرية[١٢٧]. وبإدراج هذه الجرائم الدولية نجد تطابقها إلى حد ما مع الهجمات السيبرانية، عند تعرض السلم والأمن الدوليين للخطر وحماية الإنسان وحقه في العيش الكريم، من تعرض مصالحه التي تحميها وتقررها الدول وكذلك حماية البيئة التي يعيش فيها الإنسان؛ لأن حدوث فعل الهجمات قد يلحق أضراراً قد تحدث الكثير من الجرائم الدولية السابق ذكرها.

أما عن الأساس القانوني للمسؤولية الدولية فالقانون الدولي التقليدي يرجع الأساس إلى الخطأ ونظرية المخاطر، أما في القانون الدولي المعاصر، فإن الأساس الجوهري للمسؤولية الدولية هو العمل الدولي غير المشروع[١٢٨].فالبحث في موضوع المخاطر عند ممارسة الدولة نشاطاً ذات طبيعة خطيرة وغير مألوفة تتحمل الدولة مسؤوليتها عن الأضرار التي تصيب الدول الأخرى، من هذه النشاطات وأكثر ما يهمنا في هذا الصدد الاعتبار الذي يتحدث عن التطور العلمي والتكنولوجي والأنشطة المتصلة به، فنشاط الانترنت يندرج تحت بند المخاطر الدولية التي تقع الدولة في خانة المسؤولية الدولية عند اتهامها في إحداث هجمة الكترونية دولية.

---

[١٢٧] عدس، عمر حسن، (2010)، مبادئ القانون الدولي العام المعاصر، المركز القومي للإصدارات القانونية، ط1، القاهرة، ص 540.

[١٢٨] هميسي، رضا، (1999)، المسؤولية الدولية، دار القافلة، بدون طبعة، الجزائر ص 17.

إن الأشخاص وحدهم مخاطبون بالقواعد القانونية، مهما تطورت وسائل القتال وأساليبه سيبقى الإنسان الأول والأخير المسؤول عن توجيهها واستخدامها، ومهما تطور الذكاء الاصطناعي في المستقبل، فسيكون هناك دائمًا إنسان في نقطة البداية. فالإنسان مخاطب بالقانون أما الآلة أو الوسيلة فهي غير مخاطبة به، وقد كانت الدولة سابقًاً هي الوحيدة التي تتحمل المسؤولية عن الجرائم الدولية المرتكبة من قبل الأفراد الممثلين للسلطة في الدولة، ولكن بسبب فظاعة الجرائم التي يرتكبها هؤلاء الأفراد باسم الدولة في حق الإنسان وكرامته، أصبح الشخص الطبيعي من أشخاص القانون الدولي الإنساني، يتمتع بحقوقه ويتحمل التزاماته، وفي مقدمتها المسؤولية الجنائية الدولية الفردية[١٢٩]، وتبعًا لذلك، تكلّلت الجهود الفقهية في أواخر القرن الماضي بإنشاء المحكمة الجنائية الدولية ومهمتها النظر في الجرائم التي يرتكبها الأشخاص الطبيعيون. والمقصود بالمسؤولية هي مسؤولية الرؤساء والقادة عن الأعمال المخالفة لقوانين الحرب عمومًا واتفاقيات جنيف خصوصًا، وقد قسّمها الفقه إلى نوعَين من المسؤولية: مسؤولية القائد عن أعمال مرؤوسيه والمسؤولية الفردية المنصوص عنهما تباعًا في المادتَين (25 و28) من النظام الأساسي للمحكمة الجنائية الدولية، وفيما يتعلق بالمسؤولية الجنائية الناتجة عن تعطيل وسائل الاتصال المدنية في أثناء نزاع مسلح، فإنها من حيث المبدأ، تخضع للأحكام العامة للمسؤولية الجنائية كما نصّها القانون الدولي الإنساني والذي يهدف إلى ضبط تصرفات المقاتلين وتقييد وسائل القتال وأساليبه[١٣٠]، وإن كان من المستحيل نسبة عمليات سيبرانية معادية إلى المسؤول عنها، حيث إنه لو كان الجاني لا يرتكب أي أخطاء، ويستخدم أساليب لم تُلاحَظ من قبل، ولا يترك خلفه أي أدلة تشير إليه ولا يتحدث عن العملية في مكان عام أو مُراقَب ولا يقوم بأفعاله أثناء فترة تكون فيها دوافعه لتنفيذ مثل هذه العمليات معروفة للجمهور، فإن تحديد هوية الجاني قد يكون مستحيلاً، وفي الواقع أنه في بعض الأحيان تتحقَّق كل هذه الشروط، ويشعر صناع القرار عن حق باليأس لعدم قدرتهم على التصرف بالشكل المناسب في مثل هذه الظروف، ولكن في حالات أخرى، لا تكون مشكلة تحديد المسؤولية بهذه الصعوبة، لأن واحدًا أو أكثر من هذه الشروط

---

[١٢٩] الزيات، أشرف عبد العزيز، (2011)، المسؤولية الدولية لرؤساء الدول، دراسة تطبيقية على إحالة البشير إلى المحكمة الجنائية الدولية، دار النهضة العربية للنشر والتوزيع، ط1، القاهرة، ص 2.

[١٣٠] الفتلاوي، الهجمات السيبرانية، مرجع سابق، ص 642.

لم يتحقق، وقد يكون من الممكن إصدار بعض الأحكام المفيدة (إن كانت غير كاملة) بشأن إسناد المسؤولية عن العملية، على سبيل المثال، لو لم يُعرَف مكان الآلة التي أطلقت هجومًا مُعيَّنًا، فقد تتيح المؤشرات أو الاستخبارات البشرية تحديد هوية الكيان الذي أُطلِق الهجوم تحت رعايته، وقد يكون الأمر الأخير هو كل ما يلزم لاتخاذ مزيد من الإجراءات ضد الجاني، وإمعاناً فيما سبق يمكننا القول إن الهجمات التقليدية لم تعد في الوقت الحاضر، ومع التطورات التكنولوجية، وخاصة في المجال السيبراني، هي الخيارات الوحيدة السائدة في ساحات القتال، وتطورت الهجمات السيبرانية بشكل متزايد مع التقدم التكنولوجي في مختلف البلدان، وينبغي للقانون الدولي أيضاً أن يواكب هذه الاتجاهات، وينبغي أن يكون قادراً على ذلك الإجابة على القضايا القانونية التي تنتظر المجتمع الدولي من خلال تنظيم قوانين محددة في هذا المجال إلى جانب التطورات التكنولوجية. وحتى يتحقق ذلك، سيتم اتطبيق القوانين الحالية، ومن الأمثلة على القواعد المستخدمة في هذا السياق، المادة (2) في الفقرة (4) من الميثاق المنظم لقواعد استخدام القوة، والمادة (51) التي تنظم استخدام القوة في حالة الدفاع عن النفس، فضلاً عن قواعد ومبادئ القانون الدولي الإنساني، وبالتالي فإن استخدام الهجمات السيبرانية يتم بغرض التسبب في ضرر مباشر ومادي أو التسبب في ضرر أو وفاة للبشر مصنفة ضمن استخدام القوة، لكي تتمتع الدولة المستهدفة بحقوق الدفاع عن النفس ضد مثل هذا الهجمات، يجب أن تصل الإجراءات إلى حالة الهجوم المسلح، ومن ناحية أخرى، يجب أن تتوفر في الدفاع ضد هذه الهجمات شروط التمييز، التناسب في استخدام القوة، ومبدأ الضرورة، بالإضافة إلى ذلك، هناك مسألة أخرى مهمة في مجال استخدام القوة وحق الدفاع عن النفس ضد مثل هذه الهجمات، وهي تعيين مسؤولية الدول التي ارتكبت الهجمات. إلا انه وبسبب التكنولوجية والتقنية والتعقيدات في الفضاء الإلكتروني والهجمات التي تتم في هذا المجال، فإن إسناد المسؤولية سيكون مهمة صعبة بشكل عام، ومن خلال تصرفات الأجهزة الرسمية للحكومة، مثل الجيش السيبراني والأجهزة التشغيلية، والأفراد مثل المتسللين الذين يخضعون للسيطرة الشاملة للحكومة، أو أولئك الذين لا تبذل الحكومة أي جهد للسيطرة عليهم، يمكن توفير الأساس لتعيين المسؤولية للدول، ونتيجة لذلك تكون الدولة مسؤولة عن الهجمات السيبرانية على أساس خرقها لألتزام دولي ومنها الإلتزام بعدم التدخل في الشؤون الداخلية للدول والتزام بمنع الهجمات الحاصلة، أي أن نظرية الفعل غير المشروع لها تطبيقها

على الهجمات في الفضاء السيبراني، أما نظرية المخاطر وبسبب عدم مشروعة فعل الدولة بكل الحالات فإنها غير قابلة للتطبيق عليها.

الخاتمـــة

تناولت هذه الدراسة تحديات تطبيق القانون الدولي الإنساني على النزاعات السيبرانية كنوع جديد من النزاعات بين الدول، وكيفية معالجتها في نطاق القانون الدولي الإنساني، فيما إذا وقعت على نطاق دولي وتبنتها جهة دولية. وتوصلنا من خلال الدراسة إلى جملة من الاستنتاجات والتوصيات على النحو الآتي:

أولاً- الاستنتاجات:

١- إن الهجمات السيبرانية تعد من قبيل أفعال العدوان التي يعاقب عليها القانون الدولي العام بتفعيل دور مجلس الأمن الذي يكيف فعل العدوان على أي تصرف غير شرعي يرتكب في حق دولة عضو في هيئة الأمم المتحدة في حال أنه ارتكب من خلال دولة تبنت هذا الهجوم أو جماعة معينة تتبع لدولة.

٢- أن التكييف القانوني للهجمات السيبرانية لازال ضمن مستوى القياس والاجتهاد، ولم يصل بعد إلى مرحلة إبرام اتفاقيات دولية صريحة خاصة به، بحيث تكون متعددة الأطراف، وتنظم الهجمات السيبرانية وفق نصوص وقواعد قانونية صريحة، وهو ما يُعزى إلى أسباب عدة، يأتي في مقدمتها وجود عقبات تضعها الدول المهيمنة في مجال حروب الفضاء الإلكتروني، مثل الولايات المتحدة الأمريكية، وروسيا، والصين.

٣- أن الهجوم السيبراني يعد استخداماً للقوة وفقاً للرأي الغالب في الفقه نتيجة ما يخلفه من اثار مقارنةً الدولي المعاصر، مع الهجوم المسلح، وكلاهما يحقق ذات النتيجة ويمكن أن تكون نتائج الهجوم السيبراني أكثر تدميراً وخطورة، لذا فهو يرتقي الى مستوى الهجوم التقليدي، كما أن المادة (4/2) من ميثاق الأمم المتحدة جاءت مرنه بالشكل الكافي لاستيعاب الهجوم السيبراني باعتباره صورة مستحدثة من صور القوة نتيجة آثارة المتشابهة مع ما ينتج عن استخدام القوة العسكرية التقليدية.

٤- تطابق الجرائم الدولية مع الهجمات السيبرانية، عند تعرض السلم والأمن الدوليين للخطر وحماية الإنسان وحقه في العيش الكريم، من تعرض مصالحه التي تحميها وتقررها الدول، وكذلك حماية البيئة التي يعيش فيها الإنسان؛ لأن حدوث فعل الهجمات قد يلحق أضراراً قد تحدث الكثير من الجرائم الدولية.

٥- أن الدفاع الشرعي ضد الهجمات السيبرانية يُعد استثناء من قاعدة عدم اللجوء إلى القوة؛ لأنه يهدف إلى الوقاية وليس الانتقام من المعتدي، إذ يعد سبباً للإباحة في القانون الدولي بشرط أن يسبقه هجوم سيبراني غير مشروع حال على أحد الحقوق الجوهرية التي يحميها القانون.

٦- أنطباق القانون الدولي الإنساني على الهجمات السيبرانية والتي تعتبر من أهم التحديات التي يواجهها هذا القانون أثناء النزاعات السيبرانية، إذ أنه لا يتضمن على أي قواعد صريحة بشأن الهجمات السيبرانية في الفضاء السيبراني، والسبب في ذلك هو أن هذه الهجمات ليست حركية، أي ليست هجمات مسلحة بالمعنى التقليدي، إلا أنه وبالنظر إلى الهدف الأساسي للقانون الدولي الإنساني المتمثل بحماية المدنيين من ويلات الحرب، يصبح القانون الدولي الإنساني منطبقاً، وتندرج تلك الهجمات ضمن قواعده إذا كان هدف الهجمات السيبرانية هو تعريض الأشخاص المحميين وممتلكاتهم للخطر أو المخاطرة بحدوث ذلك، ولكن يبقى التحدي في مقدرة القانون الدولي الإنساني على تنظيم أساليب ووسائل الحرب الجديدة.

٧- تكون الدولة مسؤولة عن الهجمات السيبرانية على أساس خرقها لألتزام دولي ومنها الإلتزام بعدم التدخل في الشؤون الداخلية للدول والتزام بمنع الهجمات الحاصلة، أي أن نظرية الفعل غير المشروع لها تطبيقها على الهجمات في الفضاء السيبراني، أما نظرية المخاطر وبسبب عدم مشروعة فعل الدولة بكل الحالات فانها غير قابلة للتطبيق عليها.

ثانياً- التوصيات:

١- أن يتم إعادة النظر في القواعد القانونية لمعالجة القصور وسد الثغرات لمواجهة النزاعات السيبرانية في ظل تعاون دولي بهذا الشأن.

٢- ضرورة تعديل اتفاقيات جنيف الأربع لعام 1949م والبرتوكولين المضافين اليها في عام1977 م بغرض تحريم الهجمات على البنية التحتية الحيوية التي يمكن أن تعطل الاتصالات الأساسية الدنيا وتعرض السكان المدنيين للخطر.

٣- العمل على رفع مستوى الوعي بمخاطر الاستخدامات غير السليمة للتكنولوجيا، على الصحة والاقتصاد العالمي والأمن العالمي.

٤- تفعيل التعاون الدولي ودور المعاهدات الدولية ومبدأ المساعدة القانونية والقضائية والأمنية المتبادلة في مجال مجال مكافحة الجرائم السيبرانية.

٥- ضرورة مراعاة مبادئ القانون الدولي الإنساني والالتزام بها في ممارسة حق الدفاع الشرعي ضد الهجمات السيبرانية.

المراجـــع

أولاً- المراجع باللغة العربية:

١ – الكتب:

- أبو بكر، محمد عبد الله، (2006)، جرائم الكمبيوتر والإنترنت، منشأة المعارف، الإسكندرية.
- البداينة، ذياب، (2002)، الأمن وحرب المعلومات، دار الشروق للنشر والتوزيع، الأردن.
- الزيات، أشرف عبد العزيز، (2011)، المسؤولية الدولية لرؤساء الدول، دراسة تطبيقية على إحالة البشير إلى المحكمة الجنائية الدولية، دار النهضة العربية للنشر والتوزيع، ط1، القاهرة.
- الطائي، صلاح، (2009)، حق الاسترداد في القانون الدولي، مكتبة الجامعة الحديث، القاهرة.
- الفتلاوي، أحمد عبيس نعمة، (2018)، الهجمات السيبرانية، دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر، منشورات زين الحقوقية، ط1، بيروت، لبنان.
- بوادي، حسنين المحمدي، (2008)، إرهاب الإنترنت الخطر القادم، ط1، دار الفكر الجامعي، الإسكندرية، مصر.
- أوليفا، لورنس، (2011)، أمن تقنية المعلومات، المنظمة العربية للترجمة، ترجمة محمد مراياتي، بيروت.
- إيهاب، خليفة، (2014)، القوة الإلكترونية وأبعاد التحول في خصائص القوة، مكتبة الإسكندرية، الإسكندرية للطباعة والنشر، مصر.
- إيهاب، خليفة، (2019)، مجتمع ما بعد المعلومات: تأثير الثورة الصناعية الرابعة على الأمن القومي، ط1، العربي للنشر والتوزيع، القاهرة، مصر.
- حسن، كاميران عزيز، (2021)، الجهود الدولية في مواجهة الجرائم السيبرانية، ط1، منشورات الحلبي الحقوقية، بيروت، لبنان.
- شفيق، نوران، (2016)، أثر التهديدات الإلكترونية على العلاقات الدولية، دراسة في أبعاد الأمن الإلكتروني، المكتب العربي للمعارف، القاهرة.
- صدوق، عمر، (1995)، محاضرات في القانون الدولي العام، ديوان المطبوعات، بدون طبعة، الجزائر.
- عبابنة، محمود، الرازقي، محمد معمر، (2005)، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للتوزيع والشر، عمّان.

- –عبد الصادق، عادل، (2009) ، الإرهاب الإلكتروني القوة في العلاقات الدولية، نمط جديد وتحديات مختلفة، مركز الدراسات السياسية والاستراتيجية بالأهرام، القاهرة.
- عبد الصادق، عادل، (2016)، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، وحدة الدراسات المستقبلية، مكتبة الإسكندرية، العدد 23.
- عدس، عمر حسن، (2010)، مبادئ القانون الدولي العام المعاصر، المركز القومي للإصدارات القانونية، ط1، القاهرة.
- محمد، لينا جمال، (2016)، الجرائم الإلكترونية،(ماهيتها – طرق مكافحتها)، ط1، دار خالد اللحياني للنشر والتوزيع، عمّان، الأردن.
- همیسي، رضا، (1999)، المسؤولية الدولية، دار القافلة، بدون طبعة، الجزائر.
- يونس، عمر محمد أبو بكر، (2004)، الجرائم الناشئة عن الأنترنيت، دار النهضة العربية للنشر والتوزيع، القاهرة.

٢– رسائل ماجستير:

- مروة إبراهيم محمد، (2015)، مبدأ الضرورة العسكريةٌ في القانون الدولي الإنساني، رسالة ماجستير، كلية القانون، جامعة بغداد.

٣– الدوريات والمجلات:

- الألوسي، محمود، (2006)، جرائم الحاسب الآلي ورقة عمل مقدمة من الأمانة العامة لمجلس التعاون الخليجي لاجتماع اللجنة الفنية المتخصصة بدراسة سبل مكافحة الجرائم الإلكترونية "الإنترنت" الأول والذي أنعقد بمقر الأمانة العامة بالرياض.
- الفتلاوي، أحمد عبيس نعمة، (2016)، الهجمات السيبرانية، مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية والسياسية، جامعة بابل، كلية القانون العدد 4، السنة 8.
- الفتلاوي، أحمد عبيس نعمة، محمد، زهراء عماد، (2020)، تكييف الهجمات السيبرانية في ضوء القانون الدولي، مجلة الكوفة للعلوم القانونية والسياسية، المجلد 44، العدد1، كلية القانون والعلوم السياسية، جامعة الكوفة.
- بيتر ماورير، (2014) القانون الدولي الإنساني، إجابات على أسئلتك، حقوق الطبع محفوظة للجنة الدولية للصليب الأحمر، كانون الأول.
- درويش، سعيد، 2016، ماهية الحرب الإلكترونية في ضوء قواعد القانون الدولي"، حوليات جامعة الجزائر–1، المجلد 29، العدد 2.

- سعود، يحيى ياسين، (2018)، الحرب السيبرانية في ضوء قواعد القانون الدول الانساني، المجلة القانونية، المجلد 4، العدد 4، كلية الحقوق، جامعة القاهرة، مصر.
- شميت، مايكل ن.، (2002)، "الحرب بواسطة شبكات الاتصال، الهجوم على شبكات الحاسوب والقانون في الحرب"، المجلة الدولية للصليب الأحمر.
- صالح، نائل عبد الرحمن، (2004)، واقع جرائم الحاسب في التشريع الإردني، مؤتمر القانون والكمبيوتر والانترنيت، كلية الشريعة والقانون، جامعة الإما رات العربية المتحدة، ط3، المجلد الأول.
- اللجنة الدولية للصليب الأحمر، (2011)، تقرير عن القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة، المؤتمر الدولي الحادي والثلاثون للصليب الأحمر والهلال الحمر، جنيف.
- كامل، سعيد، (1993)، جرائم الحاسوب والجرائم الأخرى في مجال التكنولوجيا، بحث مقدم إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة.
- نعوس، مصطفى، (2014)، حق الدولة في استخدام القوة في الفضاء الالكتروني للدفاع عن النفس، مجلة الحقوق، العدد الأول، جامعة الكويت.
- وستبي، جودي ر.، (2011)، دعوة إلى الاستقرار الجيوسيبراني، البحث عن السلام السيبراني، الاتحاد الدولي للاتصالات والاتحاد العالمي للعلماء.
- ¯ اللجنة الدولية للصليب الأحمر، (2021)، التكلفة البشرية المحتملة لاستخدام الأسلحة في الفضاء الخارجي والحماية التي يوفرها القانون الدولي الإنساني، ورقة موقف مقدمة من اللجنة الدولية للصليب الأحمر إلى الأمين العام للأمم المتحدة، بشأن المسائل المحددة في قرار الجمعية العامة رقم 36/75، 7 أبريل، جنيف.
- اللجنة الدولية للصليب الأحمر، (2019)، القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة، جنيف.
- اللجنة الدولية للصليب الأحمر، (2019)، الحرب السيبرانية، القانون الدولي الإنساني يوفر طبقة إضافية من الحماية، 10 سبتمبر، جنيف.
- اللجنة الدولية، (2019)، القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة، 1ديسمبر، جنيف.

ثانياً- الوثائق الدولية وقرارات هيئة الأمم المتحدة:

- اتفاقية لاهاي الخاصة باحترام قوانين وأعراف الحرب البرية لعام 1907.
- ميثاق الأمم المتحدة لعام 1945.

- اتفاقيات جنيف الأربع لعام 1949.
- البرتوكول الإضافي الأول لاتفاقيات جنيف لعام 1977.
- النظام الأساسي للمحكمة الجنائية الدولية ICC لعام 1998.
- International Court of Justice. Reports, 1996. Legality of the threat or use of nuclear weapons.
- GA/RES 56/121(23 January 2002).

ثالثاً- المراجع باللغة الإنجليزية:

- Adam Roberts and Richard Guelff. (2000). Documents on the Laws of War, 3rd ed., Oxford University Press, Oxford.
- Barrett, E. (2017). On the Relationship between the Ethics and the Law of War: Cyber Operations and Sublethal Harm, Ethics & International Affairs, 31(4).
- Clay, Wilson. (2009). Cyber power and National Security, Potomac Book.
- Decision on the Defence motion for interlocutory appeal, paras.
- Donnb, Parker. (1983). fighting computer crime, Charles Scribner Son, New York.
- Dunlap Jr, Charles J. (2011). Perspectives for cyber strategists on law for cyberwar, in Strategic 26. Spring, p. 81, Studies Quarterly.
- Geisel, Laurent, Rodenhauser, Tilman and Dormann, Knut, (2020). Twenty Years Later: International Humanitarian Law and the Protection of Civilians from the Effects of Cyber Operations during Armed Conflicts, International Review of the Red Cross, 102 (913), pp. 287-334.
- Gervais, Micheal. (2012). Cyber Attacks and the law of warfare, Berkeley Journal of international law, vol: 30 Issue.2 articles 6, p. 46.
- Gessese, Antonio (2000). The Martens Clause: Half a loaf or simply pie in the sky? European.

- Gorman, S., & Barnes, J. E. (2011). Cyber combat: Act of war. The Wall Street Journal. Y. No. (31).
- Haslam, Emily (2000). Information Warfare: Technological Changes and International Law. Journal of Conflict and Security Law. Vol (5). No (2).
- Hathaway, Oona A, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue & Julia Spiegel Levitz, Philip. (2012). The Law of Cyber-Attack, CALIFORNIA LAW REVIEW, vol. 100 (817), P.p. 817-885.
- Henckaerts, Jean-Marie, & Doswald-Beck, Louise. (2005). Customary International Humanitarian Law Volume I: Rules, International Committee of the Red Cross (ICRC), CAMBRIDGE NIVERSITY PRESS.
- Huges, Rwx. (2010). Atreaty for Cyberspace, International Affairs journal, Vol. 86. No. 2.
- Jonathan A. OPHARD, Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield, DUKE Law & Technology Review, No. 3.
- J. Pictet, (1952). Commentary on the Geneva Convention for the Amelioration of the condition of the wounded and Sick in Armed Forces in the field, ICRC, Geneva.
- Kittichaisaree, K. (2017). Public International Law of Cyberspace, Law, Governanceand Technology, Series 32.
- Levitz, Philip. (2012). The law of cyber attack, vol. 37, issue 4.
- Libicki, M. (2007). Conquest in Cyberspace: National Security and Information Warfare, Cambridge University Press, New York.
- Matthew, C. Waxman. (2011). Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4), Yale Journal of International, Vol. 36.

- Michael Robinson, Kevin jones, helge janicke. (2015). War Cyber Fare: Issues and Challenges Article in Computer and Security, Elsevier, volume- 49, march, United Kingdom.
- Nazanin Baradaran & Homayoun Habibi. (2017). Cyber Warfare and Self - Defense from the Perspective of International Law, Journal of Politics and Law (JPL), August 2017 10 No (4). Pp. 40-54.
- Prosecutor v RamushHaradinaj, IdrizBalajBrahimaj, (Trial judgment), IT-04-84-T, 3 April, 2008.
- Roscini, Marco. (2010). Worldwide Warfare: Jus ad bellum and the Use of Cyber Force. Max Planck Yearbook of United Nations Law, Vol, (14). No (1).
- Roscini, M. (2014). Cyber Operations and the Use of Force in International Law, Oxford University Press.
- SassoliM. (2006). Transnational Armed Groups and International Humanitarian Law, program on Humanitarian policy and conflict Research, Harvard University, Occasional paper Series, Winter, number 6.
- Schmitt, M. N. (1999). Computer network attack and the Use of Force in International Law: Thoughts on a Normative Framework, Columbia journal of Transnational law, vol 37. No (885). Pp. 885-937.
- Schmitt, M. N. (2002). Wired warfare: Computer network attack and jus in bello, International Review of the Red Cross, vol. 84 No 846. P. 365-399.
- -Schmitt, M. N. (2012). International Law in Cyberspace: The Koh Speech and. Tallinn Manual Juxtaposed. Harvard International Law Journal, December, Volume 54. Pp. 14-37.
- Schmitt, M. N. (2012). Classification of Cyber Conflict. Journal of Conflict & Security Law, 17(2), P. 245–260

- Schmitt, M. N. (2013). Tallinn Manual on the International Law Applicable to Cyber Warfare, (1st Edition) Cambridge University press, first publishes.
- Schmitt, M. N. (2013). Classification of Cyber Conflict, 89 INT'L L. STUD. 233, Vol. 89. Pp. 233-251.
- Schmitt, M. N. (2014). The Law of Cyber Warfare: Quo Vadis?", STANFORD LAW & POLICY REVIEW, Vol 25. No (269), P. 269-299.
- Shi Beomchul. (2011). The Cyber and The Right of Self–Defense: Legal Perspectives and the Case of the United States, IFANS, Vol, 19. 1, June.
- Shulman, Mark Russell. (1999). Legal Constraints on Information Warfare. Occasional Paper No. 7 Center for Strategy and Technology Air War College Air University Maxwell Air Force Base.
- Tallinn Manual. (2013). North Atlantic Treaty Organization, Tallinn Manual on the Jnternatonal Law applicable to Cyber Warfare, NATO Cooperative Cyber Defence Centre of Excellence, Cambridge University Press, UK, rule (14).
- Tsagourias, Nicholas. (2012). Cyber Attacks, Self Defense and the Problem of Attribution Journal of Conflict and Security Law, Oxford University Press, Vol.17, No.2, pp.229-244.
- -Thomas Rid & Peter Mcburney. (2012). Cyber–Weapons, Routledge publisher, The RUSI Journal, February.
-

رابعاً- المواقع الإلكترونية:

- غيث علاو، (2020)، الهجمات السيبرانية أكبر من حروب نووية بوسائل الكترونية، ٥ يوليو، متاح على الرابط التالي:

https://aljadah.media/archives/16835

- اللجنة الدولية للصليب الأحمر، (2013)، ما هي القيود التي يفرضها قانون الحرب على الهجمات السيبرانية؟، أسئلة وإجابات، 28 يونيو، متاح على الرابط التالي:

https://www.icrc.org/ar/doc/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm

- ما هي القيود التي يفرضها قانون الحرب على الهجمات السيبرانية؟ اللجنة الدولية للصليب الأحمر، 2013/6/28 م، متاح في الرابط التالي:

icrc.org/ar/doc/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm

- وزارة الدفاع الأمريكية، (2006)، الاستراتيجية العسكرية الوطنية لعمليات الفضاء السيبراني، متاح في الرابط التالي:

http://www.dod.mil/pubs/foi/joint_staff/jointStaff_jointOperations/07-F-105doc1.pdf

- Dörmann, Knut, (2004), Applicability of the Additional Protocols to Computer Network Attacks, INT'L COMM. OF THE RED CROSS, Nov. 19. [Online] Available at: http://www.icrc.org/eng/resources/documents/misc/68lg92. Htm.

- Traynor, Ian, (2007), Russia Accused of Unleashing Cyber War to Disable Estonia, Guardian London, May 17. [Online] Available at: http://www.theguardian.com/world/2007/may/17/topstories3.russia