جامعة القدس

كليّة الدّراسات العليا

الحرب السّيبرانيّة في القانون الدّوليّ

شيرين محمد رفيق شعراوي

رسالة ماجستير

القدس- فلسطين

1444هـ- 2022 م

الحرب السّيبرانيّة في القانون الدّوليّ

إعداد

شيرين محمد رفيق شعراوي

بكالوريوس: قانون جامعة القدس / أبو ديس القدس / فلسطين

المشرف الرئيس: د. منير نسيبة

قُدّمت هذه الرّسالة استكمالًا لمتطلبات الحصول على درجة الماجستير في القانون العام

من كلية الدّراسات العليا / جامعة القدس

القدس- فلسطين

1444هـ / 2022م

جامعة القدس

الدّراسات العليا

برنامج :القانون العام

إجازة الرّسالة

الحرب السّيبرانيّة في القانون الدّوليّ

اسم الطّالب: شيرين محمد رفيق شعراوي

الرقم الجامعيّ: 21812300

المشرف: د. منير نسيبة

نوقشت هذه الرّسالة وأجيزت بتاريخ 7/ 9/2022 م من أعضاء لجنة المناقشة المدرجة أسماؤهم وتواقيعهم:

1. رئيس لجنة المناقشة: د. منير نسيبة **التّوقيع:**.....
2. ممتحن داخليّ: د. نجاح دقماق **التّوقيع:**.....
3. ممتحن خارجيّ: د. أحمد أبو جعفر **التّوقيع:**.....

القدس- فلسطين

1444هـ / 2022م

الإهداء

قال الله تعالى: "وَوَصَّيْنَا الْإِنسَانَ بِوَالِدَيْهِ حَمَلَتْهُ أُمُّهُ وَهْنًا عَلَى وَهْنٍ وَفِصَالُهُ فِي عَامَيْنِ أَنِ اشْكُرْ لِي وَلِوَالِدَيْكَ إِلَيَّ الْمَصِيرُ". صدق الله العظيم

إلى أُمِّيَ، يا مَلاكي يا حُبِّي الباقي إلى الأَبد، وَلَم تَزَلْ يَداكِ أُرْجوحَتي وَلَمْ أَزَلْ وَلَدْ

إلى والدي، أرجو أن أكون يا والدي كما قال الشافعيّ:

أطع الإله كما أمر... واملأ فؤادك بالحذر

الدّين حق واجب... نور البصيرة والبصر

حافظ عليه فإنّه... نِعم السّعادة تتذّخر!

وأطع أباك فإنّه... رباك من عهد الصغر

إلى والدي ووالدتي، أنتم سعادتي، اللهمّ احفظهما كما رباني صغيراً.

إلى إخوتي، أنتم السند: أيمن، عنان، ناصر، أحبّكم جداً، وكيف لا أحبّكم، وقال الله تعالى: "سَنَشُدُّ عَضدّكَ بِأَخِيكَ"؟. سورة القصص، 35

إلى زوجي الغالي:

إنّما الأخلاق روح... لجمال لا يروح

أدب الإنسان عطر... في الورى دوماً يفوح

كل من يزهو بحسن... دون أخلاق قبيح

إنّ من يحيا خلوقا... ذاك يا صاح المليح

وأنا أزهو بك وأفخر!

إلى ابنتي غزل:

يا وردة في البيت ما أحلاها... سكبت بروحي عطرها وشذاها

ملأت فؤادي بهجة وتألقاً... وسعادة، في صبحها ومساها

إلى وطني الكبير فلسطين، إلى جامعتي جامعة القدس، أهدي هذه الدّراسة

إقرار

أقرّ أنا معدّة هذه الرّسالة التي تحمل عنوان «الحرب السّيبرانيّة في القانون الدّوليّ» أنّها قدمت لجامعة القدس لنيل درجة الماجستير، وأنّها نتيجة أبحاثي الخاصّة، باستثناء ما تمّت الإشارة إليه حيثمّا ورد، وأنّ هذه الرّسالة وأيّ جزء منها لم يقدّم لنيل درجة عليا لأيّ جامعة أو مؤسسة أخرى.

التّوقيع:.....

الاسم الكامل: شيرين محمد رفيق شعراوي

التّاريخ: **7**/ **9**/2022

الشّكر والعرفان

بسم الله الرحمن الرحيم

قال الله تعالى: "رَبِّ أَوْزِعْنِي أَنْ أَشْكُرَ نِعْمَتَكَ الَّتِي أَنْعَمْتَ عَلَيَّ وَعَلَى وَالِدَيَّ وَأَنْ أَعْمَلَ صَالِحًا تَرْضَاهُ وَأَصْلِحْ لِي فِي ذُرِّيَّتِي إِنِّي تُبْتُ إِلَيْكَ وإِنِّي مِنَ الْمُسْلِمِينَ". [1]

وانطلاقاً من قول النبي- صلّى الله عليه وآله وسلّم-: "من صنع إليكم معروفاً فكافئوه، فإنّ لم تجدوا ما تكافئونه، فادعوا له حتى تروا أنّكم قد كافأتموه". [2]

إنّني أتوجّه بالشّكر إلى جامعة القدس، وعمادة الدّراسات العُليا، ممثلة بمجلس أمنائها، ورئيسها والعاملين كافة على ما يبذلونه من جهد وعطاء، وإلى كل أساتذتي شكراً لكم.

كما وأشكر الدّكتور منير نسيبة وأقول له كما قال الشاعر نزار قبانيّ:

لك فضل عظيم عليَّ... يشابه فضل السّحابة

فمنه تعلمت علم الكلام... وعنه أخذت أصول الكتابة

لتفضّله بالإشراف على هذه الدّراسة، إذ كان كريماً في نصحه وإرشاده، فلم يألُ جهداً أو علماً في تقديم النّصيحة والتّوجيه والإرشاد، فقد غمرني بفضله وبشاشته وتشجيعه، وشملني برعايته، وأحاطني بتوجيهاته، كان دائماً يشدّ من أزري، ويقوّي عزيمتي؛ فكان بحق نِعْمَ المشرف! فله منّي كل شكر وتقدير وعرفان.

كما وأتقدّم بالشّكر الجزيل للجنة المناقشة الكريمة. وأخيراً، أتقدّم بأسمى آيات الشّكر والتقدير إلى أهلي وأحبتي جميعاً، الذين تحمّلوا تبعات الحياة خلال دراستي.

---

[1] الأحقاف: 1.

[2] مسند أحمد، ح 5365، 9 / 2006

الملخّص

موضوع هذه الرّسالة هو الحرب السّيبرانيّة في القانون الدّوليّ، ويقصد بذلك التنظيم القانونيّ للهجمات التي تتمّ بواسطة وسائل سيبرانية، وحواسيب رقمية؛ سواءً كانت اعتداءات أو كانت عمليّات دفاعية، وما يشمل القواعد القانونيّة التي تنطبق عليها في مجال محدّد في القانون الدّوليّ وهو القانون الدّوليّ الإنسانيّ.

الإشكاليّة الرئيسيّة التي تقدّم هذه الرّسالة إجابة عليها: هي مدى شموليّة التّنظيم القانونيّ للعلاقات الدّوليّة في الحرب السّيبرانيّة؛ أي تبيين ما ينطبق من هذه القواعد على هذا النّوع من الحروب، من خلال عرض حجج من يدّعون أنّ هذه الحروب مشمولة بنطاق القانون الدّوليّ الإنسانيّ، وعرض حجج من يخالفون ذلك، ويدّعون أنّ القانون الدّوليّ الإنسانيّ لا ينطبق إلّا على الهجمات البريّة والبحريّة والجويّة، دون انطباقها على الهجمات السّيبرانيّة، وأيضاً توضيح أركان المسؤوليّة الدّوليّة المترتبة على مخالفة قواعد السِلم الدّوليّ، والقيام باعتداء سيبرانيّ على دولة أخرى.

اتبعت الباحثة في هذه الرّسالة العديد من المناهج البحثيّة للإجابة على هذه الإشكالية الرئيسيّة وما تفرع عنها من تساؤلات، كل ذلك في إطار استعمال المنهج التّحليليّ والوصفيّ؛ لتحليل القواعد القانونيّة، ووصف ما تحتوي عليه من أحكام ظاهرة وضمنيّة.

توصّلت الباحثة من خلال أدلّة جديدة إلى أنّ القانون الدّوليّ الإنسانيّ ينطبق بشكل حتميّ على الحروب السّيبرانيّة؛ لأنّ هذا القانون يُطبّق على الهجمات المُسلّحة، والهجمات السّيبرانيّة: هي هجمات مُسلّحة، لكنَّ السّلاحَ فيها ليس متفجّراً أو حارقاً، بل هو سلاح أشدّ ضرراً وفتكاً من حيث تأثيره على البنية التحتيّة التّكنولوجيّة، التي صارت أهمّ لدى الدّول من العديد من البُنى التحتيّة الأخرى. ولذلك وجدت الباحثة في قواعد القانون الدّوليّ الإنسانيّ المكتوبة، وفي القواعد العرفيّة، ودليل "تالين" المُعتمد من قبل كبار الفقهاء في مجال القانون الدّوليّ الإنسانيّ والحروب السّيبرانيّة شمولاً تاماً لكل ما يتصوّر حدوثه في الهجمات السّيبرانيّة، وذلك باعتماد منهج تفسيريّ موسّع، يمكن من خلاله فهم

النّصوص القانونيّة فهماً موسّعاً باعتبار الغاية منها، لا بالالتزام الحرفيّ الجامد بما ورد فيها من مصطلحات كانت تعني شيئاً مختلفاً عمّا تعنيه اليوم.

Cyber Warfare in International Law

Student name: Shireen sharawi

Supervisor: Dr. Munir Nuseibah

Abstract

The topic of this thesis is cyber warfare in international law, which means the legal regulation of attacks by electronic means and digital computers, whether they are attacks or defensive operations, and the legal rules that apply to them from a specific field of international law, which is international humanitarian law.

The main problem that this thesis presents an answer to is the extent of the comprehensiveness of the rules of international relations for cyber warfare, i. e. clarifying how these rules apply to this type of war, by presenting the arguments of those who claim that these wars are covered by the scope of international humanitarian law and giving the views of those who view International humanitarian law applies only to land, sea and air attacks, not to cyber-attacks—also, clarifying the pillars of international responsibility resulting from violating the rules of international peace and carrying out a cyber-attack on another country.

In this thesis, the researcher followed many research approaches to answer this main problem and the questions that branched from it. The first was the historical approach to understanding how to keep pace with the legislative development and its interpretations of the concept of cyber war and its modern forms, as well as the inductive approach to understand what applies to real-world cyber wars. Moreover, the deductive **method** is employed to know to apply theoretical texts to realistic examples in cyber warfare. All this is

within the framework of using the analytical and descriptive approaches to **analyse** the legal rules and describe the apparent and implied provisions they contain.

The researcher concluded, with novel evidence, that international humanitarian law inevitably applies to cyber wars because this law applies to armed attacks, and cyber-attacks are armed attacks. Nevertheless, their weapon is not explosive or incendiary, but rather a more dangerous and deadly weapon in terms of its impact on the technological infrastructure, which has become more important to countries than many other infrastructures. Therefore, the researcher found in the written rules of international humanitarian law, the customary **practices** and the Tallinn Guide a complete inclusion of everything that is thought to occur in cyber-attacks by adopting an expanded explanatory approach, through which the legal texts can be understood in an expanded manner considering their purpose and not by a literal, rigid commitment to what is stated since some current terms meant something different from what they mean today.

المحتويات

مقدّمة

لكل حقبة من الزّمن عاشها الإنسان خصائصها التي تميزها عن باقي العصور، في القديم عاش البشر عصر البداوة، وغياب الصّناعات وسمّي هذا العصر بالعصر الحجريّ، حيث كان الإنسان يستعمل الحجارة في مجالات متعدّدة، وهي المرحلة الأولى التي عاشها الإنسان إلى حين اكتشاف الحديد، التي سُميت بمرحلة العصر الحديديّ إلى حين اكتشاف المعادن الأخرى، التي سُميت بعد ذلك بالعصر الصّناعيّ الأوّل.[3]

ومن ثمّ اندلعت الثّورة الصّناعيّة، وتمّ اختراع المحركات، والآلات الكاتبة، وآلة صناعة الورق. وفي أواخر القرن التّاسع عشر، تمّ اكتشاف الكهرباء من قبل العالم الأمريكيّ "توماس أديسون"، ولحقه اكتشاف البارود الذي غيّر مفهوم الصّراع البشريّ، وأصبحت الحروب البريّة، والجويّة، والبحريّة معتمدة على ما توصّل إليه الإنسان من وسائل قتالية، تُمكّنه من تحقيق النّصر في الحرب. [4]

استمرت الحركة الصّناعيّة العسكريّة في التّطوّر والتّقدّم مع تطوّر الصّناعة البشريّة، ولم يقتصر الابتكار البشريّ في الحرب على خلط البارود والحديد، ولا صناعة الدّبابات والطّائرات، والسّفن الحربيّة و الصّواريخ، بل على العكس فقد أنذر اختراع القنبلة الذريّة التي أُلقيت على اليابان في الحرب العالميّة الثّانية ببداية جانب جديد من الصّراع البشريّ، مع دخول العناصر التكنولوجيّة إلى صناعة الحرب الحديثة، وتسليح النّاس بالصّواريخ الباليستيّة، العابرة للقارات بالطّاقة الذريّة والنّوويّة، وانتهى

---

[3]. الشّكري، علي يوسف 2008، الإرهاب الدّوليّ في ظل النّظام العالميّ الجديد، ط1، دار أسامة للنشر والتّوزيع، عمّان، الأردن.

[4] https: //www. aljazeera. net/encyclopedia، 2016-3-2023%

بذلك عصر الحرب التّقليديّة، ودخل العالم عصر الحرب الحديثة **Modern Warfare**، حروب الطّاقة النّوويّة والتّكنولوجيا.

تشهد الحياة اليومية تطوّرات سريعة في مجال تكنولوجيا المعلومات، فكل تفاصيل الحياة تعتمد على شبكة المعلومات آلة لتطوير أنظمة التشغيل، وتصميم الشّبكات، وقد تمّ العثور على بعض المتسللين والمبرمجين؛ للتحكم في عمليّات إنتاج الطّاقة والمعلومات عن طريق إرسال الفيروسات وبرامج تجسسيّة، تُسمّى "الديدان" السّيبرانيّة والشفرات الخبيثة إلى أنظمة الحاسوب، ممّا يسمح للجيش باختراق الجوانب العسكريّة، والاقتصاديّة للبلد المستهدف. [5]

نشأت شبكة الإنترنت كوحدة من وحدات الجيش الأمريكيّ في الستينيات، وقد بدأت كشبكة تُسمّى **ARPAnet**، التي كانت الشّبكة الأصلية لنقل البيانات بين أجهزة الحاسوب في ذلك الوقت، وسرعان ما تطوّرت إلى شبكة **NFS** مع ما لحقها من تطور هائل في عالم الاتّصالات.

وبظهور الإنترنت تمّ ربط البنية التحتيّة بتكنولوجيا أساسيّة، وبرز في العصر الحديث فضاء سيبريّ، وظهرت حرب جديدة هي الحروب السّيبرانيّة أو السّيبرانيّة، وتسمية سيبرانية هي: استيراد للفظ الإنجليزي "سيبر" **Cyber**، وتعني هذه الكلمة في أصلها اليونانيّ القيادة أو التّحكّم، ومنذ أربعينيات القرن الماضي أصبحت كلمة سيبر تستخدم في كل ما له علاقة بالحاسوب والاتّصالات، [6] ومن هنا جاءت تسمية الحروب التي يعتمد فيها الأطراف المتقاتلون على الحواسيب، والاتّصالات والتّكنولوجيا

---

[5]. عدس، عمر حسن، 1995، مبادئ القانون الدّوليّ العام المعاصر، بدون طبعة، مطابع القواسمي، بدون مكان نشر، ص 10-15.

[6] Janczewski، L،. & Colarik، A. Eds. 2007. Cyber warfare and cyber terrorism. IGI Global, p 13-14.

بالحروب السّيبرانيّة؛ ولذلك صار مجال الحرب شاملاً للفضاء السيبرانيّ، وصارت الدول تشنّ هجمات ذات طابع سيبريّ، صارت تُسمّى "هجمات سيبرانية". [7]

وبظهور الحروب السّيبرانيّة كانت الحاجة لازمة لتعريف الهجوم السيبرانيّ، والتعريف الأشمل هو تعريفه: بأنّه "الهجوم الذي يشنّه المعتدي؛ سواءً أكان فرداً أم جماعةً أم دولة ما، باستخدام جهاز كمبيوتر واحد أو أكثر، ضدّ أجهزة كمبيوتر أو شبكات فرديّة أو متعدّدة؛ بهدف تعطيل أجهزة الكمبيوتر بشكل ضار أو سرقة البيانات، أو استخدام جهاز كمبيوتر، ثمّ اختراقه كنقطة انطلاق لهجمات أخرى، من خلال أساليب متعدّدة مثل: البرامج الضّارة، والتّصيّد الاحتياليّ، وبرامج الفدية، ورفض الخدمة". [8] وهو مصطلح مختلف عن التّجسس السيبرانيّ، والذي يعرف: بأنّه عبارة عن عدة طرق تعتمد على التّقنيّة التّكنولوجيّة والبرمجيّة؛ للحصول على معلومات غير معلنة إلى العلن، وسببه الحالة التنافسية في السّعي إلى كسب المعلومات، وهي الحالة التي لا تنتهي بين الدول العظمى وخصوصاً دول الصّراع في الشّرق الأوسط. [9]

ونطاق هذه الهجمات وأضرارها نطاق واسع، ويحدث في كل إحدى عشرة ثانية في العالم هجوم سيبراني، من فيروسات سيبرانية تختفي في لحظات معدودة بعد تنفيذ الهجوم، وتهدف إلى ضرب المنشئات العسكريّة والمدنيّة، وتسبيب خسائر ماديّة كبيرة، وقد وصلت عام 2020 إلى ستة تريليونات في السّنة. [10]

---

[7] حرب الفضاء السيبرانيّ المفهوم: الأدوات والتطبيقات، أنمار موسى جوان، كلية اليرموك، مجلة العلوم القانونيّة والسّياسيّة، ص 122-152.

[8] اللجنة الدّوليّة للصليب الأحمر، القانون الدّوليّ الإنسانيّ والعمليّات السّيبرانيّة خلال النّزاعات المُسلّحة، ورقة موقف مقدّمة إلى فريق العمل المفتوح العضوية المعني بالتّطوّرات في ميدان المعلومات والاتّصالات السّلكيّة واللاسلكيّة في سياق الأمن الدّوليّ، وإلى فريق الخبراء الحكوميين المعني بالارتقاء بسلوك الدّول المسؤول في ميدان الفضاء السيبرانيّ في سياق الأمن الدّوليّ، 2019.

[9] المركز الأوروبي لدراسات مكافحة الإرهاب والاستخبارات، https: //www. europarabct. com/

[10] أحمد بن حوكا، من مقابلة في برنامج عنوانه الحرب السّيبرانيّة: العالم المجهول، الجزيرة بودكاست: https://youtu. bee/Y472PrTxBo0.

يعتقد المؤلف والخبير "جيفري كار" أنّه يمكن لأيّ دولة أن تشنّ حرباً سيبرانيّة ضدّ دولة أخرى، بغض النّظر عن مواردها، ونظرًا لأنّ معظم الشّبكات متصلة بالإنترنت؛ فإنّ الدّول تعتبر هذا النّوع من الاتّصال بالشّبكة كافياً بحد ذاته لشن هجوم سيرانيّ، وقد طوّرت الدّول المتقدّمة صناعيّاً وماليّاً برامج هجمات ضارة في المجال السيبرانيّ، ومثال ذلك ما طوره سلاح الجو الأمريكيّ من مشاريع تتعلق بالهجمات السّيبرانيّة على أهداف من خلال فيروس "ستوكسنت"، مما تسبب في أضرار جسيمة لمنشآت التّخصيب النّوويّ الإيرانيّة عام ٢٠١٠م، وقد استخدمت كل من إسرائيل، والولايات المتّحدة الأمريكيّة هجمات بواسطة أجهزة الحاسوب؛ لإبطاء العمل في المنشآت النّوويّ ة الإيرانيّة.[11]

وبما أنّ هذه العمليّات السّيبرانيّة تهدد مصالح الدّول، وتشكّل اعتداءً من جهة ضدّ أخرى، فلا بد ّ◌َمن وضع قواعد قانونيّة تضمن حماية الدّول من مثل هذه الهجمات، وتضمن معاقبة المعتدي في مثل هذه العمليّات، وبما أن الحروب لها قواعد تُنظّم العمليّات فيها، وقواعد تُنظّم تداعياتها، فإنّ الأمر نفسه مطلوب في مجال الحروب السّيبرانيّة، أي: وجود قواعد قانونيّة تُنظّم العلاقات الدّوليّة أثناء الحرب السّيبرانيّة، ووجود قواعد قانونيّة تُنظّم تداعيات هذه الحرب على العلاقات الدّوليّة، وفي حين تمّ إيجاد مثل هذه القواعد، فإنّ المُعتدى عليه في هجوم سيبرانيّ سيكون عالِماً بما هو مسموح له، وبما هو ممنوع عليه في الاستجابة إلى مثل هذا الاعتداء، وكذلك معرفة ما يمكنه اللجوء إليه؛ لمعالجة الآثار النّاتجة عن هذا الاعتداء؛ سواء بسجن المعتدي، أو المطالبة مثلاً بتعويض عن الأضرار التي تسبب بها.

أهميّة الدّراسة:

تبرز أهميّة الدّراسة من النّاحية الموضوعيّة في كونها تسلّط الضوء على قضية بالغة الأهميّة؛ من حيث البعد السّياسيّ والإقليميّ، والاستراتيجيّ والقانونيّ، التي تصبُّ في جوهر العلاقات الدّوليّة ألا

[11] جوزيف ناي، القوة الناعمة: وسائل النّجاح في السّياسة الدّوليّة، ترجمة محمد توفيق البجيرمي، ط 1، مكتبة العبيكان للنشر، الرياض، 2007، ص20.

وهي ظاهرة الحرب السّيبرانيّة، وحماية المصالح المشروعة من الهجمات السّيبرانيّة، ومن النّاحية العمليّة: تقدّم هذه الدّراسة مساهمة جديدة في الفقه القانونيّ العربيّ؛ لسدّ النّقص الموجود حول هذا الموضوع، والذي لا بدَّ للباحثين العرب من الاستفادة فيه مما كتبه الباحثون الأجانب، وخصوصاً باللغة الإنجليزية، لضمان معرفة الاستجابة القانونيّة الصحيحة لأيّ تحدٍ ينشأ عن مثل هذه الهجمات. ومن النّاحية التّطبيقيّة: تُبيّن هذه الدّراسة كيفيّة تحديد الاعتداء السيبرانيّ، وتحديد كيفيّة الدّفاع ضدّ مثل هذا الاعتداء، وكيفيّة التّعامل مع التداعيات الناشئة عنه.

إشكالية الدراسة:

تثير الحروب السّيبرانيّة العديد من المسائل القانونيّة الشّائكة، التي تحتاج إلى المزيد من البحث القانونيّ، شأنّها شأن الأسلحة الحديثة التي تعتمد على التّكنولوجيا؛ سواء أكانت تُدار عن بعد كالطّائرات المُسيرة، أو تلك التي تنتقل عبر الفضاء السيبرانيّ، كما هو الحال في الحرب السّيبرانيّة هذه المسائل القانونيّة الشائكة دفعت فقهاء القانون الدّوليّ إلى دراسة قواعد القانون الدّوليّ الإنسانيّ التي تُنظّم العلاقات الدّوليّة أثناء الحرب وبعدها، أي: ما يجوز للدول فعله في النّزاعات المُسلّحة، وما يجوز لها فعله لمعالجة تداعياتها،[12] وقد أجمع الفقه الدّوليّ على أن الحرب السّيبرانيّة تُعدّ حرباً بالمعنى الصحيح؛ لأنّ فيها اعتداء على مصالح مشروعة للدول والأطراف الدّوليّة الأخرى،[13] وأنّ استخدام القوة من خلال هذه الآلية الحديثة ضدّ دولة ما أو جهة ما، يُشكّل اعتداءً على تلك الدّولة أو الجهة، ويعطي الأخيرة الحقّ في أن تدافع عن نفسها، وأن تطلب إصلاح الضّرر الذي وقع عليها. [14]

---

[12] أسامة صبري محمد: الحرب السّيبرانيّة ومبدأ التّمييز في القانون الدّوليّ الإنسانيّ، مجلة القانون للدراسات والبحوث القانونيّة، الإصدار 47، كلية القانون – جامعة ذي قار، 2013: https: //www. researchgate. net/publication/334635853.

[13] Michael N. Schmitt: Classification of Cyber Conflict .Journal of Conflict & Security Law، 2012، 172: pp. 245–260

[14] عمر محمود أعمر، مرجع سابق.

ومن خلال ما قامت به الباحثة من دراسات ومراجعات للقواعد القانونيّة، والأدبيّات الفقهية المُتعلّقة بالحرب السّيبرانيّة، ظهر جلياً أن قواعد القانون الدّوليّ الإنسانيّ تُنظّم الكثير من جوانب الحرب السّيبرانيّة وتداعياتها على العلاقات الدّوليّة، إلّا أنّ هناك ثغرات قانونيّة لا بدَّ من سدها، باستعمال وسائل قانونيّة ستذكرها الباحثة لاحقاً في السّياق المناسب؛ من أجل ضمان شمول هذه القواعد القانونيّة لكل ما يندرج تحت نطاق الحرب السّيبرانيّة، وما تتركه من تداعيات على العلاقات الدّوليّة،

ويتفرع عن هذه الإشكالية الأسئلة الآتية التي ستجيب عليه الدراسة: أوّلاً: هل يضيف القانون الدّوليّ الإنسانيّ شرعيّة على عسكرة الفضاء السيبرانيّ، أو الحرب السّيبرانيّة؟ ثانياً: ما هي القواعد القانونيّة اللازم إدراجها في النّظام القانونيّ الحاكم للحرب؛ حتى يتم سدّ ما فيه من فجوات؟ ثالثاً: ما هي الوسائل القانونيّة الممكن استعمالها لسدّ مثل هذه الثغرات؟

أهداف الدّراسة:

تهدف هذه الدّراسة إلى تحقيق أربعة أهداف تساهم مجتمعة في الإجابة على إشكالية الدّراسة، وهي: تحديد مدى شموليّة قواعد القانون الدّوليّ الإنسانيّ في تنظيم الحرب السّيبرانيّة وتداعياتها على العلاقات الدّوليّة:

1. توضيح حجج مذهب خضوع الهجمات السّيبرانيّة للقانون الدّوليّ الإنسانيّ، وسبب تأييد الباحثة لها.

2. توضيح التنظيم القانونيّ للعلاقات الدّوليّة أثناء الحرب السّيبرانيّة وفقاً للقانون الدّوليّ الإنسانيّ ودليل تالين، وإعلان سانت بيترزبرغ 1868.[15]

3. تفصيل مدى تحقّق المسؤوليّة الدّوليّة عن الهجمات السّيبرانيّة.

[15] مائة وخمسون عامًا على إعلان بطرسبورغ... أول اتفاقية دولية تُنظّم استخدام الأسلحة زمن الحرب، الإنسانيّ (مجلة تصدر عن المركز الإقليميّ للإعلام التابع للجنة الدّوليّة للصليب الأحمر)، 6 كانون الأوّل / ديسمبر 2018. متوفر على الرابط الآتي: https://blogs.icrc.org/alinsani/2018/12/06/2305/.

4. عرض أمثلة واقعية لاعتداءات سيبرانيّة، وكيفيّة انطباق قواعد القانون الدّوليّ الإنسانيّ عليها.

منهجيّة الدّراسة:

تتبع هذه الدّراسة المنهج التحليليّ الوصفيّ، من خلال تحليل النّصوص القانونيّة، ووصف مضامينها واستقراء ما اشتملت عليه من قواعد؛ لكي يتضح للقارئ كيفيّة تطبيق هذا النّصوص في الحروب السّيبرانيّة، ومن خلال هذا الاستقراء سيكون القارئ قادراً على تصوّر إذا ما كان هناك قواعد قانونيّة أو ثغرات قانونيّة تنطبق على الحروب السّيبرانيّة في مجال العلاقات الدّوليّة وتداعيتها؛ للوصول إلى كيفيّة تطبيقها في سياق محتمل، وكذلك في فهم التّطوّر في القواعد الأصلية الناظمة للنزاعات بين الدول.

مراجعة الأدبيّات السّابقة:

لقد تناولت العديد من الدّراسات موضوع الحرب السّيبرانيّة وآثارها في مجالات متعدّدة؛ سواءً الاجتماعيّة أو الثّقافيّة أو القانونيّة، ومن بين تلك الدّراسات، دراسة سهيلة هادي، التي حاولت رصد الاستراتيجيّات التي تقوم عليها الحرب السّيبرانيّة: من استراتيجية عسكرة التّكنولوجيا، واستراتيجيّة اختراق المنظومة الاقتصاديّة، إلى استراتيجية الهيمنة الفكريّة الثّقافيّة، الأمر الذي يجعل من الحروب السّيبرانيّة مصدراً رئيساً لتهديد الأمن القوميّ في ظل تزايد الاعتماد على الفضاء السيبرانيّ، وعليه فإنّ دراسة الاستراتيجيّات التي تقوم عليها الحروب السّيبرانيّة هي جزء من آليات مواجهة خطر هذا الجيل من الحروب.[16]

إن هذه الدّراسة قد كتبت عن الحرب الإلكترونيّة، وركزت في بحثها على رصد الاستراتيجيّات التي تقوم عليها الحرب السّيبرانيّة، وأهميّة دراستها في أنّها لا تبحث فقط في الأضرار الماديّة، التي يتسبب فيها هذا النّوع من الحروب؛ وإنّما تبحث في الجوانب النّفسيّة أيضاً، من خلال دراسة الموضوع من

[16] سهيلة هادي: الحروب السّيبرانيّة في ظل عصر المعلومات، جامعة محمد خيضر –بسكرة، مجلة رؤى استراتيجية، 2017: https: //www. researchgate. net

النّاحية العسكريّة دون الخوض في الجانب القانونيّ، حيث انصبّ البحث على الاستراتيجيّات التي تقوم عليها الحروب.

ودراسة سامر مؤيد عبد اللطيف، التي أشارت إلى أنّه قد انتقلت تداعيات هذه الثّورة المعرفية، وما يرتبط بها من تكنولوجيا، إلى ميدان الحرب وأدواتها في إطار ما يُعرف "بالحروب السّيبرانيّة"، الأمر الذي أدّى إلى تنوّع صور هذه الحرب، وأساليب إدارتها، وحتى أهدافها إذ انتقلت العديد من وسائل السّيطرة والتّحكّم الخاصّة بمعظم العمليّات الحربيّة الموجودة على الأرض إلى الحاسوب الآلي، مثلما انتقل جانب من المواجهات الحربيّة غير الدّامية إلى العالم الافتراضي، حتى أمكن تبنّي افتراض مفاده: أن الصّيغة المستقبليّة للحرب ستكون في الفضاء السيبرانيّ، وباستخدام الشّبكة الدّوليّة للمعلومات.[17]

إن هذه الدّراسة تتمحوّر حول الحرب في الفضاء الرّقميّ، حيث بيّن الباحث أنّ تداعيات الحرب الإلكترونيّة تنوّعت في الأساليب وحتى في الأهداف، حيث انتقلت الدول من وسائل السّيطرة والتّحكّم الموجودة إلى الحاسوب الآلي وهو الفضاء الرّقميّ، وتؤيد الدراسة بخصوص أن الحروب الحديثة بخلاف الحروب التّقليديّة؛ لأن الحرب الإلكترونيّة لا تحتاج إلى قتال بريّ أو بحريّ أو جويّ وأنّ الحرب الإلكترونيّة هي ميدان جديد للحروب.

ودراسة وليد غسان جلعود، التي تناولت دور الحرب السّيبرانيّة في الصّراع العربيّ الإسرائيلي، التي هدفت إلى معرفة دور وتأثير الحرب السّيبرانيّة في هذا الصراع، الأمر الذي ظهر بعد الهجمات التي تعرّض لها الفضاء السيبرانيّ الإسرائيلي من قبل مجموعاتٍ عربيةٍ وإسلاميةٍ، وأجنبيةٍ مناصرةٍ للقضية الفلسطينيّة، مما أدّى إلى جعل الفضاء السيبرانيّ ساحةً جديدةً في الصّراع العربيّ الإسرائيلي، شأنه شأن البر والبحر والجو.[18]

---

[17] سامر مؤيد عبد اللطيف، الحرب في الفضاء الرّقميّ: دراسة مستقبلية، مجلة رسالة الحقوق، المجلد السابع، العدد الثّاني، 2015.

[18] وليد غسان سعيد جلعود، دور الحرب السّيبرانيّة في الصّراع العربيّ الإسرائيلي، 2013، جامعة النّجاح الوطنية، كلية الدّراسات العليا.

تستنتج الباحثة ان هذه الهجمات التي تعرّض لها الفضاء السيبرانيّ الإسرائيلي من قبل مجموعات فردية وإسلامية مناصرة للقضية الفلسطينية، وأن الفضاء السيبرانيّ كساحة جديدة في الصّراع العربيّ الإسرائليّ، وقد تناول الباحث التّجربة الإسرائليّة والفلسطينية كحالة خاصة قبل اتفاق أوسلو وما بعدها، وكذلك التّجارب الأمريكيّة والماليزيّة، والقطاعات التي تستهدف الحرب الإلكترونيّة، وأنا أرى أنّ بحثه كان أكثر تعلقاً بالجانب السّياسيّ والتّقنيّ، ولم يتناول الجانب القانونيّ.

ودراسة سلافة طارق الشّعلان، التي تناولت قضية تكييف استخدام الحرب السّيبرانيّة في النّزاعات المُسلّحة وفقاً للقانون الدّوليّ الإنسانيّ، حيث بيّنت أنّه لا يجوز شنّ العمليّات السّيبرانيّة في النّزاعات المُسلّحة إلا بالطريقة وبالقدر الذي يكفل احترام القانون السّاري، على الرّغم من عدم نصّ القانون الدّوليّ الإنسانيّ على حظر هذه العمليّات نصّاً صريحاً، وأنّ الحرب السّيبرانيّة تعدّ بمثابة ثورة في الوسائل المستخدمة في النّزاعات المُسلّحة التّقليديّة.[19]

إن هذه الدراسة تنصب على قواعد القانون، وفي تطبيقها على الحرب السّيبرانيّة، وحول الأضرار الماديّة في سياق النّزاعات المُسلّحة. وتؤكد الدّراسة أنّ هدفها هو محاولة تصنيف نوع الهجمات الإلكترونيّة، وأن مهاجمة العدو باستخدام شبكة المعلومات لم يتضمنه القانون الدّوليّ العام وإنما تضمنته قواعد القانون الدّوليّ الإنسانيّ، من خلال الهجوم على المدنيين والممتلكات، أي أن القانون الدّوليّ الإنسانيّ ينطبق عليه. وبالرجوع إلى دليل تالين فإنّ قانون النّزاعات المُسلّحة مرتبطٌ بجميع الآثار المرتبطة بالنّزاع المُسلّح، وقد أشارت المحكمة الدّوليّة إلى مجموعة من المبادئ التي تكفل حماية المدنيين من جميع الأخطار التي تسببها الأسلحة الحديثة، وتؤيد الدراسة فيما توصّلت إليه، وتؤكد ضرورة وجود اتفاقية دوليّة تحد من إخطار السّلاح النّوويّ.

[19] سلافة الشّعلان، تكييف استخدام الحرب السّيبرانيّة في النّزاعات المُسلّحة وفقاً للقانون الدّوليّ الإنسانيّ، مجلة الكوفة، العدد 26.

ودراسة أسامة صبري محمد، التي تناولت الحرب السّيبرانيّة ومبدأ التّمييز في القانون الدّوليّ الإنسانيّ، التي أشارت إلى أن الحرب السّيبرانيّة أعمال عنف، وتندرج هذه الأعمال في تعريف القانون الدّوليّ الإنسانيّ للهجمات: بأنّها أعمال هجومية ودفاعية، والغاية من توجيه هذه الهجمات في الحرب التّقليديّة تحقيق التّفوق العسكريّ، وأن الحرب السّيبرانيّة وسيلةٌ من وسائل القتال، بدأت الدول التي تلجأ إليها في النّزاعات الحديثة، وبالتالي تخضع للمادة(٣٦) من البرتوكول الإضافيّ الأوّل، وأن الأشخاص الذين يساهمون في الحرب السّيبرانيّة يعدّون مدنيون فاقدون للحماية طيلة مشاركتهم في تلك الهجمات. [20]

إن هذه الدّراسة اعتبرت أن الحرب السّيبرانيّة وسيلة من وسائل القتال تخضع للمادة (٣٦) من البروتوكول الإضافيّ الأوّل، وهذا رأي صحيح وتؤيّده الباحثة.

ودراسة عادل عبد الصادق، التي تناولت قضية أسلحة الفضاء السيبرانيّ في ضوء القانون الدّوليّ الإنسانيّ، التي بحثت الفضاء السيبرانيّ والتحول في مفهوم الأمن والقوة والصّراع العالميّ، وأثر الفضاء السيبرانيّ في القانون الدّوليّ العام وقانون الحرب، كما تناولت تطبيقات القانون الدّوليّ الإنسانيّ على استخدامات الأسلحة السّيبرانيّة، وبحثت كذلك في التحديات والإشكاليات في سبيل التّعاطي القانونيّ مع الأسلحة السّيبرانيّة. [21]

إن هذه الدّراسة تضمّنت تحليل قواعد الحرب وتطبيقات القانون الدّوليّ الإنسانيّ، والباحثة تؤيّد ما تؤكد عليه الدّراسة من أن هناك تحول جذري في مفهوم الأمن والقوة، مما يستدعي تغيّراً في فهم قواعد قانون الحرب لتصير واجبة التطبيق على الحروب السّيبرانيّة.

---

[20] أسامة صبري محمد، الحرب السّيبرانيّة ومبدأ التّمييز في القانون الدّوليّ الإنسانيّ، مجلة القانون للدراسات والبحوث القانونيّة، مج. 2013، ع. 7، ص 62-105، 2013.

[21] عادل عبد الصادق، الفضاء السيبرانيّ والعلاقات الدّوليّة: دراسة في النّظرية والتطبيق، المركز العربيّ لأبحاث الفضاء السيبرانيّ، المكتبة الأكاديمية، 2016.

الفصل الأوّل

ماهية الحرب السّيبرانيّة وتداعياتها وآثارها:

يتناول هذا الفصل ماهية الحرب السّيبرانيّة، من حيث العناصر المكونة لها، والأحداث الأساسيّة التي تجري فيها، ويُقدّم تعريفاً لها في المبحث الأوّل، وفق وجهات النّظر القانونيّة المختلفة حول هذا الموضوع؛ أمّا المبحث الثّاني من هذا الفصل: فيقدّم تفسيراً لآثار الحرب السّيبرانيّة القانونيّة على المدنيين خصوصاً، وعرضاً لوقائع من نماذج عنها.

يُشكّل هذا الفصل الإطار النّظريّ للحرب السّيبرانيّة؛ لتمهيد فهم علاقة هذا النّوع من الحروب مع القانون الدّوليّ الإنسانيّ في الفصل اللاحق.

المبحث الأوّل: تعريف الحرب السّيبرانيّة

يُعدّ ظهور ثورة تكنولوجيا السيبرانيّات، واستخدامها في الأغراض العسكريّة، نقطة تحوّل كبيرة؛ سواء في فنّ الحرب، أو في إدارة الصّراع المُسلّح، فقد أخذت أسلحة القتال الحديثة ومعداته مكان الصّدارة في حسم أي صراع مسلح، وخاصة أسلحة الهجوم الجويّ الحديثة؛ لاعتمادها على نُظم السّيطرة والتّوجيه السيبرانيّ، التي تمكّنها من تنفيذ المهام المطلوبة منها بكفاءة وإصابة أهدافها بدقّة عالية؛ نظراً لاستخدامها نُظم ووسائل الكشف، والتّوجيه، والتّحكّم، وقيادة النيران وتصحيحها، لاسلكيّاً وحراريّاً وليزريّاً، وتليفزيونياً، وهي النُّظم التي يستوي تشغيلها واستخدامها ليلاً ونهاراً، هذا إضافة إلى النُّظم

الحديثة والمتقدّمة للتّصوير التليفزيونيّ، باستخدام آلات التصوير ذات الحساسية العالية، التي يمكنها العمل في مستوى الضوء المنخفض بكفاءة ودقة عاليتين.[22]

ومع دخول المعدّات السّيبرانيّة الحديثة، واستخدامها بتوسع في الجيوش الحديثة بصفة عامة، وفي القوات الجوية بصفة خاصة؛ سواء في أسلحة الهجوم الحديثة، أو في نظم السّيطرة الآلية على القوات ووسائلها من أجهزة وحاسبات آلية، وانطلاقاً من اعتماد أسلحة القتال الحديثة على النُّظم والوسائل السّيبرانيّة، فقد أظهرت العمليّات الحديثة في حرب فيتنام، وحرب أكتوبر ١٩٧٣م، وحرب فوكلاند وحرب الخليج الثّانية، وحرب البلقان، [23]الدّور الذي يمكن أن تؤديه الحرب السّيبرانيّة بوصفها سلاح مضاد، يمكنه التّأثير بفاعلية على الحد من إمكانات هذه الأسلحة والمعدّات في ساحة القتال؛ لما تتميز به الحرب السّيبرانيّة من القدرة على تنفيذ أعمال الاستطلاع، والإعاقة السّيبرانيّة بأنواعها المتعدّدة، ضدّ نظم السّيطرة ووسائلها، والكشف والتّوجيه السّيبرانيّة لهذه الأسلحة.[24]

ولمّا كانت إستراتيجية القوات المُسلّحة في كل دول العالم، قد تأسست على إمكانيّة تحقيق النّصر على العدو بكل الوسائل المتيسرة لديها، وبما أن الحرب السّيبرانيّة عُدّت إحدى صور الصّراع التكنولوجي، التي تؤدّي أعمالها القتاليّة إلى إيجاد الظّروف المناسبة للقوات المُسلّحة؛ لتحقيق هذا النّصر؛ لذا فإنّ الحرب السّيبرانيّة أصبحت في مقدّمة الموضوعات التي يعكف العسكريّون على دراستها، كما تعكف

---

[22]. جوزيف ناي، القوة الناعمة: وسائل النّجاح في السّياسة الدّوليّة، ترجمة: محمد توفيق البجيرمي، ط1، مكتبة العبيكان للنشر، الرياض، 2007، ص20

[23]. لطفي لمين بلفرد، "الفضاء السيبرانيّ: هندسة وفواعل"، المجلة الجزائرية للدراسات السّياسيّة، ENSSP، العدد الخامس، الجزائر، 2016، ص ص 148-150.

[24]. جوزيف ناي، القوة الناعمة: وسائل النّجاح في السّياسة الدّوليّة، تر: محمد توفيق البجيرمي، ط1، مكتبة العبيكان للنشر، الرياض، 2007، ص20

مراكز البحوث العلمية والفنية على تطويرها، وتحديثها، باستمرار؛ لمواجهة التّهديدات السّيبرانيّة لأسلحة القتال الحاليّة والمستقبليّة.[25]

المطلب الأوّل: عناصر الحرب السّيبرانيّة

للحرب السّيبرانيّة العديد من التعريفات العلمية إلا أنّها بالدرجة الأولى تتوقّف على طبيعة الاستخدام القتاليّ ومفهومه المطلوب تحقيقهما في العمليّات الحربيّة الحديثة، التي تتنوّع فيها النُّظم والوسائل السّيبرانيّة المتطوّرة لأسلحة القتال، وتعرّف على أنّها: تلك الأهداف المطلوب من الحرب السّيبرانيّة أن تتعامل معها، وتؤثر على فاعليتها؛ بهدف حرمانها من أداء مهامها الوظيفيّة بكفاءة، وبالتالي تهيئة الظّروف المناسبة للقوات الصّديقة للعمل في بيئة سيبرانيّة مناسبة تسمح بتنفيذ المهام المطلوبة بكفاءة ودقة عاليتين، وفي الزمان والمكان المناسبين. وتعرّف أيضاً على أنّها: مجموعة الإجراءات السّيبرانيّة المتضمنة استخدام بعض النُّظم والوسائل السّيبرانيّة الصّديقة في استطلاع الإشعاع الكهرومغناطيسيّ، الصّادر من نظم العدو ووسائله ومعداته السّيبرانيّة المختلفة مع الاستخدام المتعمّد للطاقة الكهرومغناطيسيّة في التّأثير على هذه النُّظم والوسائل؛ لمنع العدو، أو حرمانه، أو تقليل استغلاله للمجال الكهرومغناطيسيّ، فضلاً عن حماية الموجات الكهرومغناطيسيّة الصّادرة من النُّظم والوسائل السّيبرانيّة الصّديقة من استطلاع العدو لها، أو التّأثير عليها،[26] أو بحسب تعريف آخر، فإنّ الحرب السّيبرانيّة: هي مجموعة الإجراءات التي تُنفذ بهدف الاستطلاع السيبرانيّ للنُّظم والوسائل السّيبرانيّة المعادية، وإخلال عمل هذه النُّظم والوسائل السّيبرانيّة، ومقاومة الاستطلاع السيبرانيّ المعادي،

---

[25]. عبّاس بدران، الحروب السّيبرانيّة: الاشتباك في عالم متغير، مركز دراسات الحكومة السّيبرانيّة، بيروت، 2010، ص 4. متاح على الرابط التالي :
http://najishukri.wordpress.com/cyberwarbook.

[26]. عبّاس بدران، الحروب السّيبرانيّة: الاشتباك في عالم متغير، مركز دراسات الحكومة السّيبرانيّة، بيروت، 2010، ص 4. متاح على الرابط الآتي: http://najishukri.wordpress.com/cyberwarbook

وتحقيق استقرار عمل النُّظم السّيبرانيّة الصّديقة تحت ظروف استخدام العدو أعمال الاستطلاع، والإعاقة السّيبرانيّة.[27]

الأهداف السّيبرانيّة المعادية للحرب السّيبرانيّة:

هي الأهداف المطلوب أن تتعامل معها الحرب السّيبرانيّة بأعمال الاستطلاع، والإعاقة السّيبرانيّة، ويمكن أن نوجز أهم هذه الأهداف فيما يلي:

1. محطّات الاتّصال اللاسلكيّ، واللاسلكيّ متعدد القنوات، والميكروويف.
2. أنظمة الرّادار العسكريّة.

أ. للإنذار وتوجيه النيران.

ب. للإنذار والمراقبة الساحلية.

ج. للتوجيه لمراكز السّيطرة الجوية.

د. لقيادة نيران المدفعيّة وتصحيحها.

هـ. لمراقبة التّحركات الأرضيّة.

3. نُظم الكشف والتّوجيه، الكهروبصريّة: "تليفزيوني، وحراريّ، وليزريّ، وبصريّ".[28]

المطلب الثّاني: لمحة تاريخيّة عن الحرب السّيبرانيّة

عند تتبع تاريخ نشأة الحرب السّيبرانيّة في العالم نجد أن جذورها تعود لما قبل اندلاع الحرب العالميّة الأولى، فقد بدأت الاتّصالات بين أرجاء العالم المختلفة باستخدام المواصلات السّلكيّة من طريق المورس "جهاز البرق الصّوتي" عام 1837م، ولم يتحقق أي اتصال آخر في ذلك الوقت إلا من طريق

---

[27]. يحي اليحياوي، أوراق في التّكنولوجيا والإعلام والدّيمقراطيّة، دار الطليعة للنشر، بيروت، 2004، ص 13.

[28]. انظر بشكل عام: الحديثي، مؤيد، العولمة الإعلاميّة والأمن القوميّ العربيّ، ط 1، عمّان: الأهليّة للنشر والتّوزيع، 2002م.

تبادل المراسلات باستخدام السّفن في نقل الرسائل بين الموانئ البحريّة.[29] ومنذ اندلاع الحرب الأهليّة في الولايات المتّحدة الأمريكيّة، في أبريل 1861م، كانت خطوط التلغراف هدفاً مهماً للقوات المتحاربة إذ كان عمال الإشارة يتداخلون على خطوط المواصلات السّلكيّة، عن طريق توصيل هاتف على التّوازي مع كل خط من هذه الخطوط؛ للتنصّت على المحادثات، ولهذا السبب كان كل جانب يقطع المواصلات الخطيّة عند عدم الحاجة إليها؛ حتى لا يتداخل عليها الطرف الآخر. [30]

ثمّ كانت بداية استخدام الاتّصال اللاسلكيّ في عام ١٨٨٨م مع الألماني "هرتز"**Hhertz** وفي منتصف عام 1897 استطاع "ماركوني" **Guglielmo Marconi** المهندس، والمخترع الإيطاليّ من تطوير جهاز لاسلكي يناسب الاستخدام في البحر، ثمّ استخدم اللاسلكيّ في أعمال الاتّصالات بالمسرح البحري الأوروبي في عام 1901م، ونتيجة لتزايد الاستخدام اللاسلكيّ، كان من الطّبيعيّ أن يظهر التّشويش والإعماء على الاتّصالات اللاسلكيّة، وكان في البداية التّشويش والإعماء معهوداً؛ نتيجة لكثرة استخدام الأجهزة اللاسلكيّة، وهو ما يُعرف "بالتّداخل البينيّ للموجات الكهرومغناطيسيّة" عند إشعاعها بكثافة عالية في مساحة محدّدة، أو في مناطق مغلقة، مثل: المضائق، والممرات الجبليّة، [31] ومن هنا بدأ التّدريب على العمل في ظل التّشويش والإعماء، نتيجة الاستخدام اللاسلكيّ المكثف، ثمّ بدأ الاستخدام المتعمّد للتّشويش والإعماء؛ لإعاقة الاتّصالات اللاسلكيّة بين الوحدات العسكريّة المعادية؛ لإرباكها وشلّ سيطرتها على قواتها وأسلحتها.

وفي عام 1904 م قصفت السفينتان اليابانيتان الحربيتان "كاسوجا ونيشين" القاعدة البحريّة الرّوسيّة في ميناء "آرثر"**Arthur** ، وكانت معهما سفينة صغيرة تصحح النيران باستخدام الرّاديو

---

[29]. الصيفي، حسن، الفضائيات العربيّة في عصر العولمة: الفرص والتحديات، الواع والطموحات، ط 1، القاهرة، الهيئة العامة لدار الكتب والوثائق القوميّة، 2010م.

[30]. جوزيف ناي، القوة الناعمة: وسائل النّجاح في السّياسة الدّوليّة، ترجمة: محمد توفيق البجيرمي، ط1، مكتبة العبيكان للنشر، الرياض، 2007، ص20

[31]. عبّاس بدران، الحروب السّيبرانيّة: الاشتباك في عالم متغير، مركز دراسات الحكومة السّيبرانيّة، بيروت، 2010، ص 4. متاح على الرابط التالي :
http://najishukri.wordpress.com/cyberwarbook.

"اللاسلكيّ"، وسمع أحد عمال "الإشارة" الروس، بالمصادفة، تعليمات تصحيح النيران، فاستخدم جهاز إرساله اللاسلكيّ في إعاقة الاتّصال الياباني بالضغط على مفتاح الإرسال على تردد الشّبكة اليابانيّة نفسها، مما عطّل بلاغات تصحيح النيران من أن تُبّلغ لمدفعية السفينتين، وهكذا لم ينتج عن هذا القصف البحريّ سوى إصابات طفيفة، لعدم دقة النيران في إصابة أهدافها.

وحتى عام 1905م وخلال المعارك بين السّفن اليابانيّة والرّوسيّة، استخدمت السّفن الرّوسيّة الأسلوب نفسه ضدّ الشّبكات اللاسلكيّة اليابانيّة، وانعكس ذلك في أن السّفن الرّوسيّة استطاعت إخفاء اتصالاتها، قدر الإمكان، عن طريق تقليل فترات استخدام اللاسلكيّ لأقل فترة ممكنة، وبأقل قدرة إشعاع لاسلكيّ تحقّق الاتّصال المطلوب، وكانت السّفن الرّوسيّة تتنصّت وتراقب الإرسال اللاسلكيّ الياباني، ثمّ تشوّش عليه أثناء القصف بهذا الأسلوب نفسه. [32]

الفرع الأول: الحرب السّيبرانيّة في الحرب العالميّة الأولى

في بداية الحرب العالميّة الأولى، في أغسطس 1914م، قبل أن تدخل بريطانيا الحرب إلى جانب بلجيكا وفرنسا، ضدّ ألمانيا والنّمسا، مرت سفينتان حربيتان بريطانيتان بجوار السّفن الألمانيّة في بحر المانش، ولم تحاولا الاشتباك مع السّفن الألمانيّة. إلّا أنّ أدميرال الأسطول الألمانيّ "إرنست كينج"، أوضح أن هاتين السّفينتين البريطانيّتين، نفّذتا عمليّات التّنصّت اللاسلكيّ على الاتّصالات اللاسلكيّة للسّفن الألمانيّة، وذلك عندما حاولتا التّشويش على الاتّصالات اللاسلكيّة الألمانيّة، بهدف اختبار كفاءة أعمال الحرب السّيبرانيّة لديها في التّداخل والتّشويش والإعماء اللاسلكيّ على الشّبكات اللاسلكيّة الألمانيّة. [33]

ومن هنا ظهرت أهميّة أعمال الاستطلاع اللاسلكيّ على شبكات العدو اللاسلكيّة، بهدف الحصول على المعلومات، كما أصبحت الوحدات البحريّة على دراية بأنّ استخدام اللاسلكيّ أكثر ممّا ينبغي يمكن أن

---

[32]. سامية أبو النّصر، الإعلام والعمليّات النّفسيّة في ظل الحروب المعاصرة وإستراتيجية المواجهة، دار النشر للجامعات، ط1، 2010، ص 82.

[33]. لطفي لمين بلفرد، "الفضاء السيبرانيّ: هندسة وفواعل"، المجلة الجزائرية للدراسات السّياسيّة، ENSSP، العدد الخامس، الجزائر، 2016، ص ص 148-150.

يفصح عن حجم كبير من المعلومات المفيدة للعدو، حتى مع استخدام الكود والشّفرة في الاتّصالات اللاسلكيّة.

ولهذا السبب أكدّ القادة على أهميّة بقاء الرّاديو "اللاسلكيّ" صامتاً كلما أمكن ذلك، وتقليل تبادل الإشارات إلى الحد الأدنى عندما لا يكون آمناً، أي بمجرد أن تكون السّفن الحربيّة في مرمى بصر العدو، فكان لا يُسمح للقادة باستخدام الرّاديو "اللاسلكيّ" بِحُرية؛ حتى لا يلتقطه الجانب المعادي، وكان يُستعاض عنه في تحقيق الاتّصال باستخدام الإشارات المرئية "التأشير المنظور".[34]

بعد ذلك ظهرت أهميّة تحديد مواقع المحطّات اللاسلكيّة المعادية، التي تدّل على أماكن تمركز القوات المعادية، وبالتالي يمكن التنبؤ المُبكّر بالتّهديد، وكذلك لتوجيه أعمال التّشويش والإعماء ضدّها بدرجة تركيز مناسبة في التوقيت المناسب، ففي عام ١٩٥٨م، استغلّت البحريّة البريطانيّة الفكرة الأمريكيّة في إنشاء جهاز تحديد اتجاه الإشعاع اللاسلكيّ الصّادر من جهاز إرسال أي سفينة تستخدم الاتّصال اللاسلكيّ وهي في عرض البحر، والذي يمكن باستقباله تحديد موقع هذه السفينة "نظام المنارة اللاسلكيّة"، وعلى ضوء ذلك بدأت البحريّة المَلكية البريطانيّة بتركيب سلسلة من محطّات تحديد الاتجاه اللاسلكيّ بطول السّاحل الشّرقي لإنجلترا، حيث أمكنها تحديد موقع أي سفينة أو طائرة منطلقة في بحر الشمال. وعندما دخلت أمريكا الصّراع في أبريل ١٩١٧م، انضم الأسطول الحربي الأمريكيّ مع الأسطول البريطاني، الذي كان يمتلك أجهزة لاسلكية متقدّمة، وكانت بعض قطع الأسطول تحمل أجهزة تحديد اتجاه من نوع 995، أثبتت كفاءة كبيرة في تحديد مواقع السّفن المعادية التي كانت تتنصّت على اتصالاتها اللاسلكيّة، وتحدد مواقعها، وتتتبعها، ثمّ تدمّرها.[35]

---

[34]. سامية أبو النّصر، الإعلام والعمليّات النّفسيّة في ظل الحروب المعاصرة وإستراتيجية المواجهة، دار النشر للجامعات، ط1، 2010، ص 82.

[35]. سامية أبو النّصر، الإعلام والعمليّات النّفسيّة في ظل الحروب المعاصرة وإستراتيجية المواجهة، دار النشر للجامعات، ط1، 2010، ص 82.

ومع تزايد الاهتمام بالاتّصالات اللاسلكيّة من الجو إلى الأرض من خلال إرسال تقارير الاستطلاع التكتيكيّ عن أرض المعركة، أو لتصحيح نيران المدفعيّة في إصابة أهدافها، ولأهميّة المعلومات المتبادلة على هذه الشّبكات كان غالباً ما يُشوش عليها؛ لحرمان الجانب المعادي من الحصول على معلومات عن الأهداف المطلوب تدميرها، وكذلك حرمانه من أن يصحح نيران مدفعيته، وإصابة الأهداف بدقّة.[36]

الفرع الثّاني: الحرب السّيبرانيّة بين الحرب العالميّة الأولى والثّانية

أجرت عدة دول تجارب على قيام الطّائرات بتوجيه القنابل لاسلكياً، وفي الثلاثينيّات من القرن العشرين الميلاديّ تطوّرت أجهزة الإرسال بدرجة كبيرة، وأُنتجت أجهزة استقبال ذات حساسية عالية، وهوائيّات دقيقة التّوجيه، وهو ما أدّى إلى التّفكير في التّداخل اللاسلكيّ؛ لإفشال أعمال التّوجيه.

وفي هذا الوقت بدأت التطبيقات العمليّة للظواهر المكتشفة عام ١٩٠٠م، لصدى الصّوت؛ إذ كان عندما يُرفع الصّوت، ويُسمع صدى في الإجابة، يُعرف أنّ الصّوت وصل حائطاً بعيداً أو حاجزاً، ولا بدّ أنّه انعكس من المكان نفسه، وهكذا بدأ تطبيق تحديد المكان لأي جسم متحرك، مثل: سفينة في البحر، إذ يمكّن من تحديد مسافة تحركها في زمن محدّد، وحساب سرعتها؛ ففي البداية يحدد مكان الهدف المتحرك وتوقيته في موقع ما، ثمّ بعد فترة زمنية محدّدة، يُعادُ تحديد مكان الهدف وتوقيته في موقع آخر، وبحساب المسافة التي تحركها الهدف، بين الموقعين الأول والثّاني، والزّمن الذي استغرقه في قطع هذه المسافة، تحدد سرعة الهدف من المعادلة الآتية:

السّرعة = المسافة / الزّمن[37]

---

[36]. لطفي لمين بلفرد، "الفضاء السيبرانيّ: هندسة وفواعل"، المجلة الجزائرية للدراسات السّياسيّة، ENSSP، العدد الخامس، الجزائر، 2016، ص 148-150.

[37]. لطفي بلفرد، المرجع السّابق، ص 148.

وحتى ديسمبر ١٩٣٨م، تمكّنت الدّول الأوروبية من إنتاج رادارات ذات مدى كشف راداري 100 ميل عن الطّائرات المعادية، توفر زمن إنذار لأكثر من نصف ساعة عن هجوم قاذفات القنابل المعادية، فضلاً عن إنتاج رادار بحريّ يوفّر مدى كشف راداري خمسة عشر ميلاً عن القطع البحريّة المعادية.

ومنذ أكتوبر ١٩٣٥م، كُلّف مسؤول البرنامج البريطانيّ لتطوير الرّادار بدارسة إمكانيّة التّشويش على أجهزة الكشف الرّاداري، إذ بدأت التّجارب وأمكن تحقيق نتائج إيجابية في عام ١٩٣٨م، وفي عام 1939م، كما بدأت في إنجلترا دراسة إمكانيّة تشغيل عمّال الرّادار على أجهزتهم، في ظل قيام العدو بأعمال الإعاقة والتّشويش على الرّادارات الإنجليزية.[38]

أما الإنجاز الكبير الذي حدث بعد ذلك هو أنّه بعد سقوط فرنسا هرب العالم "موريس دولورين" إلى الولايات المتّحدة الأمريكيّة، ومعه ثلاثة من زملائه الذين كانوا يعملون في نوع جديد من أجهزة تحديد الاتجاه ذات التّردد العالي للبحريّة الفرنسيّة، وبدءوا العمل في مختبر الاتّصالات اللاسلكيّة الفيدراليّ في "أماجا نسيت" بولاية "لونـج أيلاند"**Long Island** ، وسرعان ما قاموا بتشغيل نموذج متطوّر لتحديد الاتجاه اللاسلكيّ يعمل على الشواطئ، ثمّ طوّروا جهازاً آخر للعمل بالسّفن الحربيّة، دخل الخدمة في القوات البحريّة بعد ذلك.

ومنذ أوائل ديسمبر 1941م، وقبل دخول الولايات المتّحدة الأمريكيّة الحرب مباشرة، أنتجت رادارات متقدّمة منها**SCR-270** ، ثمّ**SCR-271** وذلك بزيادة حيّز تردّداتها، رُكّبت فيما بعد بالسّفن الحربيّة، وحاملات الطّائرات والطرادات، ممّا أدّى إلى التّغلب على أعمال الاستطلاع والإعاقة الرّادارية.[39]

---

[38]. يحي اليحياوي، أوراق في التّكنولوجيا والإعلام والدّيمقراطيّة، دار الطليعة للنشر، بيروت، 2004، ص 13.

[39]. لطفي لمين بلفرد، "الفضاء السيبرانيّ: هندسة وفواعل"، المجلة الجزائرية للدراسات السّياسيّة، ENSSP، العدد الخامس، الجزائر، 2016، ص ص 148-150.

وفي الوقت نفسه كانت الإجراءات المضادة للرادارات تسير سيراً حسناً، مثل: مستقبل التّحذير الرّاداري جهاز استقبال راداري، يُركّب في الطائرة أو في القطعة البحريّة، يمكنه استقبال نبضات الرّادار المعادي؛ فيعطي إنذاراً لقائد الطّائرة/ القطعة البحريّة أنه أصبح مكَتَشفاً رادارياً، وعليه تنفيذ التّدابير السّيبرانيّة؛ لتجنب هذا الكشف من الرّادارات المعادية **Radar Warning Receiver: RWR**من نوع**P-540** ، والذي تطوّر بعد ذلك، إلى ما أطلق عليه**P-587** ، والذي أُقرَّ في مختبر الطّاقة الإشعاعيّة.

وهكذا زاد التّنافس بين القوات المتحاربة في المحيط الأطلسيّ والمحيط الهادي، مما ساعد على التّطوير المستمر في معدات الحرب السّيبرانيّة وأعمالها حتى وصلت إلى ما هي عليه الآن في ظل التّطوّر الهائل لتكنولوجيا السيبرانيّات.[40]

المطلب الثّالث: أنواع الحروب السّيبرانيّة

يبدو أنّ جميعَ الحلقات الأساسيّة للحياة الحديثة من الإمدادات النّفطيّة، والمرافق العامة إلى الحسابات المصرفيّة، وأسواق الأسهم، والمنشآت العسكريّة، وحسابات البريد السيبرانيّ...إلخ، أصبحت هدفاً للهجمات السّيبرانيّة، أو ما يُطلق عليه "هجمات الفضاء السيبرانيّ"، ويُقدر أنّ هناك خمسون ألف هجمة سيبرانية تحدث يومياً في أرجاء العالم، منها نحو: خمسة آلاف تتمّ من دون اكتشاف في الولايات المتحدة، بينما قد تكون تلك الهجمات أقلّ شناعةً ووضوحاً مقارنة بالحرب التّقليديّة، فإنّ لديها القدرة على التّسبب في القدر الكبير نفسه من الفوضى والأضرار الجانبية، بل إن هناك من يطلق عليها "الابتكار الأخطر في هذا االقرن، وقد بدأت الحرب السّيبرانيّة تصبح العنصر المهيمن في التّرسانة العسكريّة لكل الدول المتقدّمة، وتحدث تحول منظوري في الطريقة التي كان البشر يشنّون بها الحروب على مرّ الأجيال.[41]

---

[40]. يحيى اليحياوي، أوراق في التّكنولوجيا والإعلام والدّيمقراطيّة، دار الطليعة للنشر، بيروت، 2004، ص 13.

[41]. يحيى اليحياوي، أوراق في التّكنولوجيا والإعلام والدّيمقراطيّة، دار الطليعة للنشر، بيروت، 2004، ص 13.

تخلق الحالات المتزايدة بسرعة من الهجمات السّيبرانيّة فرصاً تجاريّة مغرية تحت شعار "أمن الفضاء السيبرانيّ" أو ما يُعرف بمفهوم "الأمن السيبرانيّ". ووفقاً للتقديرات، من المتوقع أن يصل الإنفاق العالميّ على أمن الفضاء السيبرانيّ إلى ستين مليار دولار هذا العام، وأن ينمو بنسبة عشرة بالمئة سنويّاً على مدى السّنوات الثلاث القادمة، ويشير تقرير لمؤسسة "برايس ووترهاوس كوبرز" للخدمات المهنية إلى أنّ إجمالي الاستثمّارات في صفقات أمن الفضاء السيبرانيّ العالميّة تجاوز اثنين وعشرين مليار دولار منذ عام ٢٠٠٨م، أي: بمعدل يزيد على ستة مليارات دولار سنويّاً.

وقد توصّلت دراسة أجرتها مؤسسة "بلومبرغ" بتكليف من الحكومة الأمريكيّة إلى "أنّ الشّركاِت بما فيها شركات المرافق العامة، والمصارف، وشركات الهاتف، سيتعين عليها أن تزيد نفقاتها على أمن الفضاء السيبرانيّ بواقع ما يقرب من تسع مرات؛ للحؤول دون أن تؤدي "بيرل هاربور" الرّقميّة إلى إغراق الملايين في ظلام دامس، أو يُصاب النّظام الماليّ بالشلل، أو تنقطّع الاتّصالات".[42]

بيد أنّ النّقطة الخلافية تكمن في ما إذا كانت هناك مدونةً لقواعد السلوك تتيح فرصاً متكافئة للجميع في عالم الإنترنت، وهل قواعد الاشتباك تحدّد ما هي الأهداف المشروعة ونظيراتها غير المشروعة؟ الجواب البسيط على ذلك هو: "لا،" ومن غير الواضح أيضاً ما إذا كانت العمليّات التي تنطوي على معلومات تعطيليّة سيبرانيّة محضة التي تقوم بها دولة ضدّ أخرى، تُعتبر عملاً من أعمال الحرب، أو عملاً أدنى درجةً من أعمال الإكراه أو العدوان.

هناك عدة عوامل تفسّر عدم الوضوح هذا، أهمها: من الممكن ألا يكون المهاجمُ في الفضاء السيبرانيّ دولةً، وإنّما مجموعة صغيرة من الأفراد، أو حتى فرد واحد يعمل بمفرده؛ ولذلك لا يعني نشوء الهجوم

[42]. أبو ربيع، مصطفى عبد العزيز، 2007، استخدام القوة بتفويض مجلس الأمن، بدون طبعة، رسالة ماجستير، آل البيت، ص 2.

في دولة أنّ تلك الدّولةُ مسؤولةٌ عنه، كما أنّ حجمَ الخسارة الذي يحدثه المهاجم يعتمدُ أيضاً على متغيرات متنوّعة.[43]

وقد زاد هذا النّوع من الهجمات في الآونة الأخيرة؛ سواء من حيث تواترها أو شدتها، وإنّ ظل نجاحها محدوداً، وفي وقت سابق من هذا العام، ذكر المصرف المركزيّ في دولة الإمارات: "إنّه صدَّ هجوماً من قراصنة الكمبيوتر حاولوا إعطاب موقعه السيبرانيّ، وقال خبراء حضروا مؤتمر البترول العالميّ في الدوحة العام الماضي: "إنّ القراصنةَ يحاولون غزو قطاع الطّاقة، ويمارسون التّجسس الصّناعي، ويهددون بإحداث فوضى عالميّة محتملة من خلال تعطيل إمدادات النفط، وحذَّر الخبراء من أنّ الهجماتِ أصبحت أكثرَ تواتراً، وأنّ التّخطيطَ لها أصبح يتسم بمزيد من العناية.[44]

وفي شهادته أمام الكونجرس الأمريكيّ أوضح لودولف لومان"، وهو أحد مديرو تكنولوجيا المعلومات في شركةِ **Shell**، "إنّه إذا تمكَّن أي شخص من دخول المنطقة التي يمكنك بها التّحكّم في فتح الصّمامات وغلقها، فإنّ لك أن تتخيل ما سيحدث! سيؤدي ذلك إلى خسارة في الأرواح والإنتاج والأموال، وسيتسبب في حرائق وتسريبات وأضرار بيئية، وسيؤدي إلى أضرار فادحة". وفي العام الماضي أعلنت شركة "سيجا" اليابانيّة لتطوير ألعاب الفيديو إنّ معلومات تخصّ 1.3 مليون عميلٍ سُرقت من قاعدة البيانات الخاصّة بها، وهي الهجمة الأحدث ضمن موجة من الهجمات السّيبرانيّة ضدّ شركات ألعاب الفيديو على المستوى العالميّ.[45]

ومن الصعوبة بمكان تحديد مدى التّهديد الذي تمثله الحرب السّيبرانيّة على الأمن العالميّ؛ لأّننا لم نشهد هجوماً كاملاً بعد، كما توجد حاجة لسياسة بشأن وضع المشاركين في الحرب السّيبرانيّة من حيث كونهم من الجنود أو الجواسيس أو المدنيين أو أي فئة أخرى. في الواقع تبدو حرب الفضاء

---

[43]. يحي اليحياوي، أوراق في التّكنولوجيا والإعلام والدّيمقراطيّة، دار الطليعة للنشر، بيروت، 2004، ص 13.

[44]. يحيى اليحياوي، المرجع السّابق، ص 13.

[45]. يسرى خالد إبراهيم، "الحرب النّفسيّة السّيبرانيّة"، مجلة الباحث الإعلامي، العدد 13، 2011، ص 117.

السيبرانيّ غير دمويّة ونظيفة إلى درجة أنّه لا تكاد توجد أي معضلات أخلاقيّة حقيقية كي يتمّ التّعامل معها، والتوصّل إلى حلّ سلميّ في الفضاء السيبرانيّ؛ لتجنب خطر حرب سيبرانية عالمية.[46]

الفرع الأوّل: الحروب المُوجّهة إلى هدف محدّد

استند هذا النّوع من الحروب على المعلوماتيّة؛ إذ إنّه يكفي لقهر الخصم، ويتمّ النّجاح باستخدام هياكل القيادة، ولديه وسائل الاتّصال مع المؤسسات الفكريّة، وكذلك تستند هذه الحروب على القنابل الذّكية التي استخدمت في حرب الخليج الثّانية عام1991، وقنابل الغرانيت القادرة على تصفير دوائر المراكز الكهربائيّة، التي استخدمت مؤخّراً ضدّ الصّرب في حرب كوسوفو، وكذلك القنابل التي استخدمت في الحرب الأمريكيّة على العراق عام2003م؛ إذ إنّه في حالة الصّراع تصبح المعارك هدفا للمواجهة، وليس فقط ما يتيح الهجوم أو الصّدام في الظّرف الملائم.

وكان أخر تطبيق عمليّ لهذه الحرب في العراق عام 2003، من خلال اعتماد الولايات المتحدة على استراتيجية الصّدمة والتّرويع، التي تقوم على قدرة تكنولوجيّة متطوّرة، ومنظومات تسليحيّة متكاملة وقادرة على تطبيق التّأثير المستهدف، من أجل التّأثير في إرادة الخصم وإدراكه، وتتطلب هذه الاستراتيجيّة عدة عناصر لنجاحها هي: المعرفة الكاملة بالذات والخصم والبيئة، ويشمل ذلك معرفة كاملة بالعمليّات الذهنيّة والمنظومات التّقنيّة، لقادة الخصم وجماهيره، والسرعة في جميع مراحل العمل العسكريّ؛ سواء في المناورات أو التّحركات داخل الميدان، وضمان السّيطرة على العمليّات؛ سواء على الأرض أو في مجال الإشارات اللاسلكيّة والبنية الأساسيّة للاتصالات، ممّا يضطر الخصم إلى الاستسلام؛ خوفا من تعرضه لدمار واسع.[47]

---

[46]. يسرى إبراهيم، المرجع السّابق، ص 117.

[47]. يسرى خالد إبراهيم، "الحرب النّفسيّة السّيبرانيّة"، مجلة الباحث الإعلاميّ، العدد 13، 2011، ص 117.

كما أنّ الحربَ المُوجّهة تستخدم أكثر الأسلحة ذكاء، وتتطلب وجود قوات ووحدات صغيرة ومترابطة؛ لكي تتمكن من تنسيق هجماتها بشكل متكرر، ومن أبرز الدّول التي تمتلك هذه القوات هي الولايات المتحدة وفرنسا وكندا وبريطانيا.

الفرع الثّاني: الحروب الشّبكيّة

وهو شكل جديد من أشكال الحروب التي تُمكّن من التّأثير على نشاطات وأعمال الخصم، وخصوصاً إذا كان مجتمعُ الخصم متطوّراً ويعتمد بدرجة كبيرة على وسائل المواصلات والاتّصالات، أمّا إذا كان الخصم أقل تطوّراً في اعتماده التّقنيّات الحديثة، فإنّ أساليب حروب الشّبكات كالفعاليات التّقنيّة والتّشويش لن يكون مؤثراً بالدرجة المطلوبة، ومن ثمّ سيتمّ الاعتماد على الأسلحة التّقليديّة المعروفة التي تعتمد على الدّقة في الإصابة والسرعة في الاستجابة؛ لذا فإنّ حروب الشّبكة موجّهة بشكل أساسيّ نحو تحجيم العدو، ومن ثمّ هي تختلف عن الحرب المُوجّهة، التي تكون نحو شلّ قدرة العدو العسكريّة [48].

الفرع الثّالث: الحروب التّجسسيّة

إن التقدّمَ التّقنيّ أصبح واحداً من أهم مفاتيح المستقبل، وعاملاً حاسماً للسّيطرة في النّظام العالميّ الجديد؛ لذا أصبحت المنافسةُ شديدةً في الميدان التّكنولوجيّ، والسّياسيّ، والاستراتيجيّ؛ لأنّ مَن سيحصل على التّكنولوجيا، فإنّه سيسيطر في المجالات الأخرى؛ لذا يرى أنّ جزءًا كبيراً من الاتّصالات آلةٌ تسيطر عليها أجهزة الأمن والأجهزة المخابراتية؛ إذ إنّ هذه الأجهزة تراقب كل شيء تقريباً، وينتشر وكلاء متخصصون في كل بلدان العالم مدعومون بأقمار صناعيّة تجسسيّة؛ لجمع المعلومات والعمل مع الآلاف من الإذاعات والقنوات، وكل ذلك يتجه لهدف واحد ألا وهو التّجسس على العالم، فالوكالات الأمنية تنتشر في كل بلدان العالم، وتسعى، وتتنافس وبكل الطرق للحصول على المعلومات مُستخدِمةً كل الوسائل المتاحة بعمليّة تصارع أشبه بالحرب ذاتها، من هنا انطلقت حرب

[48]. يسر إبراهيم، المرجع السّابق، ص 117.

التّجسس هذه، فالدّول تسعى لانفاق ثروتها على قواعدها التنصتيّة، ونصب وسائل ذات تقنية عالية الكفاءة؛ للتّجسس على العالم.[49]

الفرع الرّابع: الحرب النّفسيّة

أخذت الحرب النّفسيّة مقاربة جادة ووازنة هو أمر شائك وبالغ الصعوبة والتعقيد، وهناك من يرى أنّ الحرب النّفسيّة: "هي التي يستخدمون فيها الدّعاية من أجل التّأثير على أشخاص بين أوساط العدو" وثمّة من اعتبرها: "عمليّات تستخدم فيها وسائل الإقناع على نحو غير عنفيّ؛ لتحقيق أهداف الحرب العسكريّة"، وقد حاول الباحث "بول الينبارجر" في كتابه " الحرب النّفسيّة"، الأخذ بكل هذه التّعاريف وتدوير رؤى النّظر المختلفة، إذ عرّف الحروب النّفسيّة: "بأنّها استخدامُ الدّعاية ضدّ العدو مع إجراءات عمليّة أخرى ذات طبيعة عسكريّة أو اقتصادية أو سياسية"، في حين ذهب الباحث حامد ربيع إلى تعريف الحرب النّفسيّة: "بأنّها نوعٌ من القتال لا يتجه إلا إلى العدو"، وهي بذلك خلاف الدّعاية التي تتعدد فيها الرؤى، كما أنّها تعد فناً حربيًّا لا يسعى إلا للقضاء على الإرادة الفردية والجماعية للعدو.[50]

الفرع الخامس: الحرب الفضائيّة

منذ عام ١٩٨٣ سعت الولايات المتّحدة الأمريكيّة لتطوير برنامج حرب النّجوم، أو منظومة الدّفاع الاستراتيجيّ، وامتلاك القدرة المطلقة على صدّ أي هجوم صاروخيّ، ومنذ ذلك الوقت طور الفضاء العمليّات العسكريّة الأرضيّة في مجال المراقبة، والاتّصالات، والملاحة، والرصد الجويّ، بحيث

---

[49]. يسرى خالد إبراهيم، "الحرب النّفسيّة السّيبرانيّة"، مجلة الباحث الإعلاميّ، العدد 13، 2011، ص 117.

[50]. جوزيف ناي، القوة الناعمة: وسائل النّجاح في السّياسة الدّوليّة، تر: محمد توفيق البجيرمي، ط1، مكتبة العبيكان للنشر، الرياض، 2007، ص24

عمّقت التّكنولوجيا مفهوماً جديداً يخصّ الميدان والجبهة على كل الأبعاد يدعى "بالجبهة متعدّدة الأبعاد".[51]

وبذلك فإنّ التّكنولوجيا المتقدّمة قد بدّلت من روحيّة وديناميّة منظومة القيادة والسّيطرة، والحاسبات والاتّصالات، والمراقبة والاستطلاع، والاستخبارات في الحروب والعمليّات العسكريّة، فضلاً عن ذلك أصبحت المسافة التي تفصل بين المستوى التكتيكي والاستراتيجيّ قليلة جداً، إذ يمكن للمستوى الاستراتيجيّ قيادة العمليّات التكتيكّية مباشرة وعن بعد، وتعدّ عمليّة قتل زعيم تنظيم القاعدة "أسامة بن لادن" في عام 2011 مثالاً حيًاً على ذلك، فقد كانت فرقةٌ صغيرة من القوات الخاصّة تقوم بالعمليّة والرئيس الأمريكيّ مع طــاقم مجلس الأمن القوميّ الأمريكيّ يتابعون العمليّة مباشرةً.[52]

[51]. سامية أبو النّصر، الإعلام والعمليّات النّفسيّة في ظل الحروب المعاصرة وإستراتيجية المواجهة، دار النشر للجامعات، ط1، 2010، ص 82.

[52]. سامية أبو النّصر، الإعلام والعمليّات النّفسيّة في ظل الحروب المعاصرة وإستراتيجية المواجهة، دار النشر للجامعات، ط1، 2010، ص 82.

المبحث الثّاني: آثار الحرب السّيبرانيّة

يُعَدُّ ظهور ثورة تكنولوجيا السيبرانيّات واستخدامها في الأغراض العسكريّة نقطة تحوُّل كبيرة؛ سواء في فنِّ الحرب، أو في إدارة الصّراع المُسلّح، فقد أخَذت أسلحة القتال الحديثة ومعداته مكان الصّدارة في حسْم أيّ صراعٍ مسلَّحٍ، وخاصة أسلحة الهجوم الجوي الحديثة؛ لاعتمادها على نُظم السّيطرة والتّوجيه السيبرانيّ، التي تمكِّنها من تنفيذ المهام المطلوبة منها بكفاءة، وإصابة أهدافها بدقّة عالية؛ نظرًا لاستخدامها نُظُمَ ووسائل الكشْف والتّوجيه والتّحكّم، وقيادة النيران وتصحيحها لاسلكيًّا، ورادايًّا، وحراريّا، وليزريًّا، وتليفزيونيًّا، وهي النُّظم التي يستوي تشغيلها واستخدامها ليلاً ونهارًا، هذا بالإضافة إلى النُّظم الحديثة والمتقدّمة للتصوير التليفزيونيّ باستخدام آلات التصوير ذات الحساسية العالية، التي يُمكنها العمل في مستوى الضوء المنخفِض بكفاءة ودقَّة عاليتَيْن.

المطلب الأوّل: الوقائع التّاريخيّة للحرب السّيبرانيّة

كانت أساليب الحرب السّيبرانيّة تستعمل منذ بداية هذا القرن، وبالأخص عندما استُخْدِمت أجهزةُ الاتّصالات اللاسلكيّة في الحروب، ولكن منذ الحرب العالميّة الثّانية أصبَح موضوع الحرب السّيبرانيّة محلَّ الاهتمام من حيث المعدّات والأساليب.

تفيد المصادر أنّ أوَّلَ عمليّة في مجال الحرب السّيبرانيّة كانتْ في عام 1905م خلال الحرب الرّوسيّة اليابانيّة في معركة**tsushima** ، عندما كانت سُفنُ الاستطلاع اليابانيّة تُراقب الأسطول الرّوسيّ عن كثبٍ، وتُرسل جميع المعلومات بالرّاديو إلى القيادة الرئيسيّة اليابانيّة، وفي هذه الأثناء التقط أحد قادة الزوارق الرّوسيّة هذا الإرسال فطلب الإذنَ باستعمال جهاز الإرسال الموجود بزورقه؛ لإعاقة تلك الإرساليّات، ولكنَّ طلَبَه قُوبِلَ بالرفض، فاستمرَّ إرسال المعلومات الرّوسيّة، وبعد فترةٍ وجيزةٍ استطاعَ

أحد قادة الزوارق الرّوسيّة - دون إذنٍ مِن قيادته - التّشويش على هذه الإرساليات، ولكن بعد فَوَات الأوان، إذ كانت المعركةُ قد وقَعَت وخَسِرها الروس! [53]

أمَّا في الحرب العالميّة الأولى، فقد استُعْمِلَت أجهزة الاتّصالات وأجهزة نقْل معلومات الاستطلاع بكثرة؛ إذ استطاعَت إحدى السّفن الإنجليزيّة عام 1914م أن تُرسل بالرّاديو معلومات عن تحرُّك بعض القطَع الحربيّة الألمانيّة في البحر الأبيض المتوسط، ولكن بعد أن رصَد الألمان تلك الإرساليات، تمكَّنوا من التّشويش الكامل عليها.

وفي عام 1916 وضَع الإنجليز بعض موجدات اتجاه الإرسال قُرب الأسطول الألماني، وخلال معركة "جوتلاند" حدَّدت تلك الأجهزة موقع الأسطول، وأبلَغت القيادة الإنجليزيّة بذلك.

كانت البداية الحقيقيَّة في الحرب العالميّة الثّانية لاستخدام أجهزة الحرب السّيبرانيّة المتخصِّصة، ففي عام 1939م استخدم الألمان طريقة تقاطُع موجات الإرسال فوق الهدف **beam-intersection** ؛ لكي يقصفوا المدن الإنجليزيَّة، وخاصة أثناء الليل، فوضَع الإنجليز جهاز الإرسال**bromide** ؛ ليقوم بتشويش مخادع، ويجعل هذا التّقاطع فوق مكان غير حيويّ، واختاروا لذلك بحر "المانش"، وفعلاً وقَع قصْف الطّائرات الألمانيّة على بحر "المانش"، ولَم تتضرَّر المُدُن الإنجليزيّة، التي أراد الألمان قصْفها. [54]

---

[53]. سامية أبو النّصر، الإعلام والعمليّات النّفسيّة في ظل الحروب المعاصرة وإستراتيجية المواجهة، دار النشر للجامعات، ط1، 2010، ص 82.

[54]الحرب الإلكترونية، شبكة الألوكة، كريم حميدة، 2012/3/20راجع الرابط التالي https://rb.gy/dnpmmsتمت الزيارة في 2023/1/4.

واستخدم الحلفاء أجهزة التّشويش والنصلات **chaff** للتّشويش على الرّادارات الألمانيّة عند الساحل الغربيّ الفرنسيّ، كما استُخْدِمت في الحرب العالميّة الثّانية المناطيد والبالونات؛ للتصنُّت والمراقبة والتصوير في عُمق أراضي العدو.[55]

المطلب الثّاني: تعدد آثار الحرب السّيبرانيّة

إنّ تصاعدَ شبح الحرب النوويّة دفع بالدّول المالكة لهذا السّلاح للتّفكير بوسائل صراع تستثني المواجهة المباشرة، هذا بالضّبط ما شهده العالم خلال الحرب الباردة التي امتدت خمسًا وأربعين سنةً، وقد ظهرت خلال تلك الفترة مصطلحات عدة: "كالحرب بالوكالة،" "والحرب الاقتصاديّة،" "والحرب السّيبرانيّة" وغيرها، فضلاً عن ذلك فإنّ عدمَ اللجوء إلى استخدام السّلاح النووي لا يعني بأيّ شكل من الأشكال توقّف الدّول عن التّفكير بوسائل جديدة للمواجهة، وآخر هذه الوسائل هو التّركيز الكبير على تكنولوجيا الحرب السّيبرانيّة، التي تعدّ أهمّ و أحدث تطوّر في عالم النّزاعات والتّنافس الدّوليّ، هذه الحرب تعتمد بشكل أساسيّ على مدى التّطوّر التّكنولوجيّ العسكريّ للدّول المعنيّة، ولا يمكن لدولة تفتقر لهذه الإمكانيات أن تتمرّس فيها، كما أنّ وسائلَ الحرب السّيبرانيّة تتمايز حتى فيما بينها، فبعضها دفاعيّ يستخدم لصدّ الهجمات السّيبرانيّة المعادية، وإبطال الصّواريخ المعادية وتعطيلها، وبعضها الآخر هجوميّ يعتمد على السّيطرة والضبط؛ أمّا الوسيلة الثّالثة تندرج في مجال الأقمار الصّناعيّة وأنظمة الملاحة وأجهزة الرصد والإنذار المُبكّر.[56]

ومع ظهور الإنترنت ومواقع الويب أصبح الفضاء السيبرانيّ أحد العناصر الرئيسيّة التي تؤثر في النّظام الدّوليّ، بما يحمل من أدوات تكنولوجيا تلعب دورًا مهمًّا في عمليّة التّعبئة والحشد في العالم، فضلاً عن التّأثير في القيم السّياسيّة وأشكال القوة المختلفة؛ سواء كانت صلبة أو ناعمة، كما وتُعدّ

---

[55] الحرب الإلكترونية، شبكة الألوكة، كريم حميدة، 2012/3/20 راجع الرابط التالي https://rb.gy/dnpmms تمت الزيارة في 2023/1/4.

[56] دنيا الوطن، الحرب الإلكترونية واستهداف الدولة المصرية، عادل عامر، 2019/3/3 متوفر على الرابط التالي: https://pulpit.alwatanvoice.com/content/print/486515.html تمت الزيارة في 2023/1/4

الحروب السّيبرانيّة أحد أوجه الصّراع الدّوليّ، إذ يستطيع أحد أطراف الصّراع أن يوقع خسائر فادحة بالطرف الآخر، وأن يتسبب في شلّ البنية المعلوماتيّة والاتّصالية الخاصّة به، وهو ما يسبب خسائر عسكرية واقتصادية فادحة من خلال قطع أنظمة الاتّصال بين الوحدات العسكريّة بعضها ببعض أو تضليل معلوماتها أو سرقة معلومات سريّة عنها، أو من خلال التّلاعب بالبيانات الاقتصاديّة والمالية وتزييفها أو مسحها من أجهزة الحواسيب، وبالرغم من فداحة الخسائر إلّا أن الأسلحة بسيطة لا تتعدى الكيلو بايتس، تتمثّل في فيروسات سيبرانّية تخترق شبكة الحاسب الآليّ وتنتشر بسرعة بين الأجهزة، وتبدأ عملها في سريّة تامّة وبكفاءة عالية، وهي في ذلك لا تفرّق بين المقاتل والمدنيّ، وبين العام والخاص، وبين السّريّ والمعلوم. [57]

وقد أقرّ مجلس أوروبا في عام 2001م الاتفاقية التي حاولت ربط القانون الدّوليّ بالأمن السيبرانيّ مثل التّجسس، وهي اتفاقية "بودابست"، وتختص أكثر في الجرائم السّيبرانيّة.

إذن الفضاء السيبرانيّ أصبح وسيلة لاستخدام التنظيمات الإرهابيّة وأجهزة الدولة من خلال شبكة الإنترنت، ولذلك يجب أن يكون هناك قواعدَ تُنظّم هذا الفضاء السيبرانيّ، حيث لا يجوز ألا يكون هناك محاسبةً للدول التي تتجاوز حدودها وتعتدي على دول أخرى.

لقد تضمنت الاتفاقية أقساماً ثلاثة: الأول يتناول مجموعة الجرائم التي تتعرض لها شبكة الإنترنت والحاسب الآلي، والثّاني تناول الإجراءات الجنائيّة التي تُتّخذ في مواجهة هذه الجرائم، وتناول القسم الثّالث التّعاون الدّوليّ في مكافحة هذه الجرائم بين الدول الأعضاء، وجاء في المادة (١) من الاتفاقية تعريفات لبعض المصطلحات الحديثة في القانون الجنائي وهي: "نظام معلوماتي"، "بيانات معلوماتية"، "مفهوم مقدم الخدمة عبر الإنترنت"، "والبيانات التي تمر خلال النّظام المعلوماتيّ" وتناولت المواد جريمتين اثنتين إلى ستّ جرائم ضدّ سريّة وسلامة وإتاحة البيانات والنُّظم المعلوماتيّة،

[57]. سامية أبو النّصر، الإعلام والعمليّات النّفسيّة في ظل الحروب المعاصرة وإستراتيجية المواجهة، دار النشر للجامعات، ط1، 2010، ص 82.

وهي جرائم الدّخول غير المشروع للنظم المعلوماتيّة، والاعتراض غير القانونيّ لهذه النُّظم والاعتداء على سلامة البيانات، وتناولت المادتان(٧) و(٩) ومنها: التزوير والغش المعلوماتي، كما تناولت المادة (٩) الجرائم المتصلة بالمواد الإباحيّة للأطفال، وتضمنت المادة(١٠) الاعتداء على حقوق المُلكيّة الفكريّة والحقوق المجاورة،أمّا المادّة(١١) فقد تناولت عدة أمور:

أوّلًا: تناولت الشروع والاشتراك في هذه الجرائم،وشملت الاتفاقية مسؤوليّة الأشخاص المعنويّة عن ارتكاب هذه الجرائم، وهي مسؤوليّة مستحدثة في التّشريع الجنائي المعاصر، وأيضا الجزاءات، ثانيّا: تناولت الاتفاقية الجوانب الإجرائية؛ إذ أوصت الدّول الأعضاء باتخاذ الإجراءات اللازمة والضّروريّة لضبط ونسخ الأدلة المعلوماتيّة، واستحداث تنظيم لإجراءات هذا الضّبط، وتمكين سلطات التّحقيق من الحصول على نسخ من الأدلة، وتفتيش وضبط البيانات المعلوماتيّة المخزنة آليّاً، ووضع نُظم لمراقبة الإنترنت والتّحفظ العاجل على البيانات المعلوماتيّة واعتراضها، ثالثا: "التّعاون الدّوليّ في مكافحة الجريمة المعلوماتيّة، حيث نصّت الاتفاقية على إمكانيّة التّعاون الدّوليّ في مكافحة الجرائم المعلوماتيّة عابرة الحدود، وذلك بتسليم المجرمين والمساعدة القضائيّة المتبادلة، كما نصّت على إجراءات طلب المساعدة القضائيّة المتبادلة، وتحديد مجالات هذه المساعدة في الإجراءات الوقتيّة العاجلة وفى مجالات سلطات التّحقيق، وفي الختام، فإنّ الانضمامَ إلى هذه الاتفاقية ذو أهميّة قصوى من أجل التّعاون الدّوليّ؛ لمكافحة الجرائم السّيبرانيّة خاصة مع تنامي جرائم الإرهاب على مستوى دول العالم. [58]

وعلى المستوى العالميّ، تنظر الولايات المتحدة إلى الفضاء السيبرانيّ كحيز يجب أن تُعمّم فيه معايير ومقاييس سياسية وأيديولوجية مختلفة حسب مفهومها، وفي ربيع العام ٢٠١٠ تم إنشاء مؤسسة تابعة للبنتاغون، هي القيادة السّيبرانيّة، وفي عام2010 أعلنت وزارة الدّفاع أنّها شرعت بالتّحكّم بالشّبكات الاجتماعيّة من أجل تحسين الصورة، وللتأثير على الدول الأخرى، وقد أشارت مديرة وكالة الدّفاع

[58]. الجرائم المعلوماتيّة دولياً خطر دولي، مواجهة جرائم الإنترنت بين اتفاقية بودابست والتّشريعات الوطنية، المستشار رشدي محمد علي، https://gate.ahram.org.eg/daily/News

الأميركية للتقنيات الواعدة "ريغينا دوغان": "أنّ جهوداً إضافيّة ستبذل لإنشاء سلاح سيبرانيّ هجوميّ يُشكّل عنصراً جوهريّاً في الآلة العسكريّة مع ضرورة معرفة الإمكانات السّيبرانيّة للدول الأخرى، بهدف التّحصّن ضدّها، وهذا يعني أنّ الولاياتِ المتحدة نفسها تمارس التّجسس السيبرانيّ". [59]

ختاماً،يمكن القول: إنّ مزايا الحروب السّيبرانيّة التي تفوق مزايا الدّفاع ستدفع العالم إلى مزيد من الصّراعات وخاصة مع تطوّر آليات الهجوم السيبرانيّ بشكل متسارع؛ مما يضفي عليها مزايا إضافيّة في المراحل المختلفة لهذه التّطوّرات، فغياب الأطر القانونيّة الدّوليّة الرّادعة في الحروب السّيبرانيّة، وانتقاء القيود الشّرعيّة الدّوليّة كنتيجة لعدم إمكانيّة التّعرّف على هوية المهاجم على عكس الهجوم التقليدي، كل هذه العوامل تجعل من الفضاء السيبرانيّ ساحة جاذبية للقوى الكبرى لإدارة صراعاتها مع بعضها بعضاً، فاستبدال الحرب العسكريّة بتلك السّيبرانيّة، وانتقال الصّراع ما بين القوى الكبرى من المساحات التّقليديّة إلى الفضاء السيبرانيّ قد يسمح للقوى الدّوليّة للدّخول في مواجهات سيبرانيّة". [60]

المطلب الثّالث: نماذج تطبيقيّة عن الحرب السّيبرانيّة

لقد تنوّعت وسائل السّيطرة والتّحكّم الخاصّة بمعظم العمليّات الحيوية الموجودة على الأرض، وانتقلت إلى عالم الفضاء السيبرانيّ في صورة متعدّدة منها: أقمار صناعيّة ومحطّات فضائية، كما انتقل أيضاً قطاع واسع من الحروب والمعارك والصّراعات والثورات إلى العالم الافتراضي، الذي خلقه الإنسان منذ اختراعه للكمبيوتر والذاكرات السّيبرانيّة وشبكات المعلومات، فأنشأ داخله جغرافيا افتراضية جديدة، وأخذ الصّراع السيبرانيّ حيزاً واسعاً من خرائط الصّراع الدّوليّة؛ لذلك تمّ دراسة بعض النّماذج التّطبيقيّة على تلك الحروب على النحو التالي:

---

[59]. سامية أبو النّصر، الإعلام والعمليّات النّفسيّة في ظل الحروب المعاصرة واستراتيجية المواجهة، دار النشر للجامعات، ط1، 2010، ص 82.

[60]موقع "لا" الإخباري، متوفر على الرابط الآتي:
https://www.laamedia.com/news.aspx?newsnum=39734

الفرع الأوّل: الولايات المتّحدة الأمريكيّة وإيران

يعدُّ برنامج إيران للحرب السّيبرانيّة أحد أجنحة النّظام الإيرانيّ لمواجهة الولايات المتّحدة الأمريكيّة، الذي بدأ تشكيله عام ٢٠١٢م، ويشرف على إدارته المجلس الأعلى للفضاء السيبرانيّ، الذي تشكّل بأمر من المرشد الأعلى "علي خامنئي"، وقد أصبح المجلس ركيزةً أساسيّةً بالنسبة للحرس الثّوريّ والسياسات الخارجية الإيرانيّة، وقد أشار الضّابط السّابق في الحرس الثّوريّ والباحث الفيزيائي "محسن فحري زاده" بقوله: "إنّ إيرانَ عملت على تطوير قدراتها السّيبرانيّة منذ تأسيس المجلس الأعلى للفضاء السيبرانيّ، واستغل النّظام الإيرانيّ البرنامج؛ لشن هجمات سيبرانية وتنفيذ عمليّات تجسس سيبرانية في محاولة لإلحاق الضّرر بالبُنى الأساسيّة: المالية، والأمنيّة، والسّياسيّة الخاصّة بالدول المعادية لإيران؛"[61] لذلك إنّ للحرب السّيبرانيّة تأثيراً عالمياً كبيراً؛ إذ قد تؤدي إلى تدمير بنية تحتيّة لدولة ما، بما في ذلك سدودها المائية ومفاعلاتها النوويّة؛ لذلك فإنّ حربَ السّيبرانيّة هي تطوّر طبيعيّ في مفهوم الحروب، نقلتها إلى جيل جديد يعتمد على التّحكّم والسّيطرة عن بعد، وقبيل أعوام من توصّل المجتمع الدّوليّ إلى الاتفاق النّوويّ مع طهران، شنّت الولايات المتّحدة الأمريكيّة حربها السّيبرانيّة على مشروع إيران النّوويّ، بهدف إضعاف قدرة طهران النوويّة، وإجبارها على التّنازل على طاولة المفاوضات، وهو ما تمّ وفق خبراء، وقد وضّح "جورج ميد"، خبير فيروسات يعمل في الجيش الأمريكيّ: "إنه تمّ إرسال الفيروسات الخبيثة؛ لتخريب المنشآت النّوويّة الإيرانيّة الأمر الذي أضعف قدرتها على تخصيب اليورانيوم"، وفي الوقت نفسه لم تكن واشنطن بمأمن من الهجمات السّيبرانيّة، ففي يوم الجمعة 23 مارس2018م وجّهت وزارة العدل الأمريكيّة اتهاماتٍ جنائيّة، وفرضت عقوبات على شركة إيرانيّة وعلى تسعة ناشطين إيرانيين؛ لاختراقهم أنظمة مئات الجامعات والشّركات وضحايا آخرين؛ لسرقة البحوث والبيانات الأكاديمية والملكيّة الفكريّة، ووصفت وزارة

---

[61]. نقلاً عن: هدير عادل، باحثة أمريكي يكشف خبايا برنامج الحرب السّيبرانيّة الإيرانيّ، موقع العين الإخبارية، تاريخ النشر 3\12\2018 متاح على الرابط-https://al-ain.com/article/iran-held-accountable-cyber attacks-irgc

العدل الأمريكيّة القراصنة بأنهم عصابة تسلل سيبراني، حاول أفرادها اختراق مئات الجامعات حول العالم، وهم أفراد تابعون للحرس الثّوريّ الإيرانيّ، فضلاً عن اختراقهم لعشرات من الشّركات وقطاعات من الحكومة الأمريكيّة لحساب الحكومة الإيرانيّة، وحسب ما صدر من تقارير صادرة عن الوزارة وضّحت فيه: "إنّ الهجومَ الذي وصفته بإحدى كبرى الهجمات السّيبرانيّة التي ترعاها دولة ايران، بدأ منذ 2013 على الأقل وبه تمّت سرقة أكثر من واحد وثلاثين تيرابايتاً من البيانات الأكاديمية وحقوق المُلكيّة الفكريّة من مئة وأربع وأربعين جامعة أمريكيّة ومئة وستّ وستين جامعة في إحدى وعشرين دولة أخرى"[62].

ومن جانب آخر أوضح المحلّل السّياسيّ مجيد رفيع زاده: "إنّ النّظامَ الإيرانيّ عمل في وقت سابق على شنّ هجمات سيبرانية ضدّ الولايات المتحدة وغيرها من الدول"، والمثال على ذلك، تعرضت الأنظمة المصرفيّة الأمريكيّة لهجوم بمستوى غير مسبوق، فضلًا عن مواقع عدد من البنوك، مثل: "بنك أوف أمريكا" و"سيتي جروب"، وأوضح مسؤولون أمريكيون: "إنّ مستوى تلك الهجمات يشير إلى أنّ الفاعلَ هو الحكومة الإيرانيّة"، واتهمت وزارة العدل الأمريكيّة مؤخراً سبعة إيرانيين بشنّ هجمات تعطيل الخدمة على ستٍّ وأربعين شركة، وتستهدف بصورة أساسيّة القطاع المصرفيّ والماليّ، فضلًا عن أنّ الاستخباراتِ الأمريكيّة أشارت: "إنّ إيران وراء فيروس شمعون"، الذي استهدف شركة "أرامكو" السعوديّة، وأوضح زاده بقوله: "إنّ القادةَ الإيرانيّين مدركون لحقيقة أنّ شنَّ هجمات سيبرانية أقلُ تكلفة من الانخراط في مواجهة عسكرية مباشرة مع خصومها، خاصة وأنّ قدراتَها العسكريّة أقلُ من أعدائها"، لافتاً إلى أنه من وجهة نظر القادة الإيرانيّين البديل للحرب الفعلية هي الافتراضية التي تقدّم ميزة إخفاء الهوية، كما تصعب للغاية إمكانيّة محاسبتهم، ويرى زاده: "أنّ إيران -على الأرجح - ستحاول تصدير تلك القدرات المُتعلّقة بالحرب السّيبرانيّة إلى وكلائها إقليمياً، وقد يكون لهذا عواقب وخيمة بالنسبة لمصالح الأمن القوميّ الأمريكيّ، وكذلك أشار إلى أنّ برنامجَ

[62]. الحروب السّيبرانيّة. معارك العالم الافتراضي تنتقل إلى الميدان، لندن – الخليج أونلاين، تاريخ النشر 2018\3\24، متاح على الرابط http://alkhaleejonline.net

الحرب السّيبرانيّة الإيرانيّ أصبح مسألةَ أمن قوميّ بالنسبة للنّظام؛ خاصة وأنّه يساعد النّظام في تحقيق أهداف سياستهم الخارجية ومطامعهم في الهيمنة الإقليميّة"[63].

الفرع الثّاني: الولايات المتحدة- ورسيا

"لقد أدّى ظهور الجيوش السّيبرانيّة إلى كشف عن نوايا حروب السّيبرانيّة جديدة، وهذا ما كشف عنه وزير الدّفاع الرّوسيّ "سيرغي شويغو": "أن بلاده أنشأت بالفعل جيشاً سيبرانياً تابعاً لوزارة الدّفاع، ويتوقع أن يقوم هذا الجيش بردع الدّعاية المغرضة ضدّ بلاده وأن يكون أداةً فعالةً ذكية، وبالرّغم من أنّ مهامَ هذا الجيش ستكون سريّةً ولن تقف عند مجال الدّعاية؛ فإنّ أهميّةَ هذه التّصريحات التي أدلى بها وزير الدّفاع الرّوسيّ أنّها جاءت في أعقاب إعلان مدير الاستخبارات الألمانيّة "هانس جورج ماسن": "إنّ الهجماتِ السّيبرانيّة يمكن أن تقوم بتركيع الدّول المتقدّمة بما فيها ألمانيا"[64].

وفي عام 2010 تمّ إنشاء مؤسسة سيبرانيّة أمريكية تابعة للبنتاغون هي القيادة السّيبرانيّة، وفي عام 2011 أعلنت وزارة الدّفاع الأمريكيّة أنّها شرعت بالتّحكّم بالشّبكات الاجتماعيّة من أجل تحسين الصورة، وللتأثير على الدّول الأخرى، أمّا مديرة وكالة الدّفاع الأميركية للتقنيات الواعدة "ريغينا دوغان" فقد أعلنت أنّ جهوداً إضافيّة ستبذل لإنشاء سلاح سيبراني هجومي يُشكّل عنصراً جوهرياً في الآلة العسكريّة، مع ضرورة معرفة الإمكانات السّيبرانيّة للدول الأخرى، بهدف التحصن ضدّها وهذا يعني أنّ الولاياتِ المتحدة نفسها تمارس التّجسس السيبرانيّ[65].

---

[63]. هدير عادل، باحثة أمريكي يكشف خبايا برنامج الحرب الإلكترونيّة الإيرانيّ، موقع العين الإخبارية، تاريخ النشر 2018\12\3 متاح على الرابط https: //al-ain. com/article/iran-held-accountable-cyber-attacks-irgc

[64]. خالد الثوراني، الجيوش الافتراضية بين الصّراع الدّوليّ والتسقيط السّياسيّ المحلي، شبكة النبأ المعلوماتيّة، تاريخ النشر 25/6/ 2017.متاح على الرابط https://annabaa.org/arabic/informatics/11558

[65]. نقلاً عن: عمر حرز الله، الحرب السّيبرانيّة: صراع في العالم الافتراضي، صحيفة البيان، تاريخ النشر 4/ 3 /2012. متاح على الرابط https://www.albayan.ae/five-senses/mirrors/2012-03-04 –

ولا شكّ أنّ الحرب السّيبرانيّة التي أعلنها الرئيس الرّوسيّ، "فلاديمير بوتين" على الانتخابات الرئاسيّة الأمريكيّة في عام 2016، التي تهدف للتأثير فيها لمصلحة الرّئيس دونالد ترامب شكّلت عهداً جديداً في الحروب السّيبرانيّة، وباتت بوابةً لحروب المعلوماتيّة، وانعكست آثارها على الأرض في الولايات المتحدة، وهذه كانت المرة الأولى التي تنتقل فيها الحرب السّيبرانيّة بين الدّول إلى السّاحة الدّيمقراطيّة بعد أن كانت تقتصر على استهداف المنشآت العسكريّة والاستخبارية، وأنّ عمليّةَ القرصنة على الانتخابات الأمريكيّة تمثّل أحد أهمّ الأهداف لموسكو عن رغبتها القديمة في تقويض النّظام الدّيمقراطيّ التّحرريّ الذي تقوده الولايات المتحدة، وأنّ النّشاطاتِ الرّوسيّة في هذا المجال باتت أكثرَ تصعيداً في مباشرتها ومستوى النّشاط وسعة الجهود إذا ما قورنت بنشاطاتها السّابقة.[66]

كما أنّ الخطورة التي تشكّلها أجهزة التّشويش الرّوسيّة على القوات الأمريكيّة المتواجدة في سوريا وذلك نقلاً عن مصادر عسكرية أمريكيّة، وبحسب التّقارير فإنّ القوات الأمريكيّة المنتشرة في سوريا تضطّر بشكل متزايد للدّفاع عن نفسها أمام هجمات السيبرانية الرّوسيّة التي لها عواقب مميتة، وذكر ضباط أمريكيون اختبروا التّشويش المعروف باسم "الحرب السّيبرانيّة": "إنّه لا يقل عن الهجمات التّقليديّة بالقنابل والمدفعيّة، وقد أشار الخبير في قضايا الأمن القوميّ والقضايا العسكريّة في "معهد ليكسينغتون" "دانيال غور" بقوله:"إنّ تطوّرَ أنظمة الحرب السّيبرانيّة الجديدة في روسيا التي يمكن تركيبها على المركبات الكبيرة، أو الطّائرات وبإمكانها التّشويش على أهداف تقع على بعد مئات الأميال"[67]

وكشفت صحيفة الواشنطن بوست عن توسّع عمليّات التّجسس الأمريكيّة على روسيا، مشيرة إلى أنّها وصلت إلى أوسع نطاق لها منذ نهاية الحرب الباردة، والتّجسس الأمريكيّ على روسيا شمل العديد من

---

[66]. الحروب السّيبرانيّة. معارك العالم الافتراضي تنتقل إلى الميدان، لندن – الخليج أونلاين، تاريخ النشر 2018\3\24، متاح على الرابط http://alkhaleejonline.net

[67]. جلال خياط، فورين بولسي تتحدث عن الحرب السّيبرانيّة بين روسيا وأمريكا في سوريا، موقع اورنت نت، تاريخ النشر 2018/7/31. متاح على الرابط https://orient-news.net/ar/news_show

المفاصل الحيويّة، بالإضافة إلى أنظمة الأقمار الصّناعيّة وهو ما أدّى إلى تخصيص ميزانيات كبيرة لهذه الأعمال، وهي المبالغ التي خُصصِت سابقاً لمكافحة الإرهاب وتغطية الحروب الأمريكيّة، وأنّ الأنشطة التّجسسيّة الأمريكيّة التي تمّ إخفاؤها عن الرأي العام تعتبر جزءاً من الصّراع والمنافسة بين الولايات المتّحدة الأمريكيّة وروسيا في أعقاب عقدين من الهدوء، هدوء لن يستمر في أعقاب التوترات المتصاعدة بين البلدين على خليفة العديد من القضايا؛ إذ إنّ الشعورَ بالخشية من النشاط الرّوسيّ بلغ ذروته في أعقاب محاولة موسكو التّأثير على المؤسسات الدّيمقراطيّة في أمريكا، والسّعي الرّوسيّ الذي بدا واضحاً للتأثير في الانتخابات الرئاسيّة في أمريكا، وعلى المستوى العالميّ، تنظر الولايات المتّحدة الأمريكيّة إلى الفضاء السيبرانيّ كحيّز يجب أن تُعمّم فيه معايير ومقاييس سياسيّة وأيديولوجية مختلفة حسب مفهومها[68].

الفرع الثّالث: القدرات الإسرائليّة في الحرب السّيبرانيّة

في أواخر التّسعينيّات نجح خبير في مجال الحواسيب، يعمل في جهاز الأمن الدّاخليّ الإسرائليّ "شين بيت" من خلال تقنيات القرصنة في اقتحام نظام الكمبيوتر الخاص بمستودع "بي جالوت" للوقود شماليّ تل أبيب، كان الهدف إجراء اختبار روتينيّ لتدابير الحماية بالموقع الاستراتيجيّ، لكنّ هذه العمليّة نبّهت الإسرائيليين أيضًا إلى الإمكانيّة التي توفّرها هذه التّسللات عالية التّقنيّة؛ للقيام بأعمال تخريبية حقيقية، وأدركوا حينها إنّه بخلاف الاطلاع على البيانات السّريّة، فإنّهم يستطيعون أيضا تنفيذ تفجيرات متعمّدة بمجرد تغيير برمجة في مسار خطوط الأنابيب".[69]

---

[68]. أمريكا تشنّ أكبر عمليّات تجسس على روسيا منذ الانهيار السوفييتي، صحيفة الواشنطن بوست: ترجمة الخليج اونلاين، تاريخ النشر 2016/9/15، متاح على الرابط http://alkhaleejonline.net

[69]. انظر:

ANALYSIS-Wary of naked force، Israelis eye cyberwar on Iran، Reuters، 07 Jul 2009، at this link:

http://w w w.alertnet.org/thenews/newsdesk/LV83872.htm

ومنذ ذلك الوقت تبلورت الحرب السّيبرانيّة شيئًا فشيئًا لتصبح ركناً رئيساً في التّخطيط الاستراتيجيّ لإسرائيل، وتعتبر الوحدة "8200" في الجيش الإسرائيليّ أكثر الوحدات تطوّراً من النّاحية التّقنيّة والتّكنولوجيّة، ولها نشاطات واسعة في حروب الإنترنيت والشّبكات، وقد انضم إليها الآلاف من العقول الإسرائيليّة منذ إنشائها؛ نظراً لشهرتها الواسعة، حيث تعمل على ضمان التّفوق النّوعيّ لإسرائيل من خلال عمليّات دفاعية أو هجومية في الفضاء السيبرانيّ.[70]

وعلى الرغم من أنّه قد تمّ تصنيف الوحدة "8200" من قبل بعض المؤسسات المعنيّة بأنّها أكبر سادس مُطلِق لهجمات الإنترنيت في العالم، فإنّ هذه الوحدة ليست الوحيدة التي تتمتع بهذه القدرات التّقنيّة العالية في إسرائيل، فهناك العديد من الوحدات الأخرى التي تتمتع بقدرات متطوّرة جداً في مجال تكنولوجيا المعلومات في جميع التّخصصات، ويتمّ استقطاب وتجنيد الأطفال الإسرائيليين من النّخبة حتى قبل إنهائهم دراستهم الثانوية، عندما يبلغ هؤلاء سن خمسة وعشرين عاماً، يكون لديهم أكثر من سبعة أعوام خبرة عمليّة في مجال التّكنولوجيا.[71]

ولا يقتصر الأمر على الجيش الإسرائيلي في توظيف الأدمغة، وبناء قدرات عالية في مجال الحروب السّيبرانيّة، وإنشاء وحدات وقوات نخبة خاصة "كوماندوس" بحروب الإنترنيت، وتكون مهمتها التّعامل مع أصعب وأخطر وأعقد الحالات المُتعلّقة بهذه الحروب؛ وإنّما تدخل الاستخبارات "الشين

---

[70]. انظر:

Israel's unit 8200: cyber warfare ،Telegraph Newspaper ،30 Sep 2010، at this link:
w w w.telegraph.co.uk/news/worldnews/ middleeast/israel/8034882/Israels-unit-8200-cyber-warfare.html

[71]. موقع الجزيرة – مركز الدّراسات، https://studies.aljazeera.net/en/node/1819، مقال بعنوان المجال الخامس.الحرب السّيبرانيّة في القرن الـ21، تاريخ النشر 2011/1/12م، تاريخ المشاهدة 2022/2/20م

بيت" على الخط أيضًا للقيام بنفس المهمة، ويتم الاستفادة في هذا الإطار من العناصر المخضرمة أيضاً ومن المؤسسات التّقنيّة والمعلوماتيّة الإسرائيليّة ومن العاملين فيها كرافد مهم.[72]

وتتّجه أصابع الاتهام إلى إسرائيل فيما يتعلق بفيروس "ستكسنت" اعتماداً على عدد من المؤشرات منها: أوّلاً- توافر القدرات التّقنيّة اللازمة للقيام بمثل ذلك العمل، ثانياً- تعقيدات العمل العسكريّ التقليديّ،وتردد الأمريكيّين في الدّخول بحرب جديدة أو السمّاح لإسرائيل بفعل ذلك.

ثالثاً- توافر سوابق لإسرائيل في هذا المجال، لعلّ أبرزها كما يقول الصحفي في مجلة "جينز ديفنس"، طوني سكينر نقلا عن مصادر إسرائيلية: "إنّ قصف إسرائيل لعام 2007 لمفاعل نوويّ مزعوم في سوريا، كان مسبوقاً بهجوم سيبرانيّ عطّل الرّادارات الأرضيّة، والراجمات المضادة للطيران"،[73] لكنّ الأهم من كل ما تمّ ذكره أعلاه والمثير للاهتمام في نفس الوقت في الموضوع

أولا: أنّ رئيس شعبة المخابرات العسكريّة الإسرائيليّة الميجر جنرال "عاموس يادلين" كان قد كشف العام الماضي في خطوة نادرة أنّ مجالَ الحرب السّيبرانيّة يناسب تماماً عقيدة الدّفاع في إسرائيل، وأنّ القوات الإسرائيليّة أصبح لديها الوسائل الكافية لإطلاق هجمات سيبرانية استباقية من دون أي مساعدات خارجية، وهي تدرس بهدوء استخدام هذه التّقنيّات ضدّ الآخرين بهدف التسلل إلى معلومات أو القيام بتخريب من خلال زرع برامج في أنظمة السّيطرة والتّحكّم في المنشآت الحساسة للأعداء في المنطقة مثل إيران.[74]

ثانيا: توصّلت إسرائيل العام الماضي إلى أنّ نقطةَ ضعف إيران الكبرى إنّما تكمن في معلوماتها المحملة سيبرانيّاً، وهو ما يتيح استهدافها، وعندما سُئل "سكوت بورج"، مدير الوحدة الأمريكيّة

---

[72]. موقع الجزيرة – مركز الدّراسات، https://studies.aljazeera.net/en/node/1819، مقال بعنوان المجال الخامس.الحرب السّيبرانيّة في القرن الـ21، تاريخ النشر 2011/1/12م، تاريخ المشاهدة 2022/2/20م

[73]. المرجع السّابق.

[74]. موقع الجزيرة – مركز الدّراسات، https://studies.aljazeera.net/en/node/1819، مقال بعنوان المجال الخامس. الحرب السّيبرانيّة في القرن الـ21، تاريخ النشر 2011/1/12م، تاريخ المشاهدة 2022/2/20م

لتبعات الإنترنيت: "وهي وحدة استشارية تقدّم خدماتها في مجال الأمن السيبرانيّ لمختلف الوكالات الأمنية الوطنية الأمريكيّة" عن السيناريو الذي يمكن أن تلجأ إليه إسرائيل لاستهداف إيران، أجاب: "إنّه من الممكن استخدام "البرامج الخبيثة؛ لإفساد أو إعطاب أو السّيطرة على أجهزة التّحكّم في المواقع الحساسة، مثل: محطّات تخصيب اليورانيوم، وبما أنّ الأصول النّوويّة لإيران ستكون في الغالب غير متّصلة بالإنترنيت، فلن يتسنى للإسرائيليين زرع الفيروس عبر الإنترنيت وسيكون عليهم تسريبه إلى البرامج التي يستخدمها الإيرانيّون، أو في أجهزة محمولة يدخلها فنيّون دون علم الإيرانيّين، ويكفي توافر أي وحدة تخزين بيانات متنقلة مُلوّثة؛ لإتمام هذه المهمة"، وهو سيناريو شبيه بما حصل مؤخرا في إيران.[75]

ثالثا: يشير " ليام أو مورشو" - وهو من الذين عملوا على تفكيك "ستكسنت" ودراسة وظيفته وقدّم شرحا عمليّا لقدرته التّدميرية الماديّة من خلال تجربته على مضخّة- إلى وجود كلمة مفتاحيّة في شيفرة التعليمات الخاصّة بالبرنامج تحمل الاسم "**Myrtus**"، وهي كلمة مرادفة بالعبرية لكلمة "ايستر" في إشارة إلى ملكة اليهود بفارس -واسمها الحقيقي هاداسا- التي أقنعت زوجها الملك الفارسيّ احشورش بالقضاء على كل من يعادي اليهود ومن بينهم أخلص وزرائه "هامان"،كما يقوم "ستكسنت" عندما يجد هدفه بعرض رقم من ثمّاني خانات 19790509، وهو على الأرجح تاريخ 9 مايو/أيار 1979م، وفقا للأرشيف فإنّ هذا التّاريخ شهد موت "حبيب الغانيان" وهو أول إيرانيّ يهوديّ تم إعدامه في إيران بعد الثّورة الإسلامية بتهمة التّجسس.[76]

---

[75] شبكة فلسطين للحوار، بعد تجربته على سوريا، إسرائيل تتبنى مشروع حرب الإنترنت ضد إيران، 2009/7/19متوفر على الرابط التالي:
https://www.paldf.net/forum/showthread.php?t=449509&s=ac6c06cf5fa7142f25f708ac732409c0تاريخ الزيارة 2023/1/4.

[76]. موقع الجزيرة – مركز الدّراسات، https://studies.aljazeera.net/en/node/1819، مقال بعنوان المجال الخامس. الحرب السّيبرانيّة في القرن الـ21، تاريخ النشر 2011/1/12م، تاريخ المشاهدة 2022/2/20م

وعلى الرغم من كل هذه التخمينات فليس هناك من دليل قاطع على الجهة التي قامت بإطلاق هذا الفيروس أو المستهدف الحقيقيّ، فكل ما هو موجود هو مجرد مؤشرات قد تدّل على هذه الدّولة

الفرع الرّابع: الحرب السّيبرانيّة بين روسيا وأكرانيا

بدأت الخطوة الأولى في الغزو العسكريّ لأوكرانيا في عام 2014م، بعد أن احتلت روسيا شبه جزيرة القرم وضمتها، منذ ذلك الحين كانت الدّولةُ الأوروبية هدفًا للعديد من الهجمات السّيبرانيّة الرّوسيّة المتقدّمة، وقعت إحدى أشهر الهجمات في ديسمبر٢٠١٥م عندما انقطع التّيار الكهربائيّ عن مئتين وخمسة وعشرين ألف شخص في غرب أوكرانيا بعد أن دمّر قراصنة معدات توزيع الطّاقة، مما أدّى إلى تعقيد محاولات استعادة الطّاقة، يتوقع "دميتري ألبيروفيتش" المدير التّنفيذيّ السّابق للأمن السيبرانيّ في **CrowdStrike**، تكثيف الهجمات السّيبرانيّة مرة أخرى إذا حاولت روسيا مهاجمة أوكرانيا مرة أخرى، لكنَّه يتوقع أن تكون مزعجة وليست قاتلة، لكنَّ ما يقلق خبراء الأمن السيبرانيّ حقًا هو أن هذه الهجمات يمكن أن تتوسع لتشكّل تهديدًا للعالم بأسره.[77]

في هذا السّياق، حذرت وكالة الأمن السيبرانيّ وأمن البنية التحتيّة الأمريكيّة **CISA** مشغلي البنية التحتيّة الرّقميّة من خطر الفشل في اتخاذ إجراءات عاجلة وقصيرة المدى؛ لمواجهة التّهديدات السّيبرانيّة، قائلة: "إن الهجومَ الأخير على أوكرانيا هو علامة على اليقظة"، أسباب تهديد محتمل للولايات المتحدة، كما أشارت الوكالة إلى هجومين سيبرانيين، **"NotPetya"** و **"WannaCry"**، يعود تاريخهما إلى عام 2017، خرجا عن السّيطرة وانتشرا بسرعة عبر الإنترنت، مما تسبب في أضرار بمليارات الدولارات في جميع أنحاء العالم.[78]

---

[77]. المرجع السّابق.

[78]. موقع الجزيرة – مركز الدّراسات، https://studies.aljazeera.net/en/node/1819، مقال بعنوان المجال الخامس. الحرب السّيبرانيّة في القرن الـ21، تاريخ النشر 2011/1/12م، تاريخ المشاهدة 2022/2/20م

حدث كلا الهجومين المتخفيين على أنّهما برنامجُ فدية في عام 2017، حيث أصاب هجوم **WannaCry** الأشهر والأقل ضراوة مئتين وخمسة وثلاثين ألف جهاز سيبرانيّ في سبعين دولةً حول العالم، بما في ذلك الخدمات الصّحية في المملكة المتحدة، وخدمات الطّاقة والسياحة في إسبانيا.

آخر ما في هذا الصدّد، علّق جون "هولتكويست" مدير الاستخبارات في شركة الأمن السيبرانيّ **Mandiant**، قائلاً: "العمليّات السّيبرانيّة العدوانية هي أدوات يمكن استخدامها قبل إطلاق الرصاص والصّواريخ. " ولهذا السبب فهي أداة يمكن استخدامها في حالة إزدياد الوضع تدهوراً، وأدوات التّعامل مع الولايات المتحدة وحلفائها، خاصة وأنّ الولاياتِ المتحدة وحلفاءها يتخذون موقفاً أكثر عدوانية تجاه روسيا.[79]

يبدو ذلك ممكنا بشكل متزايد وقد قال الرئيس جو بايدن خلال مؤتمر صحفي في 19 يناير/كانون الثّاني: "إنّ الولايات المتحدة يمكن أن تردّ على الهجمات السّيبرانيّة الرّوسيّة المستقبليّة ضدّ أوكرانيا بقدراتها السّيبرانيّة الخاصّة." ما يزيد من شبح انتشار الصّراع وحتى الدّول العربيّة لن تكون في مأمن من هذا الانتشار، وهو ربما ما دفع الإمارات العربيّة المتحدة لتوقيع اتفاقية مع شركة "مانديانت" نفسها لتحسين الاستجابة للتهديدات السّيبرانيّة.

الفرع الخامس: حرب بلا دماء

المشكلة الأكبر في الهجمات السّيبرانيّة أنّها مُعديةٌ بشكل ما، حيث تتوفر الأكواد البرمجيّة الخبيثة للجميع، ويجري تطويرها باستمرار من قبل مجموعات مختلفة، ويُعاد استخدامُها في هجمات متفاوتة المستوى ومختلفة الأسباب، مما يعني أنّ هجوماً روسيّا على أوكرانيا مثلاً يمكن أن يلهم هجوماً إيرانياً على دولة خليجية فعلى عكس الحروب القديمة لا تعترف الحرب السّيبرانيّة بالحدود، ويمكن أن تخرج عن نطاق السّيطرة بسهولة.

[79]. المرجع السّابق.

على سبيل المثال: وُجّه هجوم "نوت بيتيا **NotPetya**" السيبرانيّ لعام ٢٠١٧م، الذي أمرت به موسكو في البداية إلى الشّركات الخاصّة الأوكرانية قبل أن ينتشر ويدمّر الأنظمة في جميع أنحاء العالم، تنكّر "نوت بيتيا" على أنه برنامجُ فدية، ولكنَّه في الحقيقة كان عبارةً عن كود برمجيّ مدمّر للغاية وشديد الانتشار.

يُظهر منظر شاشة كمبيوتر محمول **R** جزءا من رمز، وهو أحد مكونات فيروس كمبيوتر **Petya** الضارة وفقًا لممثلي شركة الأمن السيبرانيّ الأوكرانية **ISSP**شاشة كمبيوتر محمول تظهر جزءا من رمز، وهو أحد مكونات فيروس كمبيوتر **Petya** الضارة وفقًا لممثلي شركة الأمن السيبرانيّ الأوكرانية **ISSP**.

في نهاية المطاف، تسبب "نوت بيتيا" في عجزٍ بموانئ الشحن، وتَرَك العديد من الشّركات العملاقة متعدّدة الجنسيات والوكالات الحكومية غير قادرة على العمل، ولقد تأثر تقريباً كل شخص قام بأعمال تجاريّة مع أوكرانيا؛ لأنّ الروسَ قاموا سراً بتسميم البرامج التي يستخدمها كل من يدفع الضرائب أو يقوم بأعمال تجاريّة في البلاد. وقد خلُص البيت الأبيض إلى أن الهجوم تسبب في أضرار عالميّة بأكثر من عشرة مليارات دولار، معتبرا إيّاه الهجوم السيبرانيّ الأكثر تدميراً وتكلفة في التّاريخ". [80]

منذ عام 2017، كان هناك جدلا مستمرا حول ما إذا كان الضحايا الدّوليّون مجرد أضرار جانبية غير مقصودة، أو ما إذا كان الهجومُ يستهدف جميع الشّركات التي تتعامل مع أعداء روسيا، لكن ما لم يختلف عليه أحد أنّه مرشحٌ للحدوث مرة أخرى، وهو ما حدث بالفعل في هجوم الّشهر الماضي الذي شُنّ عبر برمجية عُرفت باسم "ويسبر جيت **WhisperGate**"، وكما هو الحال مع سابقه تنكّر "ويسبر جيت" في صورة برنامج فدية، بينما كان يهدف إلى تدمير البيانات الرئيسيّة بشكل يجعل الأجهزة المصابة غير قابلة للتشغيل يقول الخبراء: إنّ "ويسبر جيت" يشبه "نوت بيتيا" في طريقة

[80]. موقع الجزيرة – مركز الدّراسات، https://studies.aljazeera.net/en/node/1819، مقال بعنوان المجال الخامس. الحرب السّيبرانيّة في القرن الـ21، تاريخ النشر 2011/1/12م، تاريخ المشاهدة 2022/2/20م

التّدمير، لكنَّه أقلُّ تدميراً وأقلُّ قدرةً على الانتشار أيضاً، وكما هو معتاد نفت موسكو أيّ صلة لها بالهجوم.

ولكن بصرف النّظر عن إقرار روسيا بالمسؤوليّة من عدمه، يتوقع "هولتكويست" أنّنا سنشهد عمليّات سيبرانية من وكالة الاستخبارات العسكريّة الرّوسيّة **GRU**، وهي المنظّمة التي تقف وراء العديد من عمليّات الاختراق الأكثر عدوانية على الإطلاق، داخل أوكرانيا وخارجها، تُشغل الوكالة الرّوسيّة مجموعة القرصنة الأكثر شهرة عالميّاً، وتُعرف باسم "ساند وورم **Sandworm**"، وهي المسؤولة عن قائمة طويلة من أعظم الضّربات، بما في ذلك اختراق شبكة الطّاقة الأوكرانيّة لعام 2015، واختراق "نوت بيتيا" عام 2017، والتّدخّل في الانتخابات الأميركيّة والفرنسيّة، واختراق حفل افتتاح الألعاب الأولمبية في أعقاب ذلك.[81]

توصّلت الباحثة في هذا الفصل إلى أن الفرق الرئيس بين الحرب السّيبرانيّة والحرب العسكريّة هو في كون الحرب العسكريّة قائمةٌ على الهجوم الماديّ، وإحداث الأضرار الماديّة في قوات العدو؛ أمّا الحرب السّيبرانيّة فهي حرب ليس فيها دماءٌ ولا قتلى؛ إنّما فيها خسائرٌ تكنولوجيّة فقط، بالإضافة إلى أنّ الحربَ السّيبرانيّة قد تطوّرت بشكل هائل ومتسارع،؛ لتنتقل من كونها مجردَ تجسس على خطوط الاتّصالات إلى القيام بهجمات تدمّر البنية التحتيّة التّكنولوجيّة للبلاد المستهدفة، مما يعني أنّ خطرَ هذه الهجمات خطرٌ متفاقمٌ في كل لحظة.

[81]. موقع الجزيرة – مركز الدّراسات، https://studies.aljazeera.net/en/node/1819، مقال بعنوان المجال الخامس. الحرب السّيبرانيّة في القرن الـ21، تاريخ النشر 2011/1/12م، تاريخ المشاهدة 2022/2/20م

الفصل الثّاني

المبحث الأوّل: الحرب السّيبرانيّة والقانون الدّوليّ الإنسانيّ

نصّت المادة (٥١) من ميثاق الأمم المتحدة: "ليس في هذا الميثاق ما يضعف أو ينتقص الحقّ الطّبيعيّ للدول، فرادى أو جماعات، في الدّفاع عن أنفسهم إذا اعتدت قوة مُسلّحة على أحد أعضاء "الأمم المتحدة"، وذلك إلى أن يتخذ مجلس الأمن التّدابير اللازمة لحفظ السِلم والأمن الدّوليّ، والتّدابير التي اتخذها الأعضاء استعمالاً لحق الدّفاع عن النفس تُبلّغ إلى المجلس فوراً، ولا تؤثر تلك التّدابير بأي حال فيما للمجلس - بمقتضى سلطته ومسؤولياته المستمرة من أحكام هذا الميثاق - من الحقّ في أن يتخذ في أي وقت ما يرى ضرورة لاتخاذه من الأعمال لحفظ السِلم والأمن الدّوليّ أو إعادته إلى نصابه".[82]

تنص المادة (١) من اتفاقية لاهاي: "إنّ قوانين الحرب وحقوقها وواجباتها لا تنطبق على الجيش فقط، بل تنطبق أيضاً على أفراد الميليشيات والوحدات المتطوّعة التي تتوفر فيها الشروط التالية:

1- أن يكون على رأسها شخصٌ مسؤولٌ عن مرؤوسيه.

2- أن تكون لها شارةٌ مميزةٌ ثابتةٌ يمكن التّعرّف عليها عن بعد.

3- أن تحمل الأسلحة علناً.

[82] ميثاق الأمم المتّحدة . متوفر على: https://www. un. org/ar/about-us/un-charter/full-text. تمّت الزيارة في 2022/7/26.

4- أن تلتزم في عمليّاتها بقوانين الحرب وأعرافها في البلدان التي تقوم الميليشيات أو الوحدات المتطوّعة فيها مقام الجيش، أو تشكّل جزءاً منه تُدرج في فئة الجيش". [83]

نصّ دليل تالين على قواعد ثلاث، وقد اتفق على هذا الدليل الكثير من الفقهاء المختصين، لدرجة أنّه أصبح تعبيراً لما هو سائد بين فقهاء القانون الدّوليّ الإنسانيّ بخصوص الحرب السّيبرانيّة، وهذا سبب كونه مصدراً احتياطياً ثانياً كما ذُكر.

تشكّل القواعد الثلاث التالية إطاراً عاماً لما للعلاقات الدّوليّة المنظّمة قانوناً أثناء الحرب السّيبرانيّة، وهي تغطي ثلاث محاور رئيسية: الأوّل هو محور الحظر الأصيل ويُقصد بهذا المحور: القاعدة التي تحظر التّهديد أو استخدام القوة السّيبرانيّة؛ تنصّ القاعدة (١٠) من هذا الدليل على ذلك بقولها: "العمليّة السّيبرانيّة التي تتضمن التّهديد أو استخدام القوة ضدّ سلامة الأراضي أو الاستقلال السّياسيّ لأيّ دولة: أي تلك العلمية السّيبرانيّة التي لا تتفق بأي وجه آخر مع مقاصد الأمم المتحدة، تعتبر غير شرعيّة". [84]

إذن يستفاد من هذا النصّ إنّ أيَّ استعمال لأداة سيبرانية بهدف التّهديد أو التّأثير سلباً على سلامة دولة ما أو استقلالها السّياسيّ يتعبر اعتداءً غير شرعيّ، وهذا هو الإطار الضّيق لهذه القاعدة؛ أمّا الإطار الواسع فهو حظر كل استعمال يتنافى مع مقاصد الأمم المتحدة،وهي المنصوص عليها في المادّة (١) من ميثاق الأمم المتحدة وتشمل: "حفظ السِلم والأمن الدّوليّ...، وإنماء العلاقات الودّيّة بين الأمم...، وتحقيق التّعاون الدّوليّ...، وجعل هذه الهيئة مرجعاً لتنسيق أعمال الأمم... "[85]

ثانياً- بعد الحديث عن محور الحظر الأصيل، نكمل الحديث عن المحور الثّاني: وهو محور الدّفاع المشروع وهذا المحور مُتضمَّن في القاعدة (١٣) من الدليل وعنونها: الدّفاع عن النّفس ضدّ هجوم

---

[83] الاتفاقية الخاصّة باحترام قوانين وأعراف الحرب البريّة، المعروفة باتفاقية لاهاي. متوفر على: https://www. icrc. org/ar/doc/resources/documents/misc/62tc8a. htm. تمّت الزيارة في 2022/7/26.

[84] دليل تالين بشأن القانون الدّوليّ المطبق على الحروب السّيبرانيّة، مايكل شميت، 2013، ترجمة علي محمد كاظم الموسوي، 2017. متوفر على: shorturl. at/bGHKV. تمّت الزيارة في 2022/7/26.

[85] ميثاق الأمم المتّحدة . متوفر على: https://www. un. org/ar/about-us/un-charter/full-text. تمّت الزيارة في 2022/7/26.

مسلح؛ تنصّ هذه القاعدة على أنّه: "يجوز للدولة التي تكون هدفاً للعمليّات السّيبرانيّة التي تصل إلى مستوى الهجوم المُسلّح أن تمارس حقها الطّبيعيّ في الدّفاع عن النفس، وتعتبر العمليّة السّيبرانيّة هجوماً مسلحاً بالاعتماد على حجمها وآثارها". [86]

المطلب الأوّل: خضوع الحرب السّيبرانيّة لأحكام القانون الدّوليّ الإنسانيّ

تكمن خصوصية الفضاء الإلكترونيّ في عدم وجود دولة بإمكانها فرض سيطرتها وسيادتها الأحاديّة عليه، واستخدامه بشكل قد يضرّ الإنسانيّة. والاتجاه الدّوليّ في مجال تطبيق القواعد القانونيّة على الفضاء الإلكترونيّ أو الافتراضيّ أو المعلوماتيّ يتجه نحو تطبيق القواعد والمبادئ العامة التّقليديّة المعروفة في القانون الدوليّ العام، وذلك لصعوبة الوصول إلى اتفاق دوليّ جديد خاص ومُلزم للفضاء الإلكتروني، وبعيداً عن المواجهات الأيدلوجيّة فإنّ النّقاشَ الحاليّ سيكون حولَ طبيعة حكم السّلوك الإنسانيّ في الفضاء الإلكترونيّ، والذي يتمحور حول طبيعة القواعد التي ستسود الفضاء الإلكترونيّ، وكيفيّة إنشاء هذه القواعد وتطبيقها في نطاق القانون الدوليّ الإنسانيّ، حيث يُثار الجدلُ الفقهيّ في مدى إمكانية خضوع أو عدم خضوع الحرب الإلكترونيّة إلى أحكام القانون الدّوليّ الإنسانيّ القائم، وعلى هذا النّحو يوجد اتجاهان: الأول- يعدّ أنّ الفضاءَ الإلكترونيّ منطقةٌ بلا قانون، أي: يقرّ بوجود فراغ قانونيّ، بمعنى عدم خضوع الحرب الإلكترونيّة لأي قانون. [87]

الفضاء الإلكترونيّ: هو مكان أو قارة أو فضاء مستقل في حد ذاته عن كل الفضاءات الأخرى، بما فيها فضائنا الماديّ الملموس. وعرّف الفضاء: بأنّه كلُ مكانٍ أو حيّزٍ أو مجالٍ يمكّن من قيام الحياة فيه

---

[86] دليل تالين بشأن القانون الدّوليّ المطبق على الحروب السّيبرانيّة، مايكل شميت، 2013، ترجمة علي محمد كاظم الموسوي، 2017. متوفر على: shorturl. at/bGHKV. تمّت الزيارة في 2022/7/26.

[87]. الاتحاد الدّوليّ للاتصالات والاتحاد العالميّ للعلماء، دعوة إلى الاستقرار الجيوسيبراني، البحث عن السلام السيبرانيّ، ص 89.

بمختلف تشعباتها وعلاقاتها؛[88] لذلك ذهب جانب من الفقه القانونيّ الأوروبيّ والأمريكيّ إلى اعتبار منطقة الفضاء الإلكترونيّ منطقة خالية من القانون وكل شيء فيها مباح، حيث يمكن لأيّ شخص القيام بأنشطة معادية من دون قواعدَ أو ضبط النفس، فقد قيل: "إنّ كلماتِ المرور وألواحَ المفاتيح وأجهزةَ الحواسيب هي التي تُشكّل حدوداً وفواصلَ بين العالمين، ولا بدَّ من الولوج إلى هذا العالم من خلالها، فهذا العالم لا يمكن أن يتحدَد بدولة معينة، وبالتّالي لا يمكن إخضاعه حتى للقانون الدوليّ العام التقليديّ، فهذا القانون لم ينجح حتى الآن بحكم الفضاء البحريّ أو الجويّ الخارجيين؛[89] لذلك فإنّ أنصارَ الاتجاه الحر- وهو مذهب يرفض التعامل القانوني مع الإنترنت، ويتزعمه بعض السياسيين الأمريكيين وعلماء التقنية، وتساندهم فئة قليلة من فقهاء القانون، - يذهبون إلى القول: " إنّ الإنترنت لا يخضع لقانون، وحجتهم أنّ الإنترنت عالمٌ جديدٌ لا يتفق والواقعَ الماديّ التّقليديّ.[90]

وفيما يتعلق بتطبيق أحكام القانون الدّوليّ الإنسانيّ على الحرب الإلكترونية، يرى مؤيدو هذا المذهب أنّه لا يوجد نصّ قانونيّ بأيّ وثيقة من مواثيق القانون الدوليّ الإنسانيّ تعالج الهجوم على شبكات الحاسوب أو تتحدث عن حرب المعلومات أو العمليات المعلوماتيّة، كما لم يتم وضع قواعد للهجوم على شبكات الحاسوب أثناء النّزاعات المُسلّحة، كون أنّ استخدامَ تكنولوجيا الإنترنت هو حديث نسبيّاً، والقانون الدوليّ الإنسانيّ القائم لا يتلاءم مع وسائل وأساليب الحرب الإلكترونية، بالإضافة إلى أنّ المعاهداتِ القائمةِ حالياً يرجع تاريخها إلى ما قبل وجود أو ظهور الهجمات عبر شبكات الحاسوب.[91]

---

[88]. موسى، طالب حسن، أعمر، عمر محمود، 2016، الإنترنت قانونا، مجلة الشريعة والقانون، جامعة الإمارات العربيّة المتّحدة ، العدد السابع والستين، ص.339.

[89] موسى، طالب حسن، أعمر، عمر محمود، 2016، الإنترنت قانونا، مجلة الشريعة والقانون، جامعة الإمارات العربيّة المتّحدة ، العدد السابع والستين، ص.340.

[90]. Lavenue ،J. ،1996 Cyberspace ET Droit International: pour UN nouveau Jus Communications:Revue de la Recherche Juridique–droit prospectif، p. 830–832

[91]. Brown ،D. ،2006 Proposal for an international convention to regulate the use of information System in Armed Conflict، Harvard International Law review، Vol.47، p. 179.

ويؤيد أصحاب هذا الرأي حجتهم من أنّ مصطلحَ الحرب الإلكترونيّة لم ترد في ميثاق الأمم المتحدة واتفاقيات جنيف ولاهاي، ومعاهدة حلف شمال الأطلسيّ، ويستخدم ميثاق الأمم المتحدة ومعاهدة حلف شمال الأطلسيّ على حد سواء مصطلحاتٍ من قبيل "السلامة الإقليميّة"، و"استخدام القوة المُسلّحة"، و"عمل من جانب القوات الجويّة أو البريّة أو البحريّة "و"هجوم مُسلح"، وهي مصطلحات لا تنسجم مع مفهوم الحرب الإلكترونية؛ مما يضعها ظاهرياً خارج نطاق القانون الدوليّ،[92] وكما يظهر فإنّ النّزاعين يستويان بصورة مثيرة؛ النّزاع الإلكترونيّ، والتّشويش المحيط بجهود الرّد النّاجم عن عدم اليقين بشأن قواعد القانون التي من الممكن أن تطبق عليه، فعلى الرغم من جسامة الأضرار الماديّة التي لحقت بالبنية التحتية لهاتين الدّولتين واستمرار الهجمات الإلكترونيّة لعدة أيام إلا أنها لم تعّد بمثابة نزاع مُسلّح [93]،بالإضافة إلى أنّ المادةَ (٥١) من ميثاق الأمم المتحدة بيّنت "أنّه ليس في هذا الميثاق ما يضعف أو ينتقص الحقّ الطبيعيّ للدول فرادى أو جماعات في الدّفاع عن أنفسهم إذا اعتدت قوة مُسلحة على أحد أعضاء الأمم المتحدة، "هذا النّص يُعطي للدولة الحقّ في الدّفاع عن نفسها عندما تواجه هجوماً من قبل قوة مسلحة؛ أمّا في سياق الحرب السيبرانيّة فلا يعّد الهجوم السيبرانيّ نزاعاً مسلحاً؛ لأنّه لا يتضمّن استعمالاً للقوة المُسلّحة ضدّ إقليم الدولة[94]، ولا يوجد في معظم الحالات ما يثبت الأدوار التي قامت بها الدّول في هذه النّزاعات، وقد لا يصل الهجوم الإلكترونيّ من القوة؛ لكي يمكن اعتباره هجوماً مُسلحاً[95] ويُبيّن أصحاب هذا الرأي أنّه وعلى الرغم من أنّ مسمى الحرب يطلق على هجمات

---

[92]. الاتحاد الدّوليّ للاتصالات والاتحاد العالميّ للعلماء، دعوة إلى الاستقرار الجيوسيبراني، البحث عن السلام السيبرانيّ، ص 68.

[93]. جانكارلو أ. بارليتا أ. ووليام. ا وفيتالي تسجيشكو، 2011النّزاع السيبرانيّ والاستقرار الجيوسيبراني، عن الاتحاد الدّوليّ للاتصالات وبرنامج الأمن السيبرانيّ العالميّ، الناشر الاتحاد الدّوليّ للاتصالات والاتحاد العالميّ للعلماء ص51-52.

[94]. توريه، حمدون إ.، 2011، الاستجابة الدّوليّة للحرب السّيبرانيّة، البحث عن الامن السيبرانيّ، الناشر الاتحاد الدّوليّ للاتصالات والاتحاد العالميّ للعلماء، ص.89

[95]. هناك من يدعي أن نصّ المادّة (٢) فقره (٤) من ميثاق الأمم المتّحدة ينطبق فقط على التّهديد أو الاستخدام الفعلي للقوة المُسلّحةStahn :، .C، 2007، "Jus ad bellum"، – "jus in Bello" jus post bellum"?

الكمبيوتر، فهو أيضاً بحاجة إلى نظر كون أنّ الحربَ مفهومٌ يرتكز بالأساس على استخدام الجيوش النّظاميّة، وكان يسبقها إعلان واضح لحالة الحرب وميدان قتال محدد.

أما في هجمات الفضاء الإلكترونيّ العابرة، فإنها غير محددة المجال أو الأهداف كونها تتحرك عبر شبكات المعلومات والاتصال المتعديّة للحدود الدّوليّة، أو اعتمادها على أسلحة الكترونيّة جديدة تلائم السياق التّكنولوجيّ لعصر المعلومات، التي يتم توجيهها ضدّ المنشآت الحيويّة أو وضعها عن طريق العملاء لأجهزة الاستخبارات، وتجعل عملية استخدام هجمات الكمبيوتر من النّاحية السياسيّة في أي صراع أقرب إلى توصيفها بالإرهاب عن كونها حربا، كما أنّ تحديدَ وتعريفَ الأسلحة المعلوماتيّة يثير مشكلة كبيرة في كيفيّة التعامل معها.[96]

ويضيف أصحاب هذا الرأي: إنّ تطبيقَ المبادئ العامة في القانون الدوليّ الإنسانيّ على الفضاء الإلكتروني تبدو غير واقعية؛ لأن وسائل وأساليب الحرب الإلكترونية غير واضحة ومفهومة بشكل كافٍ، ولأنها تتمّ في سرية تامّة ولا يزال فهمُ الاستخدامات المحتملة لهذه التكنولوجيا وأثارها المتمثلة في الصّراع المُسلّح غيرَ جليّ، والتي تختلف جذريّا عن تلك الحرب التقليديّة، وتتسم كذلك هجمات الفضاء الإلكترونيّ بأنّها استباقية ومن دون سابق إنذرا، وأنّها غيرُ محددة المجال أو المدى، وتكون أهدافُها غيرَ مأمونة، بخلاف الحرب التقليديّة التي تكون أهدافها ومكانها محددين وتكون قوات الحرب الإلكترونيّة غيرَ معروفة وليست محددةً في دولة؛ سواء أكانت هدفاً للحرب أم مشاركة فيها، حيث لا تصبح الدولةُ هي الهدف بالضرورة، وتكون الحرب الإلكترونية متعددةَ الأوجه ومتشابكةً مع غيرها، ومن ثمّ تكون تفاعلاتُها كبيرةً فهي تتشابك مع الحرب الإعلاميّة وحرب الشّبكات والاتّصالات، والحرب السّياسيّة والسّيكولوجّية، والحرب التكنولوجية والإرهاب، وبعكس المقاتلين التقليديين، فإنّ

The European Journal of ،"Rrthing the Conception of the Law of Armed Force International of International Law، 175، 923 .p، footnot، 8.

[96]. جوزيف ناي، القوة الناعمة: وسائل النّجاح في السّياسة الدّوليّة، تر: محمد توفيق البجيرمي، ط1، مكتبة العبيكان للنشر، الرياض، 2007، ص20.

المقاتلين السّيبرانيّين ليس لهم مكانٌ ثابتٌ، ولا يحتاجُ المهاجمون" السيبرانيون إلى التواجد في المكان الذي يحدث فيه الهجوم، أو حتى في المكان الذي يظهر أنّ الهجومَ ينشأ فيه.[97]ويمكن للمهاجمين استعمال تكنولوجيا اتصال مجهول الهوية والتّشفير لإخفاء هويتهم.

كما أنّ هناك صعوبةٌ تكمن في تحديد مصدر هذه الهجمات، والتي تتمّ عادة من غير ذكر أسماء، أو من خلال برنامج تسّلل روبوتي آلي، وصعوبة تتبع أصحابها لإسناد المسؤولية إلى دولة من الدول أو منظمه أو فرد، وإيجاد رابطة ما بين تلك العمليات والصّراع المسلّح الذي يُعقّد للغاية تحديد ما إذا كان القانونَ الدوليّ الإنسانيّ ينطبق أم لا على هذا الوضع. [98]

بالإضافة إلى أنّ التّرابطَ بين أنظمة الكمبيوتر المدنيّة والعسكريّة يعقّد تطبيقَ القواعد الأساسية للقانون الدوليّ الإنساني.[99] وحسب هذا الاتجاه يمكن القول: إنّ القانونَ المعمول به حالياً لا يتماشى مع مستجدات العصر؛ لأنّه وُضع أساساً للتعامل مع النزاعات المسلحة التقليديّة، ولا ينطبق على الهجمات الإلكترونية؛لأنّه لا يعّد نزاعاً مسلحاً لغياب الأعمال العدائيّة التقليديّة.

على الرغم من الحجج الورادة ضمن هذا الاتجاه؛ فإنّه لا يمكن التسليم بوجود فراغ قانوني، فعند ظهور الثورة الصناعية الأولى لم يقل أحد بوجوب التّخلي عن القوانين النافذة، وكذلك عند ظهور الطائرة كوسيلة نقل للبضائع والركاب، حيث كانت ظاهرةً لا يربطها أي شيء بالماضي، فهي تفقد اتصالها بالأرض وتكون محلقةً في الجو بين السماء والأرض، وتحليقها يكون في الأجواء الإقليمية وأحيانا فيما وراءها، حيث لا سيادة ولا سيطرة لدولة على هذا الفضاء الخارجي، ومحكمة العدل الدولية في رأيها الاستشاريّ المتعلق بالتهديد باستخدام الأسلحة النووية ذهبت إلى القول: "إنّ "المبادئَ والقواعدَ الإنسانية قد وُضعت قبل اختراع الأسلحة النّوويّة"، ولكن هذا لا يمنع من تطبيق القانون

---

[97]. توريه، حمدون، الفضاء السيبرانيّ وتهديد الحرب السّيبرانيّة، البحث عن السلام السيبرانيّ، المرجع السّابق. ص، 11

[98].نفس المرجع، ص 11

[99]. الحرب السّيبرانيّة تشنّ من خلال الجيش والمجتمع المدني والذي يُشكّل أسلوبا عسكريا غير نمطي لإدارة الصرعات المُسلّحة من خلال اشتراك منظمات غير حكومية وأفراد مدنيين عبر الفضاء السيبرانيّ.

الدوليّ الإنسانيّ عليها، ولا يمكن التّمسك بعدم انطباق القانون الإنسانيّ على هذه الأسلحة بحجة أنها لم تكن معروفةً عند وضع قواعده وهذا ما لا يمنع من تطبيقه على الأسلحة النووية.[100]

المطلب الثاني: خضوع الحرب الإلكترونية لأحكام القانون الدوليّ الإنسانيّ.

يذهب أنصار هذا الاتجاه إلى عدم الاعتراف بوجود فراغ قانوني في الفضاء الافتراضي "**Cyberspace is not a "free zone**" واعتبار القواعد القانونية القائمة كافية لتنظيم الفضاء الإلكتروني، وأنّه يمكن تطبيقها على الفضائيات الحديثة وسميّ هذا الرأي بالمذهب القانونيّ، وأنّه يمكن التعامل مع الإنترنت قانونيا، خاصة وقد سبق أن تمّ تنظيم وسائل اتصال تشبهها مثل: الهاتف والمانتال في فرنسا والفاكس وغيرها من الوسائل الإلكترونية، وما على القانونيين سوى التعاون مع التقنيّين وخاصة أنّ العديد من النّصوص القانونيّة الموجودة قابلةٌ للتّطبيق عليها.[101] وبهذا الخصوص بيّن المستشار القانوني للجنة الدّوليّة للصليب الأحمر **Droege Cordula** أن الإطارَ القانونيّ الدّوليّ الإنسانيّ القائم يُطَبق على النّزاعات" السيبرانية "ويجب احترامه، وقد تمّ تفنيد مزاعم مَن يعّدون خلوّ الفضاء الإلكتروني من القوانين، وعدم انطباق القانون الدوليّ الإنسانيّ على الحرب الإلكترونية بقولهم: "إنّ هذه ليست المرة الأولى التي يحدث فيها تطويراً وتغييراً في التكنولوجيا المستخدمة، وقد تعامل معها القانون الدوليّ الإنسانيّ أو قانون النّزاعات المسلحة، بمعنى أنّ القانون القائم قادر على التعامل مع هذه التطورات الجديدة دون الحاجة إلى إشعار أو وضع قواعد قانونية خاصة بالفضاء الإلكتروني[102] وأما القول:" إنّ الميثاقَ قد اشترط استخدام القوة وعدم اعتبار الهجوم السيبرانيّ نزاعاً مسلحاً؛ لأنّه لا يتضمن استعمالا للقوة المسلحة، فميثاق الأمم المتحدة في المادة 2 فقرة 4 حظر على الدول اللجوء إلى الحرب، أو التهديد باستعمال القوة أو استخدامها ضد سلامة الأراضي، أو الاستقلال

---

[100]. حمودي، ناصر، 2012، العقد الدّوليّ السيبرانيّ المبرم عبر الإنترنت، بدون دار نشر، ص. 54.

[101]. علوان، عبد الكريم، 2006، الوسيط في القانون الدّوليّ العام، دار الثقافة، عمّان، ص34

[102]. عبّاس بدران، الحروب السّيبرانيّة: الاشتباك في عالم متغير، مركز دراسات الحكومة السّيبرانيّة، بيروت، 2010، ص 4. متاح على الرابط الآتي: http://najishukri.wordpress.com/cyberwarbook.

السياسيّ لأي دولة أو على أي وجه آخر لا يتفق ومقاصدَ الأمم المتحدة، لكن الميثاق ترك تحديد المعنى الحقيقي لهذه القاعدة القانونية لمجلس الأمن الذي يقررها تبعاً للظروف المحيطة بكل حالة على حدة، وهذا واضح من نص المادة 39 من الميثاق التي تمنح مجلس الأمن سلطة تقرير الإجراءات القهرية، حيث إنّ هذا النص ورد بصورة غير ملزمة وذلك بسبب تمتع مجلس الأمن بصلاحيات تقرير ما إذا وقع تهديد للأمن والسِلم الدوليين، أو إخلال به أو كان قد وقع عمل من أعمال العدوان[103]، وقد يلجأ مجلس الأمن إلى اتخاذ هذه الإجراءات بصرف النظر عن نص المادة 2 فقرة 4 في حال رأى المجلس -في موقف معين- تهديدا للسلم، وذلك لعدم مخالفة هذا الإجراء لأحكام الميثاق أو لقواعد ومبادى القانون الدولي[104]، كل هذا يعني أنّ الفقرة الرابعة من المادة الثانية من ميثاق الأمم المتحدة والمواد ذات الصلة من الميثاق تنطبق على الهجمات الإلكترونية، بغض النظر عن نوع الأسلحة المستخدمة، ويعّد ذلك استخداما للقوة بالمعنى المقصود في المادة 2/4 من الميثاق، وفي حال العمليات الإلكترونية ضدّ دولة فعلى مجلس الأمن التابع للأمم المتحدة أن يحدد إذا كانت الهجمة الإلكترونية تشكّل تهديداً للسِلم أو خرقاً له أو عملاً من أعمال العدوان، ويجوز له أن يأذن بأخذ التدابير غير القسريّة بما في ذلك العمليات الإلكترونية، وإذا كانت هذه التدابير غيرَ كافية فله أن يُصدر قرارا بالتدابير القسريّة بما في ذلك العمليات الإلكترونيّة، ويجوز لأي دولة أن ترد على هجوم مسلح ناجم عن أنشطة شبكة الإنترنت، أو تهديد وشيك به، من خلال ممارسة حق الدفاع عن النفس المنصوص عليه في المادة (٥١) من الميثاق وباستخدامها وسائل إلكترونية أو تقليديّة، كما فعلت الولايات المتحدة في استراتيجيتها الدوليّة للفضاء السيبرانيّ لعام 2011[105]، خاصة وأنّ المادة (٥١) من ميثاق الأمم المتحدة لا تشير إلى استخدام نوع محدد من الأسلحة في الرد على الهجمات التي تتعرض لها لدول؛ مما يعني أن نوع

---

[103]. الفتلاوي، احمد عبيس نعمة، الهجمات السّيبرانيّة، المرجع السّابق. ص.49

[104]. علوان، عبد الكريم، 2006، الوسيط في القانون الدّوليّ العام، دار الثقافة، عمّان، ص 34.

[105]. See e.g., Schmitt, M., 1999، Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework، 37 COLUM. J. TRANSNAT'L L. 885، 913

السلاح المستخدم في الهجمات ليس له تأثير في نفي استخدام القوة، وأنّ ما يعتد به هو الأثار المادية لهذا السلاح على أرض الواقع فالهجوم" السيبرانيّ "يعّد استخدما للقوة تِبعًا لنتائجه المادية ويشكّل تهديداً للأمن والسِلم الدوليّين، ويعطي الحقّ للدولة التي تعرضت للهجوم بأن تطلب التعاون من دول أخرى لمواجهة هذه الهجمة.

لقد أجمع الفقه الدوليّ على أن الحرب الإلكترونية تعّد حرباً بالمعنى الصحيح عندما تكون أثارها على العالم الماديّ أثاراً مدمرة[106]، وإنّ استخدام القوة من خلال هذه الآليّة الحديثة ضد دولة يُشكّل حقّاً وطنيّاً للدولة المعتدى عليها للدفاع عن نفسها. [107]

وفي قضية "نيكا راغوا" ضدّ الولايات المتحدة الأمريكيّة، والمتعلقة بالأنشطة العسكريّة وشبه العسكرية في عام1986، بينت محكمة العدل الدولية أن المادة (٥١) لا تشير إلى أسلحة محددة وأنّ مفهومَ الأسلحة ينطبق على أي استخدام للقوة،[108]وبغض النظر عن حقيقة أن الهجماتَ السّيبرانيّة "لا تستخدم الأسلحة الحركية التقليديّة، فإن ذلك لا يعني بالضرورة أنّها لا يمكن أن تكون مسلحةً، ويمكن اعتبار استخدام أي جهاز ينتج عنه خسائر كبيرة في الأرواح أو تدمير واسع للممتلكات مستوفٍ لشروط الهجوم المسلح"، ويدعم هذا الاستنتاج تأكيد مجلس الأمن على ذلك الحقّ في الدفاع عن النفس رداً على هجمات 11 سبتمبر 2001 على الولايات المتحدة[109]

وهناك من حاول تحديد مفهوم الهجوم المسلح: بأنّه فعل أو بداية سلسلة من أعمال القوة المسلحة ذات الحجم الكبير، التي تؤدي إلى إلحاق دمار كبير في الركائز الأساسية داخل الدولة، ويؤثر على شعبها

---

[106]. وضع مايكل سميث عدة معايير لاعتبار العمليّات السّيبرانيّة بمثابة استخدام للقوة ومنها شدة الإصابة والفورية وتقييم الأثار وتورط الدولة والقرينة القانونيّةSchmitt :، .M، 2012، .Classification of Cyber Conflict Journal of Conflict & Security Law، 172، 260–P. 245

[107]. شميت، مايكل ن.، 2002 الحرب بواسطة شبكات الاتّصال: الهجوم على شبكات الكمبيوتر الحاسوب والقانون في الحرب، المجلة الدّوليّة للصليب الأحمر، ص87.

[108]. ICJ Reports 1986، see note 64، 176 para. 94

[109]. Roscini، .M، World Wide Warfare –Jus ad bellum and Use of Cyber Force، p. Cit. p. 115

والبنية الاقتصادية والأمنية الطبيعية الخاصة بها، ويُفقد الدولة جزءاً من سلطتها الإقليمية أي الاستقلالية الكاملة، كما أنّ استخدامَ الهجمات الإلكترونية بهدف التأثير على الموراد الصناعيّة والاقتصاديّة الرئيسية للدولة، قد تصل إلى هجمات مسلّحة إذا كانت واسعة النطاق وتسببت بفقدان السيطرة على أنظمة التحكّم التي تمر عبر أجهزة الحواسيب، مثل: انقطاع التيار الكهربائيّ، وإغلاق أجهزة الكمبيوتر التي تتحكم في محطات المياه والسدود التي ينتج عنها الفيضانات في المناطق المأهولة بالسكان، وكذلك الحوادث الهندسيّة المميتة والمتعمدة، مثل:المعلومات الخاطئة التي تغذيها أجهزة الكمبيوتر للطائرات" و "انهيار في محطات الطاقة النووية وانطلاق المواد المشعة في المناطق ذات الكثافة السكانية العالية"، وقد اعتبر أن الهجمات الإلكترونية الخطرة تمثّل هجوماً مسلّحاً، حتى ولو لم يكن هناك إصابات، وحالها حال الهجمات التقليدية التي لا ينتج عنها إصابات أو خسائر في الممتلكات،هذا استنتاج مختلف فيما يتعلق بالهجمات "السّيبرانيّة" ضدّ النظم المدنيّة.

كما يعطي دليل تالين الحقَّ للدولة التي تتعرض لهجوم الكتروني شن حرب هجومية الكترونية مضادة على الدولة الأخرى، كما ذكر دليل تالين إنّه يمكن استخدامُ القوة العسكريّة الحقيقية في حالة تم شنّ هجوم إلكتروني على دولة وأدّى هذا الهجوم لخسائر بالأرواح البشريّة.[110]

اللجنة الدولية التابعة لحلف شمال الأطلسيّ والمكونة من خبراء قانونيين وعسكريين نشرت في عام 2013 ما يعرف" بدليل تالين " الذي يشير إلى إمكانية تطبيق القانون الدوليّ الإنسانيّ كما هو على الحرب الإلكترونية،" ويتمسك هذا الدليل بالتقسيم التقليديّ للنازعات المسلحة الدولية والنّزاعات المسلّحة غير الدولية، ويقرّ بأن العملياتِ الإلكترونيّة وحدها قد تشكّل نزاعاتٍ مسلّحة تبعا للظروف، وقد اعتبر الهجوم الإلكتروني بمثابة استخدام للقوة إذا كان أثر هذا الهجوم عند مقارنته بالاستخدام الفعليّ للقوة مساوياً له، أو قريباً منه[111]"، ففي هذه الحالة يجب إخضاع هذا النوع من الهجمات لقانون النّزاعات المسلحة، بحيث يتم إخضاع أطراف النّزاع للاتفاقيات الدوليّة التي تنظم هذه النّزاعات،

[110]. الفصل 14 من دليل تالين.

[111]. المادّة ٦٩ من دليل تالين

لاسيما الآثار المدمرة لتلك العمليات،[112] ويقدم الدّليل في هذا الصدد تعريفاً للهجوم السيبرانيّ "بموجب القانون الدولي الإنسانيّ: بوصفه عملية الكترونيّة سواء هجوميّة أو دفاعيّة يتوقع أن تتسبب في إصابة أو قتل أشخاص أو الأضرار بأعيان أو تدميرها، كما يعّد توقف أحد الأعيان عن العمل قد يشكّل ضرر ماديا[113]"، وتتمثل وجهة نظر اللجنة الدولية في أنّه إذا تعطّل أحد الأعيان فليس من المهم كيفيةُ حدوث ذلك، سواء بوسائل حركية أو عملية الكترونية، وهذه القضيّة مهمة للغاية في الممارسة العمليّة، حيث إنّ أيّ عملية إلكترونية تستهدف تعطيل شبكة مدنيّة خلاف ذلك لن يشملها الحظر الذي يفرضه القانون الدولي. [114]

إن غيابَ أيُّ إشارات في القانون الدوليّ الإنسانيّ على الاستهداف المباشر للأشخاص المدنيين والأعيان المدنيّة للعمليات التي تدور في الفضاء الإلكترونيّ، لا يعني أن قواعد القانون الدوليّ الإنسانيّ لا تغطي وسائل وأساليب الحرب الإلكترونيّة ما دامت هذه الوسائل تنتج نفس الآثار التي يمكن أن ينتج عن الأسلحة التقليديّة من دمار وانقطاع الخدمات الحيوية والضرر، أو الإصابة أو الوفاة. ويخضع استخدام هذه الوسائل لنفس قواعد الأسلحة التقليدية، باعتبار أنّ القانونَ الدوليّ الإنسانيّ واسع بما فيه الكفاية لاحتضان التقدم الحاصل في التكنولوجيا، بالإضافة إلى أنّه يمكن الرجوع إلى شرط "مارتينز" كأساس لتفسير معاهدات القانون الدوليّ الإنسانيّ، كلما وجدت الشكوك حول معنى بعض الأحكام الورادة فيها، واستنادًا إلى هذه القاعدة فإنّ كلَ ما يقع أثناء المنازعات يخضع لمبادئ القانون الدوليّ الإنسانيّ، مما يعني عدم خلوّ الهجوم على شبكات الحاسوب من القانون أثناء النّزاع المسلح ويوضّح الرّأي الاستشاري لمحكمة العدل الدولية في مشروعية التهديد بالأسلحة النووية أو استخدامها، أنّ المادة (٤٢) والمادة (٥٢) من ميثاق الأمم المتحدة تحظر استخدام القوة بغض النظر عن الأسلحة المستخدمة، فالمبادئ والقواعد الإنسانية قد وُضعت قبل الأسلحة النوويّة،

---

[112]. المادّة 80 من دليل تالين.

[113]. المادة 92من دليل تالين

[114]. Decision on the Defence motion for interlocutory appeal، paras. 120، 124

ومع ذلك فإنّه لا يوجد شك بانطباق القانون الدولي الإنساني على الأسلحة النوويّة، وليس هناك ما يدعو للتمييز بين الأسلحة النووية وأسلحة الحاسوب، من حيث الزمن الذي استحدثت فيه؛ مما يعني إمكانية تطبيق القانون الدولي الإنساني عليها.[115] إنّ البروتوكول الإضافيّ الأول لعام 1977 الملحق إلى اتفاقية جنيف المؤرخة في 12 آب 1949 ينصّ في المادة (٣٦) تحت بند الأسلحة الجديدة، أنّه عند دراسة أو تطوير أو اقتناء سلاح جديد أو أداة للحرب أو اتباع أسلوب للحرب، لا بدّ من التّحقق مما إذا كان ذلك محظوراً في جميع الأحوال أو في بعضها بمقتضى هذا اللحق " أي: البروتوكول " أو أيّة قاعدة أخرى من قواعد القانون الدولي التي يلتزم بها الطرف السامي المتعاقد وهذا النّص يدل على قابلية القانون الدولي الإنساني على أن يطبق على الحرب الفضائية.

فيما يتعلق باعتبار أنّ الهجوم على شبكات الحاسوب ليس نزاعاً مسلحاً لغياب الأعمال العدائية التقليدية، ولأن وجود النّزاع المسلح هو شرط لتطبيق القانون الدولي الإنساني، لم يتبن القانون الدولي الإنساني تعريفاً موحداً لفكرة النّزاع المسلح، وانّما فرق فقط بين النّزاعات المسلحة الدولية والداخلية، فقد نصت المادة الثانية المشتركة من اتفاقية جنيف لعام 1949، بانطباق هذه الاتفاقية بغض النظر عن الشروط المحددة التي تتعلق بوقت السلم على جميع حالات الحرب المعلنة، أو أي نزاع مسلح أخر ينشب بين طرفين أو أكثر من الأطراف السّامية المتعاقدة، حتى لو لم يعترف أحدها بحالة الحرب، وأصبحت الحرب المعلنة شكلاً من أشكال النّزاعات المسلحة[116]. الفهم الموضوعيّ لهذه المادة أخذ بالحالة الواقعية للحرب؛ لكي يطبق عليها قانون النّزاعات المسلحة بصرف النظر عن أي معيار شكليّ أخر يفرض متطلبات إضافيّة.[117]

---

[115]. لطفي لمين بلفرد، "الفضاء السيبرانيّ: هندسة وفواعل"، المجلة الجزائرية للدراسات السّياسيّة، ENSSP، العدد الخامس، الجزائر، 2016، ص ص 148-150.

[116]. للمزيد من المعلومات انظر. العنبكي، نزار، تصنيف النّزاعات المُسلّحة، ورقة عمل قدمت لمؤتمر التطبيق الأمين للقانون الدّوليّ الإنسانيّ وذلك بتاريخ 6-7 نيسان 2016 في جامعة العلوم التّطبيقيّة الخاصّة / قصر المؤتمرات

[117]. هينين ويجنر، مفهوم بشأن السلام السيبرانيّ، البحث عن السلام السيبرانيّ، البحث عن السلام السيبرانيّ، الناشر الاتحاد الدّوليّ للاتصالات والاتحاد العالميّ للعلماء، ص.7

ويرى بعض الفقهاء أن النّزاع يكون دولياً في حالة اللجوء إلى العنف المسلح بين دولتين أو أكثر سواء كان ذلك بإعلان سابق للحرب أو بدونه، ويفرض على الأطراف المتحاربة تطبيق القانون الدوليّ الإنسانيّ، سواءً أعترفت بقيام النّزاع أم لم تعترف به، وهذا ما عبّر عنه البعض أيضا بقولهم: "إنّ النّزاع المسلح الدولي هو نزاع مسلح بين دولتين أو أكثر" ونفس الحال عندما تقوم بعض الجهات الفاعلة من غير الدول التي تكون تحت" سيطرة شاملة لدولة أخرى بهجوم مسلح ضدّ دولة أخرى من داخل أو خارج أراضي الدولة الأخيرة، سواءً تمّ إعلان الحرب أم لم تُعلن والمحكمة الجنائية الدولية الخاصة ليوغوسلافيا سابقا، وفي حكمها في قضية" تاديتش "قضت، بأنّ النّزاع المسلح يكون دولياً إذا وقع بين دولتين أو أكثر وكذلك يمتد ليشمل حالة النّزاع المسلح غير الدوليّ إذا تدخلت دولة أخرى بقوة عسكرية، أو إذا كانت مشاركةً لأحد الفصائل المحلية المتنازعة تدخلاً بالنيابة عن دولة أخرى، حيث أصبحت النّزاعاتِ المسلحة الداخلية ذات الطابع الدوليّ السمة الغالبة على النّزاعات في الوقت الحاليّ.[118]

إنّ الهجوم على شبكات الحاسوب إن لم يحدث في سياق النّزاع المُسلّح وكانت آثره لا تصل إلى نفس تأثير الهجوم العسكريّ الفعليّة لا ينطبق عليه القانون الدّوليّ الإنسانيّ، هل يخضع لقوانين الجنائيّة في الوطنية؟ بحث حسب هذا الرأي بيّن أنّ القانون الدّوليّ الإنسانيّ ينطبق على الحرب الإلكترونيّة على الرغم من عدم استخدام القوات المُسلّحة التّقليديّة، وذلك عندما ينصّب الفعل على دولة وكانت نتائجُ هذا الهجوم على درجة عالية من الخطورة؛ بمعنى الأخذ بالنّتائج الماديّة على أرض الواقع وليس بالأفعال العنيفة، مثل: الأعمال التي الذي قد تستهدف التّحكّم في مركز الحاسوب والشّبكات الوطنية لتوليد الطّاقة ومحولات الكهرباء وامتلاك الأسلحة النّوويّة الذي جعلها تدمّر نفسها من النّاحية العمليّة؛ وذلك للتحكم في حركه الملاحة الجويّة مما يؤدي إلى تصادم الطّائرات.

[118]. المرجع السّابق.

المطلب الثّالث: الحرب السّيبرانيّة والصّراع الدّوليّ

خلال العقود الأخيرة من القرن العشرين دخلت أدوات وتقنيّات التّكنولوجيا إلى ساحات الصّراع المتعدّدة، التي تشكّل في نظر البعض امتداداً للحرب السّيبرانيّة، وكذلك استخدام التّكنولوجيا أدّى إلى التغيير في شكل الصّراع الدّوليّ، التي تطوّرت واتسعت مع نهاية الحرب العالميّة الثّانية، وخاصة خلال فترة ما سميّ الحرب الباردة، ومع بداية القرن الحادي والعشرين أصبحت الشّبكة أساسيّة في أغلب الاتّصالات والتّعاملات وأجهزة التّحكّم، وبالإضافة إلى أنّها شكلت وسيلة تجسس للبعض، كما تحولت إلى أداة للحرب بمختلف صورها، وعليه فقد تمّ تقسيم هذا المبحث على وفق الشكل الآتي.

الفرع الأوّل: التّحوّلات في الصّراع الدّوليّ

شكلت ثورة المعلومات متغيراً اكتسب أهميّة قصوى في عالم ما بعد الحرب الباردة، وقد وصفت هذه الثّورة المعلوماتيّة بالموجة التّطوّرية الثّالثة، انطلاقا من كونها قادت إلى إدخال المجتمعات الإنسانيّة في حيز تطوّر قائم على محورية المعرفة والمعلومات، إذ يعيش العالم مرحلة متطوّرة من التقدّم المعلوماتيّ من حيث ثورة المعلومات الشاملة، وثورة وسائل الاتّصال الحديثة التي بلغت الأقمار الصّناعيّة، وثورة الحاسبات السّيبرانيّة التي امتزجت مع وسائل الاتّصال والثّورة المعرفية الشاملة، باندماج الحاسبات السّيبرانيّة مع التلفزيون والاتّصالات السّلكيّة واللاسلكيّة، وسطوة المعلومات كمتغير دوليّ بعد الحرب الباردة[119].

وفي كل مرحلة من مراحل تطوّر النّظام الدّوليّ تهيمن على طبيعة تلك المرحلة ما تحمله من أفكار وتوجّهات لتشكّل النّمط السائد لما تتصف به تلك المرحلة، وهذه الطبيعة المتغيرة عبر العصور هي أساس توجيه شكل العلاقات والأعمال، ومنها: العلاقات الدّوليّة في ذلك العصر. فالعصور الوسطى شهدت هيمنة فكرة الدين ثمّ جاء عصر التنوير؛ ليشهد هيمنة العقل جاءت فيما بعد مرحلة القرنين

[119]. وليد غسان سعيد جلعوط، دور الحروب السّيبرانيّة في الصّراع العربيّ الإسرائيلي، رسالة ماجستير غير منشورة، جامعة النّجاح الوطنية، فلسطين، 2013، ص75.

التّاسع عشر والعشرين؛ لتشهد هيمنة النزعة القوميّة، إلى أن وصلنا إلى ألالفية الثّالثة، لتهيمن عليها فكرة العلم والتّكنولوجيا[120].

لذلك برزت خصخصة العنف وهو مصطلح صاغة "جوزيف.سي. ناي" ويعدُّ من أهم الملامح التي أدّت إلى زيادة الحروب الأهليّة من خلال ما يمكن تسُميتة "دمقرطة التكنلوجيا": بمعنى سابقاَ كان يتطلب قيام رئيس دولة هتلر وستالين جهاز حكومة شموليّة لشنّ الحرب، إلّا إنّه أصبح من السّهل تصوّر قيام شبكات مُسلّحة وتنظيمات؛ للقيام بشنّ كثير من الهجمات بدون أجهزة الحكومات ويرجع ذلك إلى أنّ أدواتِ التّدمير أصغرُ وأرخص وأسهل إتاحةً؛ للوصول إلى سلسة من الافراد والشّبكات والتنظيمات المُسلّحة أوسع بكثير من ذي قبل، وبينما كانت القنابلُ وأجهزةُ توقيتاتها ثقيلةً وغاليةً الثمّن، فإنّ المتفجراتِ البلاستيكية وأجهزةَ توقيتاتها الرّقميّة غدت رخيصةً وخفيفةً[121].

وقد تطوّرت أجيال الحروب بما تحتويه من مجالاتٍ وقدراتٍ وأسلحةٍ ومعداتٍ وتكتيكاتٍ، فتعاظمت مع هذا التّطوّر خسائره بالقدر نفسه لتعاظم مكاسبه، فوجد العديد من المشكلات التي واجهها بعد انتهاء حربه وقهر أعدائه، فعلى الرغم من كونه قد خرج منتصراً انتصاراً حربياً وقد هزم أعداءه واستولى على خيراتهم، إلّا أنّه اكتشف بعد إعادة حساباته بعد انتهاء القتال، أنّه قد مُني بخسائر اقتصادية وبشرية فادحة، وقد نتجت عن حربه –على الرغم من كونه منتصراً- مشكلات متعدّدة ومتنوّعة، اجتماعيّة ونفسيّة وفكريّة وبيئيّة، ففكّر في وسائل أخرى لهزيمة أعدائه ونيل جميع مطامعه، من دون تكبد خسائر الحروب التّقليديّة أو دفع تكلفتها العالية، فابتكر الجيل جديد من الحروب بتطوراته كافة، لقد ساعد التّطوّر التّكنولوجيّ في تطوير أدوات الحروب الحديثة بتسارع بنحو يتعين على الجيوش الحديثة أن تلاحقه، وهذا كان سبب تطور أساليب الصّراع فيما يسمى بالجيل الأوّل للحرب، ثمّ الجيل

---

[120]. كمال مساعد، الحرب الافتراضية وسيناريوهات محاكاة الواقع، مجلة الجيش اللبناني، العدد253، 2006، متاح على الرابط https://www.leparmy.gov.lb/artical.asp

[121]. غادة محمد عامر، تطوّر الصّراع الدّوليّ وفق التقدّم التّكنولوجيّ وظهور الحروب اللامتماثلة الحروب غير النمطية، مركز البيان للدراسات والتخطيط، بغداد، 2014، ص8.

الثّاني ثمّ الجيل الثّالث، ومع القفزة التّكنولوجيّة الهائلة التي ظهر تأثيرها على العلاقات الدّوليّة وعلى رأسها بالطبع أدوات الصّراع العسكريّ، ظهرت فكرة الجيل الرّابع للحرب -التي كانت بعد ذلك جزءا من الحروب اللامتماثلة غير النمطية- في الجيش الأمريكيّ باعتباره أكثر جيوش العالم امتلاكاً للتكنولوجيا الحديثة والفائقة[122].

الفرع الثّاني: أثر الحروب السّيبرانيّة في الصّراع الدّوليّ

إنّ تصاعد شبح الحرب النّوويّة دفع بالدول المالكة لهذا السّلاح بالتفكير بوسائل صراع تستثني المواجهة المباشرة، هذا بالضّبط ما شهده العالم خلال الحرب الباردة التي أمتدت خمسة وأربعين عاماً، وقد ظهرت خلال تلك الفترة مصطلحات عدة، "كالحرب بالوكالة" "والحرب الاقتصاديّة" "والحرب السّيبرانيّة" وغيرها، فضلاً عن ذلك فإنّ عدم اللجوء إلى استخدام السّلاح النّوويّ لا يعني بأي شكل من الأشكال توقّف الدّول عن التفكير بوسائل جديدة للمواجهة، وآخر هذه الوسائل هو التركيز الكبير على تكنولوجيا الحرب السّيبرانيّة التي تعد أهم و أحدث تطوّر في عالم النّزاعات والتّنافس الدّوليّ، هذه الحرب تعتمد بشكل أساسيّ على مدى التّطوّر التّكنولوجيّ العسكريّ للدول المعنية، ولا يمكن لدولة تفتقر لهذه الإمكانيات أن تتمرّس فيها، كما أنّ وسائل الحرب السّيبرانيّة تتمايز حتى فيما بينها، فبعضها دفاعيّ يستخدم لصدّ الهجمات السّيبرانيّة المعادية، وإبطال الصّواريخ المعادية وتعطيلها وبعضها الآخر هجوميّ يعتمد على السّيطرة والضبط، الوسيلة الثّالثة تندرج في مجال الأقمار الصّناعيّة، وأنظمة الملاحة وأجهزة الرّصد والإنذار المُبكّر[123].

وعلى المستوى العالميّ، تنظر الولايات المتحدة للفضاء السيبرانيّ كحيز يجب أن تُعمّم فيه معايير ومقاييس سياسيّة وأيديولوجية مختلفة حسب مفهومها، وفي ربيع عام2010 تمّ إنشاء مؤسسة تابعة

---

[122]. غادة محمد عامر، تطوّر الصّراع الدّوليّ وفق التقدّم التّكنولوجيّ وظهور الحروب اللامتماثلة الحروب غير النمطية، مركز البيان للدراسات والتخطيط، بغداد، 2014، ص8.

[123]. الحرب السّيبرانيّة في مستقبل الصّراع الدّوليّ، موقع ارتي عربية، تاريخ النشر 10/3/ 2017. متاح على الرابط https://arabic.rt.com/world/902434

"للبنتاغون"، وهي القيادة السّيبرانيّة وفي عام2010 أعلنت وزارة الدّفاع أنّها شرعت بالتّحكّم بالشّبكات الاجتماعيّة من أجل تحسين الصورة، وللتّأثير على الدول الأخرى، وقد أشارت مديرة وكالة الدّفاع الأميركية للتقنيات الواعدة "ريغينا دوغان": "أن جهوداً إضافيّة ستبذل لإنشاء سلاح سيبرانيّ هجوميّ يُشكّل عنصراً جوهرياً في الآلة العسكريّة، مع ضرورة معرفة الإمكانات السّيبرانيّة للدول الأخرى، بهدف التّحصن ضدّها، وهذا يعني أن الولايات المتحدة نفسها تمارس التّجسس السيبرانيّ"[124].

ختاماً يمكن القول إنّ مزايا الحروب السّيبرانيّة التي تفوق مزايا الدّفاع، ستدفع العالم إلى مزيد من الصّراعات، وخاصة مع تطور آليات الهجوم السيبرانيّ بشكل متسارع؛ مما يضفي عليها مزايا إضافيّة في المراحل المختلفة لهذه التّطوّرات، فغياب الأطر القانونيّة الدّوليّة الرّادعة في الحروب السّيبرانيّة وانتقاء القيود الشّرعيّة الدّوليّة كنتيجة لعدم إمكانيّة التّعرّف على هوية المهاجم على عكس الهجوم التقليدي، كل هذه العوامل تجعل من الفضاء السيبرانيّ ساحة جاذبية للقوى الكبرى لا لإدارة صراعاتها مع بعضها بعضاً، فاستبدال الحرب العسكريّة بتلك السّيبرانيّة وانتقال الصّراع ما بين القوى الكبرى من المساحات التّقليديّة إلى الفضاء السيبرانيّ، قد يسمح للقوى الدّوليّة الدّخول في مواجهات سيبرانية"

خلصت الباحثة في هذا المبحث إلى أن الحرب السّيبرانيّة ستكون محوراً من محاور الصّراع الدّوليّ وليست مجرد حادث جانبيّ مرافق للهجمات العسكريّة التّقليديّة؛ مما يعني أن الاستقرار الدّوليّ والأمن بين الدول سيكون متوقّفاً على قدرتها على كبح الهجمات السّيبرانيّة، بالإضافة إلى أن آثار الحرب السّيبرانيّة أشد فتكاً في بعض القطاعات من الحروب التّقليديّة العسكريّة، مثل قاطع الخدمات التّكنولوجيّة والاتّصالات وأنظمة الأمان والسجلات السّيبرانيّة المدنيّة. كل ذلك يتطلب أن تكون

[124]. نقلاً عن: عمر حرز الله، الحرب السّيبرانيّة: صراع في العالم الافتراضي، صحيفة البيان، تاريخ النشر 4/ 3 /2012. متاح على الرابط https://www.albayan.ae/five-senses/mirrors/2012-03-04 –

الهجمات السّيبرانيّة خاضعة ً لأحكام القانون الدّوليّ الإنسانيّ؛ حتى ترتدع الدول ويحاسب من ينتهك هذه القواعد أمام محكمة الجنايات الدّوليّة.

المبحث الثّاني: المسؤوليّة الدّوليّة والإرهاب السيبرانيّ

القانون الدّوليّ الإنسانيّ منذ نشوئه لتنظيم القواعد والضوابط التي تحكم سير العمليّات العسكريّة خلال النّزاعات المُسلّحة بنوعيها الدّوليّة غير الدولة، وعلى الرغم من عدم قدره هذا القانون على منع الحرب الّا أنّه يسعى للحد من آثار النّزاع المُسلّح في ما بين الأطراف المتنازعة بشكل خاص حماية المدنيين الذين لا يشاركون في القتال، والأشخاص الذين أُسرفوا على المشاركة في القتال والسّعي؛ لتحييد الأعيان المدنيّة عن سير الأعمال العدائية خلال سير العمليّات القتاليّة التّقليديّة ظهرت هذه المبادئ في ضوء الحروب التّقليديّة ومع تقدّم التّطوّر التّقنيّ دخل مفهوم الحرب الإلكترونيّة إلى النّزاعات المُسلّحة كان من المفترض وجود ضوابط لحمايه البيئة المحلية في سياق هذه النّزاعات الإلكترونيّة التي تكوّن أهدافها بحسب يحيى الزهراني: "استغلال معلومات الآخرين للمصلحة الشخصية، أي التّجسس، وخداع العدو، وتعطيل نُظم معلومات العدو أو حرمانه مؤقتاً، أو تغييرها أو تدمير هذا النّظام، وتشمل الطرق مهاجمة البيانات، مثل إغراق البريد الإلكترونيّ برسائل إعلاميّة يمكن أن تزيد الحمل على نظام الحاسوب وتسبب له التعطل، واختراق أجهزة الحاسوب نأجل انتزاع معلومات أو بث معلومات مغايرة، وعلميات مهاجمة البرامج مثل الفيروسات والديدان الإلكترونيّة والقنابل المنطقية".[125]

يتألف النّظام السيبرانيّ من عدد كبير من أنظمة الكمبيوتر العسكريّة ويترابط مع الأنظمة المدنيّة، ولذلك فإنّه ليس من السهل إطلاق هجوم إلكتروني على البنية التحتيّة العسكريّة والحد من آثارها بدون تقويض البنية التحتيّة المدنيّة والذي من شأنه أن يكون مثالاً لانتهاك القانون الدّوليّ الإنسانيّ من خلال ضرب الأهداف العسكريّة والمدنيّة على حد سواء؛ فجميع قواعد القانون الدّوليّ الإنسانيّ من الممكن أن تطبق على نزاع مسلح دولي،ولكن يدور السؤال الأهم حول مدى إمكانيه تطبيقها على النّزاع الإلكترونيّ؛ لأنه كما يقول الباحث علي عبد المعطي حمدان: فإنّ مصطلح حرب الإنترنت أو الحرب

[125] يحيى مفرح الزهراني، الأبعاد الاستراتيجيّة والقانونيّة للحرب السّيبرانيّة، مجلة البحوث والدّراسات، المجلد 14، العدد 23، ص 225.

المعلوماتيّة: "يشير بشكل عام إلى مجموعة من الأعمال غير الودّيّة التي تمارس ضدّ دولة ما وتسبب لها أضراراً مباشرة تصيبها أو تصيب رعاياها". [126]

المطلب الأوّل: المسؤوليّة الدّوليّة عن الهجمات السّيبرانيّة

يعرف فقهاء القانون الدولي المسؤولية الدولية بأنها: "الجزاء القانوني المترتب على عدم احترام أحد أشخاص القانون الدولي لالتزاماته الدولية".[127] واختلفت الاتجاهات الفقهية حول محل المسؤولية الدولية في القانون الدولي، فمنهم من يرى أن الدولة وحدها هي المسؤولة عن الجريمة الدولية وآخرون يرون أن المسؤولية مزدوجة وتشمل الدولة والفرد، والرأي الأخير يرى أن الشخص الطبيعي هو المحل الوحيد للمسؤولية الجنائية الدولية.[128]

إن الهجمات السّيبرانيّة في عالم متغير ومتسارع وفي السباق التّقنيّ الدّوليّ تسبب خلافات اقتصادية وعسكرية قد لا تظهر مقابل خطورة ودقة الفضاء السيبرانيّ، وما يحصل فيه من مناورات وصراعات قوية وسوف تكون مثارة للجدل الشارع في وقت قريب؛ مما لا يسمح ولا يدع مجالاً للشك في حدوث مثل هذه الهجمات وواقعية حصولها، وحتى أحياناً دراسة خطورة نتائجها؛ لأنّها سوف تقع فجأة ودون سابق إنذار؛ لأن الحرب الفضائيّة خدعةٌ أيضاً كالحرب التّقليديّة.

وبظهر لدينا في معرض الحديث عن الهجمات السّيبرانيّة وتأثيرها على الدول، المسؤوليّة الدّوليّة التي تكون بالالتزام الذي تتحمله الدول أو المنظّمة الدّوليّة بحكم القانون الدّوليّ المنسوب إليها بارتكاب أفعال أو امتناع مخالف لالتزاماتها الدّوليّة بتعويض للمجني عليها في شخصها أو في رعاياها، وقيام المسؤوليّة الدّوليّة يقوم على عنصرين: أهمهما أن يكون منسوباً إلى دولة أو منظّمة شخص من

---

[126] علي عبد المعطي الحمدان، الحرب المعلوماتيّة وإمكانيّة تطبيق قواعد حقوق الإنسان، مجلة العلوم الشّرعيّة، المجلد 12، العدد 1، ص 767.

[127] عبد العزيز محمد سرحان، القانون الدولي، القاهرة، دار النهضة العربية، 1998، ص 385، وإبراهيم العناني القانون الدولي العام، القاهرة، دار النهضة العربية، 1998، ص 84.

[128] للاستزادة، انظر محمد عبد المنعم عبد الغني، الجرائم الدولية، دراسة في القانون الدولي الجنائي، دار الجامعة الجديدة، الإسكندرية، 2011، ص 426 وما بعدها.

أشخاص القانون الدّوليّ العام، أو يكون مخالفاً لمقتضيات قاعدة قانونيّة دولية، وبذلك تنحصر لدينا شروط المسؤوليّة الدّوليّة 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 الشّرعيّة الدّوليّة [129].

وبهذا الالتزام المفروض على الدولة أو المنظّمة الدّوليّة نجد أن حصول هجمة سيبرانية تأخذ طابعاً دولياً بمعنى أن القائم عليها دولة أو منظّمة دوليّة، واستهدفت دولة أو منظّمة دولية، فإنّ ذلك واستناداً إلى مبدأ المسؤوليّة الدّوليّة يحمل هذه الجهة القائمة على الهجمة السّيبرانيّة أن تقوم بتعويض الجهة المجني عليها استناداً إلى مبدأ هذه المسؤوليّة الدّوليّة التي ترتب عنها هذا الإخلال، وعند قياس فعل الهجمات السّيبرانيّة على عناصر المسؤوليّة الدّوليّة فإنّنا نجد أن المقياس الأوّل أن تخضع هذه الهجمة إلى الصفة الدّوليّة: أي أنّه يجب أن تتبناها جهة دولية أو منظّمة دوليّة، حتى يتم إلحاقها بالمسؤوليّة الدّوليّة، أما المقياس الثّاني: فإنّ تكون هذه الهجمة السّيبرانيّة الدّوليّة تخرق معاهدة أو عرف أو ميثاق دولي وبتوضيح أكثر لهذا العنصر يجب أن يترتب على هذه الهجمة الإضرار بمصالح الدولة المُعتدى عليها الاقتصاديّة، والسّياسيّة والاستراتيجيّة، أو أنّها تخل بمبدأ من مبادئ الأمم المتحدة التي كان من أهم مقاصدها هو صون السِلم والأمن الدّوليّين والمحافظة عليهما من أي اختراق أو تدخل يضر بمصالح الدول الأساسيّة التي لا يجوز انتهاكها، ونستنتج من المسؤوليّة الدّوليّة مبرر آخر يورد لدينا أحقية فعل الدّفاع الشرعيّ في حال حصول هجمة سيبرانية دولية، وتنحصر شروط المسؤوليّة الدّوليّة بما يلي: [130]

1. وجود فعل أو امتناع عن فعل من شخص من أشخاص القانون الدّوليّ العام.
2. إلحاق ضرر بشخص من أشخاص القانون الدّوليّ العام بأي شكل.

---

[129]. نقلاً عن: عمر حرز الله، الحرب السّيبرانيّة: صراع في العالم الافتراضي، صحيفة البيان، تاريخ النشر 4/ 3 /2012. متاح على الرابط https://www.albayan.ae/five-senses/mirrors/2012-03-04 –

[130]. فيصل عبد الغفار: الحرب السّيبرانيّة، الطبعة الأولى، عمّان، الأردن: دار الجنادرية للنشر والتّوزيع، 2014.

3. أن يكون هذا الفعل أو التصرف غير مشروع وفق القانون الدّوليّ العام.

وفي محاولة للربط بين شروط قيام المسؤوليّة الدّوليّة والهجمات السّيبرانيّة نجد أن حصول الهجمة من شخص قانوني دولي وذلك بالرجوع للشرط الأوّل فهذا يعني حصولها من جهة غير دولية لا يبرر قيام المسؤوليّة الدّوليّة، وعند البحث بالشرط الثّاني وهو الحاق الضّرر، فهذا أمر جوهري وفي غاية الأهميّة فعند الحديث في السّابق في دراستنا أوردنا الخطورة الكبيرة التي ممكن أن تلحقها الهجمات السّيبرانيّة عندما تستهدف مصالح استراتيجية دولية وحساسة، في نفس الوقت فعنصر الضّرر شيء واقع لا محال عندما تقع بشكل كبير وعدواني، وكذلك أن هذا الموضوع –الضّرر- ليس بحاجة إلى التبرير؛ لأنه مبرر أساسيّ لحصول المسؤوليّة الدّوليّة، لأنه على الأغلب تكون الهجمة السّيبرانيّة الدّوليّة باستهداف مصالح ذات قيمة وأهميّة، وليست بمصالح فردية بسيطة، وبذلك لا نستطيع إبعاد عنصر الضّرر عن الهجمة الدّوليّة لأن الضّرر والتّأثير هو ديدن هذه الحرب؛ لأنّها ستكون حرب القرن الحادي والعشرين.[131]

وعند البحث في الشرط الأخير نجد أن الفعل غير المشروع الذي يعدُّ انتهاكاً لأحكام القانون الدّوليّ العام أو مخالفة لقواعد القانون الدّوليّ أو المبادئ العامة للقانون، وبذلك أن فعل الهجمات السّيبرانيّة هو غير مشروع ابتداء، وهو بحد ذاته ينتهك أحكام وقواعد القانون الدّوليّ؛ لأنه يخترق أسرار ووثائق الدول، ويستهدف مصالحها الكبرى ويختلق مشاكل وقضايا دولية معاصرة لم تكن موجودة في السّابق في عهد الحروب التّقليديّة ولا حتى الحرب الباردة، فهذا التسابق في التسلح التّقنيّ الجديد نعتبره في غاية الخطورة والدّقة والأهميّة.[132]

ومن خلال ما سبق نصّل إلى نتائج بعد دراسة عناصر وشروط المسؤوليّة الدّوليّة أهمها أن الإخلال بالالتزام الدّوليّ ينتج المسؤوليّة الدّوليّة التي بحد ذاتها تخترق وتخل بقواعد القانون الدّوليّ الذي يوجب

---

[131]. النقروز، ايناس عبد الله، حرب المعلومات، جمعية المكتبات والمعلومات الأردنية، عمّان، 2014، ص 213

[132]. الصيفي، حسن، الفضائيات العربيّة في عصر العولمة: الفرص والتحديات، الواقع والطموحات، ط 1، القاهرة، الهيئة العامو لدار الكتب والوثائق القوميّة، 2010م.

التعويض، وبحصول الضّرر من الفعل المخالف لأحكام القانون الدّوليّ؛ أما إذا لم يحصل ضرر فإنّ المسؤوليّة الدّوليّة لا تقوم إذاً الضّرر هو الأساس في قيام المسؤوليّة ولزوم التعويض.

وفي المحصلة النهائية للحديث عن قيام المسؤوليّة الدّوليّة عن إحداث الهجمات السّيبرانيّة واشتراكها في الجرائم الدّوليّة نستخلص مبرر جديد ألا وهو قيام وظهور استراتيجيات الدّفاع [133]، وهذه الاستراتيجيّات التي تؤمن بها الدول وحق لا يمكن إنكاره ويقوم عندما تنتهك سيادة وحقوق الدول من حصول جرائم دولية تؤدي إلى إلحاق الأضرار الجسيمة بمصالحها، وإدراج فعل الهجمات السّيبرانيّة يؤكد ويساعد في نهوض المجتمعات الدّوليّة على وضع خطط وبرامج واستراتيجيات تحمي فضائها وبنيتها السّيبرانيّة والفضائيّة والتّقنيّة.

ونرى مخاوف الأمريكيّين خير مثال من تتبع اتصالاتهم وحساباتهم البنكية ونجدهم ينفقون مليارات الدولارات على اتصالاتهم بإيجاد الوسائل الكفيلة لذلك وهذا مثال حي وواقعي نستطيع أن ندرجه تحت موضوع استراتيجيات الدّفاع.[134]

وعند الحديث عن الأساس القانونيّ للمسؤولية الدّوليّة كان أساسه الخطـأ ونظرية المخاطر، هذا في القانون الدّوليّ التقليدي، أما في القانون الدّوليّ المعاصر، فإنّ الإحساس الجوهري للمسؤولية الدّوليّة هو العمل الدّوليّ غير المشروع، فالبحث في موضوع المخاطر عند ممارسة الدولة نشاطاً ذا طبيعة خطيرة وغير مألوفة تتحمل الدولة مسؤوليتها عن الأضرار التي تصيب الدول الأخرى، من هذه النشاطات وأكثر ما يهمنا في هذا الصّدد الاعتبار الذي يتحدث عن التّطوّر العلمي والتّكنولوجيّ والأنشطة المتصلة به، فنشاط الانترنت يندرج تحت بند المخاطر الدّوليّة التي تقع الدولة في خانة المسؤوليّة الدّوليّة عند اتهامها في إحداث هجمة سيبرانية دولية.

---

[133]. لطفي لمين بلفرد، "الفضاء السيبرانيّ: هندسة وفواعل"، المجلة الجزائرية للدراسات السّياسيّة، ENSSP، العدد الخامس، الجزائر، 2016، ص ص 148-150.

[134]الحروب السّيبرانيّة. معارك العالم الافتراضي تنتقل إلى الميدان، لندن – الخليج أونلاين، تاريخ النشر 2018\3\24، متاح على الرابط http://alkhaleejonline.net

المطلب الثّاني: الهجمات السّيبرانيّة كظاهرة إرهابيّة دولية

عرفت الاتفاقية العربية لمكافحة الإرهاب مصطلح الإرهاب بأنه: "كل فعل من أفعال العنف أو التهديد أياً كانت بواعثه أو أغراضه يقع ضد المدنيين أو لترويعهم بإيذائهم أو تعريض حياتهم أو حريتهم أو أدميتهم للخطر، وإلحاق الضرر بالبيئة أو بأحد المرافق أو الأملاك العامة أو الخاصة أو احتلالها أو الاستيلاء عليها أو تعريض أحد الموارد الوطنية للخطر".[135] ويفهم من هذا التعريف أن الإرهاب الدولي يتضمن كل واحد من هذه الأعمال التي يقوم بها المنفذون على المستوى الدولي.

في مطلع الحديث عن الإرهاب الدّوليّ تجدر الإشارة إلى الحديث عن ظهور مصطلح الإرهاب بصورته العصرية الحديثة، فكانت أحداث الحادي عشر من سبتمبر نقطة التحول العالميّة الجديدة في مفهوم الإرهاب الدّوليّ، ويستخدم مصطلح "الإرهاب" للدلالة على إعمال العنف تهدف إلى إثارة الرعب في المجتمع الدّوليّ أو الدّاخليّ.[136]

واهتمام الدول والمجتمع الدّوليّ في مكافحة الأعمال الإرهابيّة لا سيما في إطار منظّمة الأمم المتحدة إلاّ أن هذا الاهتمام في خلاف مستمر على تعريف مصطلح الإرهاب لسبب عدم توافر النية السّياسيّة للتوصّل إلى تعريف محدّد للإرهاب من كافة الدول الأعضاء في المنظّمة.[137]

وبدقّة أكثر لأننا عندما نتحدث عن هجمات سيبرانية بمفهومها الدّوليّ الصّادر من جهة دولية أو منظّمة دولية ضدّ جهة دولية أخرى فإنّ خطر الإرهاب الدّوليّ سوف يتسع تأثيره ومداه إلى المصالح الفردية؛ لأن الدولة في الأساس من أهم واجباتها حماية مقدرات الأفراد من التّعدي والعبث والدمار،

---

[135] أحمد الرشيدي، نحو مدخل موضوعي لفهم ظاهرة الإرهاب وسبل التصدي لها، مركز دراسات الشرق الأوسط، الأردن، 2003، ص 19.

[136]. الحروب السّيبرانيّة. معارك العالم الافتراضي تنتقل إلى الميدان، لندن – الخليج أونلاين، تاريخ النشر 2018\3\24، متاح على الرابط http://alkhaleejonline.net

[137]. خالد الثوراني، الجيوش الافتراضية بين الصّراع الدّوليّ والتسقيط السّياسيّ المحلي، شبكة النبأ المعلوماتيّة، تاريخ النشر 2017 /6/25.متاح على الرابط https://annabaa.org/arabic/informatics/11558

فخطر الهجمات السّيبرانيّة أثره كبير وفعال كخطر الإرهاب الدّوليّ، وكما أنّ للإرهاب الدّوليّ دوافع سياسيّة واقتصادية وتاريخيّة ثمّ إعلامية وشخصية، فإنّ للهجمات السّيبرانيّة نفس الدوافع لا بل أكثر أحياناً [138].

وترى الباحثة سلافة طارق الشّعلان أن: "الأهداف المحتملة للحرب الإلكترونيّة باستخدام شبكات الحاسوب لا تخلف عنها في الحرب التّقليديّة ويمكن أن تصنف إلى ثلاثة أنواع: الأضرار التي تصيب المدنيين والأهداف المدنيّة، والمقاتلين، والأهداف العسكريّة ". [139]

وعند إدراج الدوافع الاقتصاديّة؛ لأنّها كما هو معلوم القوة الجديدة في نظريات العالم المعاصر لأن تسمية غني ارتبطت بقوي وضعيف ارتبطت بفقير، فأصبح التّدمير المتعمد لاقتصاديات بعض الدّول من أهم دوافع الإرهاب في الوقت الحاضر، كما هو من أهم دوافع الهجمات السّيبرانيّة، فعندما قامت بعض الجهات المجهولة بزرع ألغام بحرية بجزء من البحر الأحمر من أجل حرمان مصر من عائدات قناة السويس والإضرار باقتصاد دول الخليج؛ لأن البترول وكما هو معروف أهم ركيزة للاقتصاد الخليجي، مثلما فعل تماماً منفذو الهجمة السّيبرانيّة على مفاعل بوشهر الإيرانيّ والمنشآت النّوويّة الإيرانيّة وأجهزة الطرد المركزي هناك التي تعتبر الساعد المهم في الاقتصاد الإيرانيّ في حال نجاح هذا المفاعل وتحقيق أهدافه، وبذلك نجد أن الدافع الاقتصادي يوازي إلى حد كبير بين الإرهاب الدّوليّ والهجمات السّيبرانيّة.

وعند الحديث عن الأسباب الدينية نجد أن الولايات المتّحدة الأمريكيّة وفي مرحلة ما بعد حرب الخليج الثّالثة 2003، واحتلال بغداد حاولت إثارة الفتنة الطائفية بين المسلمين السّنة والشيعة، ونجد أن أمريكا وضعت أسلوب جديد للتدخل وهو التّدخّل؛ لأسباب دينية بجانب يضفي عليه الصفة التّشريعيّة

---

[138]. عمر حرز الله، الحرب السّيبرانيّة: صراع في العالم الافتراضي، صحيفة البيان، تاريخ النشر 4/ 3 /2012. متاح على الرابط https://www.albayan.ae/five-senses/mirrors/2012-03-04

[139] سلافة طارق الشّعلان، تكييف استخدام الحرب الإلكترونيّة في النّزاعات المُسلّحة وفقاً للقانون الدّوليّ الإنسانيّ، المجلد 9، العدد 26، ص 121.

فأصدر الكونجرس عام 1998 تشريعاً يسمح للولايات المتّحدة الأمريكيّة فرض عقوبات اقتصادية، وعسكرية وسياسيّة على لدول التي تمارس الاضطهاد ضدّ الأقليات الدينية والطوائف المضطهدة [140].

ونجد أن الدوافع الدينية في الهجمات السّيبرانيّة حذت حذو الإرهاب الدّوليّ وواضح ذلك جلياً في كشف مؤامرات الربيع العربيّ عندما تم نشر موقع ويكليكس الذي عملت الجماعات المناهضة للربيع العربيّ وثورات الفيس بوك على اختراق هذا الموقع، وكشفت ادعاءات ومؤامرات القادة والساسة وأهدافهم الدينية قبل السّياسيّة للأعمال القمعية التي كانوا يمارسونها على شعوبهم، وكشف النوايا المستترة عندهم. ولعل الدافع الأبرز والأهم المرتبط ارتباطاً وثيقاً بين الإرهاب الدّوليّ من جهة والإرهاب السيبرانيّ والهجمات السّيبرانيّة من جهة أخرى هو الدافع الإعلاميّ.

ونجد أن التّطوّر العلمي الهائل الذي امتد ليشمل كل نواحي الحياة والذي أصبح يتيح للقنوات الإعلاميّة نشر أخبار وآراء الإرهابيين ويكون ذلك من خلال تغطية إعلامية، ونقل الحدث لحظة بلحظة وعلى الهواء مباشرة ونتيجة لهذا التسابق المحموم بين وسائل الإعلام في السرعة لنقل الخبر وتهويله وجدت الجماعات الإرهابيّة تتخذ من الإعلام وسيلة لتسويق جرائمها وأعمالها الإرهابيّة إن لم تتخذ في بعض الأحيان قناة خاصة لها. ومثل جريمة الإرهاب الدّوليّ المرئية على الإعلام نجد أن الهجمات السّيبرانيّة تستخدم الشّبكات السّيبرانيّة نفسها التي يستخدمها الإرهابيون الدّوليّين.

بحيث إن عمليّة قرصنة الواقعة السّيبرانيّة والدّخول على عناوين البريدية تعود لأشخاص آخرين أصبح من السهل التشهير بهم من خلال بث المعلومات غير الصحيحة والمشوهة عنهم، من خلال مواقع التواصل الاجتماعي والشّبكات الغير محمية، بحيث يتطلع كل شخص على هذه المعلومات التي تكون في غاية السّريّة والدّقة أحياناً.[141] ولذلك نجد أن هذه الحروب والهجمات السّيبرانيّة ستكون أكثر تدميراً في

---

[140]. جلال خياط، فورين بولسي تتحدث عن الحرب السّيبرانيّة بين روسيا وأمريكا في سوريا، موقع اورنت نت، تاريخ النشر 2018/7/31. متاح على الرابط https://orient-news.net/ar/news_show

[141]. موسى، طالب حسن، أعمر، عمر محمود، 2016 الإنترنت قانونا، مجلة الشريعة والقانون، جامعة الإمارات العربيّة المتّحدة ، العدد السابع والستين، ص.339.

المستقبل؛ ومما لا يقبل الشك فيه أنّها سوف تتسبب في شلل بلاد كاملة وعزلها عن العالم وإبعادها كل البعد وإعادتها إلى عصور الظلام البدائية؛ لأنه حتى أقل الدول حضارة وتقدّما تكنولوجيّا أصبحت شبكة الإنترنت عبارةً عن القلب النابض بكل ما فيها من خدمات واقتصاديات حتى أنّها دخلت في كل مجالات الدولة الحديثة ومقدراتها، وأصبحت حمايتها واجبةً، مما يجسد التّدخّل الدّوليّ الإنسانيّ عن طريق القرارات الصّادرة عن مجلس الأمن طبقاً للفصل السابع من الميثاق".[142]

يخلص هذا الفصل إلى أن الحرب السّيبرانيّة لها صور كثيرة لا حصر لها، لأنّها متنوّعة بتنوّع البرنامج المستعمل في الهجوم وفي القطاع التّكنولوجيّ المستهدف؛ مما يستوجب ضرورة الحرص على تنظيمها بقواعد مناسبة تضمن الردع الكافي، بالإضافة إلى أن الهجمات السّيبرانيّة هي هجمات إرهابيّة؛ لأن المستهدف فيها على الأغلب هم مدنيون، يتم استهدافهم من أجل تحقيق مكاسب سياسيّة معينة في النّزاعات بين الدول، مما يُشكّل صوراً من صور الإرهاب. وهذا ما أكد عليه الباحث "تيلمان رودنهاوسر" بقوله: "إن العليات السّيبرانيّة تنطوي على خطر المبالغة في رد الفعل من جانب الدول المستهدفة وتصعيد العنف لاحقاً".[143]

[142] حساني خالد، مشروعية استخدام القوة بتفويض من مجلس الأمن بين أحكام الميثاق والممارسة الدّوليّة، المجلة الأكاديمية للبحث القانون، عام 2017، عدد خاص، ص 101.

[143] لوران جيزل وتيلمان رودنهاوسر وكنوت دورمان، بعد عشرين عاماً: القانون الدّوليّ الإنسانيّ وحماية المدنيين من آثار العمليّات السّيبرانيّة أثناء النّزاعات المُسلّحة، المجلة الدّوليّة للصليب الأحمر، المجلد 102، العدد 913، ص 287.

الخاتمة

هدفت هذه الرّسالة إلى الإجابة عن إشكالية رئيسية، وهي مدى شموليّة قواعد القانون الدّوليّ الإنسانيّ في تنظيم الحرب السّيبرانيّة وتداعياتها على العلاقات الدّوليّة؟ والمقصود بهذا السؤال هو تحديد مظاهر وجوانب الحرب السّيبرانيّة، المُعتمدة على الحواسيب والبرامج السّيبرانيّة، التي يوجد لها تنظيم في مصادر القانون المذكور، وهي اتفاقية لاهاي واتفاقيات جنيف الأربعة، والبروتوكولان الإضافيان، القواعد العرفية، ودليل تالين المُعتمد من قبل كبار الفقهاء كدليل لتنظيم الحرب السّيبرانيّة.

وقد خلصت الباحثة إلى نتيجة مهمة، دعمتها بأدلة جديدة، دعمت فيها أنصار المذهب القائل بانطباق القانون الدّوليّ الإنسانيّ على الحروب السّيبرانيّة، وكذلك قامت الباحثة بتقديم تفسيرات لم تقدّم من قبل لنصوص قانونيّة كثيرة من نصوص اتفاقيات القانون الدّوليّ الإنسانيّ. وكانت تلك النتيجة المهمة أن التفسير الموسع لقواعد القانون الدّوليّ الإنسانيّ يؤدي إلى شمول هذا القانون لكل مظاهر الحروب السّيبرانيّة المحتملة؛ لأن هذه الحروب السّيبرانيّة هي مكونة من عمليّات هجومية مُسلّحة، هدفها التّأثير على الأمن الدّوليّ والاستقرار السّياسيّ في الدول المستهدفة، أي أن التفسير السليم لقواعد القانون، وتطبيق مبادئ الحروب الشّرعيّة، يقدم شمولاً كاملاً لكل مظاهر الحرب السّيبرانيّة وهذه المبادئ هي: مبدأ التناسب الذي لا يسمح بالهجوم إلا حين تكون الأضرار متناسبة مع تحقيق ميزة عسكرة ملمومة ومباشرة، ومبدأ التّمييز الذي يحرم استهداف المدنيين والأعيان المدنيّة وخصوصاً بالأسلحة العشوائية، ومبدأ الحرص الذي يوجب على الأطراف استعمال كل الطرق الممكنة لضمان أن الهجمات التي يريدون القيام بها لن تستهدف سوى أهدافا مشروعة تحقّق تقدّماً عسكرياً ملحوظاً للمهاجم وأخيراً مبدأ الشرف الذي يحرم استعمال القانون بسوء نية بما يضر الطرف الآخر. وفيما يلي أهم النّتائج والتّوصيات التي ترتبت على هذه الخلاصة.

النّتائج

1. انطباق قواعد القانون الدّوليّ الإنسانيّ المكتوبة على الحرب السّيبرانيّة، وهي اتفاقية لاهاي واتفاقيات جنيف الأربعة لعام 1946، والبروتوكولان الإضافيان لعام 1977 بشكل ضمني، وكذلك انطباق القواعد الموجودة في المصادر الاحتياطية للقانون الدّوليّ الإنسانيّ على هذه الحروب، وهي القواعد الموجودة في دليل القواعد العرفية للقانون الدّوليّ الإنسانيّ، ودليل تالين المُعتمد من كبار الفقهاء في مجال تنظيم قواعد الاشتباك في الحروب السّيبرانيّة.

2. احتواء مصادر القانون الدّوليّ المكتوبة والعرفية على قواعد ضمنية كافية لتنظيم الحروب السّيبرانيّة، شريطة أن يتم تفسير هذه القواعد تفسيرياً يراعي المقصد منها وهو منع الهجمات العدائية غير الضّروريّة، وليس مجرد تفسيرها تفسيراً يوافق فقط السّياق التّاريخيّ الذي تم إقراراها فيه.

3. تأييد المذهب القائل: إنّ القانون الدّوليّ الإنسانيّ ينطبق على الحروب السّيبرانيّة، وذلك على عكس ما ذهب إليه المذهب المناقض والمسمى بالمذهب الحر؛ لأن القانون الدّوليّ الإنسانيّ ينظم الاشتباك في الهجمات المُسلّحة، والهجمات السّيبرانيّة تعتبر هجمات مُسلّحة من حيث الضّرر والفتك والدمار الذي تسببه على المدنيين والأعيان المدنيّة والبنية التحتيّة الّتكنولوجيّة.

4. التأكيد على أن المسؤوليّة الدّوليّة تقوم على الدول المعتدية المهاجمة لدول أخرى، وذلك أن الأركان الثلاثة تكون متحققة في مثل هذه الهجمات العدائية، وهي الخطأ والضّرر والعلاقة السببية بين فعل الدولة الخاطئ والضّرر الذي أحدثته.

التوصيات

1. ضرورة اعتماد المنهج التفسيري الموسع في تفسير قواعد القانون الدّوليّ الإنسانيّ لتطبيقها على الحروب السّيبرانيّة، وذلك باعتبار أن هذه الحروب هي صور أخرى من صور الهجمات المُسلّحة بأسلحة سيبرانية لا بأسلحة تقليدية؛ ولذلك، عدم اعتماد المنهج الحرفي الضيق؛ لأنه لا يراعي التّطوّر التّاريخيّ والسّياق الجديد للحروب الحديثة.
2. ضرورة اعتماد دليل تالين ليكون اتفاقية ملزمة بين الدول، وأنّه ليس مجرد مصدرًا احتياطيا مبنيا على آراء الفقهاء، وهذا أمر ممكن من خلال اعتماد لجنة الصليب الأحمر له ودعوة الدول للتوقيع عليه.
3. ضرورة تفسير القواعد العرفية للقانون الدّوليّ والإنسانيّ بما يتوافق مع مبدأ التناسب ومنع أسلحة الضّرر العشوائي، وهما مبدآن كافيان للحكم بعدم شرعيّة الهجمات السّيبرانيّة.
4. ضرورة توسيع دائرة التجريم في الحروب لتشمل الحروب السّيبرانيّة، وتكون بذلك الهجمات السّيبرانيّة صوراً من صور جرائم الحرب، لا مجرد اعتداءات يترتب عليها حق التعويض لدول المتضررة في مواجهة الدول المسؤولة عن هذه الهجمات.

المصادر والمراجع

الاتفاقيات الدّوليّة:

1. ميثاق الأمم المتحدة. متوفر على: **https://www.un.org/ar/about-us/un-charter/full-text**. تمّت الزيارة في 2022/7/26.

2. اتفاقية جنيف الأولى لتحسين حال الجرحى والمرضى بالقوات المُسلّحة في الميدان. متوفر على:

https://www.icrc.org/ar/doc/resources/documents/misc/7umf63.htm

. تمّت الزيارة في 2022/7/26.

3. اتفاقية جنيف الثّانية لتحسين حال جرحى ومرضى وغرقى القوات المُسلّحة في البحار. متوفر على:

https://www.icrc.org/ar/doc/resources/documents/misc/5nslh8.htm.

تمّت الزيارة بتاريخ 2022/7/26.

4. اتفاقية جنيف الثّالثة بشأن معاملة أسرى الحرب. متوفرة على:

https://www.icrc.org/ar/doc/assets/files/other/conv_iii_geneva_1949.pdf.

تمّت الزيارة في 2022/7/26

5. اتفاقية جنيف الرّابعة بشأن حماية الأشخاص المدنيين في وقت الحرب. متوفر على:

https://www.icrc.org/ar/doc/resources/documents/misc/5nsla8.htm. تمّت الزيارة في 2022/7/26.

6. الملحق (البروتوكول) الأوّل الإضافيّ إلى اتفاقيات جنيف. متوفر على:

https://www.icrc.org/ar/doc/resources/documents/misc/5ntccf.htm. تمّت الزيارة في 2022/7/26.

7. قواعد القانون الدّوليّ الإنسانيّ العرفي، ص 3. متوفر على: **https://www.icrc.org/data/files/publications/ar/icrc_004_pcustom.pdf**. تمّت الزيارة في 2022/7/26.

8. دليل تالين بشأن القانون الدّوليّ المطبق على الحروب السّيبرانيّة، مايكل شميت، 2013،

9. ترجمة علي محمد كاظم الموسوي، 2017. متوفر على: **shorturl.at/bGHKV**. تمّت الزيارة في 2022/7/26.

الكتب:

1. أبو ربيع، مصطفى عبد العزيز، (2007)، استخدام القوة بتفويض مجلس الأمن، بدون طبعة، رسالة ماجستير، آل البيت.

2. عبد الغني، محمد عبد المنعم، الجرائم الدولية، دراسة في القانون الدولي الجنائي، دار الجامعة الجديدة، الإسكندرية، 2011

3. سرحان، عبد العزيز محمد، القانون الدولي، القاهرة، دار النهضة العربية، 1998.

4. العناني، إبراهيم القانون الدولي العام، القاهرة، دار النهضة العربية، 1998.

5. الرشيدي، أحمد، نحو مدخل موضوعي لفهم ظاهرة الإرهاب وسبل التصدي لها، مركز دراسات الشرق الأوسط، الأردن، 2003.

6. الصيفي، حسن، الفضائيات العربيّة في عصر العولمة: الفرص والتحديات، الواع والطموحات، ط 1، القاهرة، الهيئة العامة لدار الكتب والوثائق القوميّة، 2010م.

7. النقروز، إيناس عبد الله، حرب المعلومات، جمعية المكتبات والمعلومات الأردنية، عمّان، 2014

8. جوزيف ناي، القوة الناعمة: وسائل النّجاح في السّياسة الدّوليّة، تر: محمد توفيق البجيرمي، ط1، مكتبة العبيكان للنشر، الرياض، 2007، ص20.

9. سامية أبو النّصر، الإعلام والعمليّات النّفسيّة في ظل الحروب المعاصرة وإستراتيجية المواجهة، دار النشر للجامعات، ط1، 2010.

10. عبّاس بدران، الحروب الإلكترونيّة: الاشتباك في عالم متغير، مركز دراسات الحكومة الإلكترونيّة، بيروت، 2010.

11. كمال مساعد، الحرب الافتراضية وسيناريوهات محاكاة الواقع، مجلة الجيش اللبناني، العدد (253)، 2006، متاح على الرابط **https: //www. leparmy. gov. Ib/artical. asp**

12. لسان العرب المؤلف: محمد بن مكرم بن على، أبو الفضل، جمال الدين ابن منظور الأنصاري الرويفعى الإفريقى (المتوفى: 711هـ) الناشر: دار صادر - بيروت الطبعة: الثّالثة - 1414 هـ

13. يحي اليحياوي، أوراق في التّكنولوجيا والإعلام والدّيمقراطيّة، دار الطليعة للنشر، بيروت، 2004.

14. الحديثي، مؤيد، العولمة الإعلاميّة والأمن القوميّ العربيّ، ط 1، عمّان: الأهليّة للنشر والتّوزيع، 2002م

15. الشّكري، علي يوسف (2008)، الإرهاب الدّوليّ في ظل النّظام العالميّ الجديد، ط1، دار أسامة للنشر والتّوزيع، عمّان، الأردن.

16. عدس، عمر حسن، (1995)، مبادئ القانون الدّوليّ العام المعاصر، ط1، مطابع القواسمي، دار النهضة العربيّة للنشر والتّوزيع.

17. عمر محمود أعمر: الحرب الإلكترونيّة في القانون الدّوليّ الإنسانيّ، دراسات، علوم الشريعة والقانون، **2019**.

18.فيصل عبد الغفار: الحرب الإلكترونيّة، الطبعة الأولى، عمّان، الأردن: دار الجنادرية للنشر والتّوزيع، **2014**.

19. **Michael N. Schmitt: Classification of Cyber Conflict. Journal of Conflict & Security Law، 2012، 17(2): pp. 245–260.**

الدوريات والمجلات والمقالات:

1. يحيى مفرح الزهراني، الأبعاد الاستراتيجيّة والقانونيّة للحرب السّيبرانيّة، مجلة البحوث والدّراسات، المجلد 14، العدد 23، ص 225.
2. علي عبد المعطي الحمدان، الحرب المعلوماتيّة وإمكانيّة تطبيق قواعد حقوق الإنسان، مجلة العلوم الشّرعيّة، المجلد 12، العدد 1، ص 767.
3. سلافة طارق الشّعلان، تكييف استخدام الحرب الإلكترونيّة في النّزاعات المُسلّحة وفقاً للقانون الدّوليّ الإنسانيّ، المجلد 9، العدد 26، ص 121.
4. حساني خالد، مشروعية استخدام القوة بتفويض من مجلس الأمن بين أحكام الميثاق والممارسة الدّوليّة، المجلة الأكاديمية للبحث القانون، عام 2017، عدد خاص، ص 101.
5. لوران جيزل وتيلمان رودنهاوسر وكنوت دورمان، بعد عشرين عاماً: القانون الدّوليّ الإنسانيّ وحماية المدنيين من آثار العمليّات السّيبرانيّة أثناء النّزاعات المُسلّحة، المجلة الدّوليّة للصليب الأحمر، المجلد 102، العدد 913، ص 287.
6. حرب الفضاء الإلكترونيّ المفهوم: الأدوات والتطبيقات، أنمار موسى جوان، كلية اليرموك، مجلة العلوم القانونيّة والسّياسيّة
7. لطفي لمين بلفرد، "الفضاء السيبرانيّ: هندسة وفواعل"، المجلة الجزائرية للدراسات السّياسيّة، **ENSSP**، العدد الخامس، الجزائر، 2016.

8. يسرى خالد إبراهيم، "الحرب النّفسيّة الإلكترونيّة"، مجلة الباحث الإعلاميّ، العدد 13، 2011.

9. فهمي، عبد القادر، الحروب التّقليديّة وحروب الفضاء الإلكترونيّ: دراسة مقارنة في المفاهيم وقواعد الاشتباك، مجلة العلوم القانونيّة والسّياسيّة، العراق، 2018.

الروابط الإلكترونيّة:

1. الحرب الإلكترونية، شبكة الألوكة، كريم حميدة، 2012/3/20. راجع الرابط التالي **https://rb.gy/dnpmms** تعدد آثار الحرب السيبرانية

2. دنيا الوطن، الحرب الإلكترونية واستهداف الدولة المصرية، عادل عامر، 2019/3/3. متوفر على الرابط التالي: **https://pulpit.alwatanvoice.com/content/print/486515.html** . تمت الزيارة في 2023/1/4.

3. شبكة فلسطين للحوار، بعد تجربته على سوريا، إسرائيل تتبنى مشروع حرب الإنترنت ضد إيران، 2009/7/19. متوفر على الرابط التالي:

https://www.paldf.net/forum/showthread.php?t=449509&s=ac6c06cf5fa7142f25f708ac732409c0. تاريخ الزيارة 2023/1/4.

1. الاتفاقية الخاصّة باحترام قوانين وأعراف الحرب البريّة، المعروفة باتفاقية لاهاي. متوفر على:

https://www.icrc.org/ar/doc/resources/documents/misc/62tc8a.htm.

تمّت

الزيارة في 2022/7/26.

2. ما هي قواعد الحرب وما هي أهميتها، اللجنة الدّوليّة للصليب الأحمر، متوفر على:

https://www.icrc.org/ar/document/what-are-rules-of-war-Geneva-Conventions. تمّت الزيارة في 2022/7/26

3. مائة وخمسون عامًا على إعلان بطرسبورغ... أول اتفاقية دولية تُنظّم استخدام الأسلحة زمن الحرب، الإنسانيّ (مجلة تصدر عن المركز الإقليميّ للإعلام التابع للجنة الدّوليّة للصليب الأحمر)، 6 كانون الأول / ديسمبر 2018. متوفر على الرابط الآتي:

/https://blogs.icrc.org/alinsani/2018/12/06/2305

4. المحسن، عبد الكريم، ساحة المعارك العظمى التالية: الفضاء الإلكترونيّ، في: شبكة الحوار المتمدن – محور الأبحاث السّياسيّة، (ع: 3604/ 11 كانون الثّاني\ يناير 2012) **https: //www. ahewar. org/debat/show. art. asp?aid=291166**
5. الحروب الإلكترونيّة. معارك العالم الافتراضي تنتقل إلى الميدان، لندن – الخليج أونلاين، تاريخ النشر 24\3\2018، متاح على الرابط **http: //alkhaleejonline. net**
6. **%2023-3-2016،https: //www. aljazeera. net/encyclopedia**
7. المركز الأوروبي لدراسات مكافحة الإرهاب والاستخبارات، **https: //www. europarabct. com/**
8. المرهون، عبد الجليل، عصر الردع الإلكترونيّ، في: موقع قناة الجزيرة على شبكة الإنترنت، 26 تشرين الأوّل أكتوبر، 2012م. **https: //www. aljazeera. net/opinions/**
9. أمريكا تشنّ أكبر عمليّات تجسس على روسيا منذ الانهيار السوفييتي، صحيفة الواشنطن بوست: ترجمة الخليج أونلاين، تاريخ النشر 2016/9/15، متاح على الرابط **http: //alkhaleejonline. net**
10. بعد الهجوم على أوكرانيا. ما هي الهجمات الإلكترونيّة وكيف تحدث؟، سعيد، كريم، 17-2-2022م، **https: //al-ain. com/article/ukraine-exposed-cyber-attacks**

11.جلال خياط، فورين بولسي تتحدث عن الحرب الإلكترونيّة بين روسيا وأمريكا في سوريا، موقع اورنت نت، تاريخ النشر 2018/7/31. متاح على الرابط **https: //orient-news. net/ar/news_show**

12.خالد الثوراني، الجيوش الافتراضية بين الصّراع الدّوليّ والتسقيط السّياسيّ المحلي، شبكة النبأ المعلوماتيّة، تاريخ النشر 6/25/ 2017. متاح على الرابط **https: //annabaa. org/arabic/informatics/11558**

13.عابد، هشام، الحرب عند كارل فون كلاوزفيتز من خلال كتاب -في الحرب-، 5-11-2011، **https: //www. ahewar. org/debat/show. art. asp?aid=284870**

14.محمد جمعة جبالي، مقال بعنوان الإنترنت تاريخ من التّطوّر المذهل، **https: //www. skynewsarabia. com/technology**، بتاريخ **twelve** مارس 2014م

15.موقع الجزيرة – مركز الدّراسات، **https: //studies. aljazeera. net/en/node/1819**، مقال بعنوان المجال الخامس. الحرب الإلكترونيّة في القرن الـ 21، تاريخ النشر 2011/1/12م.

16.موقع الجزيرة ميدان، **https: //www. aljazeera. net/midan/reality/**، مقال بعنوان بلا قنابل أو أسلحة. هكذا يمكن لروسيا تدمير البنية التحتيّة في أوكرانيا، تاريخ النشر 2022/2/12م.

17.موقع دنيا الوطن، **https: //www. alwatanvoice. com**، مقالة بعنوان الفضاء الإلكترونيّ الإسرائيلي. ما بين الأمن والتّجسس، تاريخ النشر 2021/11/4م.

18.عمر حرز الله، الحرب الإلكترونيّة: صراع في العالم الافتراضي، صحيفة البيان، تاريخ النشر 4/ 3 /2012. متاح على الرابط **https: //www. albayan. ae/five-senses/mirrors/2012-03-04** –

19.هدير عادل، باحثة أمريكي يكشف خبايا برنامج الحرب الإلكترونيّة الإيرانيّ، موقع العين الإخبارية، تاريخ النشر 2018\12\3 متاح على الرابط **https: //al-ain. com/article/iran-held-accountable-cyber-attacks-irgc**

20.أسامة صبري محمد: الحرب الإلكترونيّة ومبدأ التّمييز في القانون الدّوليّ الإنسانيّ، مجلة القانون للدراسات والبحوث القانونيّة، الإصدار (**47**)، كلية القانون - جامعة ذي قار، **2013: https: //www. researchgate. net/publication/334635853**.

21.رماح الدلقموني: الحرب الإلكترونيّة عندما يصبح الحاسوب فتاكاً، الجزيرة نت، حرر بتاريخ: **2016/ 10/16**.

22.سهيلة هادي: الحروب الإلكترونيّة في ظل عصر المعلومات، جامعة محمد خيضر-بسكرة، مجلة رؤى استراتيجية، **2017**: **https: //www. researchgate. net**

23.المجال الخامس. الحروب الإلكترونيّة في القرن 21، **https: //studies. Aljazeera. net/ar/issues/2010/20117212274346868. html**

24.الحروب السّيبرانيّة. العالم المجهول، **https: //podcasts. apple. com/sb/podcast**

25.القانون الدّوليّ الإنسانيّ وفتوى محكمة العدل الدّوليّة بشأن مشروعية التّهديد بالأسلحة النّوويّة أو استخدامها، 16 آذار / مارس 2016، موقع اللجنة الدّوليّة للصليب الأحمر، متوفر على الرابط الآتي: https://www.icrc.org/ar/publication/Ihl-icj-opinion-advisory-weapons-nuclear-use-or-threat-legality

26.الحرب السّيبرانيّة والقانون الدّوليّ الإنسانيّ، ورقة موقف، موقع اللجنة الدّوليّة للصليب الأحمر، متوفر على الرابط الآتي: https://www.icrc.org/ar/document/%D8%A7%D9%84%D8%AD%D8%B1%D8%A8%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%

-D9%86%D9%8A%D8%A9%

D9%86%D9%88%%D9%88%D8%A7%D9%84%D9%82%D8%A7%

-D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A%-D9%86

D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%

D9%8A%