جـــامـعـة الـــشـرق الأوسـط
MIDDLE EAST UNIVERSITY
Amman - Jordan

حروب الفضاء الإلكتروني؛ دراسة في مفهومها وخصائصها وسبل مواجهتها

Cyber War; A Study of its Concept, Characteristics and Ways to Confront it

إعداد:

صلاح حيدر عبدالواحد

إشراف:

الأستاذ الدكتور عبدالقادر محمد فهمي الطائي

قدّمت هذه الرسالة استكمالاً لمتطلبات الحصول على درجة الماجستير في العلوم السياسية

قسم العلـــوم السياسية

كلية الآداب والعـــــلوم

جامعة الشرق الأوسط

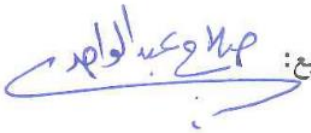
تموز، 2021

تفويض

أنا **صلاح حيدر عبدالواحد**، أفوّض جامعة الشرق الأوسط بتزويد نسخ من رسالتي ورقياً وإلكترونياً للمكتبات أو المنظمات أو الهيئات والمؤسسات المعنية بالأبحاث والدراسات العلمية عند طلبها.

الاسم: صلاح حيدر عبدالواحد.

التاريخ: 28 / 07 / 2021.

التوقيع: 

قرار لجنة المناقشة

نوقشت هذه الرسالة والموسومة بـ : **حروب الفضاء الإلكتروني؛ دراسة في مفهومها وخصائصها وسبل مواجهتها.**

للباحث: صلاح حيدر عبدالواحد.

وأجيزت بتاريخ: 28 / 07 / 2021.

أعضاء لجنة المناقشة

الاسم	الصفة	جهة العمل	التوقيع
د. ريما لطفي أبو حميدان	عضوًا من داخل الجامعة ورئيسًا	جامعة الشرق الأوسط	
أ. د. عبدالقادر فهمي الطائي	مشرفًا	جامعة الشرق الأوسط	
د. سحر محمد الطراونة	عضوًا من داخل الجامعة	جامعة الشرق الأوسط	
أ. د. وليد عبدالهادي العويمر	عضوًا من خارج الجامعة	جامعة مؤتة	

شكر وتقدير

اللهم لك الحمد حمداً كثيراً طيباً مباركاً، أحمدك وأشكرك على أن يسّرت لي إتمام هذه الرسالة على الوجه الذي أرجو أن ترضى به عني.

وأتقدّم بجزيل الشكر والعرفان لكلّ **من ساهم في تدريسي من دكاترة وأساتذة في جامعة الشرق الأوسط** الذين يرجع لهم الفضل – بعد الله عزّ وجلّ – في اجتياز هذه المرحلة.

كما أتقدّم بالشكر والتقدير والإمتنان لأستاذي ومشرفي **الأستاذ الدكتور عبدالقادر فهمي الطائي** على كلّ شيء قدّمه لي في هذا البحث المتواضع، الذي أسال الله تعالى أن يضيف قيمة إلى هذا العلم.

وأخيراً أتقدّم بجزيل شكري وامتناني إلى **كلّ من مدَّ يد العون والمساعدة** في إخراج هذه الرسالة على أكمل وجه، وكلّ من وقف معي وكان سنداً وعوناً لي في هذه المرحلة، أدامهم الله وجزاهم كلّ خير.

الباحث: صلاح حيدر عبدالواحد

الإهداء

إلى **والدي الغالي** رحمة الله عليك ... يامن غرست حب العلم في قلوبنا

إلى **أمي الغالية** ... أطال الله بقائك، وأكرمني بدعائك وعوضك تعبك خلال مشوار حياتنا

إلى **زوجتي وأولادي الأعزاء** ... من دعمني وتحمّلني طول فترة دراستي

إلى **إخواني وأخواتي** عنوان المودة والطيبة

إلى **أصدقائي**

إلى **بلدي الحبيب ... العراق**

فهرس المحتويات

الموضوع **الصفحة**

الفصل الأول: خلفية الدراسة وأهميتها

الفصل الثاني: الإطار المفاهيمي لحروب الفضاء الإلكتروني

الفصل الثالث: خصائص حروب الفضاء الإلكتروني ومسؤوليتها الدولية

الفصل الرابع: السُبُل والإمكانيات المتاحة لمواجهة حروب الفضاء الإلكتروني

الفصل الخامس: الخاتمة، الاستنتاجات والتوصيات

حروب الفضاء الإلكتروني؛ دراسة في مفهومها وخصائصها وسبل مواجهتها

إعداد: صلاح حيدر عبدالواحد

إشراف الأستاذ الدكتور: عبدالقادر محمد فهمي الطائي

الملخّص

هدفتْ الدراسةُ الى معالجةِ موضوع يعد من الموضوعاتِ الحديثةِ والبالغة الأهمية في الفكر الاستراتيجي ألا وهو موضوع حروب الفضاء الإلكتروني التي يمكن أن تمثلَ المظهر الجديد لحروب المستقبل. حيث اختصت الدراسة بالوقوف على ماهية هذه الحروب، وما الخصائص والسمات التي تتميز بها وما السبل والإمكانيات المتاحة لمواجهتها؟ وتمثلتْ مشكلةُ الدراسة بالوقوف على هذا النمط الجديد من الحروب، الذي يمثل ميدانه الفضاء الإلكتروني والأسلحة المستخدمة فيها شكلاً جديدا عن الأسلحة التقليدية أو النووية. كذلك تبيان الأضرار التي تلحق بالمرافق والمؤسسات ونظم المعلومات وطريقة إدارته مما يؤدي إلى شلّها وتعطيلها الأمر الذي يترتب عليها خسائر فادحة على الدولة والمجتمع وانتظام عمل المؤسسات بمختلف الميادين.

وعلى هذا، انطلقت الدراسةُ من افتراضٍ مفاده: أنّ ثمة توجه واهتمام ملحوظ لأن تكونَ حروبُ الفضاءِ الالكتروني وبفعل الخصائصِ والسماتِ التي تتميزُ بها بالمقارنة مع الحروب التقليدية أو الحروبِ التي تستخدمُ فيها أسلحة استراتيجيةٌ فوق التقليدية، هي البديلُ أو النمط المرجّح لحروبِ المستقبل.

وللتثبتِ من صحة هذا الافتراض اعتمدت الدراسة على عدة مناهج تحليلية منها، المنهجُ التاريخي الذي يذهبُ إلى تتبعِ المراحل التاريخية التي مرتْ بها الظاهرة موضع الدراسة، والمنهجُ المقارن الذي يعتمدُ على المقارنةِ بين ظاهرتين من خلالِ إبرازِ اوجهِ الشبهِ والاختلافِ بينهما، وما النتائج المترتبة على كلٍ منهما. والمنهجُ الوصفي التحليلي الذي يعتمدُ على الأسلوبِ الوصفي للظاهرةِ والعملِ على تحليلِ العناصر المتحكمة فيها، وصولاً إلى نتائج منطقية بشأنها، فضلاً عن المنهجِ القانوني الذي يعالج في جانب منه موضوع الحرب ومدى شرعيتها، وما المسؤولية القانونية المترتبة على الأطراف التي تلجأ إليها.

وعلى هذا، تمت معالجةُ موضوع حروب الفضاء الإلكتروني في ثلاثةِ فصولٍ، اختصّ الفصل الثاني منها بالإطارِ المفاهيمي لحروبِ الفضاء الإلكتروني، وفيه تمت معالجةُ مفهوم الحروب الإلكترونية وبعض النماذج التطبيقية التي جسدتْ ظاهرة الحرب الالكترونية، وانصرف الفصل الثالث إلى دراسةِ وتحليلِ خصائص حروب الفضاء الإلكتروني والسمات التي تتميزُ بها، بالاضافة الى معالجة الوضع القانوني لهذا النمط من أنماطِ الحروب، وما المسؤولية الدولية المترتبة على الأطراف

التي تلجأُ إليها من وجهة نظر القانون الدولي العام. أما الفصل الرابع من الدراسة فقد اختصَّ بتحديدِ أبرز السبل والامكانيات المتاحة لمواجهةِ حروبِ الفضاء الالكتروني والتعامل معها من خلالِ التعرف الى نوعينِ من الخياراتِ: الأول هو الخيارُ التقني، والثاني هو الخيارُ التشريعي.

هذا وقد خلصت الدراسة إلى خاتمة وعدة استنتاجات، نذكر منها:

1. أنّ الفضاءَ الإلكتروني، وبفعلِ عواملَ معينةٍ يمكن أن يكونَ ميدان الحروب المستقبلية بدلاً عن الميدان الأرضي في الحروبِ التقليدية.
2. أنّ الفضاء الإلكتروني الذي تجري فيه الحروب الالكترونية هو فضاء افتراضي، وبالتالي له طبيعةٌ وخصائصٌ مغايرةٌ عن العالمِ المادي، وعلى هذا، فإنّ الهجمات الإلكترونية عَزَّزت من مستوياتِ وفرصِ الحرب اللامتماثلة، مع تمكينِ دول متفاوتة بالقوة عن شنّ هجماتٍ ضدَّ دولٍ أقوى منها.
3. بسبب من طبيعة أسلحة الفضاء الإلكتروني، فإن قيمةَ الردع لم تعدْ تعمل كما هو عليه الحال في نظامِ الأسلحة التقليدية أو الأسلحة الاستراتيجية النووية بمعنى أنّ قيمةَ الردع كأسلوبِ واستراتيجيةِ العمل العسكري تراجعت إلى أبعاد واضحة، إن لم نقلْ أنّ استراتيجيةَ الردع في ظلّ منظومةِ أسلحة الفضاء الإلكتروني، أصبحت واهنة ولم يعد لها تأثير واضح.
4. أنّ التحدي الأكبر الذي يواجهُ التنظيم القانوني للهجمات في الفضاءِ الإلكتروني هو عدمُ وجود إرادة دولية على صعيدِ المفاوضات أو على صعيد قرارات مجلسِ الأمن، حيثُ تَغيبُ الإرادة الدولية اللازمة للدفعِ باتجاهِ ذلك، وخصوصاً من قبلِ القوى المهيمنة في هذا المجال.

كما وخلصت الدراسة إلى عدد من التوصياتِ أهمها: ضرورةُ تطوير استراتيجيات جديدة في الدولِ العربيةِ تتلاءم مع التحدياتِ الأمنية المستجدةِ للعصر الرقمي، وزيادة التركيز على الأمن الإلكتروني باعتبارِه مرتبطاً بقضايا التنمية الاقتصادية والاجتماعية والاستقرار السياسي، وضرورة صياغة استراتيجية عربية مشتركة لمواجهةِ تصاعد الأخطار الإلكترونية وتعزيز أمن الفضاء الإلكتروني والتعاون في مجالاتِ مكافحةِ المخاطر الإلكترونية.

الكلمات المفتاحية: الحرب، حروب الفضاء الإلكتروني، الهجمات الإلكترونية.

Cyber War; A Study of its Concept, Characteristics and Ways to Confront it

Prepared by: Salah Hayder Abdul Wahid

Supervised by: Prof. Dr. Abdel Qader Mohammad Fahmi Al-Taie

Abstract

The study aimed to address one of the modern and extremely important topics in strategic thought, which is the topic of cyber wars, which could represent the new aspect of future wars.

The study focused on finding out what these wars are, what are the characteristics and features that characterize them, and what are the means and possibilities available to confront them?

The problem of the study was to identify this new type of warfare, the field of which is cyberspace and the weapons used in it a new form of weapons. In addition to showing the damage to facilities, institutions and information systems, and the way they are managed, which leads to their paralysis and disruption, which results in huge losses for the state and society and the regularity of the institutions' work in various fields.

Accordingly, the study proceeded from the assumption that: There is a noticeable tendency and interest for cyber wars, due to the characteristics and features that characterize them, compared to conventional wars or wars in which unconventional strategic weapons are used, as the likely alternative or pattern for future wars.

To verify the validity of this assumption, the study relied on several analytical approaches, including the historical approach, which goes to trace the historical stages that the phenomenon under study has gone through, and the comparative approach, which depends on the comparison between two phenomena by highlighting the similarities and differences between them, and the results of each of them. And the descriptive-analytical approach that relies on the descriptive method of the phenomenon and work on analyzing the elements that control it, leading to logical conclusions about it, as well as the legal approach that deals in part with the issue of war and the extent of its legitimacy, and what is the legal responsibility of the parties that resort to it.

Accordingly, the topic of cyberspace wars is dealt with in three chapters. The second chapter is devoted to the conceptual framework of cyber wars, in which the concept of cyber wars and some applied models that embodied the phenomenon of cyber war were

addressed. The third chapter focused on studying and analyzing the characteristics and features of cyberspace wars, in addition to addressing the legal status of this type of war, and the international responsibility of the parties that resort to it from the point of view of international law. As for the fourth chapter of the study, it was devoted to identifying the most prominent ways and possibilities available to confront and deal with cyber wars by identifying two types of options: the first is the technical option, and the second is the legislative option.

The study reached several conclusions, including:

1. That cyberspace, due to certain factors, could be the field of future wars instead of the ground field in conventional wars.
2. The cyberspace in which cyber wars take place is a virtual space, and therefore has a different nature and characteristics from the physical world, and accordingly, cyber-attacks have enhanced the levels and opportunities of asymmetric warfare, by enabling countries with varying strength to launch attacks against countries that are stronger than them.
3. Because of the nature of cyber weapons, the value of deterrence no longer works as it is in the case of conventional weapons or strategic nuclear weapons, meaning that the value of deterrence as a method and strategy of military action has declined to specific dimensions, if we do not say that the strategy of deterrence under the cyber weapons system, has become weak and no longer visible effect.
4. The biggest challenge facing the legal regulation of attacks in cyberspace is the lack of an international will at the level of negotiations or at the level of Security Council resolutions, where the necessary international will to push for this is absent, especially by the dominant powers in this field.

The study also concluded a number of recommendations, the most important of which are: the need to develop new strategies in the Arab countries that are compatible with the emerging security challenges of the digital age, and to increase the focus on electronic security as it is linked to issues of economic and social development and political stability, and the need to formulate a joint Arab strategy to confront the escalation of electronic dangers and enhance space security. e-mail and cooperation in the areas of combating cyber risks.

Keywords: War, Cyber wars, Cyber-attacks.

الفصل الأول
خلفية الدراسة وأهميتها

الفصل الأول
خلفية الدراسة وأهميتها

المقدمة

طالما كانت الحرب وسيلة لتحقيق أهداف وغايات منشودة من ورائها، تتمثل أساساً في إرغام العدو والخصم الخضوع لإرادة القوة التي اختارت اللجوء لخوض الحرب، وذلك عبر استخدام الوسائل العسكريّة. وقد استمر التغيير في شكل الحروب والمواجهات المسلحّة مع استمرار التغيير في الأدوات والتقنيات المستخدمة فيها بغرض التغلّب على الطرف الآخر؛ بدءاً من أبسط الأدوات القتالية التي وظفّتها المجتمعات البدائية وصولاً في العصر الحديث إلى الأسلحة النوويّة، والكيميائيّة، والبيولوجيّة، التي تم تطويرها خلال عقود من الزمن. ومع هذا التغيير في تقنيات الأدوات القتالية المستخدمة في الحروب فإن العنصر الثابت فيها بقي متمثلاً في ثني إرادة الخصم وإخضاعها لإرادة الطرف المنتصر.

مع التطوّرات الحاصلة في مجال التقنيات وتزايد اعتماد الدوّل على الاتصالات والشبكات الالكترونيّة في إدارة وتوجيه مختلف البُنى والمفاصل الحيويّة في مؤسسات الدولة، العسكريّة منها والمدنيّة، بدأ يظهر بشكل متزايد خطر محدق جديد يتمثل في إمكان لجوء الأعداء إلى إلحاق الضرر والأذى والدمار بالدولة من خلال الاقتصار على استهداف هذا الفضاء الالكترونيّ المتشكّل حديثاً، دون الحاجة إلى اللجوء لتحشيد الجيوش والمقاتلين وما يرافق ذلك من بيانات وإعلانات الحرب الصريحة، وهكذا ظهر تدريجياً ما بات يعرف بحروب الفضاء الالكترونيّ.

ونظراً لاختلاف خصائصها، واختلاف طبيعة المواجهة فيها، عمّا كان الحال عليه في الحروب التقليديّة، بات من الجليّ أن هذه الحروب لم تأتِ فقط بتقنيات مختلفة للمواجهة والاستهداف، وإنما

حملت معها أيضاً تغييراً في أسس العقيدة القتاليّة التي تقوم عليها الحروب التقليديّة، وغيّرت جذرياً من مفاهيم الإرغام والردع التي كانت سائدة في الحروب التقليّديّة؛ حيث بات العدو متخفياً وباتت المعارك تدار بطرق غير مباشرة، وباتت الهجمات توجّه من مصادر ومواقع مجهولة، وبالتالي أصبح الردّ عليها مسألة أكثر تعقيداً. وهكذا، فإن حروب الفضاء الإلكترونيّ أضحت تلحّ وبشكل متزايد إلى المزيد من الفحص والتحليل، بغية الخروج باستنتاجات تساهم في بلورة تحديد أدقّ لمفهومها، وخصائصها، وأساليبها، وكذلك تصوّر آفاقها المستقبليّة.

مشكلة الدراسة

تمثلتْ مشكلةُ الدراسة بالوقوف على هذا النمط الجديد من الحروب، الذي يمثل ميدانه الفضاء الإلكتروني والأسلحة المستخدمة فيها شكلاً جديدا عن الأسلحة التقليدية أو النووية. كذلك تبيان الأضرار التي تلحق بالمرافق والمؤسسات ونظم المعلومات وطريقة إدارته مما يؤدي إلى شلّها وتعطيلها الأمر الذي يترتب عليها خسائر فادحة على الدولة والمجتمع وانتظام عمل المؤسسات بمختلف الميادين.

أهداف الدراسة

تهدف الدراسة إلى:

1. التعرّف إلى ماهيّة حروب الفضاء الالكترونيّ.
2. التعرّف على الخصائص التي تتميز بها حروب الفضاء الالكترونيّ.
3. التعرّف على السبل والإمكانات المتاحة لمواجهتها.

فرضية الدراسة

تقوم الدراسة على افتراض مفاده: الثورة العلمية في المجال التكنو–معلوماتي أسهمت بشكل واضح في انتاج أدوات يمكن توظيفها لتكون النمط المرجح لحروب المستقبل.

أسئلة الدراسة

تحاول الدراسة الإجابة عن الأسئلة التالية:

1. ما حروب الفضاء الإلكترونيّ؟
2. ما الخصائص التي تتميز بها حروب الفضاء الإلكترونيّ؟
3. ما السبل والإمكانات المتاحة لمواجهتها؟

أهمية الدراسة

تتمثل أهمية الدراسة في جانبين:

الأهمية العلميّة

تأتي الأهمية العمليّة من خلال تركيزها على الفضاء الإلكتروني الذي عالجته بعض الدراسات الأكاديمية العربيّة والأجنبيّة، وذلك إن دراسة حرب الفضاء الإلكترونيّ واستراتيجيّة مواجهتها يعتبر حقلاً جديداً في مجال الدراسات الاستراتيجيّة والأمنيّة، الذي يبدو أنه لم يتحرر بعد وبشكل واضح من قيود الدراسات التقليديّة المختصّة بالحروب وأساليب مواجهتها مثلما بحث في حقل العلاقات الدولية.

الأهمية العمليّة

إن دراسة وفهم الحروب السيبرانية هي من الأهمية بمكان، إذ إن المؤشرات تتزايد على توجه الدول على نحو متسارع لاعتماد الهجمات الإلكترونية في تكتيكاتها واستراتيجياتها فيما يخص علاقاتها

بالدول الأخرى ونزاعاتها معها، وبالتالي فإن الفهم الأفضل والأعمق لها يفرض على الباحثين وصنّاع القرار العمل من أجل تطوير استراتيجيات تتبنى وتوظّف هذه الأساليب المستحدثة على أفضل وجه، من أجل التصديّ لأيّ هجمات متوقعة من هذا النوع في المستقبل.

حدود الدراسة

- **الحدود الزمنية:** منذ عقد عام 1991م من القرن الماضي، وحتى العام 2020م.
- **الحدود المكانية:** جميع دول العالم.

مصطلحات الدراسة

1. الحرب (War)

- لغةً:

هي قتال ونِزال بين فئتين، وهي عكس السلم (ابن منظور، 1994، ج4: 188).

- اصطلاحاً:

عرفها كارل فون كلاوزفيتز بأنها: ليست فناً ولا علماً؛ هي أكثر من ذلك، هي شكل من أشكال الوجود الاجتماعي، إنها نزاع بين المصالح الكبرى يسويه الدم. إن السياسة هي الرحم الذي تنمو فيه الحرب، وتختفي فيه الملامح التي تكونت بصورة أولية، كما تختفي خصائص المخلوقات الحية في أجنتها (كلاوزفيتز، 1988: 167).

- إجرائياً:

المقصود بالحرب في هذه الدراسة هي الحروب والمواجهات التي تجري في الفضاء الإلكتروني.

2. الفضاء الالكترونيّ (Cyber Space)

- لغةً:

هو ما اتسع من الأرض (ابن منظور، 1994، ج15: 158)

- اصطلاحاً:

عرّفه عبد القادر محمد فهمي بأنه: يمثّل مجموع شبكات الحاسوب في العالم، وكل ما ترتبط به وتتحكم فيه هذه الشبكات. وهو لا يقتصر على شبكة الانترنت فقط، وإنما يشمل العديد من شبكات الحاسوب الأخرى، فالفضاء الإلكتروني يشمل كل شبكات الحاسوب التي تدير نشاط الدول ومؤسساتها ومرافقها وكل ما يتعلق ببيئتها الحيوية، وفي القطاعات المدنيّة والعسكريّة (فهمي، 2018: 17).

- اجرائياً:

المقصود به في هذه الدراسة مجموع شبكات الحاسوب وكل ما ترتبط به وتتحكم فيه هذه الشبكات.

3. حروب الفضاء الالكترونيّ (Cyber War)

- اصطلاحاً:

عرفها جون أركويلا وديفيد رونفيلدت بأنها: "تنفيذ العمليات العسكرية، والاستعداد لتنفيذها، وفقاً للمبادئ المعلوماتية، من خلال تعطيل، أو تدمير، نظم المعلومات والاتصالات على أوسع نطاق. وتشمل أيضاً: تدمير العقيدة العسكرية للعدو، التي يعتمد عليها لتحديد هويته، وخططه، وتصرفاته، وأهدافه، والتحديّات التي يواجهها، وذلك عبر معرفة كل شيء عن العدو، ومنعه في الوقت نفسه من معرفة أي شيء عن الطرف الآخر، وتحويل ميزان المعرفة ليكون في مصلحة هذا الطرف" (Arquilla, 1993: 1).

وعرفها جوزيف ناي بأنها: "الأعمال العدائية في الفضاء السيبراني التي لها آثار تعادل أو تفوق العنف الحركي التقليدي" (Nye, 2011: 18).

وعرفها كينيث جيرز بأنها: "القدرة على الدفاع عن والهجوم على المعلومات، من خلال شبكات الحاسب الآلي عبر الفضاء الإلكتروني، بالإضافة إلى شلّ قدرة الخصم على القيام بهذه الهجمات نفسها. وتشمل هذه الحرب خمسة عناصر رئيسيّة، هي: التجسس، والدعاية، والحرمان من خدمة الإنترنت، وتعديل البيانات والتلاعب بها، والتلاعب أيضاً بالبنية التحتيّة" (Geers, 2013: 1).

وعرّفها عبد القادر محمد فهمي بأنها: هجمات تستخدم فيها المنظومة الشبكيّة والأجهزة الحاسوبيّة للدولة، أو الفاعلين من غير الدول، لتعطيل كفاءة السيطرة والقدرة على التحكم في منظومة أجهزة أو شبكات الحاسوب وما تتضمنه من بيانات ومعلومات للفاعلين الآخرين من الدول وغير الدول، أو تقليلها، أو حتي تدميرها، سواء كان ذلك على مستوى البنية التحتية الوطنية للدولة، أو على مستوى منظومات قوّتها العسكريّة، وبالشكل الذي يعرّض الأمن القومي للدولة إلى تهديد جسيم (فهمي، 2018: 20).

- اجرائياً:

هي الهجمات التي شنتها بعض الدول مثل الولايات المتحدة الأمريكية والصين واسرائيل وايران، وكان مسرحها هو الفضاء الالكترونيّ، بغرض إلحاق الضرر بالمنشآت والبنى التحتية والأهداف العسكرية للدولة التي تعرضت للهجوم.

الإطار النظري والدراسات السابقة

أولاً: الإطار النظري

تعرّف الحرب أنها مواجهة مسلحة لقوّات نظاميّة بين دولتين أو أكثر، توظف فيها كل أدوات ووسائل العنف المادي، بكل صنوفه القتاليّة، بهدف الانتصار على العدو وإخضاعه وفرض الإرادة السياسية عليه. وهي من أقدم الظواهر التي عرفتها البشريّة، وقد عرفتها المكونات الاجتماعية بدءاً من الأسرة ومروراً بالقبيلة، وانتهاءاً بالتنظيم السياسي الأكثر تعقيداً، وهو الدولة. والحرب هي امتداد للسياسة ولكن بوسائل أكثر عنفاً، تلجأ إليها الدولة عندما تجد أن مصالحها باتت مهددة، فتكون بمثابة الحلّ النهائي والوسيلة الأخيرة بعد أن تعجز الوسائل الأخرى عن حسم التناقضات (فهمي، 2014: 123).

كغيرها من الظواهر، أصاب ظاهرة الحرب الكثير من التغيّر في الأدوات والوسائط المستخدمة فيها، الأمر الذي جعل عقيدتها العسكريّة متغيّرة بالتوازي مع ما يستحدث من وسائل وأدوات قتاليّة. ومع دخول عصر حروب الفضاء الإلكتروني، فإنّ العقيدة العسكريّة والمذهب القتاليّ المعتمد فيها تغيّر عن الذي كان سائداً في الحروب التقليديّة، وتحوّلت إلى عقيدة جديدة مفادها أن الفضاء الإلكترونيّ أصبح يمثل ساحة المعركة الجديدة وميدانها، وأن من يسيطر على هذا الفضاء يسيطر على سير المعارك على الأرض وفي الجو، وبذلك يستطيع حسم المعركة لصالحه ومن ثم الانتصار في الحرب؛ فحروب الفضاء الإلكترونيّ تكون عبر الدخول في الشبكات الإلكترونيّة والسيطرة عليها أو تدميرها، ما يعني شلّ قدرات الدولة ونشاطها وتعطيل عمل مؤسساتها. إنّ حروب الفضاء الإلكتروني غيرت بالفعل طبيعة الحرب ذاتها، وأخرجتها من النمط التقليدي إلى نمط آخر جديد؛ وذلك نتيجةً لاختلاف ميدان المعركة والأدوات المستخدمة، والأهداف المراد تحقيقها والنتائج المترتبة

عليها، بالمقارنة مع الحروب التقليدية؛ إذ لا تستهدف الحروب الالكترونية في غاياتها تدمير الآلات والمعدّات العسكريّة والبشريّة للعدو، ولا يدخل في أجندتها الاستيلاء على أرض العدو واحتلالها، وإنما يكون مسرحها هو الفضاء الشبكيّ، والأهداف فيها تكون برامجيّة، وبذلك فهي قد اسهمت أسس العقيدة العسكريّة السائدة في الحروب التقليديّة (فهمي، 2018: 20).

هذا التطوّر في العقيدة العسكريّة التقليديّة الذي أسهم في تغييرها حروب الفضاء الالكترونيّ فرض على الدول البحث عن استراتيجيات لمواجهتها، من قبيل تطوير وسائل تقنية دفاعيّة، مثل تطوير أنظمة إنذار مبكر ضد الهجمات، وتطوير برامج الحماية والتصديّ. وكان في مقدمة الإجراءات أيضاً قيام عدد من الدول بتأسيس جيوش ووحدات عسكرية سيبرانيّة خاصّة بهدف تعزيز قدراتها الدفاعيّة في الفضاء السيبرانيّ، وتزويدها بالكوادر المدربة، وتدعيم قدراتها بأحدث تقنيات المواجهة في الفضاء السيبراني، وفي سبيل ذلك عمدت إلى تجنيد محترفي القرصنة والبرمجة في وحدات قتاليّة خاصة ضمن صفوف القوات المسلحة، ومن أمثلة ذلك: القيادة السيبرانية الأمريكية، والوحدة (61398) في الصين، وقراصنة الظل التابعين للحكومة الروسية، والوحدة (8200) في إسرائيل (خليفة، 2018: 20).

إضافة إلى ذلك قام عدد من الدول بتأسيس مراكز متخصصة للقيام بمهمة الدفاع السيبراني، ومن ذلك قيام بريطانيا بتأسيس مركز وطني للتصدي للهجمات الإلكترونية عام 2017م، والذي يرتبط بشكل مباشر بوكالة الاستخبارات البريطانية، وأنيطت به مهمات هي: تحسين معايير الأمن السيبراني في البلاد، وتحديد هوية ومصدر الهجمات حال وقوعها ومن ثم تحديد طرق الرد عليه، وتقديم الدعم لمن تقع عليهم أضرار جراء تلك الهجمات السيبرانية وخاصة في القطاع المالي. وكذلك فرنسا، ففي أعقاب إعلان الجيش الفرنسي عن إحباط أربعة وعشرين ألف هجوم إلكتروني على وزارة

الدفاع عام 2016م، تم الإعلان عن تأسيس قيادة عسكرية للدفاع الإلكتروني عام 2017م، ومع تنامي مخاطر الهجمات الإلكترونية أعلنت وزيرة الدفاع الفرنسية، فلورنس بارلي، في كانون الثاني (يناير) من العام 2019م، عن "إمكانية التوجه نحو خيار القيام بضربات استباقية". باعتبار ذلك حقاً دفاعياً مشروعاً. وكذلك اتجهت الولايات المتحدة الامريكيّة لتبني استراتيجية تقوم عمل على نوع من الردع، مفادها شنّ الهجوم المضاد في حال التعرض لأيّة هجوم، وجاء الإعلان عن ذلك عام 2018م، على لسان جون بولتون، مستشار الرئيس الأميركي دونالد ترامب للأمن القومي، إثر الإعلان عن أول وثيقة رسمية أمريكيّة للدفاع الإلكترونيّ (صحيفة العرب، 2018/9/21).

ثانيا: الدراسات السابقة

الدراسات باللغة العربيّة

- **دراسة محمود، محمد سعد (2020). الحرب السيبرانية: أدواتها، وقودها، خسائرها.**

هدفت الدراسة إلى التعريف بالحرب السيبرانية، واستعراض تاريخ ومراحل تطورها، وبيان مدى خطورتها وآثارها على الدول والشعوب. وافترضت الدراسة أن الحروب لم تعد مقتصرة على استخدام الأسلحة الفتّاكة التي تحملها الطائرات أو المدرعّات أو الجنود، فهذه توشك ان تتوارى في المستقبل، وراء ظلّ حروب ستكون اكثر فتكاً، وهي الحروب الالكترونية. وقد تناولت الدراسة الطرق والتقنيات الهجومية المستخدمة في حروب الفضاء الإلكتروني، مع التفصيل في أهم أنواع البرامج الخبيثة المستخدمة في هذه الهجمات. كما تضمنت الدراسة تعريفاً بأهم الطرق والوسائل الإلكترونية المتاحة للحماية من هذه الهجمات. وخَلُصّت الدراسة إلى أن الوسائل لمستخدمة في هذه الحروب تشهد تطوراً متسارعاُ في أدواتها وبرمجياتها ما يستوجب الاستمرار في تطوير المنظومات المضادة وتطوير منظومات شاملة من أجل الحماية من هذه الهجمات.

- **دراسة خليفة، إيهاب (2018): الحرب السيبرانية؛ مراجعة العقيدة العسكرية استعداداً للمعركة القادمة.**

هدفت الدراسة إلى توضيح المقصود بمفهوم الحرب السيبرانية، والجدالات النظريّة حولها، واستدعاء بعض المؤشرات والدلالات التي تسهم في بلورة المفهوم، بالإضافة إلى استيضاح أثر الحرب السيبرانية على مفهوم الأمن، وكذلك على بنية الجيوش والمؤسسات العسكرية للدول. وافترضت الدراسة أن هذا النوع من الحروب كان له أثر مباشر في توسيع مفهوم الأمن وتجاوز التعريفات التقليدية المرتبطة بالبعد العسكري. تناول الباحث ظاهرة تشكيل الجيوش السيبرانية، مع بيان أبرز المهام التي يمكن أن تقوم بها. كما تناول الباحث محفزات اندلاع حرب سيبرانية قريبة، واعتبر إنها تتمثل في سرعة تطور شكل الهجمات السيبرانية، وضيق الفجوة الزمنية بين الهجمات الكبرى، إضافة إلى تزايد التوجه نحو الاعتماد على العملات الإفتراضية الرقمية، وتزايد مستويات ومعدلات الرقمنة عموماً.

وخلصت الدراسة إلى عدد من النتائج أهمها أن هناك دور بارز للفاعلين من غير الدول في هذه الحروب، يكون مساوياً لدور الدول، بما في ذلك الحركات الإرهابيّة أو حتى الأفراد العاديين. وأن هناك تزايد في فرص اندلاع هذه الحروب مع انتشار التكنولوجيا، وتوجه الجيوش نحو الاعتماد على الاسلحة القتالية ذاتية التشغيل، وتوجه الدول نحو تبني نماذج المدن الذكيّة التي تعتمد بشكل كليّ على تكنولوجيا المعلومات والاتصالات لإدارة جميع متطلبات الحياة اليومية فيها، إضافة إلى التوجه نحو اعتماد النظم المالية والمصرفية والإدارية المعتمدة على الإنترنت.

- **دراسة شكر، عمر (2018): المجال الخامس؛ الفضاء الإلكتروني.**

هدفت الدراسة إلى التعرّف على أبعاد ومدى خطورة الصراع في الميدان الإلكتروني. وافترضت الدراسة أنه بازدياد الاعتماد على الحاسوب وشبكات الإنترنت في البنية التحتية تزداد إمكانية تطوّر الهجمات الإلكترونية لتصبح سلاحاً حاسماً في النزاعات بين الدول. واعتبر الباحث أنه من المتوقع

أن تصبح الحرب الإلكترونية نموذجاً تسعى إليه العديد من الجهات نظراً للخصائص العديدة التي تنطوي عليها، ومنها: أن التكلفة المتدنيّة نسبياً للأدوات اللازمة لشنّ هكذا حروب يعني أنه ليس هناك حاجة لتصنيع أسلحة مكلفة جداً مثل حاملات الطائرات والمقاتلات المتطورة. بالإضافة إلى فشل نماذج الردع المعروفة في هذا الفضاء؛ حيث الردع بالانتقام أو العقاب لا ينطبق على هذه الحروب؛ إذ من الصعب رصد هذه الهجمات وتحديد جهتها، وبعضها يحتاج أشهراً لذلك.

وبيّنت الدراسة أن مخاطر هذه الهجمات تتعدى استهداف المواقع العسكرية؛ إذ لا ينحصر إطار حروب الفضاء الإلكتروني باستهداف المواقع العسكرية، وإنما هناك جهود متزايدة لاستهداف البنى التحتية المدنيّة والحسّاسة. واستعرض الباحث أبرز الهجمات الإلكترونية في العقدين الماضيين، ثم استعرض الإجراءات الوقائية التي اتخذتها الدول لمواجهة الهجمات الإلكترونية، مبيناً أن هناك إجراءات على المستوى القانوني، كإقرار تشريعات متعلقة بالحماية، وإجراءات على مستوى التعاون بين الدول، كتوقيع اتفاقيات ومعاهدات دفاع إلكتروني.

وخلصت الدراسة إلى عدد من النتائج أهمها إن هناك تزايد في اهتمام الدول، خاصة المتقدمة، بالمجال الخامس، وهو الفضاء الإلكتروني، بما في ذلك إنشاء جيوش قادرة على شن الهجمات، وهو ما بات يأخذ حيزاً كبيراً في سياسات الدول واستراتيجياتها. وأن الهجمات الإلكترونية باتت أكثر خطراً؛ خاصة مع التطور التكنولوجيّ، وعليه فإن السلاح الإلكتروني بات بالفعل المجال الخامس إلى جانب المجالات الأربعة (البر، والبحر، والجو، والفضاء) التي تتنافس عليها الدول.

- **دراسة محمد فهمي، عبد القادر (2018): الحروب التقليدية وحروب الفضاء الإلكتروني؛ دراسة مقارنة في المفاهيم وقواعد الاشتباك.**

سعت الدراسة إلى التعرّف على حقيقة الخصائص التي جاءت بها الحروب الإلكترونيّة، وتحديد طبيعتها، وما الذي حملته من سمات جعلت منها شكلاً متميزاً عن الحروب التقليدية. وقامت الدراسة على افتراض أن الفضاء الإلكترونيّ اخرج موضوع الحرب من أطرها وأحكامها التقليدية إلى آفاق لم تكن مألوفة من قبل، ومن هذه الفرضية اشتق الباحث فرضية أخرى مفادها أن حروب الفضاء الإلكتروني يمكن أن تكون النمط المرجح لحروب المستقبل. وللتثبت من صحة الفرضيتين تم اعتماد المنهج المقارن وذلك بغرض دراسة طبيعة حروب الفضاء الإلكترونيّ وتحليلها، واستكشاف ما الذي تميزت به عن الحروب التقليديّة.

في المبحث الأول تناولت الدراسة معنى الحرب وماهيّتها، وبيّن بأنها مرتبطة بالإرادة السياسية. ثم تناول مفهوم الحرب الإلكترونية، ومفهوم الفضاء الإلكتروني، كما استعرض خصائص حروب الفضاء الإلكتروني، وأبرزها: قلة تكلفتها، وانعدام ضحاياها البشرية، وسرعتها. وفي المبحث الثاني، تناول الباحث مستويات الحروب الإلكترونية بالمقارنة مع الحروب التقليدية، وذلك وفقاً لمستويين: المستوى المرتبط بالعقيدة العسكريّة وقواعد الاشتباك، والمستوى المرتبط بالفاعلين والأسلحة المستخدمة.

وخلصت الدراسة إلى عدة نتائج أهمها الكشف عن وجود فوارق نوعيّة بين الحروب الإلكترونية والحروب التقليدية. وأن حرب الفضاء الإلكتروني حقيقة واقعة، وإن ما نشهده حتى الآن لا يقارن بما يمكن أن يحدث، وأنه على خلاف الحروب التقليدية، فإن حرب الفضاء الإلكتروني تحدث بسرعة الضوء، وهو ما يخلق مخاطر جديّة أمام صناع القرار أثناء الأزمات.

الدراسات باللغة الأجنبية

- **Geers, Kenneth (2008): Cyberspace and the Changing Nature of Warfare.**

دراسة جيرز، كينيث (2018): الفضاء السيبراني والتغير في طبيعة الحرب.

يفترض الباحث بأن حروب الفضاء الإلكترونيّ ذات جدوى عالية بالنسبة للطرف المهاجم فيها، وهو ما جعل اللجوء لها في تصاعد مستمر بين الدول. ويقدم تحليلاً لأسباب هذا التصاعد لجوء الدول؛ إذ يرى بأن أهم الأسباب هو إمكانية وسهولة الاستهداف في الفضاء الإلكتروني وعدم وجود تكلفة رادعة، وكذلك عدم كفاية أنظمة الدفاع القائمة.

يعرض الباحث لشرح أهم التكتيكات المعتمدة في هذه الحروب، بدايةً من بثّ الخطابات المعاديّة (البروباجاندا) عبر وسائل الإعلام الالكترونيّة، وحتى الهجوم على قواعد البيانات المتحكمة بالبنى التحتية والتلاعب بها. تعرض الدراسة أيضاً نماذج ودراسات حالة لحروب الفضاء الالكترونيّ.

خلصت الدراسة إلى عدّة نتائج أهمها أن جميع الحروب اليوم بات لها بعد إلكترونيّ؛ بحيث بات جانب هام منها بالضرورة يُدار على مستوى الفضاء الالكترونيّ. وفي النهاية توصي بضرورة رفع الوعي لدى القيادات العسكريّة بطبيعة هذه الهجمات.

- **Graham, David (2010): Cyber Threats and the Law of War.**

دراسة جراهام، ديفيد (2010): التهديدات السيبرانيّة وقانون الحرب.

هدفت الدراسة إلى الاجابة على سؤال كيفيّة تطبيق قوانين الحروب الدوليّة على حروب الفضاء الالكترونيّ. وافترضت الدراسة إن القوانين الحالية تشملها، وإن كان ذلك ضمناً لا نصاً؛ وذلك باعتبار أن هذه الحروب تستهدف البنى التحتية للدولة التي تتعرض للهجوم، وبالتي هي تشترك مع الحروب

التقليديّة من حيث النتيجة النهائية للعمل الهجوميّ. وقد استخدم الباحث المنهج القانوني لإثبات فرضيته هذه.

تناول الباحث إشكالية عدم شمول ميثاق الأمم المتحدة صراحةً لهكذا نوع من الحروب، إذ إن البنود والمواد تتحدث عن القوة المادية. إلا أنه ذهب إلى اعتبار أن مفردات "القوّة" و"الهجوم" الواردة في النصوص قد تتسع لتشمل الهجمات الالكترونيّة.

وتعرض الباحث لسؤال إذا ما كانت هجمات الفضاء الإلكتروني تعتبر بمثابة هجمات مسلحة، مشيرة إلى إشكاليات عدّة تتمثل أساساً في إشكالية تحديد الجهة المسؤولة عن الهجمات، وإشكالية تحديد مكان الانطلاق، خصوصاً مع إمكان توظيف الدول لوكلاء غير رسميين للقيام بمثل هكذا هجمات.

وخلصت الدراسة إلى عدد من النتائج أهمها أن للدول الاحقيّة في قيامها باجراءات دفاعية إزاء هذا الهجمات، بما في ذلك استهداف منشآت وبنى تحتية يثبت أن الهجمات الإلكترونية تنطلق منها، ويجد الباحث بان مثل هذه السلوك الدفاعيّ هو سلوك شرعي طبقاً للمادة (51) من ميثاق الأمم المتحدة؛ إذ أن الهجمات السيبرانيّة تنتهي بالنهاية لإحداث الأضرار المادية والبشرية في الدولة المستهدفة. ويوصي الباحث بضرورة انخراط الدول في معاهدات أمنيّة مشتركة تضمن عدم تورط أياً منها في مثل هذا النوع من الهجمات.

- **Robinson, Michael (2015): Cyber Warfare: Issues and Challenges.**
دراسة روبنسون، مايكل (2015): الحرب السيبرانية؛ قضايا وتحديّات.

سعى الباحث للإجابة على سؤال ما هي الحرب السيبرانيّة؟ وقد توسع الباحث في البحث بالتعريفات التي تم تقديمها لهذه الحروب ومقارنتها، وخلص إلى ملاحظة أنه لا يوجد حتى تاريخ

الدراسة تعريف تم تبنيه على نطاق واسع. ثم سعى في محاولة صياغة مفهوم محدد لها، حاول فيه شمول الفاعلين من غير الدول ضمن التعريف، اضافة إلى محاولة تحديد حدود الفضاء الإلكتروني المستخدم في الحروب، وما هي المساحات التي لا يمكن اعتبارها من ضمنه. كما سعى الباحث إلى التفريق بين الهجمات من حيث الأهداف، ما بين أهداف عسكريّة وأخرى ماليّة وغيرها.

وخلص الباحث إلى أنه هناك جوانب تقنيّة في الحروب السيبرانيّة لا يمكن تجاوزها فهما؛ إذ لا يمكن حصرها بحال ضمن الأبعاد العسكريّة؛ وبالتالي فإنه لا بد من تطوير مقاربة متعددة التخصصات، تشمل حتى البرمجيّات الالكترونيّة، في سبيل دراسة وتحليل هذا النوع المستجدّ من الحروب.

ثالثاً: ما يميز هذه الدراسة عن الدراسات السابقة

سوف تتميز هذه الدراسة في تناولها للأبعاد المتعلقة بطبيعة حروب الفضاء الإلكترونيّ، بما في ذلك استخلاص وتحديد ملامح العقيدة القتالية المتبعة فيها، وقواعد الاشتباك، وكذلك تعالج الدراسة أهم استراتيجيات المواجهة والدفاع التي تبنتها الدول في هذه الحروب.

منهجيّة الدراسة

للتثبت من صحة فرضيّة التي انطلقت منها الدراسة، فإنه تم الاعتماد على المناهج التالية:

المنهج التاريخي

ينطلق المنهج التاريخي من افتراض مفاده إن هناك ضرورة في العودة إلى الأحداث الماضية لغرض فهم وتحليل امتداداتها من أحداث وظواهر راهنة. ومن أهم رواد هذا المنهج المؤرخ اليوناني ثيو ديديس، وابن خلدون، ومن المعاصرين المؤرخ البريطاني آلان تايلور.

وقد تم توظيف هذا المنهج في الدراسة عبر الرجوع إلى تاريخ حروب الفضاء الالكترونيّ والبحث في نشأتها وتطورها.

المنهج الوصفي التحليلي

ينطلق هذا المنهج من توصيف الظاهرة موضع الدراسة، من خلال عرض ما تتميز به من خصائص ومحددات، ومن ثم يُقرن الوصف بالبحث في الأسباب التي أدت إلى تشكيل الظاهرة وتحديد خصائصها المميزة لها دوناً عن غيرها من الظواهر، وذلك بالعودة إلى المسببات الأولى التي لا تحيل إلى غيرها.

وقد تم توظيف هذا المنهج في الدراسة من خلال دراسة واستعراض خصائص حروب الفضاء الإلكتروني والبحث في الأسباب التي أكسبتها هذه الخصائص ،بما في ذلك الميزات التي تتمتع بها أو السلبيات التي تعيبها.

المنهج المقارن

يعتمد هذا المنهج على المقارنة بين ظاهرتين؛ بحيث يتم إبراز أوجه الشبه والاختلاف. وسوف يتم تحليل خصائص الظاهرة موضع الدراسة.

وقد تم توظيف هذا المنهج في الدراسة من خلال المقارنة بين الحروب التقليدية وحروب الفضاء الإلكترونيّ من حيث طبيعة وخصائص كل منهم.

المنهج القانوني

هو منهج يدرس مؤسسات النظام السياسي والدولي والعلاقة بينها وما حدودها وما الصلاحيات التي تتمتع بها، وذلك وفقاً لما تنصّ عليه الدساتير والتشريعات والقوانين الدولية.

وقد تم توظيف هذا المنهج في الدراسة عبر معالجة موضوع الحرب الإلكترونية ومدى شرعيتها، وما المسؤولية القانونية المترتبة على الأطراف التي تلجأ إليها.

منهج تحليل النُظُم

يعتمد هذا المنهج على فكرة أن هناك عوامل خارجيّة يطلق عليها "المدخلات" تتفاعل مع وسط نظاميّ وتسمى التفاعلات بـ "العمليات"، ويترتب عليها نتائج تسمى "مخرجات"، وهي عبارة عن قرارات تتخذها مراكز صنع القرار لمواجهة ظاهرة ما ولاتخاذ السياسات وتحديدها، كما أن هذه العملية يرافقها تغذية راجعة، تتمثل في آثار وعواقب هذه القرارات. وأبرز من كتب في هذا المنهج هما "ديفيد ايستون"، و"مورتن كابلان".

وقد تم توظيف هذا المنهج في الدراسة من خلال دراسة العوامل والمسببات التي أدّت إلى تطور الهجمات السيبرانية ومن ثم تتبع الأثر الذي أحدثته هذه الهجمات في طبيعة الحروب وتتبع انعكاساتها على العلاقات بين الدول.

الفصل الثاني

الإطار المفاهيمي لحروب الفضاء الإلكتروني

الفصل الثاني
الإطار المفاهيمي لحروب الفضاء الإلكتروني

تتضمن حرب الفضاء الإلكتروني سلسلة هجمات تستهدف الأنظمة المعلوماتية للدول والجهات المعاديّة، وبحيث تشنّ عبر الفضاء الإلكتروني، بغرض سرقة أو تخريب البيانات أو المنشآت المرتبطة بها. وقد باتت الدول تعتمد وبشكل متزايد على اعتماد خيار الهجمات الإلكترونية وذلك في إطار الحروب والصراعات والأزمات المندلعة بينها، وبحيث باتت خياراً بديلاً يتم تفضيل اللجوء إليه في كثير من الحالات على اللجوء إلى استخدام مديان القوة التقليدي. وهو ما يأتي بسبب من خصائص عديدة تتمتع بها هذه الحروب، تجعلها خياراً مفضلاً لدى الدول، فهي تبقى أقل كلفة، وأقل عبئاً من ناحية المسائلة والتبعات، نظراً لما تتّسم به من سريّة وغموض، وذلك مع قدرتها في كثير من الأحيان على تحقيق الأهداف المرجوة المتملتلفة في توجيه الضربات وإلحاق الضرر بالخصم.

وفي هذا الفصل سوف يتم التعرّف إلى مفهوم الحروب الإلكترونيّة عبر الإطلاع بدايةً على أهم التعريفات التي تم وضعها لها، ومن ثم الخروج بتعريف عام يقوم بتحديد أهم عناصرها وما يميّزها عن غيرها من الحروب وأساليب المواجهة. وتوافقاً مع التعاريف ستعرض الدراسة إلى عدد من الهجمات الإلكترونيّة خلال السنوات الأخيرة، وبحيث يتم عبر تحليلها الخروج بخلاصات حول طبيعة وخصائص هذا النوع المستجدّ من الحروب.

المبحث الأول
التعريف بحروب الفضاء الإلكتروني

بفضل ما أحدثته الثورة التكنومعلوماتيّة من ثورة في المجال الإلكتروني، أصبح الفضاء الإلكتروني، تبعاً لذلك، مرشحاً بقوة لأن يكون ساحة جديدة لصراعات وحروب تُدار بأسلحة وأدوات مختلفة تماماً، بالشكل والمضمون عن تلك الحروب التي تعتمد على الأسلحة التقليدية. وهنا، جاء ظهور مسمى حروب الفضاء الإلكتروني، أو "الحروب السيبرانية"، والتي أصبح لها قواعد اشتباك خاصة مختلفة عن تلك الموجودة في الحروب التقليدية. وقد غيّرت حروب الفضاء الإلكتروني من طبيعة الحرب ذاتها؛ فهي لا تستهدف في غاياتها تدمير الآلات والمعدّات العسكريّة والقوات البشرية للعدو، ولا تهدف للاستيلاء على أرض العدو واحتلالها، وإنما إلحاق الضرر البالغ ببناه التحتيّة بأقلّ كلفة ممكنة (فهمي، 2018: 18).

بدايةً، وعند تعريف حروب الفضاء الإلكتروني، لا بد من الإشارة إلى الجهود الفكريّة لعدد من المعنيين بدراسة حروب الفضاء الإلكتروني، منها ما تقدم به جون أركويلا وديفيد رون، اللذان عرفا حروب الفضاء الإلكتروني بأنها: ((إجراء، أو استعداد لإجراء عمليات عسكريّة بالاعتماد على المبادئ والآليات المعلوماتيّة، ما يعني تعطيل، أو تدمير، نظم المعلومات والاتصالات في الدولة العدو)) (Arquilla, 1993: 1).

كما عرفتها ماريا روزاريا تاديو، الباحثة في معهد أكسفورد للإنترنت، بأنها: ((حرب تركز على استخدامات معينة لتكنولوجيا المعلومات والاتصالات ضمن استراتيجية عسكريّة هجوميّة أو دفاعية، أقرتها الدولة، وتهدف إلى التعطيل الفوري أو السيطرة على موارد العدو، والتي تشن داخل بيئة

المعلومات، مع أهداف تتراوح ما بين الصعيد المادي، والمجالات غير المادية، والتي قد يختلف مستوى الدمار فيها حسب طبيعة وحجم الهجوم)) (Taddeo, 2012: 1).

وعرفها عبد القادر محمد فهمي بأنها: ((هجمات تستخدم فيها المنظومة الشبكيّة والأجهزة الحاسوبيّة للدولة، أو الفاعلين من غير الدول، لتعطيل كفاءة السيطرة والقدرة على التحكّم في منظومة أجهزة أو شبكات الحاسوب وما تتضمنه من بيانات ومعلومات للفاعلين الآخرين من الدول وغير الدول، أو تقليلها، أو حتى تدميرها، سواء كان ذلك على مستوى البنية التحتية الوطنية للدولة، أو على مستوى منظومات قوّتها العسكريّة، وبالشكل الذي يعرّض الأمن القومي للدولة إلى تهديد جسيم)) (فهمي، 2018: 20).

وعرفها بدران بأنها: ((الحروب التي تتم بالتعاون مع الحرب العسكريّة، إذ أنها تصوّب نيرانها نحو الأهداف الإلكترونية والرقميّة والمعلوماتية، كالتجسّس على الإشارات الصادرة من الأجهزة الحاسوبية التابعة للفئات المستهدفة، وتتبع الموجات المُنطلقة من الهواتف النقالة وغيرها. وبالتالي، تستهدف هذه النيران الإلكترونية المصالح القوميّة والسياسيّة والعسكريّة والأمنية للفئة المستهدفة، متخذةً لأجل ذلك شكل الهجمات الإلكترونية أو الاختراقات الإلكترونية الهادفة لتعطيل البُنية المعلوماتية لها)) (بدران، 2010: 30).

فيما عرفت وزارة الدفاع الأمريكيّة حرب الفضاء الإلكتروني بأنها: ((توظيف القدرات السيبرانيّة، وذلك بهدف تحقيق غرض أساسيّ، يتمثل في تحقيق الأهداف أو الآثار العسكريّة في الفضاء السيبراني أو من خلاله)) (Schreier, 2015: 16).

وقد عرّف مجلس الأمن الدولي حرب الفضاء الإلكتروني بأنها: ((هي استخدام أجهزة الحاسوب، أو الوسائل الرقمية، من قبل حكومة، أو بمعرفة، أو موافقة صريحة من تلك الحكومة ضد دولة

أخرى، أو مُلكية خاصة داخل دولة أخرى، بما في ذلك: الوصول المتعمد أو اعتراض البيانات، أو تدمير البنية التحتية الرقمية، وإنتاج وتوزيع الأجهزة التي يمكن استخدامها لتخريب النشاط المحلي)) (Schreier, 2015: 16).

ومن هذه التعاريف يمكن أن نستدل، أن حروب الفضاء الإلكتروني لها أدوات جديدة ومسرح جديد، و ميدان جديد، هو الفضاء الإلكتروني والذي يمكن تعريفه بأنه: المجال الخامسة للحرب، يُضاف إلى المجالات التقليدية الأربعة: البحر، اليابسة، الجو، الفضاء. وهو يشير إلى البيئة التي أنشأها التقاء الشبكات التعاونية لأجهزة الحاسوب، والبنى التحتية للاتصالات المستخدمة لربطها، وكل ما يتصل بهذه الشبكات من معدات وأجهزة يتم التحكم بها من خلالها (Wingfield, 2000: 14).

أما بخصوص طبيعة وماهيّة عمليات الهجوم الالكتروني فهي تشمل عمليات التسلل إلى أنظمة الحاسب الآلي، وجمع البيانات، أو تصديرها، أو إتلافها، أو تغييرها، أو تشفيرها، كما تشمل عمليات زرع برمجيّات ضارّة للتجسس. ويرى محمد فهمي بأن الهجمات الإلكترونية تشمل أشكال كثيرة، من سرقة المعلومات، والتجسس، ونشر معلومات سريّة وفضح الأنظمة السياسة لأغراض التحريض، ونشر أفكار مضادة، وخلق تيارات معارضة، وإثارة احتجاجات. وما زاد من تحدي الحروب الإلكترونية هو القدرة على توظيف الفضاء الإلكتروني من قبل فاعلين من غير الدول، يمتلك البعض منهم قدرات تقنيّة قد تفوق ما تمتلكه الحكومات؛ إذ أن أسلحة الفضاء الإلكتروني ليست حكراً على الدولة، قد يمتلكها فرد أو جماعة إرهابيّة، وهي بذلك تعتبر إحدى أشكال الحرب اللامتناظرة (فهمي، 2018: 22).

تتفق الدراسة مع تعريف جون أركويلا وديفد رون بأن حروب الفضاء الإلكتروني تستهدف تعطيل، أو تدمير، نظم المعلومات والاتصالات في الدولة العدو. وكذلك توافق ماريا روزاريا تاديو، بأنها حرب تركز على استخدامات معينة لتكنولوجيا المعلومات والاتصالات ضمن استراتيجية عسكرية هجومية أو دفاعية، تقرّها الدولة، وتهدف إلى التعطيل الفوري أو السيطرة على موارد العدو، وبأنها تشن أساساً داخل بيئة المعلومات.

كما وتوافق الدراسة تعريف محمد فهمي في أن حرب الفضاء الإلكتروني تستهدف تعطيل كفاءة السيطرة والقدرة على التحكم في منظومة أجهزة أو شبكات الحاسوب وما تتضمنه من بيانات ومعلومات للفاعلين الآخرين، أو تقليلها، أو حتى تدميرها، سواء كان ذلك على مستوى البنية التحتية الوطنية للدولة، أو على مستوى منظومات قوّتها العسكريّة. وتتفق الدراسة أيضاً مع تعريف بدران في أنّ حرب الفضاء الإلكتروني تستهدف المصالح القوميّة والسياسية والعسكرية والأمنية للجهة المستهدفة، متخذةً لأجل ذلك شكل الهجمات الإلكترونية أو الاختراقات الإلكترونية الهادفة لتعطيل البُنية المعلوماتية لها.

وهكذا، فإن الدراسة تعرّف حروب الفضاء الإلكتروني بأنها: الحروب التي تستهدف تعطيل، أو تدمير، نظم المعلومات والاتصالات في الدولة العدو. وهي تشن أساساً داخل بيئة المعلومات. وبحيث تستهدف تعطيل كفاءة السيطرة والقدرة على التحكم في منظومة أجهزة أو شبكات الحاسوب وما تتضمنه من بيانات ومعلومات للفاعلين الآخرين، أو تقليلها، أو حتى تدميرها، سواء كان ذلك على مستوى البنية التحتية الوطنية للدولة، أو على مستوى منظومات قوّتها العسكريّة.

وحروب الفضاء الإلكتروني يمكن إن تشن من قبل فاعلين من غير الدول، وهي بهذا تتميز بصعوبة وتعذر إمكانية تحديد العدو والجهة المهاجمة.

وهذه الحروب تكون بيئتها هي البيئة المعلوماتية، والتي يكون فضائها هو شبكات الحاسوب، حيث تكون المعلومات مخزنة ومشاركة عبر هذه الشبكات بما في ذلك مشاركتها عبر شبكة الإنترنت. وإن نية المهاجم هي العامل الحاسم في تحديد إذا ما كان الهجوم جزءاً من حرب إلكترونية أو إن كان مجرد عملية إختراق عاديّة ذات طابع جنائي، لا يمكن اعتبارها جزءاً من حرب إلكترونية. وهي في دخولها ضمن تكتيكات الهجوم لدى الدول باتت جزءاً من منظومة أساليب وتكتيكات الحروب الهجينة، والتي تتجه لمزج أدوات متعددة في تنفيذ الهجمات، مع عدم الاعتماد فقط على الأسلحة التقليديّة.

وبالعودة إلى تاريخ هذا النوع من الحروب وتطبيقاتها، نجد أن مورتن كابلان، عالم السياسة الأمريكي، يرى بأنها تطوّرت في سياق الحرب الباردة، حين كان الجواسيس الأمريكيون والروس يعترضون على نحو دوريّ منتظم اتصالات بعضهم، من إشارات راديوية، واتصالات هاتفية، بهدف جمع معلومات استخبارية بشأن نوايا وقدرات الطرف الآخر، والحصول على أفضليّة في الحرب المنتظرة القادمة (كابلان، 2019: 15).

أما التطبيق الأول المباشر لهذا النوع من الهجمات في حرب فعليّة، فقد جاء مع حرب الخليج الثانية عام 1991م، حين قامت القوّات الأمريكية باختراق وتعطيل منظومة الدفاع الجويّ العراقيّة. كما قامت بتدمير كابلات الألياف الضوئية وشبكة الاتصالات العسكريّة الممتدة من بغداد حتى البصرة. وبذلك يرى كابلان أن هذه الهجمات كانت بمثابة الحملة الأولى لوسائل الحرب المضادة للقيادة والسيطرة التي تنذر بمجيء حروب الكترونية قادمة (كابلان، 2019: 37).

ومع نهاية عقد التسعينات من القرن الماضي برزت الهجمات الإلكترونية المتبادلة بين الهند وباكستان، وذلك على خلفية النزاع طويل الأمد بين البلدين بشأن كشمير، إذ انتقلت المواجهات إلى

الفضاء الإلكتروني، مع بدء المتسللين من كل دولة المشاركة في مهاجمة نظام قاعدة بيانات الحوسبة للدولة الأخرى. وقد زاد عدد الهجمات الإلكترونية سنويًا بين البلدين تصاعادياً، من (45) هجمة في عام 1999م، إلى (133) في عام 2000م، و(275) عام 2001م (عبد الصادق، 2018: 43).

في عامي 2009م و2010م، برزت الهجمات التي نفذتها الوحدة (8200) الإسرائيلية بالتعاون مع "وكالة الأمن القومي" الأمريكية، على المنشأة النووية الإيرانية في نطنز. إذ تمكنت الوحدة من نشر فيروس حاسوبي يطلق عليه اسم "ستوكسنت" (Stuxnet) داخل المرفق. واستهدف الفيروس نظام التشغيل لأجهزة الطرد المركزيّ المستخدمة في تخصيب اليورانيوم، ما أدى إلى جعلها تتحرك بوتيرة خارجة عن السيطرة وأدى بالنهاية إلى تكسّرها. وكانت هذه الأجهزة من طراز "سيمنز سي 1000" وهي أجهزة متطورة، واتجهت الاتهامات الإيرانيّة مباشرةً إلى الولايات المتحدة الأمريكية وإسرائيل، إلا أنهما نفتا الاتهامات (عيتاني، 2019: 49).

وفي عام 2010م، تجددت الهجمات الإلكترونية المتبادلة بين الهنود والباكستانيين، إذ قام متسللين هنود، منضوين تحت اسم "الجيش السيبراني الهندي"، بشن هجوم استهدف (36) موقعاً لقاعدة بيانات حكومية باكستانية. وفي عام 2013م كذلك، اخترق المتسللين الهنود الموقع الرسمي للجنة الانتخابات في باكستان. ورداً على ذلك، قام متسللون باكستانيون، يطلقون على أنفسهم "جيش السايبر الحقيقي"، باختراق وتشويه مواقع الويب التابعة لهيئات الانتخابات الهنديّة (عبد الصادق، 2018: 45).

ومع اندلاع النزاع في شبه جزيرة القرم وتدخل روسيا عسكرياً فيه في آذار/مارس من عام 2014م، أعلنت شركة "روستك" العسكريّة الروسيّة تمكنها من الاستيلاء على طائرة أمريكيّة بدون طيّار من طراز (MQ-5B) فوق شبه جزيرة القرم، بعد هجمة من التشويش الكهرومغناطيسي،

لتتكرس بذلك الهجمات الإلكترونية كأحد التكتيكات والأساليب المعتمدة في ميدان القتال العسكري المباشر كذلك (Saalbach, 2019: 47).

وفي كانون الثاني/ يناير من عام 2017م، أصدر مكتب مدير الاستخبارات الوطنية الأميركية، جيمس كلابر، تقريراً يوضّح تفاصيل الحملة الروسية التي استهدفت التأثير على الانتخابات الرئاسية الأميركية التي أجريت في تشرين الثاني/نوفمبر عام 2016م. ووفقا لما ورد في التقرير، فإن الرئيس الروسي، فلاديمير بوتين، أصدر أوامر بالسعي للتأثير على الانتخابات الرئاسية الأميركية، عبر تشويه صورة المرشحة للرئاسة هيلاري كلينتون والإضرار بترشُحها وفرصها في الفوز بالرئاسة، وذلك عبر بث ونشر رسائل عن طريق وسطاء من دول أخرى ومستخدمي وسائل التواصل الاجتماعي ومخترقي الإنترنت مدفوعي الأجر (رويترز، 2018/1/26). وستعالج الدراسة بشكل موسع النماذج التطبيقية في المبحث الثاني من الفصل الثاني.

تجد الدراسة بأن حرب الفضاء الإلكتروني هي الحرب التي تستهدف تعطيل، أو تدمير، نظم المعلومات والاتصالات في الدولة العدو. وهي تشن أساساً داخل بيئة المعلومات. كما تجد أنّ عدد الهجمات الإلكترونية قد تزايد خلال العقدين الأخيرين، من القرن الحالي والقرن الواحد والعشرين، حتى باتت إحدى أهم الوسائل والتكتيكات المعتمدة بين الأطراف المتصارعة حول العالم، وذلك نظراً لتدني كلفتها والخسائر التي قد تنجم عنها للطرف المهاجم مقارنة مع حجم ما يمكن تحقيقه والحاقة من أضرار بالخصم عبر توظيفها. وبأن هناك تنوع في الأدوات والوسائل وأشكال الهجمات الإلكترونية، بما في ذلك على سبيل المثال، بث فيروسات والبرامج تخريبية والمدمرة للأنظمة والشبكات الحاسوبيّة، أو إختراق حسابات والوصول إلى معلومات سرية وتسريبها أو الاستفادة منها لأغراض عسكريّة وأمنيّة عدائيّة.

وفضلاً عن ذلك، هناك تنوع في الأهداف المراد التعرض لها، وعدم اقتصارها على أهداف عسكرية، إذ يمكن إن تستهدف الضربات الإلكترونية أهدافاً مدنيّة وقطاعات خدميّة وانتاجيّة. كذلك تجد الدراسة بأن الهجمات الإلكترونية قد عززت من مستويات وفرص الحرب اللامتماثلة، وذلك مع تمكن دول متفاوتة القوة، وحتى تنظيمات من غير الدول، من شن الهجمات ضد الدول ذات القوة العسكرية والاقتصادية الأكبر. إضافة إلى أنها باتت أسلوباً معتمداً بشكل متزايد ضمن استراتيجة الحروب الهجينة من قبل عدد متزايد من الدول.

المبحث الثاني
النماذج التطبيقيّة لحروب الفضاء الإلكتروني

باتت الدول تعتمد بشكل متزايد على خيار شنّ الهجمات الإلكترونية بهدف إلحاق الضرر بالخصوم والأعداء، وذلك باعتبار أنها وسيلة غير مكلفة، إذا ما قورنت بوسائل الهجوم العسكريّة التقليديّة، كما إنها تلحق ضرراً كبيراً بالخصم. هذا بالإضافة إلى أنها تتسم بصعوبة تحديد مصدر الهجوم، وبالتالي تجنب الدول الإدانة والتبعات القانونية، والتبعات العسكريّة للهجوم، بما في ذلك تجنيبها أي ردود عسكريّة مباشرة على الهجمات.

وبالنظر إلى أبرز الهجمات الالكترونية خلال السنوات الأخيرة، نجد من بينها الهجوم الذي وقع في السابع والعشرين من حزيران/يونيو عام 2017م، وفي ظلّ الأزمة المستمرّة بين روسيا وأوكرانيا حول شبه جزيرة القرم والمناطق الشرقية والجنوبية الشرقية من البلاد، بدأت سلسلة من الهجمات الروسية الإلكترونيّة على مواقع المنظمات والمؤسسات الأوكرانية، بما في ذلك البنوك والوزارات والصحف وشركات الكهرباء، واستخدم المهاجمون الروس فيها برمجيّات خبيثة من نوع "بيتا" (Saalbach, 2019: 48).

وأدى الهجوم إلى تعطيل أنظمة المعلومات وتوقف أجهزة الحاسوب، مع مطالبة بدفع فدية بالعملة الإلكترونية (بيتكوين)، التي لا يمكن تعقبها. وأوضحت السلطات الأوكرانية لاحقا أن طلب الفدية كان مجرد ستار، وأن الهجوم كان يهدف إلى تعطيل أعمال الشركات الحكومية والخاصة في أوكرانيا، وإحداث زعزعة سياسية في البلاد (Saalbach, 2019: 49).

وفي تاريخ سابق، كانت وزارة الطاقة الأوكرانيّة قد أعلنت في كانون الأول/ ديسمبر 2015م أنّ متسللين استخدموا شركة إنترنت مقرها روسيا وشنّوا هجوماً إلكترونياً منسقاً على شبكة الكهرباء

الأوكرانيّة، ما تسبب في انقطاعات بالكهرباء في حينه. واعتبرت هذه الحادثة على نطاق واسع أول انقطاع للكهرباء ناجم عن هجوم إلكتروني، وهو ما ضاعف من مخاوف أوكرانيا والدول الاخرى من احتمالية تعرض منشآت البنية التحتية المدنيّة للخطر بفعل هجمات إلكترونيّة.

جاءت هذه الهجمات إثر توتر العلاقات بين أوكرانيا وروسيا، بعد أن ضمت روسيا شبه جزيرة القرم الأوكرانية إلى أراضيها عام 2014م، ومن ثم اندلعت أعمال عنف وتمرد من جانب انفصاليين موالين لروسيا في شرق وجنوب شرق أوكرانيا.

وبالرغم من تكرار الاتهامات الموجهة لروسيا بشن الهجمات الالكترونيّة، إلا إنها كانت هي أيضاً هدفاً لها، ففي عام 2019م أعلن نائب مدير المركز التنسيقي الروسي لمواجهة حوادث الحاسوب، نيقولاي موراشوف، أن هجوماً سبرانياً موسعاً وقع ضد روسيا من الخارج، وذلك في يوم الانتخابات الرئاسية في آذار/مارس من عام 2018م. وبيّن موراشوف، أن المركز بدأ برصد هجمات سيبرانية اعتباراً من حزيران/يونيو 2017م، وبلغت الهجمات ذروتها يوم فعالية "الخط المباشر" مع الرئيس فلاديمير بوتين في الخامس عشر من حزيران/يونيو 2017م. ومن ثم تجددت الهجمات وتكثّفت في الثامن عشر من آذار/ مارس 2018م، يوم الانتخابات الرئاسيّة، واستهدفت تحديداً تعطيل عمل مراقبة عمليات التصويت عبر الفيديو (روسيا اليوم، 2019/1/31).

وفي كانون الأول/ ديسمبر من العام 2017م، واجهت بريطانيا هجوماً الكترونيّاً كبيراً، عرف باسم هجوم "واناكراي" الإلكتروني، واستهدف منظومة المعلومات التابعة لوزارة الصحة، ما أدى إلى تعطّل في السجلات الطبيّة لدى مجموعة من المستشفيات، وتوقف بعض المنشآت الصحية عن العمل جراء الأعطال التي تسببت بها هذه الهجمات على أجهزة الحاسوب المتعلّقة بالنظام الصحي

الإلكتروني وتلف في جزء من بيانات المرضى. وقد ألقت المملكة المتحدة باللوم على عناصر مرتبطة بكوريا الشمالية بالوقوف وراء الهجوم (العربية، 2017/12/27).

كانت روسيا قد تعرضت لهجمات أيضاً خلال استضافتها لبطولة كأس العالم عام 2018م، حيث واجهت روسيا خلالها حوالي خمسة وعشرين مليون هجوم إلكتروني على البنية التحتية لتكنولوجيا المعلومات (فرانس 24، 2018/7/16).

وفي حزيران/ يونيو من عام 2019، أعلنت روسيا أن شبكتها الكهربائية تتعرض لهجوم سيبراني من قبل الولايات المتحدة الأمريكية، وذكرت صحيفة نيويورك تايمز في حينه أن المتسللين الأمريكيين زرعوا برامج ضارة قادرة على تعطيل الشبكة الكهربائية الروسيّة (New York Times, 17/6/2019).

على صعيد آخر، وفي التاسع عشر من كانون الأول/ ديسمبر من العام 2018م، ذكرت شركة "آريا 1 سيكيوريتي" الأميركيّة المتخصصة في أمن المعلومات، أنّ وحدة إلكترونيّة تابعة لجيش التحرير الشعبي الصيني، تعمل بأوامر من الحكومة الصينيّة، اخترقت شبكة اتصالات يستخدمها الاتحاد الأوروبي لتنسيق السياسات الخارجيّة، حيث تمكن القراصنة من الوصول إلى آلاف البرقيات الدبلوماسية، بحسب صحيفة نيويورك تايمز التي قدمت لها الشركة (1100) برقية نشرت مجموعة منها. ومن هذه التقارير ما يتضمن تحليلات لتوجهات السياسات العالمية والتجارة، وخصوصاً دور الصين وتحولات سياساتها تحت حكم الرئيس شي جينبينغ، وكذلك علاقات الاتحاد الاوروبيّ مع كل من روسيا والولايات المتحدة الأمريكيّة، ولمحات من اجتماعات مغلقة (فرانس 24، 2018/12/19).

ويظهر مثل هذا التقرير نوعاً من الهجمات الإالكترونيّة أنه لا يهدف إلى الحاق الدمار بالخصم وإنما فقط إلى الاختراق والتوصل إلى معلومات ذات طبيعة سريّة.

على صعيد آخر، وفي حزيران/ يونيو من العام 2019م، وبعد قيام إيران بإسقاط طائرة استطلاع أميركية قرب مضيق هرمز، أفادت وسائل إعلام أميركية، أن الولايات المتحدة الأمريكية شنّت هجمات إلكترونية استهدفت أنظمة حاسوبية إيرانية تستخدم لإطلاق الصواريخ. وجاء بعدها إعلان إيران عن التصدّي لهجمتين الكترونيتين خلال أسبوع واحد، كانتا قد استهدفتا منظومة الاتصالات الدفاعيّة.

وبعد نحو أربعة أشهر، أعلنت شركة مايكروسوفت، في الخامس من تشرين الأول (أكتوبر) 2019م، أنّ مجموعة من القراصنة المرتبطين بإيران شنوا هجمات إلكترونيّة، استهدفت حسابات صحافيين أميركيين وشخصيات حكومية رسميّة وحسابات مرتبطة بالحملة للانتخابات الرئاسية التي ستجري في عام 2020م، بهدف التأثير عليها (مونتي كارلو الدولية، 2019/10/5).

وأوضح توم بيرت، نائب الرئيس المكلّف بشؤون الأمن وثقة المستخدم في شركة ميكروسوفت، أنّ مركز أمن الإنترنت في الشركة راقب خلال فترة شهر مجموعة قراصنة، مقرّها إيران، مع اعتقاد الشركة بأنها مرتبطة بالحكومة الإيرانيّة، قامت بأكثر من (2700) محاولة لكشف حسابات بريد إلكتروني تعود لمستخدمي مايكروسوفت، وقامت باختراق (241) من هذه الحسابات، موضحاً أن حسابات البريد الإلكتروني هذه عائدة لفريق حملة دونالد ترامب للانتخابات الرئاسية الأميركية، ولمسؤولين حكوميين وصحفيين، وذلك خلال الفترة الممتدة بين آب/أغسطس وأيلول/سبتمبر من العام 2019م (الحرة، 2019/10/5).

إلا أن بيرت أكدّ أن الهجمات لم تكن متطورة تقنياً، وتمثلت بمحاولة استخدام معلومات شخصيّة تم جمعها واستخدام أنظمة تسمح بتغيير كلمات المرور. ويظهر مثل هذا المثال كيف أن الهجمات

الإلكترونيّة قد تكون بسيطة ودون استخدام برمجيات معقدة. إضافة إلى أنه مثال على إمكان اعتماد الحكومات في الهجمات على مجموعات قراصنة لا تمتلك أي صفة رسمية، ما يجنبها أي مساءلة أو تبعات.

وفي مواجهة أخرى، شهد العام 2019م تصاعداً في عمليات الهجوم الإلكتروني المتبادلة بين إيران وإسرائيل. ففي شباط/ فبراير 2019م صرحّ نعوم شعار، الضابط في وحدة الدفاع الإلكتروني التابعة للجيش الإسرائيلي لوكالة بلومبيرغ الأمريكيّة بأنّ الوحدة أحبطت عملية اختراق إيرانية استهدفت نظام التنبيه ضد الصواريخ في إسرائيل. وبيّن شعار أن هذه المحاولات الإيرانية بدأت منذ فترات تعود للعام 2017م. مبيناً بأن التقنيين الإسرائيليين رصدوا برمجيات خبيثة تحاول الدخول لمنظومة التنبيه التي تعمل على إطلاق تحذير في المدن الإسرائيلية عند حصول هجمات صاروخيّة. وقد تعاملت وحدة الدفاع الإلكترونية الإسرائيلية مع هذا التهديد بإنشاء المزيد من التحصينات التي تمنع المخترقين من الوصول إلى أنظمة التحكم، مع وضع أنظمة مراقبة للنشاطات البرمجية على الشبكة (تايمز أوف إسرائيل، 2019/2/25).

وفي تطوّر لاحق، أعلن جهاز الأمن الإلكتروني الوطني الإسرائيلي، في السادس والعشرين من نيسان/أبريل 2020م، عن إحباط هجوم إلكتروني على منظومة المياه في إسرائيل، تضمن الهجوم على الأنظمة الحاسوبيّة لست منشآت مياه ومجارٍ في إسرائيل بواسطة قراصنة، مع الترجيح بوقوف إيران وراء الهجوم. وقد اخترق القراصنة البرمجيات المسؤولة عن التحكم في عمليات تشغيل المحطات، ما أدى إلى توقف أجهزة التحكم الرئيسيّة فيها. وقد تبيّن بأنّ المهاجمين استخدموا خوادم (سيرفرات) أمريكية لشنّ الهجوم، وذلك بهدف التمويه.

وعلى إثر هذه الهجمات، عقد المجلس الوزاري الإسرائيلي الأمني المصغر (الكابينت)، اجتماعاً في السابع من أيار/مايو 2020م لبحث الهجوم الإلكتروني غير المسبوق الذي تعرضت له البنية التحتية للمياه، مع ترجيح الاشتباه بكون إيران تقف وراءه. وبالرغم من أنّ الهجوم لم يتسبب في أضرار بالغة باستثناء عدة أعطال في منشآت المياه التابعة لعدد من المجالس المحلية، إلا إن الجانب الإسرائيلي رأى في الهجوم تصعيداً خطيرا من قبل الإيرانيين، لاسيما في ضوء استهدافه منشآت البنية التحتية المدنية (الأخبار، 2020/5/11).

بعد الاجتماع بيومين، في التاسع من أيار/مايو 2020م، ردّت وحدة الأمن الإلكتروني الوطني الإسرائيلي على الهجوم، مستهدفةً حواسيب ميناء "الشهيد رجائي" في بندر عباس، وهو مركز مهم للاقتصاد وحركة الشحن جنوب إيران، يمر عبره أكثر من خمسين بالمئة من واردات وصادرات إيران عبر البحر. وأسفر الهجوم عن وقوع انسداد في القنوات وغمر الطرق المؤدية للميناء. وقد ذكرت صحيفة واشنطن بوست في تقريرها الصادر عن الحادثة أن إسرائيل هي التي نفذت الهجوم، وذلك كرد فعل انتقامي من إسرائيل ضد إيران، بعد الهجمات التي شنتها قبل ذلك الوقت بنحو أسبوعين (وكالة أنباء الأناضول، 2020/5/19).

وفي نهاية حزيران/ يونيو ومطلع تموز/ يوليو 2020م جاءت المرحلة التالية من المواجهة الإيرانية الإسرائيليّة في الفضاء الإلكتروني، وذلك مع وقوع سلسلة من التفجيرات الغامضة في عدة مواقع بإيران، وبلغت ذروتها في اليوم الثاني من ذلك الشهر، حين وقعت تفجيرات في منشأة نطنز النوويّة، حيث المبنى الرئيسي لتخصيب اليورانيوم في إيران. وفي الثالث والعشرين من تموز/يوليو 2020م صرحّ عضو لجنة الأمن القومي بالبرلمان الإيراني، جواد كريمي قدوسي، أن الانفجار الذي وقع في نطنز ناتج عمّا أسماه "خرق أمني". مستبعداً بشدة "ضرب المجمع بجسم خارجي"، في إشارة

إلى الحديث عن احتمال الاستهداف بقنابل أو صواريخ، كما ذكرت بعض المصادر. مع الإشارة إلى احتمالية عالية بان يكون الهجوم قد تم بسبب إختراق شبكات التحكم بالمنشاة كما حصل في هجوم الفيروس "ستوكسنت" عام 2010م. وقد نشّرت الباحثة داليا داسا كاي، مديرة مركز السياسة العامة للشرق الأوسط بمؤسسة راند الأمريكية، تحليلاً في صحيفة واشنطن بوست ترجّح فيه التورط الإسرائيلي بالتفجيرات (Washington Post, 15/7/2020).

وجاء الرد الإيراني بعد نحو أسبوعين، في يوم السابع عشر من تموز/يوليو 2020م، وذلك عبر تكرار الهجوم الإلكتروني على منشآت المياه الإسرائيليّة. حيث كشفت مصادر إسرائيلية أن هجومين إيرانيين نفذا، استهدف أحدهما مضخات المياه الزراعيّة في الجليل الأعلى، واستهدف الثاني البنية التحتية في وسط إسرائيل. وإثر هذا الهجوم، أجرى وزير الدفاع الروسي، سيرغي شويغو، ونظيره الإسرائيلي، بيني غانتس، مكالمة هاتفيّة، طلب فيها غانتس نقل تحذير إلى إيران، مؤكداً أن "إسرائيل مصممة على منع إيران من تحقيق طموحاتها النووية" (الشرق الأوسط، 2020/7/18).

تواصلت المواجهة الإسرائيليّة الإيرانيّة في الفضاء الإلكترونيّ وفي يوم الرابع عشر من تشرين الأول/أكتوبر 2020م، أعلنت منظمة تكنولوجيا المعلومات التابعة للحكومة الإيرانيّة عن وقوع هجوم إلكترونيّ واسع النطاق، استهدف ميناء بندر عباس مجدداً، كما شمل الهجوم استهداف خدمات وزارة الاتصالات ووزارة المواصلات وأنظمة الجمارك وانظمة اتصالات لمؤسسات مختلفة بينها بنوك (مونتي كارلو الدولية، 2020/10/15).

وأخيراً، وفي كانون الأول (ديسمبر) 2020م، تعرّضت الولايات المتحدة الأمريكيّة لهجمات إلكترونية واسعة، شملت عمليات قرصنة إلكترونية واسعة النطاق، استهدفت وكالات حكومية أميركية، من بينها إدارة الأمن النووي، ووزارات الدفاع والخارجية والطاقة والخزانة، وشركات خاصة مرتبطة

بالحكومة الفدرالية. إثر الهجوم نقلت صحيفة وول ستريت جورنال عن مسؤول أميركي استخباري قوله ((إن التوصل إلى معرفة أبعاد عملية القرصنة الإلكترونية الأخيرة وتجاوُز تداعياتها يحتاج إلى أشهر إن لم يكن سنوات)). وأضاف: ((إن أبعاد العملية مذهلة وكبيرة بالنظر إلى طبيعتها الحذرة والمتخفية، وأن أكثر ما يزعج فيها هو عدم القدرة حتى الآن على تحديد أنظمة الكمبيوتر المتأثرة)) (Wall Street Journal, 17/12/2020).

بالرغم من أن روسيا نفت مسؤوليتها عن الهجوم، فإن عدداً من المسؤولين الأميركيين أصرّوا على اتهامها بالسؤولية عن هذا الاختراق الكبير، ومنهم من أشار إلى أن مجموعة "كوزي بير" المرتبطة بأجهزة الاستخبارات الروسية، هي من قامت بالهجوم. وفي موقف يؤيد ما ذهب إليه العديد خبراء الاستخبارات الأمريكية، قال السيناتور الجمهوري، ماركو روبيو، أنه ((يتضح بشكل متزايد أن المخابرات الروسية هي من نفذت أخطر اختراق إلكتروني في تاريخ الولايات المتحدة)). وعقب الهجوم توعد الرئيس المنتخب حديثاً في وقتها، جو بايدن، توعد الروس، باعتبار أنهم يقفون وراء الهجوم الإلكتروني الواسع، وأكدّ أن الأمن السيبراني سيكون من بين أولويات إدارته. وزير الخارجية الأمريكي، مايك بومبيو، كذلك وجه الاتهام إلى روسيا والرئيس الروسي بوتين بالوقوف وراء الهجمات، وقال: ((يمكننا أن نقول بوضوح تام أن الروس هم من شاركوا في هذا النشاط))، بالرغم من عدم تقديمه أي تفاصيل تعزز اتهامه (بي بي سي، 2020/12/19).

تجد الدراسة بأنّه ومن خلال الهجمات الإلكترونيّة بات عدد متزايد من الدول يتجه إلى خيار استهداف المنشآت والبنى التحتية المدنيّة ذات الاهمية بالنسبة لخصومها، هذا فضلاً عن إمكانية استهداف المواقع العسكريّة، إضافة إلى الهجمات القائمة على أساس إختراق الحسابات والوصول إلى المعلومات السريّة.

كما تجد الدراسة أنه ومن أهم عناصر ومميزات هذا النوع من الهجمات إن الدول تلتزم في معظم الأحيان بعدم الإقرار بالهجوم وتعمد إلى استخدام وسائل لإخفاء هوية الفاعل، كما في حالة اللجوء إلى استخدام "سيرفرات" من دول أخرى، وكلّ ذلك يؤكد على خاصية عدم إمكانية تحديد مصدر الهجوم، التي يتميّز بها هذا النوع من الحروب، ويجعله مختلفاُ عن الحروب التقليديّة، الأمر الذي يؤدي إلى زعزعة قواعد الاشتباك التقليديّة وإضعاف سياسة الردع.

وترى الدراسة أيضاً أنّ جانباً كبيراً من الصراعات بين الدول بات ينتقل شيئاً فشيئاً إلى ميدان الفضاء الإلكترونيّ، وذلك باعتباره ساحة بديلة عن المواجهة العسكريّة التقليدية، بالنظر لكون هذا الفضاء أقل كلفة، ويحرّر الدولة المهاجمة من التبعات، ويضعف احتمالية توجيه الإدانة اليقينيّة لها بشكل مباشر.

كما وتخلص الدراسة إلى أن هذه الهجمات مقترنة بالضرورة بنيّة إلحاق الضرر بالخصم، وذلك في إطار حالة من الخصومة والعداء بين الدول والأطراف، وهذا ما يجعلها مختلفة عن الهجمات ذات الطابع الجنائي، التي قد تتشابه في بعض حيثيات الهجوم، مثل حالات إختراق حسابات والوصول إلى معلومات، ولكنها تبقى مفتقدة عنصر النية بإلحاق الدمار والضرر بالخصم في إطار حالة من الأزمة والصراع بحيث يكون هذا الضرر نوعاً من التصعيد وسبباً للضغط عليه، بُغية الوصول إلى نوع من الإذعان وتقديم التنازلات من قبله، وهو ما يكون متحققاً في حالة الهجمات الإلكترونية، والتي تأتي ضمن سياق ما يمكن تسميته بالحرب الإلكترونيّة.

الفصل الثالث

خصائص حروب الفضاء الإلكتروني ومسؤوليتها الدولية

الفصل الثالث

خصائص حروب الفضاء الإلكتروني ومسؤوليتها الدولية

امتازت حروب الفضاء الإلكتروني بخصائص عديدة كانت الدافع وراء اعتماد العديد من الفاعلين الدوليين عليها، سواء كانوا دول، او فاعلين من دونها، ويأتي في مقدمة هذه الخصائص انخفاض تكلفتها بالمقارنة مع أدوات الحرب التقليدية، فضلاً عن ما يمكن أن تحققه من نتائج ملموسة في إطار الصراعات والنزاعات. هذا إذا أضفنا إليها ضعف الدلائل التي توجه للأطراف المباشرين بها في إطار تحميلهم المسؤولية.

يضاف إلى ما تقدّم، فإن الخصائص التي تنفرد بها وجعلت منها حروب متميزة عن الحروب التقليدية هو اختلاف عقيدتها العسكرية وقواعد الاشتباك فيها عن نظيرتها في سائر أشكال الحروب السابقة التي عرفتها البشريّة.

وعليه، تسعى الدراسة في هذا الفصل إلى التعرف على أهم الخصائص التي تمتاز بها حروب الفضاء الإلكتروني، بالإضافة إلى معالجة التكييف والوضع القانوني والأطر القانونية الناظمة لها من وجهة نظر القانون الدولي.

المبحث الأول

الخصائص التي تتميز بها حروب الفضاء الإلكتروني

لطالما دارت المواجهات العسكريّة ضمن أربعة فضاءات، وهي الجويّة، والبريّة، والبحريّة، والصاروخيّة، ولكن في عصر الإنترنت والشبكات المعلوماتيّة، ظهر فضاء جديد تدور فيه المعارك والحروب، وهو الفضاء الإلكتروني، ما استدعى حدوث تطويرات على أساليب القتال والهجوم والدفاع، وغيّر من طبيعة الأسلحة المستخدمة، والعقائد العسكريّة، وقواعد الاشتباك المتبعّة.

وبالإمكان اعتبار حروب فضاء الإلكتروني بمثابة الانعكاس والمخرجات للثورة الرقمية والالكترونية في الميدان العسكريّ، وهي تقوم على أساس شنّ الهجمات على هياكل تكنولوجيا المعلومات الحيويّة للخصم، والتي تكون مشغّلة لمصالحه المدنيّة وقدراته العسكرية، وبحيث يكون إلحاق الضرر بها موازٍ ومعادل للقصف العسكري المباشر، بواسطة الأسلحة التقليديّة وغير التقليديّة، في العصر الصناعيّ (كلارك وكنيك، 2012: 286).

وقد جاء التحوّل المتزايد من قبل الدول والفاعلين السياسيين نحو الاعتماد بصورة متزايدة على خيار المواجهة في الفضاء الإلكتروني بسبب ما تتمتع به من خصائص، ويأتي في مقدمتها انخفاض تكلفة المواجهة فيها نسبياً، بالمقارنة مع الحروب التقليديّة. فهي لا تحتاج لمعدات وجيوش مجهّزة، كما أن احتمالية وقوع الضحايا والخسائر البشريّة في صفوف القوة المهاجمة تكون منعدمة. وبالتالي، فإن التوجه المتزايد نحوها يأتي من مبدأ السعي لتحمّل أقل كلفة، مع إلحاق أكبر ضرر بالعدوّ (كلارك وكنيك، 2012: 287).

ولا يقف تدني الكلفة عند النواحي الماديّة والبشريّة، وإنما تكون كذلك أيضاً من ناحية المسؤولية. إذ أن هذه الهجمات تضمن تحقيق مبدأ إخلاء المسؤولية، وذلك بالنظر إلى صعوبة تحديد الجهة

والمكان الذي صدر منه الهجوم. وكذلك إمكانية التلاعب والتمويه العالية فيما يتعلق بمصدر ومكان توجيه وشنّ الهجوم الإلكتروني، إضافة إلى إمكانية استخدام سلسلة من الوكلاء في شنّ الهجوم بما يبدد أيّ احتمالية تتبع مباشر للدولة صاحبة القرار في شنّ الهجوم (كلارك وكنيك، 2012: 289).

من ناحية أخرى، استدعت حروب الفضاء الإلكتروني حدوث تغيّرات على مستوى الأهداف وعلى مستوى الفاعلين. من ناحية الأهداف، فإن هذه الحروب تتجه نحو استهداف بنك متنوع من الأهداف، فهي تستهدف البنى التحتية المدنيّة، ولا تقتصر على العسكريّة. والأساس في الهدف بالنسبة لها هو أن يكون مرتبطاً بشبكات المعلومات، وهو ما بات يتوافر بشكل متزايد في شتّى مناحي الحياة والمصالح الحيوية حول العالم، وذلك بفعل التحوّل المتسارع نحو الرقمنة لمختلف الأنشطة والمنشآت. بحيث باتت التعاملات التجاريّة معتمدة على الفضاء الإلكتروني، وكذلك الصحة والتعليم، وصولاً حتى شبكات المياه والكهرباء، وكذلك المؤسسات والمعاملات الحكوميّة (فهمي، 2018: 18).

كلّ ذلك أدى إلى توسعة بنك الأهداف المتاحة أمام هجمات أسلحة الفضاء الإلكترونيّ، وجعل من مخاطرها متعديّة للمواقع العسكريّة، إذا تتعداها إلى استهداف البُنى التحتيّة والحسّاسة في البلدان المستهدفة، وهو أمر أصبح واقعيّاً في ظل القدرة على استهداف شبكات الكهرباء، والمياه، والطاقة، وشبكات النقل، والنظام المالي، والمنشآت الصناعيّة، بواسطة فيروس يمكنه إحداث أضرار ماديّة حقيقيّة تؤدي إلى وقوع انفجارات أو دمار هائل.

وكمثال على ذلك، فإن هجوماً على أنظمة التحكم بشبكات المواصلات قادر على إيقاع حوادث تصادم القطارات والسيارات، وبحيث تكون خسائرها البشريّة والماديّة كبيرة. كذلك الهجوم على أنظمة التحكم الجويّ، إذ بالإمكان أن يؤدي إلى إسقاط الطائرات من الجو. أو الهجوم على منشآت الطاقة،

حيث يمكن أن يؤدي إلى إيقاع حوادث كبرى. والهجوم على محطات تزويد الكهرباء والمياه، يمكن أن يؤدي إلى تعطيل خدمات المياه والكهرباء عن مدن بأكملها. وكلّ ذلك يتم دون إطلاق رصاصة واحدة. ما يمكن اعتباره بمثابة عملية تدمير صامتة وخفيّة.

وقد تصاعدت خطورة مثل هذه الهجمات مع تحوّل معظم قطاعات الاقتصاد نحو الرقمنة، وبحيث باتت تعتمد على التكنولوجيا، من البنوك والتعاملات المالية، إلى قطاع الاتصالات، إلى قطاع التجارة الإلكترونية المتنامي. وكذلك مع الاعتماد والانتشار المتزايد للمعلومات وتداولها عبر الشبكات، حيث بات بإمكان الدولة المهاجمة بث الفوضى المعلوماتية في البلد المستهدف، عبر نشر معلومات مغلوطة، قد تكون ذات تأثيرات وارتدادات سياسية بالغة، كما قد يحصل مثلاً في فترة الانتخابات.

وعلى مستوى الفاعلين، تركت حروب الفضاء الإلكتروني تأثيرات هامة في طبيعة المواجهات، حيث بات بالإمكان أن يكون هناك أطراف فاعلة من غير الدول، إذ أن الأسلحة المستخدمة في هذه الحروب ليست حكراً بيد الدولة، وبحيث بات يتردد الوصف لحروب الفضاء الإلكتروني بأنها حروب غير تناظرية (Asymmetric).

وذلك عائدٌ إلى التكلفة المتدنية نسبياً للأدوات اللازمة لشنّ هكذا حروب. فلكي ينخرط فيها طرف من غير الدول، فليس هناك حاجة لأن يقوم بتصنيع اسلحة مكلفة جداً، مثل حاملات الطائرات والمقاتلات المتطوّرة لتفرض تهديداً خطيراً وحقيقياً على الاطراف الأخرى، وإنما يكفي تطوير البرمجيات اللازمة وامتلاك الأجهزة الحاسوبيّة. وهكذا، بات بإمكان وصف المجال الإلكتروني للمواجهات باعتباره ليس حكراً على الدول فقط، ولكن أيضاً تنخرط فيه الجهات الفاعلة من غير الدول.

ويتصل بذلك إحدى أهم خصيصات حرب الفضاء الإلكتروني، وهي فشل إمكانية تطبيق فكرة ومبدأ الردع في حروب الفضاء الإلكترونيّ، والتي عادة ما تستخدم من قبل دولة ضد دولة اخرى في إطار منظومة الحروب التقليديّة أو النوويّة، أما في الحروب الإلكترونية فهذا الجانب غائب. وذلك عائد إلى خصائص عدّة، إذ أن هناك معضلة في تحديد الدولة والجهة التي قامت بالهجوم، فبإمكان القوة المهاجمة شنّ هجوم على دولة لصالح دولة، انطلاقاً من دولة ثالثة (عبر استخدام خوادم تكون موجودة هناك). وربما يكون هناك يكون طرف ثالث يريد إشاعة الخلافات بين دولتين فيقوم بالهجوم على إحداهما حتى تظن أن الثانية هاجمتها وبالتالي تتوتر العلاقات بينهما (فهمي، 2018: 24).

وبذلك فإن نماذج الردع المعروفة في الحروب التقليدية، والحروب غير التقليديّة (النوويّة والبيولوجية والكيميائية) تفشل في هذه الحروب، فهي غير ممكنة في العالم المعلوماتي، إذ يتعذر إظهار القوة الإلكترونية المهاجمة، بحيث يتم ردع العدو عن الهجوم. فالردع بالانتقام أو العقاب لا ينطبق على هذه الحروب، على عكس الحروب التقليدية، حيث ينطلق الصاروخ المهاجم – على سبيل المثال – من أماكن محددة، يتم رصدها، ومن ثم يكون بالإمكان الرد على الجهة المهاجمة. خلافاً لما هو الحال عليه في حروب الفضاء الإلكتروني، إذ يكون من الصعوبة بمكان، بل ومن المستحيل في كثير من الأحيان، تحديد مصدر الهجمات الإلكترونية.

وحتى إذا ما تم تتبع مصدر الهجمات الإلكترونيّة، وتبيّن أنها تعود إلى دول محددة، أو فاعلين غير حكوميين، فإنه في هذه الحالة لن يكون لديهم قواعد أو فضاءات ماديّة حتى يتم الرد إليها عبر استهدافها. كما أن بعض الهجمات قد تتطلب أشهراً لرصدها، وهو ما يلغي مفعول الردع بالانتقام، عبر توجيه ضربة تالية للضربة الأولى التي وجهها الطرف البادئ بالهجوم.

ويقترن بهذه الخاصيّة، خاصيّة أخرى تميّز حروب الفضاء الإلكتروني عن الحروب التقليديّة، وهي أنه لا توجد حدود جغرافية واضحة في هذه الحروب. كما لا يتواجد مفهوم "السيادة"، بمعناه السائد في العالم الواقعي، بحيث يتم منع الأطراف الأخرى من الدخول إلى المناطق الخاضعة لسيادة دولة ما مثلاً. بل إنه بالإمكان وصف الحدود في الفضاء الإلكتروني بأنها حدود مائعة. وبالاحرى، فإنه لا توجد حدود في العالم الافتراضي، إذ أن الحدود تتداخل مع بعضها، حيث أنّ كل الدول، صغيرة وكبيرة، تشترك في نفس الشبكات، التي يمكن اعتبارها بمثابة سحابة واحدة. وحتى خوادم الشبكات (Network Servers) تكون في كثير من الأحيان موجود في بلدان أخرى، غير البلدان المستخدمة لها والمشغلة لها. وبالتالي فإنه بالإمكان التأكيد على أن مفهوم السيادة في العالم الإلكترونية مفهوم مائع، وذلك مما يقتضيه طبيعة العالم الافتراضي المتداخلة.

وبالنظر لما تتمتع به هذه الحروب من خصائص و مميزات، جعلتها ذات طبيعة مختلفة عن المواجهات في الحروب التقليدية، فإن قواعد الاشتباك فيها لا تنطبق على قواعد الاشتباك المتبعّة في الحروب التقليديّة. وبالحديث عن قواعد الاشتباك في العالم الافتراضي، فإنه بالإمكان الحديث عن مراحل تسير وفقها، فهناك بدايةً مرحلة يمكن تسميتها بمرحلة التحضير للحرب، يسود فيها عمليات التجسس والاستطلاع وجمع المعلومات، وتطوير البرمجيات، وتجنيد المخترقين (بدران، 2010: 32).

ومن ثم، تأتي مرحلة التصعيد، والتي يجري فيها الهجوم على الأهداف، ضمن هجمات متفرقة ومتباعدة، سواء أكانت شخصيات أو مؤسسات. والتي تتم وفق ما تم إعداده وجمعه أثناء تحضير بنك الأهداف الإلكترونيّة. والتي تتنوع ما بين استهداف أنظمة القطاع الخاص، أو استهداف أنظمة القطاع العام والمرافق العامة. وفي هذه المرحلة تتخذ الهَجَمات شكل عمليات الاختراق للمواقع

الإلكترونية وقواعد البيانات المستهدفة، ومن ثم المباشرة في تخريبها أو مسحها أو سرقة المعلومات منها أو التجسس عليها أو تعطيل المواقع جملة والعبث بما يرتبط بها من أنظمة وحسابات.

ومن ثم، فإنه يمكن الحديث مرحلة لاحقة، هي مرحلة الحرب الإلكترونية المشتعلة. حيث يكون هناك تنظيمات محترفة ومدربة تدريبا جيداً ولديها الموارد، والأماكن المجهّزة، والأجهزة والمعدات والبرمجيات اللازمة، والتي تقوم بتوفيرها الدول المنخرطة فيها. وفي هذه المرحلة تستخدم الأسلحة الإلكترونية بغرض إلحاق أضرار مادية بالغة بمنشآت العدو، بما في ذلك المدنية والعسكرية منها، بحيث يكون هناك أضرار ماديّة واسعة وملموسة تنجم عن الهجمات الإلكترونيّة. وعادة ما تكون هذه المرحلة مؤازرة لحرب ومواجهة عسكريّة تقليديّة. فتكون بمثابة مؤازرة من الميدان الافتراضي للميدان العسكري. وقد يشتمل ذلك على عمليات تعتبر ضرورة لإسناد العمل العسكري، من التجسس على الإشارة، أو التشويش على نظام التموضع العالمي (GPS) وإعاقته لدى العدو، وعرقلة عمليات توجيه الأسلحة العسكرية المعادية (بدران، 2010: 34).

أما بخصوص طبيعة الأسلحة والأدوات المستخدمة وأنواعها في الحرب الإلكترونية. فإنّ القوة الإلكترونيّة تعتمد بصفة أساسية على الأجهزة والبرامج. الأجهزة تشتمل على أنظمة الحاسوب، مثل وحدة المعالجة المركزية (CPU)، أو محرك الأقراص الضوئية (CD Drive)، أو لوحة المفاتيح، أو الشاشة، وكذلك الكابلات، والأقمار الصناعيّة (Schreier, 2015: 103).

أما البرامج فهي الصياغات البرمجيّة المستخدمة لتوجيه عمليات الحاسوب. وفي هذه الحروب يتم استخدام البرامج الضارّة، والفيروسات، مثل، لغة الاستعلام الهيكليّة (SQL)، والتي هي عبارة عن مجموعة من التعليمات المستخدمة للتفاعل مع قواعد البيانات، وعمليات الحقن الإلكتروني عبر إدخال برمجيات ضارّة في الأنظمة الحاسوبيّة المستهدفة، أو البرمجة النصيّة للمواقع، لتشويه صفحات

الويب الخاصة بالعدو واتلافها. حيث يستحوذ هذا الشكل من الفيروسات على الموقع لبضع ساعات أو أيام، ويقوم بعرض صور ونصوص تهدّد الضحية وتسيء له. كما حصل في الهجوم الإلكتروني الروسي على إستونيا إثر نزاع الجندي البرونزي عام 2007م، عندما هاجم قراصنة روس مواقع تابعة للحكومة الإستونيّة، على إثر قرارها بإزالة تمثال جندي يرمز للحقبة السوفيتية، وذلك ضمن أساليب ناعمة يكون لها آثار نفسيّة كبيرة (Brandon and Manes, 2015: 34).

وتبرز الاختراقات كأحد أهم أساليب الهجوم في الحرب الإلكترونيّة، وهي تعتمد على برامج فعّالة لسرقة المعلومات الحساسة. كذلك هناك تكتيك الحرمان من خدمة الموزع، ويؤدي هذا النوع من الهجمات دوراً رئيسيّاً عبر محاولة جعل مورد الحاسوب غير متوفر للمستخدمين المقصودين به (Saalbach, 2019: 38).

وتتنوع البرمجيات المستخدمة في عمليات التسلل والاختراق، ومن أهمها: القنابل المنطقيّة، والتي هي عبارة عن هو قطع من التعليمات البرمجية المدرجة عمداً في نظام برمجي يقوم بإطلاق وظيفة ضارة عند استيفاء شروط محددة، والفيروسات، والديدان الحاسوبية (Computer worms). ونظراً الى كونها أدوات جديدة وتتطور بسرعة وباستمرار، فإنّ ذلك يجعل من يزيد من تعذر إسناد الهجمات الإلكترونيّة إلى جهات فاعلة، إذ أن البرامج المستجدّة تحتاج باستمرار إلى التعرف عليها وفك شيفرتها. هذا بالإضافة إلى القيود التقنيّة المتضمنة في البرامج ذاتها، والتي تمنع ضحية الهجوم الإلكترونيّ من التعرف على المهاجم (Mahnken, 2011: 58).

في ضوء ما تقدّم، يمكن القول بأن حرب الفضاء الإلكتروني يسود فيها حالة من ضباب الحرب (Fog of War)، كما في تعبيرات كلاوزفيتز. وبالتالي، كلّ ذلك يؤدي إلى عدم القدرة على ردع المعتدي المحتمل، مجهول الهوية. ويستدعي تطوير مقاربات جديدة للخطط والاستراتيجيات العسكريّة.

وبالإمكان القول بانّ جوهر العقيدة العسكرية في حروب الفضاء الإلكتروني تقوم على أساس السعي لكسب الحروب من خلال ضرب القلب الاستراتيجي للهياكل الإلكترونيّة للخصم. وذلك مع الاستمرار في تطوير استراتيجيات وقدرات للحماية، عبر تطوير أنظمة الدفاع السيبراني، وهو ما سيتم مناقشته بتوسع في الفصل القادم.

تجد الدراسة بأنّ حروب الفضاء الإلكتروني باتت ركن أساسيّ في الصراعات حول العالم، وقد حدث ذلك بالتزامن مع دخول عصر الثورة الصناعية الرابعة، وما نتج عنها من طمس للخطوط الفاصلة بين المجالات المادية والرقمية، والتحول المتسارع باتجاه الاقتصاد الرقمي، وكذلك التحول العسكريّ نحو تطوير الأسلحة الروبوت، التي تعتمد على أنظمة التحكم عن بعد والذكاء الاصطناعي، كل ذلك جعل من الفضاء الإلكتروني المعلوماتي مجالاً أكثر إغراءاً لتوجيه الضربات للخصوم والأعداء، حيث بات سبباً لإلحاق أضرار بالغة وشديدة التأثير بالخصم، وذلك مع إنفاق كلف متدنيّة نسبياَ.

ونظراً لأن هذا الفضاء الذي تجري فيه هذه الحروب هو فضاء افتراضي، وأنّ طبيعته مغايرة لطبيعة وخصائص العالم المادي، فإن ذلك انعكس على خصائص وطبيعة هذه المواجهات، فهي لا تعرف الحدود المكانيّة والجغرافيّة، ومن المتعذر فيها تحديد مصدر الضربات وخط سيرها، ولا يوجد فيها أي من الاعتبارات والتكتيكات العسكرية السائدة في الحروب التقليدية، والقائمة على أساس التنقل والحركة والتكتيك الميداني، في مجالات البحر والجو واليابسة، كلّ ذلك جعل منها نوعاً جديداً من المواجهات مغايراً لما عرفته البشرية عبر تاريخها، وهو ما ترك تأثيره على العقائد العسكرية وقواعد الاشتباك المتبعّة.

المبحث الثاني
المسؤولية الدولية المترتبة على حروب الفضاء الإلكتروني

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

مع تزايد الهجمات الإلكترونية وبروزها منذ العقد الأول من الألفية الثالثة، بدأت تبرز بالتزامن مع ذلك معضلة التكييف القانوني لهذه الهجمات. وبرز بالتحديد التساؤل حول مدى إمكانية تطبيق مبادئ وقواعد القانون الدولي الإنساني على هذا الشكل الجديد من الحروب. وجاءت المعضلة بسبب من توقيت إبرام الاتفاقيات التي صاغت مبادئ وقواعد القانون الدولي، إذ أنها تعود إلى فترات تبدأ منذ منتصف القرن الثامن عشر وما بعدها. وبالنظر إلى تواريخ أهم الاتفاقيات نجد اتفاقية لاهاي الأولى المقرّة عام 1899م، والثانية عام 1907م. ومن ثم اتفاقيات جنيف لعام 1949م، والبروتوكولان الإضافيان لعام 1977م، إذ لم يكن للهجمات السيبرانية خلال إبرامها جميعاً أي وجود يذكر (الفتلاوي، 2018: 39).

وبالتالي، لم يقع تنظيمها بشكلٍ صريح، ما استدعى الحاجة للاجتهاد بعد بروزها. إلا إن إشكاليات عدّة سرعان ما ظهرت إزاء ذلك، وتمثلت بشكل أساسيّ في صعوبة القدرة على تحديد

طبيعتها وعناصرها، إضافة إلى كون أغلب الهجمات السيبرانية لا تعلن الدول رسميّاً عن تبنيها لها، عدا عن إشكالية عدم القدرة على إثبات الدليل المادي على استخدام الهجمات الالكترونية، على عكس طرق القتال الأخرى المعروفة، إذ في بعض الهجمات لا يكون حتى هناك دمار لمنشآت وإنما فقط تلاعب وتعطيل لأنظمة، خلافاً للهجمات بالأسلحة التقليديّة وغير التقليدية التي تخلف دماراً ملموساً جزئيً أو كليّاً. كلّ ذلك شكل تحدياً أمام المختصين في القانون الدولي، وعنى صعوبةً في تحديد نطاقها ضمن القانون الدولي الإنساني، وما يترتب عليها من تبعات المسؤولية الدولية.

وقد وقع اختلاف في آراء المختصين القانونيين، ما بين من يرى أن المبادئ والقواعد التي أرساها القانون الدولي الإنساني تنطبق على تلك الهجمات، ومن يذهب – مثل إيميلي هاسلام – إلى أن المُدّة التي جرى فيها تقنين القواعد القانونية ذات الصلة باستخدام وسائل وطرائق القتال، لم يكن لاستخدام الانظمة الالكترونية للأغراض العسكرية الهجومية وجود يذكر، ما يعني أنها غير مقننة، وغير منظمة وفقاً للقواعد الدولية؛ أيّ أنها خارج التنظيم القانوني الدولي، وهي بحاجة لقوانين جديدة صريحة تنصّ على تنظيمها بشكل لا يدع أي مجال للاجتهاد والتأويل (Haslam, 2000: 157).

وكان أهم المبادئ القانونية الذي فتح مجالاً أمام القياس وإنزال حالة الحروب الإلكترونية عليه هو مبدأ الامتناع عن استخدام القوّة عموماً من قبل أي دولة ضد أيّ دولة أخرى، والذي جاء النصّ عليه في الفقرة الرابعة من المادة الثانية من ميثاق الأمم المتحدة، ونصّها: ((يمتنع أعضاء الهيئة جميعاً في علاقاتهم الدولية عن التهديد باستعمال القوة أو استخدامها ضد سلامة الأراضي أو الاستقلال السياسي لأية دولة أو على أي وجه آخر لا يتفق ومقاصد الأمم المتحدة)) (موقع الأمم المتحدة الإلكتروني، ميثاق الأمم المتحدة).

وهنا ظهر الجدل حول إمكانية اعتبار الهجمات الإلكترونيّة بمثابة خرق واضح لحكم هذه الفقرة. ما بين اعتبار أنها تقتصر على التهديد أو الاستخدام الفعلي للقوات المسلحة فحسب، حيث تحبذ هذا التفسير الدول المتفوقة في مجال الحرب الإلكترونيّة، أما الدول الأخرى فتميل الى توسعة نطاق مدلول كلمة "القوّة" في الفقرة، لتشمل الإلكترونيّة أيضاً.

وقد ذهب كُلاً من شين، وروسيني إلى أنه من الممكن أن تعد الهجمات الإلكترونيّة بمثابة خرق واضح لأحكام الفقرة (4) من المادة (2)، شريطة أن تتسبب بتعطيل أو دمار واسع للبنى التحتية الضرورية في حياة الناس (Roscini, 2010: 130).

ووفقاً لهما، فإنه وإن تم ذلك فللدولة المعتدى عليها الحق في اللجوء الى استخدام القوة تحت طائلة المادة (51) من الميثاق، والتي تنصّ على: ((ليس في هذا الميثاق ما يضعف او ينتقص الحق الطبيعي للدول، فرادى أو جماعات، في الدفاع عن أنفسهم إذا اعتدت قوة مسلحة على أحد أعضاء الأمم المتحدة".. والتي تتيح الحق في الدفاع عن النفس.. يمكن للقواعد العرفية الدولية أن تؤدي دوراً متميزاً في تكييف تلك الهجمات، ولا سيما في ظل عدم وجود اتفاقيات دولية تنظم الهجمات السيبرانية)) (موقع الأمم المتحدة الإلكتروني، ميثاق الأمم المتحدة).

ووفقاً لهذا الاجتهاد فإنّ للدولة الحق في الدفاع عن نفسها إزاء أي هجوم، بغض النظر عن شكله ووسيلته. وقد جاء إعلان وزارة الدفاع الأمريكية (البنتاغون) في عام 2011م ليؤكد على هذا الاعتبار، إذ جاء فيه بأن توجيه هجمات إلكترونيّة ضد الولايات المتحدة الأمريكيّة، وما ينجم عنها من أضرار، يعني تبرير استخدام القوة العسكرية اللازمة، للرد على هذا الاعتداء، باعتبار ذلك حرباً مبررة وعادلة (Barnes: 2011, 2 & Gorman).

أما المبدأ القانوني الثاني الذي بالإمكان تكييف الهجمات الإلكترونية وفقاً له فهو مبدأ وجوب التمييز بين المدنيين والمقاتلين، وخصوصاً إن جانب كبير من الهجمات الإلكترونية يستهدف القطاعات الاقتصادية، والأمنية، والزراعية، والصناعية وغيرها من القطاعات المدنيّة التي لا غنى عنها لبقاء السكان المدنيين على قيد الحياة، ولا تقتصر في أهدافها على المنشآت والأهداف العسكريّة.

وقد جاء في المادة (48) من البروتوكول الإضافي الأول لعام 1977م الملحق باتفاقيات جنيف: ((تعمل أطراف النزاع على لتمييز بين السكان المدنيين والمقاتلين وبين الأعيان المدنية والأهداف العسكرية، ومن ثم توجه عملياتها ضد الاهداف العسكرية دون غيرها، وذلك من أجل تأمين احترام وحماية السكان المدنيين والأعيان المدنية)) (موقع اللجنة الدولية للصليب الأحمر الإلكتروني، البروتوكول الأول الإضافي إلى اتفاقيات جنيف، على الرابط: https://www.icrc.org).

ونصّت الفقرة الثانية من المادة (51) من البروتوكول على: ((لا يجوز أن يكون السكان المدنيون بوصفهم هذا، وكذا الأشخاص المدنيون، محلاً للهجوم، وتحظر أعمال العنف أو التهديد الرامية إلى بث الذعر بين المدنيين. أما الفقرة الرابعة من المادة (51) فقد نصّت على عدم جواز استعمال وسائل وطرق قتال من شأنها أن تؤدي إلى هجمات عشوائية، وحددتها بأنها: ((تلك التي لا توجه إلى هدف عسكري محدد. أو تلك التي تستخدم طريقة أو وسيلة للقتال لا يمكن أن توجه إلى هدف عسكري محدد. أو تلك التي تستخدم طريقة أو وسيلة للقتال لا يمكن حصر آثارها على النحو الذي يتطلبه هذا الملحق، ومن ثم فإن من شأنها أن تصيب في كل حالة كهذه الأهداف العسكرية والأشخاص المدنيين أو الأعيان المدنية دون تمييز)) (موقع اللجنة الدولية للصليب الأحمر الإلكتروني، البروتوكول الأول الإضافي إلى اتفاقيات جنيف، على الرابط: https://www.icrc.org).

ونصّت الفقرة الخامسة من المادة (51) من البروتوكول على: "يحظر الهجوم الذي يتوقع منه أن يسبب بصورة عارضة خسائر في أرواح المدنيين او اصابات بينهم، أو أضراراً بالأعيان المدنية.. ويكون مفرطاً في تجاوز ما ينتظر أن يسفر عنه من ميزة عسكرية ملموسة ومباشرة" (موقع اللجنة الدولية للصليب الأحمر الإلكتروني، البروتوكول الأول الإضافي إلى اتفاقيات جنيف، على الرابط: https://www.icrc.org).

ويُضاف إلى هذه الموادّ شرط مارتنز، وهو المنسوب إلى فريدريك مارتنز، المندوب الروسي في مؤتمر السلام المنعقد في لاهاي عام 1899م، يعتبر بمثابة شرط إضافي يؤكد على ضرورة تصويب وتحديد الوضع القانوني للهجمات الإلكترونيّة، إذ ينصّ على: ((في الحالة التي لا تنطبق فيها معاهدة أو قانون عرفي، فإن المدنيين والعسكريين يتمتعون بحماية مبادئ القانون الدولي المشتقة من العرف المستقر، ومن المبادئ الإنسانية، وما يمليه الضمير العام)) (Gesses, 2000: 187).

وبالتالي، فإنه ووفقاً لهذا المبدأ (التمييز بين المدنيين والعسكريين) يتوجب على أطراف النزاع المسلح التمييز بين المقاتلين والمدنيين في الهجمات، وهو ما لا يتحقق في جانب كبير من الهجمات الإلكترونية، والتي تؤدي إلى تدمير منشآت حيوية مدنيّة محمية وفقاً للقانون الدولي. وبالتالي يمكن اعتبار بأن هذه الهجمات محظورة ومُدانة وفقاً لما تقرره المبادئ الدولية التي تحظر ذلك.

منطلق قانوني آخر يدفع باتجاه ضرورة تحديد الوضع القانوني للهجمات الإلكترونيّة يتمثل في ما جاء بالمادة (36) من البروتوكول الإضافي الأول لعام 1977م الملحق باتفاقيات جنيف، والتي نصّت على: ((يلتزم أي طرف سامٍ متعاقد، عند دراسة سلاح جديد أو تطويره أو اقتنائه أو أداة حرب أو اتّباع أسلوب للحرب، بأن يتحقق مما إذا كان ذلك محظورًا في الأحوال كافة أو في بعضها بمقتضى هذا الملحق البروتوكول أو أي قاعدة أخرى من قواعد القانون الدولي التي يلتزم بها ذلك

الطرف السامي المتعاقد)) (موقع اللجنة الدولية للصليب الأحمر الإلكتروني، البروتوكول الأول الإضافي إلى اتفاقيات جنيف، على الرابط: https://www.icrc.org).

وبالتالي، فإنّ هذه المادة تنصّ على ضرورة التنظيم القانوني لوسائل وأساليب القتال الجديدة، ومن بينها بالطبع الوسائل الإلكترونيّة المستخدمة في شنّ الهجمات الإلكترونيّة.

هكذا، يُلاحظ بأنّ التكييف القانوني للهجمات الإلكترونيّة لا زال ضمن مستوى القياس والاجتهاد، ولم يصل بعد إلى مرحلة إبرام اتفاقيّات دوليّة صريحة خاصّة به، وبحيث تكون متعددة الأطراف، وتنظّم الهجمات الإلكترونيّة وفق نصوص وقواعد قانونيّة صريحة، وهو ما يُعزى إلى أسباب عدّة، يأتي في مقدمتها وجود عقبات تضعها الدول المهيمنة في مجال حروب الفضاء الإلكتروني، مثل الولايات المتحدة الأمريكية، وروسيا، والصين. إذ انّ هذه الدول لا تفضل طرح موضوع التنظيم على المنابر الدولية حتى لا تفقد موقعها المهم بين الدول المهيمنة، وهو ما يضرّ بأمنها القوميّ. يضاف إلى ذلك، أن بقاء الموضوع خارج حدود القضايا القانونية يتيح للدول مساحة واسعة لكي تتحرك في توظيف أسلحتها الإلكترونية لتحقيق أهدافها، وهي بذلك تبقى خارج نطاق المسائلة القانونية

يترتب على ذلك كلّه مسألة أخرى تتعلق بطبيعة المواجهات في الفضاء الإلكتروني، إذ أن من الصعوبة بمكان إثبات المسؤولية عن الهجمات، والتي تتخذ من الفضاء الإلكتروني مجالها الرحب، لكونها تصرفات غير مادية، ولا يمكن إثباتها بالطرق العادية. وما يزيد من الصعوبة في التنظيم أيضاً هو استخدام هذه التقنيات لا من الدول فقط، بل من مجموعات من غير الدول أيضاً.

بالرغم من ذلك، فقد برزت بعض المحاولات لبلورة اتفاقيات دوليّة بهذا الشأن، إلا أنّها لم ترقَ إلى مستوى تنظيم الحروب والهجمات الإلكترونية، بقدر ما كانت أقرب لإقرار أطُر لما بات يُعرف بالجرائم الإلكترونية، ذات الطابع الجنائيّ، وذلك تحديداً على المستويات الوطنيّة. ومن أبرز هذه

المساعي اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، المقرّة في تشرين الثاني (نوفمبر) من عام 2001م، والتي تعرف أيضاً باسم "معاهدة بودابست لمكافحة جرائم الفضاء المعلوماتي". وقد بُنيَ عليها لاحقاً تشريعات وطنية استندت إليها، سواء في أوروبا أو غيرها من الدول حول العالم (محمد، 2016: 94).

تضمنت هذه الاتفاقية إقراراً لأطرٍ قانونية للسلوك الالكتروني المُجرّم، ووضع الجزاءات الواجب إيقاعها على المتهم بارتكابها. ونجد المادة الثانية من اتفاقية مجلس أوروبا تحدد بأن: ((كل دولة طرف في المعاهدة تعتمد ما قد يلزم من تدابير تشريعية وتدابير اخرى لتجريم الفعل التالي في قانونها، إذا ما ارتكب عمداً وبغير حق: الدخول على كامل او جزء من منظومة كمبيوتر. الاعتراض باستخدام وسائل فنية، لعمليات إرسال غير عمومية لبيانات كمبيوتر أو من خلال منظومة كمبيوتر. إتلاف أو محو او إفساد أو تعديل او تدمير بيانات موجودة على الكمبيوتر. الإعاقة الخطيرة لعمل منظومة الكومبيوتر عن طريق إدخال او إرسال أو إتلاف أو محو او تغيير أو تبديل او تدمير بيانات كمبيوتر)) (موقع مجلس أوروبا الإلكتروني، اتفاقية مجلس أوروبا المتعلق بالجريمة الإلكترونية، على الرابط: رابط الموقع: https://cas.coe.int/).

وبالتالي فإن مفهوم الجريمة الالكترونية، وفقاً لهذه الاتفاقية، قد اقتصر على هذه الحالات، ولم يتطرق إلى مستوى الهجمات والحروب الإلكترونية التي تكون أطرافها من الدول أو من المنظمات المرتبطة بها.

ومن ثم جاء القرار الصادر عن الجمعية العامة للأمم المتحدة رقم (56/121)، في كانون الثاني/يناير 2002م، والموسوم بـ "مكافحة إساءة استعمال تكنولوجيا المعلومات". والذي جاء فيه:

((دعوة الدول الأعضاء، لوضع قوانين وسياسات وممارسات وطنية لمكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية)) (United nations, 2002: 2).

وفي عام 2013م، صدر دليل تالين، والذي وسم أنه دليل "بشأن القانون الدولي المطبق على الحروب السيبرانية"، والذي أعدّ من قبل مجموعة من الخبراء الدوليين، وبدعوة من "مركز التميز التابع لحلف الناتو". وتضمن قواعد غير إلزاميّة.

ومن أهم ما جاء في هذا الدليل الإشارة في القادة (37) منه إلى أنه ((لا يجوز أن تكون الأعيان المدنية هدفًا للهجمات الإلكترونيّة، فلا يجوز على سبيل المثال توجيه الهجمات السيبرانية التي من شأنها تدمير الأنظمة المدنية والبنية التحتية، ما لم تعد هذه الأنظمة من قبيل الأهداف العسكرية التي يجوز استهدافها وفق الظروف السائدة)) (Schmitt et al, 2013: 106).

تجد الدراسة بأنّ التحدي الأكبر الذي يواجه تنظيم الهجمات في الفضاء الإلكتروني قانونياً هو عدم وجود إرادة دولية على صعيد المفاوضات أو على صعيد قرارات مجلس الأمن، حيث تغيب الإرادة الدولية اللازمة للدفع باتجاه ذلك، وخصوصاً من قبل الدول المهيمنة في هذا المجال. كما وتجد الدراسة أنّ القانون الدولي الإنساني يذهب إلى تنظيم استخدام الأسلحة بصورتها التقليديّة وغير التقليديّة، في حين لا يبدو أن الهجمات الإلكترونية، حتى الآن، تصنف على هذا النحو، باعتبارها أسلحة ماديّة، وذلك باعتبار بقاء النظر لها باعتبارها تعمل في الحيز الافتراضي غير المادي، كما في عمليات الاستحواذ على ملفات رقمية أو تعطيل مواقع إلكترونية.

الفصل الرابع

السُبُل والإمكانيات المتاحة لمواجهة حروب الفضاء الإلكتروني

الفصل الرابع
السُبُل والإمكانيات المتاحة لمواجهة حروب الفضاء الإلكتروني

أمام الزيادة المتسارعة في وتيرة لجوء الدول لاعتماد الفضاء الالكتروني كسبيل لإلحاق الضرر بالأعداء والخصوم، والتزايد في قيمة الأضرار الناجمة عن هذه الهجمات التي تصيب المعلومات والشبكات ضمن الفضاء الالكتروني، وما يقترن ويرتبط بها من أنظمة ومنشآت ومصالح لا تقتصر على الجانب العسكري، وإنما تشمل ما هو مدني أيضاً، من منشآت وبنى تحتيّة حيوية وحساسة. إزاء كل ذلك تزداد حاجة الدول لبلورة وتملّك منظومة دفاعيّة تسهم في صد الهجمات ومنعها، أو على الأقل التخفيف من ضررها في حال وقوعها، وذلك بالإضافة إلى تطوير الأساليب والأدوات القتالية الهجومية ضمن هذا الفضاء.

ولا تقتصر الأنظمة الدفاعية ضمن الفضاء الالكتروني على جانب واحد، بل هي متعددة، ويمكن تلخيص أهمها في جانبين، هما التقني البرامجيّ، والجانب التشريعي القانوني. في الجانب الأول هناك تقدم مستمر مصاحب للتطور المستمر في البرمجيات والتقنيات المعتمدة في عمليات الهجوم والاختراق، ومقارب له بالوتيرة والسرعة، في حين أن تطور المنظومة التشريعية الدفاعيّة ظلّت أبطأ من وتيرة تطور الهجمات الإلكترونية، وهو ما يعود لأسباب متعددة سوف نتعرف عليها في هذا الفصل.

المبحث الأول
المنظومات التقنية للحدّ من الهجمات الإلكترونية

تتعدد أساليب المواجهة والتصدي التقنية للهجمات الإلكترونية، وتتلخص بالأساس في اعتماد ثلاث نوعيات من التقنيات والأنظمة الأكثر انتشاراً وثقةً وكفاءةً، ويأتي في مقدمتها جدران الحماية أو ما يُعرف بـ "الجدران الناريّة" (Firewall). ومن ثم هناك البرامج المضادة للبرمجيات الخبيثة من فيروسات وغيرها (Antivirus program)، وأنظمة كشف التسلل (IDS). وبالإضافة إلى هذه التقنيات هناك إجراءات احتياطية تقنية بسيطة تلجأ لها الدول ولكنها تكون ذات ومفعول مردود أمني عالي، كإجراءات فصل وتقسيم الشبكات، والتشديد على بيانات الدخول، وإجراء عمل النسخ الاحتياطي (Backup).

تعتبر جدران الحماية من أهم وسائل الدفاع التقنيّة لصدّ الهجمات الالكترونيّة من محاولات إختراق وبثّ للبرمجيّات الضارّة، وهي تعرف أيضاً بـ "الجدار الناري" (Firewall)، وتقوم جدران الحماية على مبدأ الفصل بين المناطق الموثوق بها والمناطق غير الموثوق بها في شبكات الحاسوب. وبحيث يقوم برنامج جدار الحماية بمراقبة العمليات التي تمر بالشبكة ويرفض أو يسمح فقط بمرور البرامج طبقاً لقواعد معينة (ستولينج، 2011: 622).

أصل الفكرة والتسمية جاءت من الحائط الذي يبنى بالطوب الأحمر العازل بشكل يوقف انتقال النيران المحتملة إلى داخل البيوت، ويطلق على هذا الحائط الطوبي اسم الـ "حائط الناري". وبالمثل يقوم برنامج جدار الحماية بمنع اختراق الشبكة، ويمنع البرامج الضارة من الدخول إلى الجهاز أو الشبكة، وذلك عبر آلية ترشيح البيانات المُستقبَلة، وهو يسمح في الوقت نفسه للاتصالات غير الضارة بالوصول بحريّة (ستولينج، 2011: 623).

ظهرت هذه التقنية في أواخر عقد الثمانينات من القرن الماضي، وذلك استجابةً لعدد من الاختراقات لشبكة الإنترنت المستجدة حينذاك. وقد ظهر منها عدة أجيال: الجيل الأول يعرف بـ "مرشحات العبوة" (Packet Filters)، ويقوم مبدأ عمله على فلترة (ترشيح) "العبوة" (Packet)، والتي تمثل الوحدة الأساسيّة المخصصة لنقل البيانات بين الحواسيب على الإنترنت. فإذا كانت العبوة تطابق مجموعة شروط الجدار، فإنه يسمح بمرور العبوة، أو يرفضها ويتخلص منها ويقوم بإرسال إشارة "خطأ" (Error) للمصدر، في حال لم تكن مطابقة (حسين، 2011: 196).

لكن هذا النظام من "مرشّحات العبوات" لم يكن يعير اهتماماً إلى كون العبوة جزءاً من تيار من المعلومات والبيانات المتدفقة، إذ لا يقوم بتخزين سلسلة من البيانات والمعلومات، وإنما يقوم بترشيح العبوات بناءاً على المعلومات المختزنة في العبوّة نفسها، ويتعامل مع كلٍ منها على حدى، ما استدعى تطوير الجيل الثاني من جُدُرْ الحماية والمعروف بـ "فلتر محدد الحالة" (Stateful Filter)، والذي يقوم بمراقبة حقول مُعَيّنة في المعلومات المستقبلة، ويقارنها بالحقول المناظرة لها في سلسلة كاملة من المعلومات الواردة ضمن السياق نفسه، ومن ثم يجري رفض المعلومات التي تنتمي لسياق مُعيّن إذا لم تلتزم بقواعده، لأن ذلك يكون دليلاً على أنها زرعت في السياق وليست جزءاً منه، مما يثير الشكوك بأنها برامج خبيثة (حسين، 2011: 197).

ومن ثم ظهر أخيراً الجيل الثالث والمعروف باسم "طبقات التطبيقات" (Application Layer Firewall)، والفائدة الرئيسية منه أنه يمكن أن يفهم ويتعامل مع التطبيقات والأنظمة المُعَقدة، ومن ثم بإمكانه اكتشاف إذا ما كان هنالك نظام غير مرغوب فيه يتم تسريبه، أو إذا كان هنالك نظام يتم استخدامه بطريقة مؤذية (حسين، 2011: 198).

أما التقنية الثانية من ضمن التقنيات الأكثر اعتماداً وانتشاراً في مجال التصدي للهجمات الإلكترونيّة فهي البرامج المعروفة باسم مضادات الفيروسات (Antivirus). ومُضاد الفيروسات هو برنامج يتم استخدامه لاكتشاف البرمجيات الضارّة ومنعها من إلحاق الضرر بالحاسوب أو سرقة البيانات الشخصية، وذلك عن طريق إزالتها أو إجراء التعديلات عليها وإصلاحها. وبحيث يمكن لهذا البرنامج أن يتصدى لبرامج التجسس، وبرامج أحصنة طروادة، والتي هي عبارة عن شيفرات صغيرة تقوم ببعض المهام الخفيّة وغالباً ما تتركز على إضعاف قوى الدفاع واختراق جهاز الحاسوب وسرقة بياناته. وكذلك تتصدى مضادات الفيروسات لـ "الديدان الحاسوبيّة"، كما توصف، وهي برامج صغيرة، تصنع للقيام بأعمال تدميرية، أو لغرض سرقة البيانات الخاصة ببعض المستخدمين أثناء تصفحهم للإنترنت (الخالد، 2018: 99).

تم تطوير برامج مضادات الفيروسات أواخر الثمانينات من القرن الماضي، وقد ازداد تطورها بفعل زيادة حجم المخاطر التي تهدد الحواسيب. ولتحديد الفيروسات والبرامج الخبيثة، تقارن برامج مضادات الفيروسات محتويات الملف إلى قاموس فحص الفيروس. ولأن الفيروسات يمكنها تضمين نفسها في الملفات، عندها يتم البحث في الملف بأكمله لضبطها والكشف عنها. وهناك أسلوب آخر يعتمده مضاد الفيروسات، يتم عبر الكشف على نشاط البرمجيات الضارة، بحيث يقوم برصد نظام للاشتباه في تصرفات البرنامج. فإذا ما تم الكشف عن سلوك مريب، يقوم مضاد الفيروسات بعمل مزيد من التحقيق والفحص في البرنامج. ويمكن استخدام هذا الأسلوب لتحديد الفيروسات غير المعروفة أو نُسخ أخرى من الفيروسات الموجودة (طيطي، 2010: 191).

ومن ثم هناك أسلوب "مضاهاة ملف" (File Emulation)، وفيه يتم تنفيذ البرنامج في بيئة افتراضيّة، وتسجيل الإجراءات التي ينفذها، ومن ثم، واعتماداً على الإجراءات التي تم تسجيلها،

يستطيع برنامج مضاد الفيروسات تحديد ما إذا كان البرنامج ضار أم لا ومن ثم تتخذ الإجراءات المناسبة (طيطي، 2010: 192).

أما التقنية الثالثة المستخدمة ضمن أنظمة التصدي لهجمات الفضاء الإلكتروني فهي أنظمة كشف التسلل (Intrusion Detection Systems)، وتعرف اختصاراً بـ (IDS). ونظام التصدي هو برنامج مصمم للكشف عن محاولات الوصول إلى نظام الحاسب الآلي غير مرغوب بها أو محاولة تعطيل هذا النظام بشكل عام والتلاعب به، وبحيث أن هذه المحاولات يمكن أن تتخذ عدة أشكال وسبل، منها كسر الحماية، أو استخدام البرامج الضارة (الفيروسات، حصان طروادة، والديدان) (الخالد، 2018: 63).

تتألف أنظمة كشف التسلل من عدة مكوّنات، هي: جهاز استشعار ينبّه على وقوع الأحداث، ولوحة تحكم لمراقبة الأحداث والتنبيهات والتحكم بأجهزة الاستشعار، ومحرّك يقوم بتسجيل إدخالات الأحداث المتلقاة من خلال أجهزة الاستشعار في قاعدة بيانات. وتكون أنظمة كشف التسلل مصنّفة بالاعتماد على نوع وموقع أجهزة الاستشعار والمنهجيات المستخدمة على المحرّك (الخالد، 2018: 64).

وعدا عن استخدام البرمجيات والأنظمة التقنيّة لمواجهة الهجمات الإلكترونية هناك وسائل تقنيّة أخرى يمكن تفعيلها أيضاً لتفادي وتقليل آثار هذه الهجمات، وذلك دون الحاجة إلى استخدام برمجيات وأنظمة متطوّرة ومعقّدة، ومن ذلك اللجوء إلى عمل فصل جزئي احتياطي بين الشبكات فلا تكون كلها كتلة واحدة، وبحيث يتم تقسيم الشبكات إلى شبكات فرعيّة (Subnetting)، لكل منها قواعد محددة للدخول، وذلك بهدف الحدّ من الاتصال بينها وبين أيّ شيء خارج هذه الشبكات. ومثال على

ذلك، إذا وقعت هجمة تستهدف إحدى شبكات المعلومات أو البنى التحتية فإن الأضرار تكون مقتصرة على تلك الشبكة دون امتدادها إلى شبكات أخرى (محمود، 2016: 81).

إلى جانب ما تقدّم، هناك إجراءات احترازية سهلة التطبيق، مثل التشديد وعدم السماح للدخول إلى الشبكة إلا بعد تقديم وإبراز معلومات شخصية من قبل كافّة المستخدمين على الشبكات الحيويّة، مثل بوابات الحكومة الالكترونيّة، وذلك بتأكيد هويتهم عند الدخول إليها، باستخدام عُنصرَين على الأقل من عناصر تحديد الهوية، وبحيث تكون المعلومات بمثابة البصمة التي لا يمكن استنساخها أو الاشتراك بها. ومن الأمثلة على ذلك استخدام الأرقام الوطنية، وأرقام الهاتف، وكذلك التأكد من الهوية عبر إرسال رسائل التفعيل إلى أرقام الهواتف (المبيضين، 2020: 106).

هناك إجراء آخر قد يكون بسيطاً، ولكن يمكن أن يساهم في تلافي أضرار الهجمات الإلكترونيّة بدرجة كبيرة. هذا الإجراء يتمثل في ضرورة المواظبة على عمل نسخ احتياطي (Backup) وبشكل دوريّ منتظم، لكافة الملفات والمعلومات والبيانات المهمة على الشبكة وفي قواعد البيانات، بما في ذلك البيانات الخاصّة بالمؤسسة والعملاء. وبحيث في حال التعرض لأي تخريب أو هجوم إلكتروني يستهدف قرصنة المعلومات وتخريبيها ومسحها، فإنه يتم الحدّ من تأثيره. ففي حالة توفر النسخ الاحتياطيّة فإنه سرعان ما يتم استعادة ورفع جميع البيانات من جديد وبكامل تفاصيلها وصحتها ودقتها، وكلما كانت عملية النسخ دورية ضمن مدد زمنية أقصر كلما كان حجم البيانات المفقودة أقل. ويتم إجراء النسخ الاحتياطي من خلال شراء أقراص صلبة خارجية ذات مساحات كبيرة حتى تستوعب نسخ احتياطية من جميع الملفات.

مما تقدّم تخلص الدراسة إلى أنه هناك العديد من الوسائل التقنيّة المتاحة لمجابهة الهجمات في الفضاء الإلكتروني والتصدي لها، وبحيث إن الالتزام بتطبيق وتفعيل أكبر قدر منها يمكن إن يكون

معينا إلى حد بعيد في التصدي لهذه الهجمات والحدّ من تأثيرها في حال وقوعها، وهو ما تزداد الحاجة إليه لدى مختلف الدول وبخاصّة في ظل عدم التوصّل إلى اجماع دولي واسع يفضي إلى بلورة معاهدات ومنظومة قانونية وقائية تحول وتحد من وقوع هذه الهجمات.

كما وتجد الدراسة، أن وسائل التصدي التقنيّة لا تقتصر فقط على البرمجيات المعقدة والمتطوّرة، وإنما هناك إجراءات تقنية بسيطة نسبيّاً يمكن من خلال الالتزام بها تفادي جانب كبير من مخاطر الهجمات، بما في ذلك اللجوء إلى تقسيم الشبكات، والتشديد على إجراءات الدخول إلى الشبكات، والمواظبة على عملية النسخ الاحتياطي لكافة البيانات والمعلومات الهامة.

المبحث الثاني
الاتفاقيات الدولية المتعلقة بالحدّ من حروب الفضاء الإلكتروني

بسبب من المخاطر المتنامية لما يترتب على هجمات الفضاء الإلكتروني بادر العديد من دول العالم لاتخاذ تدابير وقائية لها صفة تشريعية، بما في ذلك سنّ تشريعات وقوانين على المستوى الوطني لتجريم الجهات والأطراف التي تقدم عليها، وترتيب جزاءات على من يقوم بمخالفتها. ولكن التحدي الأكبر ظلّ كامناً في سنّ التشريعات ذات الفعالية والأثر الأكبر والتي تكون ضمن الأطر الإقليميّة والدوليّة، من اتفاقات ومعاهدات أمنيّة يكون لها الأثر في الحد من حروب وهجمات الفضاء الإلكتروني. وبحيث تنصّ هذه المعاهدات صراحةً على تحريم وتقييد الهجمات ضمن الفضاء الإلكتروني، إلّا أنّ الاستمرار في غياب الإجماع الدوليّ اللازم استمر في كونه العقبة الأكبر أمام مثل هذه الاتفاقيات.

والملاحظ على المستوى الوطني، لم تكن عملية التشريع الخاصة بالهجمات في الفضاء الإلكتروني، أو كما تعرف بـ "الهجمات السيبرانية"، والتي في الغالب جاءت متقاطعة مع تشريعات تجريم جرائم الفضاء الإلكتروني (الجرائم السيبرانيّة)، تتصف بالسهولة، بل مثّلت تحديّاً كبيراً للمنظومات التشريعيّة والمشرعين، وهو ما يعود إلى أسباب عدّة، وذلك أنّ عملية التشريع تستغرق وقتًا طويلاً، وهو ما لا يتواءم مع طبيعة الجرائم في الفضاء الإلكتروني، التي تتصف بالتطوّر السريع، وذلك بالتزامن مع اكتشاف التقنيات وأساليب الاختراق الجديدة وتطوّر، وتعقّد الانتهاكات المصاحبة لها، وبحيث أن هذا التطوّر يكون متفوّقاً باستمرار على وتيرة تعديل القوانين الجزائية لمكافحتها. فالتعديلات الضروريّة للقانون الجزائي غالباً ما تكون بطيئة (فوزي، 2015: 63).

تُضاف إلى ذلك، الصعوبات العديدة المقترنة بهذه الجرائم بحكم ما يميزها من خصائص عن غيرها من سائر الجرائم. ومن ذلك صعوبة كشف هوية المشتبه بهم وما يستخدمونه من أجهزة وبرامج، وكذلك الصعوبات التي تواجه عملية استعادة الملفات المحذوفة، وتحديد الأدلة ذات الصلة بالجرائم، وفك تشفير الملفات (فوزي، 2015: 64).

على الصعيدين الإقليمي والدولي، ورغم عدم تطوّر وصياغة منظومة متكاملة كما هو الحال في ميادين الحروب التقليديّة وغير التقليدية، فإنه قد برز السعي والعمل على صياغة تشريعات تتعلق وترتبط بمحاولات تنظيم وتقييد هجمات الفضاء الإلكتروني، في إطار السعي لصياغة ما عرف بـ "أمن الفضاء الإلكتروني" أو "الأمن السيبراني" أو "أمن الشبكات"، والذي جاء جانب كبير من المساعي ضمنه بهدف وضع تشريعات لمكافحة الجرائم ذات الطابع الجنائي والتي تتخذ اجهزة الحاسوب وشبكات الإنترنت وسيلةً وميداناً لها. في حين لم يتم الوصول إلى مستوى تناول هذه الهجمات باعتبارها تأتي ضمن سياق حروب ومواجهات بين دول بينها خلافات ونزاعات. وبات مصطلح "الأمن السيبراني" يستخدم لتلخيص السياسات العامة والتدابير الأمنية، والمبادئ التوجيهية، وطرق إدارة المخاطر، والحماية، والتدريب، ومختلف التقنيّات والأدلة التي يمكن استخدامها واعتمادها لحماية أجهزة الحاسوب وشبكات الإنترنت والبيانات المخزنة والمتداولة عبرها (العلي، 2017: 226).

جاءت بداية الجهود الدوليّة على هذا الصعيد مع نشر الجمعية العامة للأمم المتحدة للدليل المعروف باسم "دليل منع الجرائم المتصلة بأجهزة الكمبيوتر ومكافحتها" في العام 1994م. وتضمن هذا الدليل الإشارة إلى أن مدى انتشار الجرائم الحاسوبية قد يكون واسعاً بقدر اتساع نظم الاتصالات الدولية. وكان تركيز الدليل يتمحور حول مفهوم "الجريمة الحاسوبيّة"، دون اعتماد مسميات "جرائم الفضاء الإلكتروني" أو "الجرائم السيبرانيّة"، وبحيث لم يتم التطرق لها بشكلها الحالي المعتمد على

تكنولوجيا التواصل المعلوماتي المعولمة، متمثلةً في شبكة الإنترنت، وما يقترن بذلك من ارتكاب أعمال إجرامية ذات نطاق دولي (United Nations, 1994: 3).

وفي السابع عشر من نيسان/أبريل عام 2000م، صدر عن مؤتمر الأمم المتحدة ما عرف بـ "إعلان فيينا بشأن الجريمة والعدالة"، وجاء النصّ في الفقرة الثامنة عشرة منه على "الجرائم الحاسوبيّة"، حيث نصّت على: ((نقرر صوغ توصيات سياساتية ذات توجه عملي بشأن منع ومكافحة الجريمة المتعلقة بالحواسيب، وندعو لجنة منع الجريمة والعدالة الجنائية إلي الاضطلاع بعمل في هذا الشأن، آخذةً في الاعتبار الأعمال الجارية في محافل أخرى. ونعلن التزامنا أيضاً بالعمل على تعزيز قدرتنا على منع الجريمة المرتبطة بالتكنولوجيا الراقية والحواسيب والتحري عن تلك الجرائم وملاحقتها)) (United Nations, 2000: 2). إلا إن مثل هذه التوصيات ظلّت في إطار السعي لبلورة منظومة تشريعيّة تنطلق من التعامل مع هجمات الفضاء الإلكتروني باعتبارها مسألة تتعلق بجرائم ذات طابع جنائي بالدرجة الأولى وليست باعتبارها نوعاً وشكلاً جديداً من المواجهات الدوليّة.

في شهر نيسان/أبريل العام 2001م اعتمد البرلمان الأوروبي "الاتفاقية الأوروبيّة بشأن الجريمة السيبرانية" في جلسته التي عُقدت حينها بالعاصمة الهنغارية، بودابست. وكانت اللجنة الأوروبية لمشاكل الجريمة (CDPC) قد أنشأت عام 1996م لجنة خبراء للتعامل مع مشكلة الجريمة في الفضاء الإلكتروني، عملت بين العامين 1997م و2000م على إعداد مشروع الاتفاقية التي اعتمدها البرلمان، وبحلول العام 2010م وصل عدد الدول المصادقة على الاتفاقية إلى ثلاثين دولة.

هدفت الاتفاقية الأوروبيّة إلى توحيد التشريعات الجزائيّة المتعلقة بالجرائم الإلكترونية، وتوفير الإجراءات القانونية اللازمة للتحري وملاحقة الجرائم المرتكبة الكترونياً بواسطة الحواسيب. كما هدفت إلى تأسيس نظام سريع وفعّال للتنسيق والتعاون الدولي فيما يتعلق بالتصدي لجرائم وهجمات الفضاء

الإلكتروني، بما في ذلك إجراءات المساعدة المتبادلة في جمع حركة المعلومات واعتراضها، والحفاظ على البيانات المخزّنة على أجهزة الحاسوب والإفصاح عن حركة هذه البيانات، وجمع المعلومات عن حركة البيانات وعن إمكان وجود تدخّل في محتواها، والتعاون في تسليم المجرمين (موقع مجلس أوروبا الإلكتروني، اتفاقية مجلس أوروبا المتعلق بالجريمة الإلكترونية، على الرابط: رابط الموقع: https://cas.coe.int/).

ووفقاً للاتفاقية فإن مصطلح "جرائم الإنترنت" يتناول النشاطات غير المشروعة المرتبطة بأجهزة الحاسوب وباستخدام شبكة الإنترنت. وقد صنّفت جرائم الإنترنت إلى أربعة أنواع هي: أعمال القرصنة والجرائم ضد سلامة المعلومات وخصوصيتها، وجرائم التدخل بأنظمة الحاسوب وبرامجه، والجرائم التي تتعلّق بالعلامات التجارية والملكيّة الفكريّة، والتجسس على البيانات والمعلومات. وقد أوجبت الاتفاقية على الدول الأعضاء اتخاذ تدابير تشريعية للنصّ على المسؤولية عن الشروع والتدخل والتحريض في ارتكاب هذه الجرائم، وذلك بغرض وجود رادع عام لما لهذه الجرائم من تأثير بالغ على اقتصاديات الدول (موقع مجلس أوروبا الإلكتروني، اتفاقية مجلس أوروبا المتعلق بالجريمة الإلكترونية، على الرابط: رابط الموقع: https://cas.coe.int/).

وفي التاسع عشر من كانون الأول/ديسمبر 2002م صدر عن الأمم المتحدة القرار رقم (121/56) بشأن مكافحة استخدام نظم المعلومات الإدارية الجنائية لتقنية المعلومات. وتضمن هذا القرار دعوة الدول الأعضاء، إلى وضع التشريعات الوطنية لمكافحة إساءة استعمال تكنولوجيا المعلومات (United nations, 2002: 2).

وفي الثامن عشر من كانون الأول/ديسمبر 2003م صدر القرار (32/58) والذي جاء بعنوان حول موضوع التطورات في ميدان المعلومات والاتصالات في سياق الأمن الدولي. وانطلق من التأكيد

على ملاحظة تحقق تقدم كبير في تطوير وتطبيق أحدث تكنولوجيات المعلومات ووسائل الاتصالات السلكية واللاسلكية، ومن ثم التأكيد على أن تكنولوجيات المعلومات والاتصالات ذات الاستخدام المزدوج يمكن استخدامها لأغراض مشروعة وخبيثة على حد سواء (United Nations, 2003: 1).

وشدّدَ القرار على الحاجة إلى تعزيز التنسيق والتعاون بين الدول في مكافحة إساءة استخدام تكنولوجيا المعلومات لأغراض إجراميّة، مع التأكيد في هذا السياق على الدور الذي يمكن أن تؤديه الأمم المتحدة وغيرها من المنظمات الدولية والإقليميّة. كما وشدّد على أن من مصلحة جميع الدول تشجيع استخدام تكنولوجيات المعلومات والاتصالات في الأغراض السلميّة، بهدف صوغ مستقبل مشترك للبشرية جمعاء في الفضاء الإلكتروني، وأن للدول أيضاً مصلحة في منع نشوب النزاعات الناشئة عن استخدام تكنولوجيا المعلومات والاتصالات (United Nations, 2003: 1).

وفي الثاني والعشرين من نيسان/أبريل 2005م عقدت ورشة عمل بعنوان "التدابير الرامية إلى مكافحة الجريمة المتصلة بأجهزة الحاسوب"، كجزء من مؤتمر الأمم المتحدة الحادي عشر لـ "منع الجريمة والعدالة الجنائية"، المنعقد في العاصمة التايلانديّة بانكوك. وأعقبه صدور قرار الجمعية العامة للأمم المتحدة رقم (177/60) والذي تضمن دعوة الحكومات لتنفيذ جميع التوصيات التي اعتمدتها الورشة (United Nations, 2006: 1).

في شباط/ فبراير 2013م صدر الدليل المعروف باسم "دليل تالين بشأن القانون الدولي المنطبق على الحرب الإلكترونية"، والمشهور اختصاراً بـ "دليل تالين"، والذي أعدّ من قبل مجموعة من الخبراء الدوليين، وبدعوة من "مركز التميّز" التابع لحلف الناتو. وتضمن هذا الدليل قواعد وتوصيات غير إلزاميّة. وفي العام 2017م صدرت نسخة ثانية محدّثة من الدليل. تضمنت مجموعة من المبادئ

المتعلقة بالحرب الإلكترونية، أعدها فريق من تسعة عشر خبيراً، هدفت لتحديد القواعد التي يجب على الدول اتباعها عند القيام بشنّ هجمات في الفضاء الإلكتروني. وانطلق الدليل من تعريف "الهجوم السيبراني" بأنه ((عملية إلكترونية سواء هجوميّة أو دفاعيّة، يُتوقع أن تتسبب في إصابة أو قتل أشخاص أو الإضرار بأعيان أو تدميرها)) (Schmitt et al, 2013: 17).

تمحور الدليل حول طرح تساؤلات إشكاليّة وجداليّة بخصوص هجمات الفضاء الإلكتروني، وكانت النقطة الجوهريّة في الدليل هي تعريف ما ينبغي أن يُفهم على أنه "ضرر" في الفضاء الإلكتروني. وبعد مناقشات مكثفة، اتفق الخبراء على أنه علاوة على الضرر المادي المباشر – الناجم عن القصف بصورته التقليديّة – فإنّ توقف أحد المنشآت المدنيّة عن العمل نتيجة لهجوم إلكتروني قد يُشكّل ضرراً أيضاً. وذلك باعتبار أنه إذا تعطل، فليس من المهم كيفية حدوث ذلك سواء باستخدام أسلحة ناريّة أو عملية إلكترونيّة. أيّ أن الهجمة الإلكترونية التي تستهدف تعطيل شبكة مدنية خلاف يشملها الحظر الذي يفرضه القانون الدولي الإنساني على الاستهداف المباشر للأشخاص المدنيين والأعيان المدنية (Schmitt et al, 2013: 18). وبالتالي فإن هذا الدليل ووفقاً لهذا الاعتبار قد اتجه إلى التعامل مع حروب الفضاء الإلكتروني باعتبارها مماثلة للحروب الأخرى من حيث المسؤولية وما يترتب عليها لاحقاً من تبعات.

بحسب البروفيسور مايكل شميت، المشرف على عمل فريق الإعداد فإن هذا الدليل يهدف إلى أن يكون مصدراً ثانوياً للقانون، أيّ أنه يشرح القانون لكنه لا يضعه ويقرّه، وإنما الدول هي التي تضع القانون. وهو يبيّن أن الهدف من الدليل هو أن يوجد على مكتب كل مستشار قانوني لوزراء الدفاع والخارجية وأجهزة الاستخبارات، بحيث يمكن للمستشارين أن يقدموا مشورتهم لصناع القرار حول ما يمكن القيام به واتخاذ القرار بصدده بناءاً على وجهة النظر القانونيّة، وبحيث تصبح المناقشات

ناضجة، بدلاً عما اعتبره حالة التوحش السائدة في هجمات الفضاء الإلكتروني (Schmitt et al, 2013: 91).

في نيسان/ أبريل عام 2015م صدر تقرير عن مجموعة من الخبراء – شكّلت من قبل مجلس الأمم المتحدة – وأقرّته مجموعة العشرين، يقضي بوضع معايير للحدّ من المواجهات في الفضاء الإلكتروني. وقد تضمن هذا التقرير الصادر عام 2015م معايير لمعالجة سلامة وأمن البيانات، وكان هناك اتفاق عام على تدابير بناء الثقة، ووضع قواعد لقضايا من قبيل الجريمة وحرب المعلومات (ناي، 2015: 1).

ويعود تشكيل مجموعة الخبراء إلى اقتراح روسي عام 1999م بوضع معاهدة للأمم المتحدة لحظر الأسلحة الإلكترونية والمعلوماتية، ثم واصلت روسيا مع الصين وغيرها من أعضاء منظمة شانغهاي للتعاون الدفع من أجل إقرار واصدار اتفاقية بهذا الصدد عن الأمم المتحدة. إلا أن مقاومة الولايات المتحدة الامريكية لما اعتبرته محاولة للحد من القدرات الأميركية، واعتبارها أنّ أي معاهدة عامة من هذا القبيل مضللة ولا يمكن التحقق منها، الأمر الذي حال دون بلورة مثل هذه الاتفاقيّة. وبدلاً من ذلك، اتفقت الولايات المتحدة الأمريكيّة وروسيا وثلاثة عشر دولة أخرى عام 2004م، على أن يعين الأمين العام للأمم المتحدة مجموعة من الخبراء الحكوميين، وبناءاً عليه تشكّلت هذه المجموعة الدوليّة.

خلال سنوات ارتفع عدد الدول الأعضاء المشاركة في فريق الخبراء الحكوميين ووصل إلى خمسة وعشرين دولة، وأصبحت القضايا موضوع النقاش أكثر دقّة. ولكن مع تنامي الأعداد ازدادت صعوبة التوصل إلى اتفاق. إلا إن الفريق فشل في تموز/يوليو 2017م في إصدار تقرير بتوافق أوسع. وكان السبب أن الولايات المتحدة والدول الغربيّة المقاربة لوجهة نظرها، ضغطت من أجل

مزيد من التوضيح لكون القوانين الدولية المتعلقة بالصراع المسلح، بما في ذلك حق الدفاع عن النفس في الفضاء الإلكتروني، وهو ما تعذّر تحقيق التوافق من قبل الخبراء بخصوصه (ناي، 2015: 3).

وقد ظلّت عملية البلورة متعثرة خلال السنوات اللاحقة حتى يومنا هذا، وذلك لكونها تتطلب مناخ سياسي دولي إيجابي وتفاهمات وتوافقات دولية موسّعة وهو ما لم يكن متوفراً خلال السنوات الأخيرة، مع زيادة حدّة الخلافات والتنافس الدولي وبخاصّة بين كل من روسيا والصين والولايات المتحدة.

تجد الدراسة أنّ ثمةَ محاولات وجهود متعددة ومتواصلة، منذ نحو العقدين بشكل خاص، من أجل بلورة إطار تشريعي ينظّم ويقيّد ويحدد من عمليات الهجوم في الفضاء الإلكتروني، إلا إن الجهود على المستوى الدولي ظلّت دون بلورة توافقات عالمية واسعة ذات صيغة واضحة وفعّالة، وهو ما يعود إلى غياب التوافق السياسي بين الدول لبلورة مثل هذا الإطار، وغلبة طابع التشكيك في النوايا.

كما تخلص الدراسة أيضاً إلى إن صعوبة بلورة مثل هذا الإطار تعززت بحكم طبيعة الوسائل المستخدمة في الهجوم ضمن الفضاء الإلكتروني، والتي لا زالت تتطور بوتيرة عالية يمكن معها تحقيق اختراقات للقيود باستمرار وبسرعة عالية تفوق ما هو عليه من تطورات على صعيد الأسلحة التقليديّة وغير التقليديّة المستخدمة في الميدان الواقعي.

الفصل الخامس

الخاتمة، الاستنتاجات والتوصيات

الفصل الخامس
الخاتمة، الاستنتاجات والتوصيات

أولاً: الخاتمة

باتت دول عديدة تلجأ بوتيرة متنامية إلى الاعتماد على الفضاء الإلكتروني من أجل شنّ هجمات إلكترونية تلحق الأذى بالخصوم، وبحيث ترغمهم على الإذعان والخضوع لمطالب الدولة المهاجمة في إطار النزاعات والصراعات الدولية. إذ أصبح هناك إدراك متزايد بأنّ هذه الهجمات لها القدرة على تحقيق آثار بالغة وذات تأثير هام على الدول الأخرى، حيث يمكنها إلحاق أضرار فارقة في البنى التحتية، سواء منها المدنية أو العسكريّة، وذلك في ظل التطوّر المتسارع الذي تشهده أسلحة وتقنيات الهجوم الإلكتروني، وفي ظل الأتمتة والتحول المتسارع لشتى مناحي الحياة نحو الارتباط بالبرمجيات الإلكترونية، بما في ذلك المنشآت الحيوية والمعاملات الحكوميّة الرسميّة.

كما يأتي هذا اللجوء لخيار الحرب الإلكترونية اغتناماً واستفادةً من الغياب للأنظمة التشريعية اللازمة لردع وتقييد هذا النوع من الهجمات، إضافة إلى ما توفره الطبيعة والخصائص التقنيّة لهذه الهجمات من إمكانية ومجال للتملص من المسؤولية والمحاسبة.

وبذلك فإن هجمات الفضاء الالكتروني، وفي كثير من الأحيان، باتت هي الخيار المُفضّل، وبخاصّة أن الدول لا تميل عموماً لخيار الحروب والمواجهات العسكرية المسلحة المباشرة، لما تتطلبه ويترتب عليها من إنفاق وتكاليف عالية وتجهيزات لوجستيّة، واحتمالية وقوع الخسائر في الأرواح، عدا عن التعرّض للمساءلة القانونيّة الدوليّة، وما قد يترتب عليها من ردّات فعل وعقوبات، فبالتالي باتت الدول تلجأ أكثر فأكثر إلى نقل جانب كبير من الصراعات نحو الميدان والفضاء الإلكتروني.

بذلك فإنه يمكن القول بأن الفضاء الإلكتروني، وبما يتمتع به من مزايا وخصائص عديدة، قد فرض نفسه كبعد استراتيجي جديد في الصراعات والنزاعات الدوليّة، ولم يعد مجرد مجال لجمع المعلومات وإرسالها وإجراء الاتصالات أو الاكتفاء بمحاولة عرقلتها والتجسس عليها، وإنما هو فضاء مثالي لتوجيه أعتى الضربات للخصوم وبأقل الكلف والتبعات.

يجدر القول بأن حرب الفضاء الإلكتروني ليست كُلّاً واحداً أو درجة واحدة، وإنما بالإمكان تقسيمها وتصنيفها ضمن مستويات ثلاثة أساسيّة، فهناك بدايةً المستوى منخفض الشدة، والذي يبدأ من توظيف أدوات وأساليب القوة الناعمة من شنّ الهجمات الإعلامية وحملات الدعاية والتضليل وبث الشائعات، والتي منها ما يندرج في إطار شن الحروب النفسية، ومنها ما يمكن اعتبارها بمثابة حرب أفكار وشائعات تهدف لتأليب الرأي العام وبث الفتن وتشجيع الاضطرابات الداخلية أو تغيير مجرى العمليات الانتخابية في الدول المستهدفة.

من ثُمّ تأتي حرب الفضاء الإلكتروني متوسطة الشدة، والتي تتخذ فيها الهَجَمات شكل عمليات الاختراق للمواقع الإلكترونية وقواعد البيانات المستهدفة، ومن ثم المباشرة في تخريبها أو مسحها أو سرقة المعلومات منها أو التجسس عليها أو تعطيل المواقع جملة والعبث بما يرتبط بها من أنظمة وحسابات.

تأتي أخيراً حرب الفضاء الإلكتروني مرتفعة الشدة، والتي تستخدم فيها الأسلحة الإلكترونية بغرض إلحاق أضرار مادية بالغة بمنشآت العدو، بما في ذلك المدنية والعسكرية منها، وذلك عبر أساليب كالوصول إلى أجهزة التحكم وإعطابها والتسبب في إشعال الحرائق والانفجارات في أجهزة التشغيل بحيث يكون هناك أضرار ماديّة واسعة وملموسة تنجم عن الهجمات الإلكترونيّة.

كما نشير إلى أنّ التوقعات العسكريّة المستقبلية تتجاوز ما سبق إلى درجة أعلى من الحرب الإلكترونية تتمثل في تجهيز وإعداد روبوتات آلية فتاكة تقوم بالهجوم مباشرة على منشآت العدو.

ورغم عدم الوصول لمثل هذه الدرجة والشكل من الهجمات بعد، إلا أنّ احتمالات وجودها مُستقبلًا تتزايد مع تطوّر القدرات التكنولوجية واتساع الاعتماد على القطع ذاتية القيادة أو التي يتم التحكم بها عن بعد، كما هو الحال في الطائرات المسيّرة عن بعد، والمعروفة بـ "الطائرات بدون طيار" أو "الدرونات".

وأيّاً كان الشكل أو المستوى فإن حروب الفضاء الإلكتروني قد أصبحت واقعا ليس بإمكان أي دولة التغاضي عنه أو اغفاله، حيث لا تكاد تسلم دولة اليوم من التعرض لإحدى أشكالها، بما في ذلك حروب المعلومات والشائعات، أو التجسس والاختراقات، وكل ذلك يستدعى المبادرة الأخذ بالتدابير الوقائية، بداية من تطوير منظومات الدفاع الإلكتروني والامن السيبراني، وحتى المشاركة والدفع باتجاه تطوير منظومات تشريعية دولية تسهم في تحديد تقييد هذه الحروب بشكل حاسم وفعال.

ثانياً: الاستنتاجات

في ضوء الاجابة على أسئلة الدراسة توصلت الدراسة إلى الاستنتاجات التالية:

1. تزايد عدد الهجمات الإلكترونية خلال العقدين الأخيرين، حتى باتت إحدى أهم الوسائل والتكتيكات المعتمدة بين الأطراف المتصارعة حول العالم، وذلك نظراً لتدني كلفتها والخسائر التي قد تنجم عنها للطرف المهاجم مقارنة مع حجم ما يمكن تحقيقه والحاقة من أضرار بالخصم عبر توظيفها. إضافة إلى أنّ الفضاء الإلكتروني يحرّر الدولة المهاجمة من تبعات المساءلة القانونية الدولية، ويضعف احتمالية توجيه الإدانة اليقينيّة لها بشكل مباشر.
2. هناك تنوع في الأدوات والوسائل وأشكال الهجمات الإلكترونية، بما في ذلك على سبيل المثال، بث فيروسات والبرامج التخريبية والمدمرة للأنظمة والشبكات الحاسوبيّة، أو إختراق حسابات والوصول إلى معلومات سرية وتسريبها أو الاستفادة منها لأغراض عسكريّة وأمنيّة عدائيّة. كما

أنّ هناك تنوع في الأهداف التي تتعرض لها الهجمات الإلكترونيّة، وهي لا تقتصر على الأهداف العسكرية، إذ يمكن إن تستهدف الضربات الإلكترونية أهداف مدنيّة وقطاعات خدميّة وانتاجيّة.

3. عززت الهجمات الإلكترونية من مستويات وفُرَص الحرب اللامتماثلة، وذلك مع تمكن دول متفاوتة القوة، وحتى تنظيمات من غير الدول، من شن الهجمات ضد الدول ذات القوة العسكرية والاقتصادية الأكبر. إضافة إلى أنها باتت أسلوباً معتمداً بشكل متزايد ضمن استراتيجة الحروب الهجينة من قبل عدد متزايد من الدول.
4. من أهم عناصر ومميزات هجمات الفضاء الإلكتروني أنّ الدول تلتزم في معظم الأحيان بعدم الإقرار بالهجوم وتعمد إلى استخدام وسائل لإخفاء هوية الفاعل، كما في حالة اللجوء إلى استخدام "سيرفرات" (خوادم) من دول أخرى، وكلّ ذلك يؤكد على خاصية عدم إمكانية تحديد مصدر الهجوم، التي يتميّز بها هذا النوع من الحروب، ويجعله مختلفاُ عن الحروب التقليديّة، الأمر الذي يؤدي إلى زعزعة قواعد الاشتباك التقليديّة وإضعاف الردع.
5. هجمات الفضاء الإلكتروني مقترنة بالضرورة بنيّة إلحاق الضرر بالخصم، وذلك في إطار حالة من الخصومة والعداء بين الدول والأطراف، وهذا ما يجعلها مختلفة عن الهجمات ذات الطابع الجنائي، التي قد تتشابه في بعض حيثيات الهجوم، مثل حالات إختراق حسابات والوصول إلى معلومات، ولكنها تبقى مفتقدة عنصر النية بإلحاق الدمار والضرر بالخصم في إطار حالة من الأزمة والصراع بحيث يكون هذا الضرر نوعاً من التصعيد وسبباً للضغط عليه، بُغية الوصول إلى نوع من الإذعان وتقديم التنازلات من قبله، وهو ما يكون متحققاً في حالة الهجمات الإلكترونية، والتي تأتي ضمن سياق ما يمكن تسميته بـ "الحرب الإلكترونيّة".
6. نظراً لأن الفضاء الإلكتروني الذي تجري فيه حروب الفضاء الالكتروني هو فضاء افتراضي، وأنّ طبيعته مغايرة لطبيعة وخصائص العالم المادي، فإن ذلك انعكس على خصائص وطبيعة

هذه المواجهات، فهي لا تعرف الحدود المكانيّة والجغرافيّة، ومن المتعذر فيها تحديد مصدر الضربات وخط سيرها، ولا يوجد فيها أي من الاعتبارات والتكتيكات العسكريّة السائدة في الحروب التقليدية، والقائمة على أساس التنقل والحركة والتكتيك الميداني، في مجالات البحر والجو واليابسة، كلّ ذلك جعل منها نوعاً جديداً من المواجهات مغايراً لما عرفته البشرية عبر تاريخها، وهو ما ترك تأثيره على العقائد العسكرية وقواعد الاشتباك المتبعّة.

7. هناك العديد من الوسائل التقنيّة المتاحة لمجابهة الهجمات في الفضاء الإلكتروني والتصدي لها، وبحيث إن الالتزام بتطبيق وتفعيل أكبر قدر منها يمكن أن يكون معيناً إلى حد بعيد في التصدي لهذه الهجمات والحدّ من تأثيرها في حال وقوعها، وهو ما تزداد الحاجة إليه لدى مختلف الدول وبخاصّة في ظل عدم التوصّل إلى اجماع دولي واسع يفضي إلى بلورة معاهدات ومنظومة قانونية وقائية تحول وتحد من وقوع هذه الهجمات.

8. التحدي الأكبر الذي يواجه التنظيم القانوني للهجمات في الفضاء الإلكتروني هو عدم وجود إرادة دولية على صعيد المفاوضات أو على صعيد قرارات مجلس الأمن، حيث تغيب الإرادة الدولية اللازمة للدفع باتجاه ذلك، وخصوصاً من قبل الدول المهيمنة في هذا المجال. وما زاد من التحدي هو أنّ القانون الدولي يذهب إلى تنظيم استخدام الأسلحة بصورتها التقليديّة وغير التقليديّة، في حين لا يبدو أن الهجمات الإلكترونية، حتى الآن، تصنف على هذا النحو، باعتبارها أسلحة ماديّة، وذلك باعتبار بقاء النظر لها باعتبارها تعمل في الحيز الافتراضي غير المادي.

9. بات من غير المختلف عليه أنّ أمن الدول لم يعد متعلقًا فقط بحمايتها من الهجمات العسكرية، بالأسلحة التقليدية أو غير التقليدية، وإنما امتد واتسع ليشمل الحاجة لحماية مجتمعاتها ومنشآتها الحيوية وبنيتها التحتية من التعرض للهجمات باستخدام تكنولوجيا الاتصال والمعلومات.

ثالثاً: التوصيات

1. ضرورة تطوير استراتيجيات جديدة في الدول العربية تتلاءم مع التحديات الأمنيّة المستجدة للعصر الرقمي بما حمله من تغيرات فى حسابات القوى والردع، وزيادة التركيز على الأمن الإلكتروني باعتباره مرتبطاً بقضايا التنمية الاقتصادية والاجتماعية والاستقرار السياسي.
2. صياغة استراتيجية عربية مشتركة لمواجهة تصاعد الأخطار الإلكترونية، وتعزيز أمن الفضاء الإلكتروني والتعاون فى مجالات مكافحة المخاطر الإلكترونية. وبحيث يتم صياغتها بتعاون وتنسيق من قبل مراكز الدراسات والمؤسسات الرسميّة المعنيّة.
3. تطوير قدرات الدول العربية على إنتاج وتطوير أسلحة إلكترونية تُمكِّنها من تحقيق أهدافها فى الفضاء الإلكتروني. إلى جانب تطوير وحدات وجيوش الكترونية مختصّة.
4. تطوير برامج حماية إلكترونية لمواجهة الهجمات الإلكترونية، وفي سبيل ذلك عقد شراكات بين الدول والقطاع الخاص في كل دولة لتطوير البنية التحتية.
5. إعداد برامج توعوية حول الأمن الإلكتروني يتم تقديمها وبثها بطريقة واضحة ومبسّطة لعامة الناس.
6. اعادة النظر في القواعد القانونية الدولية التي تنظم هذا النوع من الحروب، وضرورة بلورة توافق دولي بهذا الخصوص.

قائمة المصادر والمراجع

1- المراجع العربية

أولاً: المصادر

ابن منظور، محمد بن مكرم (1994). **لسان العرب**. الطبعة الثالثة. لبنان – بيروت: دار صادر.

موقع الأمم المتحدة الإلكتروني، **ميثاق الأمم المتحدة**. رابط الموقع: https://www.un.org/.

موقع اللجنة الدولية للصليب الأحمر الإلكتروني، **البروتوكول الأول الإضافي إلى اتفاقيات جنيف**. رابط الموقع: https://www.icrc.org.

موقع مجلس أوروبا الإلكتروني، **اتفاقية مجلس أوروبا المتعلق بالجريمة الإلكترونية**. رابط الموقع: https://cas.coe.int/.

ثانياً: المراجع

بدران، عباس (2010). **الحرب الإلكترونية: الاشتباك في عالم المعلومات**. الطبعة الأولى. لبنان – بيروت: مركز دراسات الحكومة الإلكترونية.

حسين، أسامة سمير (2011). **الاحتيال الإلكتروني: الأسباب والحلول**. الطبعة الأولى. الأردن – عمّان: الجنادرية للنشر والتوزيع.

الخالد، ساري محمد (2018). **اتجاهات في أمن المعلومات وأمانها: أهمية تقنيات التعمية – التشفير**. الطبعة الأولى. السعودية – الرياض: العبيكان للنشر.

ستولينج، ويليام (2011). **أساسيات أمن الشبكات: تطبيقات ومعايير**. ترجمة: السيد محمد الألفي، ورضوان السعيد عبدالعال، وعلاء الدين أمين. الطبعة الأولى. السعودية – الرياض: العبيكان للنشر.

شكر، عمر حامد (2019). **المجال الخامس؛ الفضاء الإلكتروني**. تركيا – اسطنبول: المعهد المصريّ للدراسات.

طيطي، خضر مصباح اسماعيل (2010). **أساسيات أمن المعلومات والحاسوب**. الطبعة الأولى. الأردن – عمّان: دار الحامد للنشر والتوزيع.

عبد الصادق، عادل (2018). **أسلحة الفضاء الالكتروني في ضوء القانون الدولي الإنساني**. الطبعة الأولى. مصر – القاهرة: المركز العربي لأبحاث الفضاء الإلكترونيّ.

العلي، علي زياد (2017). **المرتكزات النظرية في السياسة الدوليّة**. الطبعة الأولى. الطبعة الأولى. مصر – القاهرة: دار الفجر للنشر والتوزيع.

عيتاني، فاطمة (2019). **الوحدة الإسرائيلية 8200 ودورها في خدمة التكنولوجيا التجسسية الإسرائيلية**. الطبعة الأولى. لبنان – بيروت: مركز الزيتونة للدراسات.

الفتلاوي، أحمد عبيس نعمة (2018). **الهجمات السيبرانيّة؛ دراسة قانونيّة تحليليّة بشأن تحديات تنظيمها المعاصر**. الطبعة الأولى. لبنان – بيروت: منشورات زين الحقوقيّة.

فهمي، عبدالقادر (2014). **المدخل إلى دراسة الاستراتيجيّة**. الطبعة الثانية. الأردن – عمّان: دار مجدلاوي للنشر والتوزيع.

فوزي، شروق سامي (2015). **تكنولوجيا الإعلام الحديث**. الطبعة الأولى. مصر – القاهرة: مؤسسة طيبة للنشر والتوزيع.

كابلان، فريد (2019). **المنطقة المعتمة؛ التاريخ السريّ للحرب السيبرانيّة**. ترجمة: لؤي عبد المجيد. الطبعة الأولى. الكويت – الكويت: المجلس الوطني للثقافة والفنون والآداب.

كلارك، ريتشارد، وكنيك، روبرت (2012). **حرب الفضاء الإلكتروني: الخطر القادم على الأمن القومي وسُبُل مواجهته**. الطبعة الأولى. الإمارات العربية المتحدة – أبو ظبي: مركز الإمارات لدراسة السياسات.

المبيضين، صفوان (2020). **الحكومة الإلكترونية: النماذج والتطبيقات والتجارب الدولية**. الطبعة الأولى. الأردن – عمّان: دار اليازوري العلمية للنشر والتوزيع.

محمد، لينا جمال (2016). **الجرائم الإلكترونية (ماهيتها – طرق مكافحتها)**. الطبعة الأولى. الأردن – عمّان: دار خالد اللحياني للنشر والتوزيع.

محمود، محمد (2016). **مدخل إلى عالم الشبكات**. الطبعة الأولى. الأردن – عمّان: دار غيداء للنشر.

محمود، محمد سعد (2020). **الحرب السيبرانية: أدواتها، وقودها، خسائرها**. الطبعة الأولى. منشور إلكترونياً.

ثالثاً: الدوريات

خليفة، إيهاب (2018): الحرب السيبرانية؛ مراجعة العقيدة العسكرية استعداداً للمعركة القادمة. **مجلة السياسة الدوليّة**. العدد (211). المجلد (53). ص: 17–22. مصر – القاهرة: مركز الأهرام للدراسات.

فهمي، عبد القادر (2018). الحروب التقليدية وحروب الفضاء الإلكتروني؛ دراسة مقارنة في المفاهيم وقواعد الاشتباك. **مجلة العلوم القانونية والسياسية**. المجلد (16). السنة الثامنة. العدد (2). كانون الأول 2018.

رابعاً: المواقع الالكترونية

الأخبار، 2020/5/11. **«هجمات إيران السيبرانية» على طاولة «الكابينت» للمرّة الأولى**. رابط الموقع: https://al-akhbar.com/. تاريخ الزيارة: 2020/11/28.

بي بي سي، 2020/12/19. **الهجوم الإلكتروني على الولايات المتحدة: بومبيو يتهم روسيا ويصف رئيسها بأنه خطر حقيقي**. رابط الموقع: https://www.bbc.com/. تاريخ الزيارة: 2021/4/22.

تايمز أوف إسرائيل، 2019/2/25, **إيران حاولت اختراق نظام الإنذار الصاروخي الإسرائيلي**. رابط الموقع: https://ar.timesofisrael.com/. تاريخ الزيارة: 2020/11/28.

الحرة، 2019/10/5. **تقارير: قراصنة على صلة بإيران حاولوا اختراق حملة ترامب**. رابط الموقع: https://www.alhurra.com/. تاريخ الزيارة: 2020/11/28.

روسيا اليوم، 2019/1/31. **أقوى هجمات سيبرانية استهدفت روسيا**. رابط الموقع: https://arabic.rt.com/. تاريخ الزيارة: 2021/1/14

رويترز، 2018/1/26. **مجلة: فريق مولر أجرى مقابلة مع موظف من فيسبوك بشأن تحقيق روسيا**. رابط الموقع: https://www.reutersagency.com/ar/. تاريخ الزيارة: 2020/11/19.

الشرق الأوسط، 2020/7/18. **هجوم إلكتروني إيراني على منشآت مياه إسرائيلية**. رابط الموقع: https://aawsat.com/. تاريخ الزيارة: 2020/11/28.

صحيفة العرب، 2018/9/21. **واشنطن تكشف عن إستراتيجية جديدة لمواجهة الحرب السيبرانية**. رابط الموقع: https://alarab.co.uk/. تاريخ الزيارة: 2020/6/10.

العربية، 2017/12/27. **لندن: بيونغ يانغ مسؤولة عن هجوم "واناكراي" الإلكتروني**. رابط الموقع: https://www.alarabiya.net/. تاريخ الزيارة: 2020/10/25.

فرانس 24، 2018/7/16. **بوتين: روسيا تصدت لنحو 25 مليون هجوم إلكتروني خلال كأس العالم**. رابط الموقع: https://www.france24.com/. تاريخ الزيارة: 2021/1/14.

فرانس 24، 2018/12/19. **الاتحاد الأوروبي يحقق في قرصنة "آلاف" البرقيات الدبلوماسية**. رابط الموقع: https://www.france24.com/. تاريخ الزيارة: 2020/11/28.

مونتي كارلو الدولية، 2020/10/15. **إيران تعلن عن هجوم الكتروني "خطير وواسع النطاق" استهدف مؤسساتها الحكومية**. رابط الموقع: https://www.mc-doualiya.com/. تاريخ الزيارة: 2020/11/28.

مونتي كارلو الدولية، 2019/10/5. **مايكروسوفت تكشف عن هجمات إلكترونية إيرانية على حملة الانتخابات الرئاسية الأمريكي**. رابط الموقع: https://www.mc-doualiya.com/. تاريخ الزيارة: 2020/10/26.

ناي، جوزيف (2015). **معايير دولية في الفضاء السيبراني**. بروجيكت سينديكيت. رابط الموقع: https://www.project-syndicate.org/. تاريخ الزيارة: 2021/3/22.

وكالة أنباء الأناضول، 2020/5/19. **صمت إسرائيلي حول "هجوم إلكتروني" تعرض له ميناء إيراني**. رابط الموقع: https://www.aa.com.tr/. تاريخ الزيارة: 2020/11/28.

2- المراجع الأجنبية

أولاً: المصادر

United Nations (1994). **Manual on the Prevention and Control of Computer-related Crime**. International Review of Criminal Policy. No. 43-44. United Nations publication.

United Nations (2000). **Report of the Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders**. Vienna, 10-17 April 2000. United Nations publication.

United Nations (2002). **Resolution adopted by the General Assembly, on: Combating the criminal misuse of information technologies**. At: UN.org. accessed at: 21/3/2021.

United Nations (2003). **Resolution adopted by the General Assembly, on: Developments in the field of information and telecommunications in the context of international security**. At: UN.org. accessed at: 21/3/2021.

United Nations (2006). **Resolution adopted by the General Assembly, Follow-up to the Eleventh United Nations Congress on Crime Prevention and Criminal Justice**. At: UN.org. accessed at: 21/3/2021.

ثانياً: المراجع

Brandon, Valeriano and Manes, Ryan (2015). **Cyber War versus Cyber Realities: Cyber Conflict in the International System**. U.S: New York: Oxford University Press.

Geers, Kenneth (2008). **CyberSpace and the changing of warfare**. Estonia - Tallinn: The NATO Cooperative Cyber Defence Centre.

Schmitt, Michael (ed.) et al. (2013). **Tallinn Manual on The International Law Applicable to Cyber Warfare**. 1st edition. Estonia - Tallinn: The NATO Cooperative Cyber Defence Center of Excellence.

Schreier, Fred (2015). **On Cyber Warfare**. 1st edition. DCAF. Switzerland: Geneva.

Wingfield, T. C. (2000). **The law of information conflict: national security law in cyberspace**. 1st edition. USA - Virginia: Falls Church: Aegis Research Corporation.

Winterfeld, Steve, and Andress, Jason (2011). **Cyber Warfare Techniques: Tactics and Tools for Security Practitioners**. Second edition. UK - London: Elsevier.

ثالثاً: الدوريات

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

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

Graham, David (2010). Cyber Threats and the Law of War. **Journal of National Security Law**. Vol (4). P: 87 - 102. USA - Virginia: George Mason University School of Law.

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

Mahnken, Thomas, (2011). bloodless yet potentially devastating new method of warfare. **America's Cyber Future: Security and Prosperity in the Information Age**. vol. (II). Pp: 57-63.

Nye, Joseph (2011). Nuclear Lessons for Cyber Security? **Strategic Studies Quarterly**. No. (4). Pp: 18-38. USA - Virginia: Air University Press.

Robinson, Michael (2015). Cyber Warfare: Issues and Challenges**. Journal of Computer and security**.

Roscini, Marco (2010). World Wide Warfare: Jus ad bellum and the Use of Cyber Force. **Max Planck Yearbook of United Nations Law**. Vol (14). No (1). Pp: 85-130.

رابعاً: رسائل الماجستير وأطروحات الدكتوراة

Saalbach, Klaus-Peter (2019). **Cyber war Methods and Practice**. Germany - Osnabrueck: Osnabrueck University.

خامساً: المؤتمرات

Taddeo, Mariarosaria (2012). "**An analysis for a just cyber warfare**," 4th International Conference on Cyber Conflict (CYCON 2012), Tallinn, 2012, pp. 1-10.

سادساً: المواقع الالكترونية

Arquilla, John, Ronfeldt, David (1993). **Cyberwar is Coming!** Rand Corporation. At: www.rand.org. Accessed on: 15/4/2020.

New York Times, 17/6/2019. **New York Times: US ramping up cyber attacks on Russia**. At: https://www.nytimes.com/. Accessed on: 25/10/2020.

Wall Street Journal, 17/12/2020. **Hack Suggests New Scope, Sophistication for Cyberattacks**. At: https://www.wsj.com/. Accessed on: 25/4/2021.

Washington Post, 15/7/2020. **Has Israel been sabotaging Iran? Here's what we know**. At: https://www.washingtonpost.com/. Accessed on: 28/11/2020.