وزارة التعليم العالي والبحث العلمي
جامعة محمد بوضياف بالمسيلة

كلية الحقوق والعلوم السياسية
قســـم العلوم السياسية

ميدان الحقوق والعلوم السياسية
تخصص علاقات دولية

عنوان المذكرة

التطورات التكنولوجية الحديثة والحروب السيبرانية: "تحديات الأمن القومي والدولي"

مذكرة مقدمة لنيل شهادة الماستر الأكاديمي، تخصص: علاقات دولية

إعداد الطالب:
دحيري ربيع

إشراف الأستاذ الدكتور:
فلاك نور الدين

لجنة المناقشة

الإسم واللقب	الرتبة	المؤسسة الجامعية	الصفة
		جامعة المسيلة	رئيسا
نور الدين فلاك	أستاذ تعليم العالي	جامعة المسيلة	مشرفا ومقررا
		جامعة المسيلة	ممتحنا

السنة الجامعية 2024- 2025

* ملحق بالقرار رقم ....1082.... المؤرخ في ..... 27 ديسمبر 2020

الذي يحدد القواعد المتعلقة بالوقاية من السرقة العلمية ومكافحتها

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

مؤسسة التعليم العالي والبحث العلمي: جامعة محمد بوضياف - المسيلة -

نموذج التصريح الشرفي
الخاص بالالتزام بقواعد النزاهة العلمية لإنجاز بحث

أنا الممضي أسفله،

السيد(ة): دحيري ربيع الصفة: طالب، أستاذ، باحث طالب

الحامل(ة) لبطاقة التعريف الوطنية رقم: 204133413 والصادرة بتاريخ 04 - 02 - 2019

المسجل(ة) بكلية / معهد العلوم السياسية قسم العلوم السياسية

والمكلف(ة) بإنجاز أعمال بحث (مذكرة التخرج، مذكرة ماستر، مذكرة ماجستير، أطروحة دكتوراه).

عنوانها: التطورات التكنولوجية والحروب السيبرانية

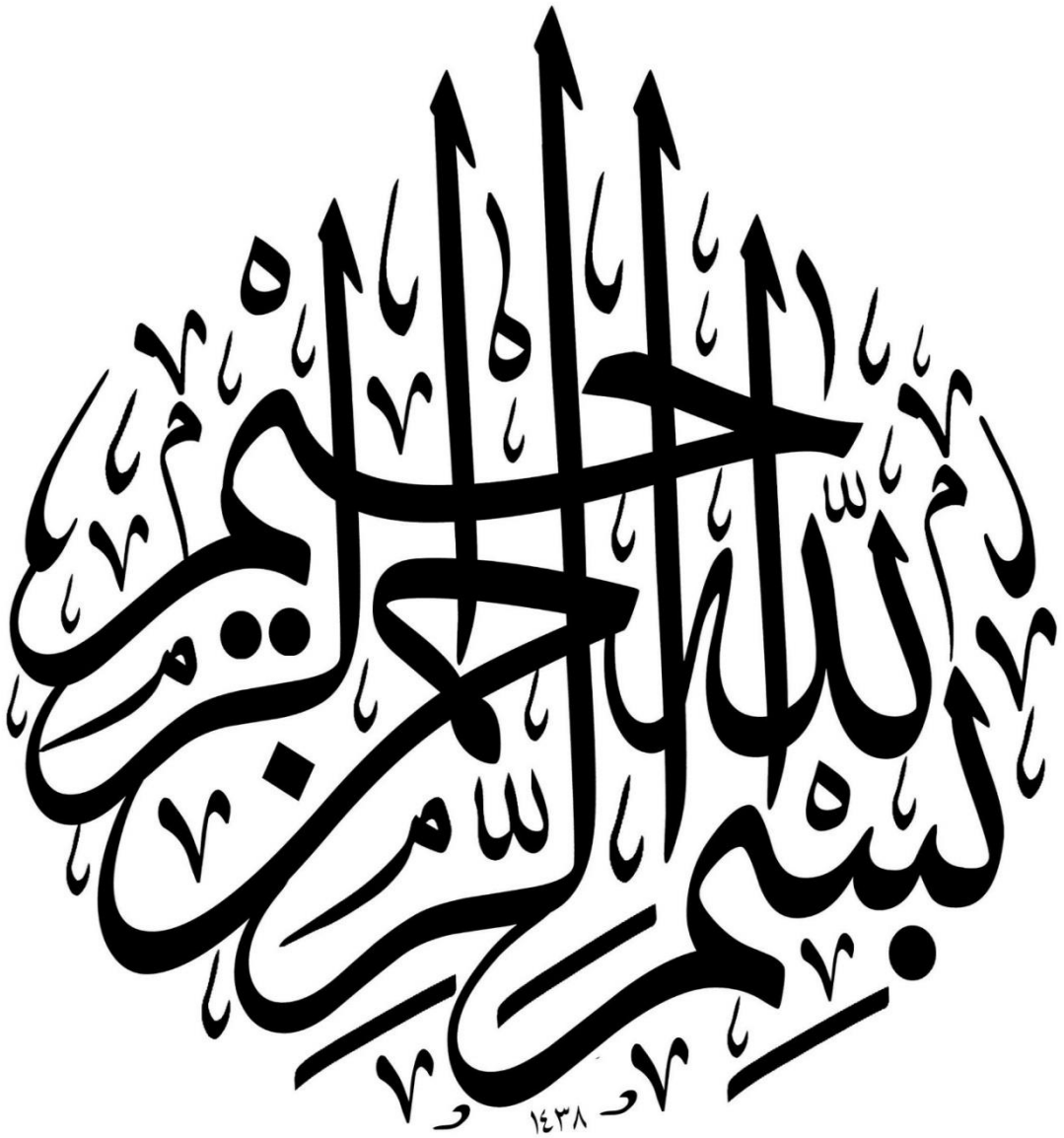
تداعيات الأمن القومي والدولي

أصرح بشرفي أني ألتزم بمراعاة المعايير العلمية والمنهجية ومعايير الأخلاقيات المهنية والنزاهة الأكاديمية المطلوبة في إنجاز البحث المذكور أعلاه .

التاريخ: 25 - 05 - 2025 05 جوان 2025

توقيع المعني (ة)

نظرا لصحة إمضاء السيد(ة)
الساكن
الموضوع
بوسعادة في 05 جوان 2025
عن رئيس المجلس الشعبي البلدي
وبتفويض منه
العون المفوض


بسم الله الرحمن الرحيم
١٤٣٨

"التحدي الذي يواجهنا في القرن الجديد تحد صعب، إنه يتمثل في الدفاع عن أمننا ضد المجهول، غير المؤكد وغير المنظور وغير الواضح."

دونالد رامسفيلد **Donald Rumsfeld**

"إن الانتصار الحقيقي لا يكون بالدخول في مواجهات عسكرية مع الخصوم، و إنما في الانتصار عليهم دون خوض حرب."

صون تزو -جنرال وخبير عسكري صيني-

شكر و تقدير

أتقدم بجزيل الشكر والامتنان لأستاذي الفاضل: الأستاذ الدكتور نور الدين فلاك.

الذي كان نعم الداعم والموجه خلال إعداد هذه المذكرة، فقد كانت توجيهاته العلمية السديدة وملاحظاته القيمة وتشجيعه المستمر حجر الأساس الذي بنيت عليه هذا العمل.

لقد تعلمت منك أستاذي الكثير ليس فقط على الصعيد الأكاديمي بل أيضاً في أسلوب البحث والتفكير والتحليل ولا يسعني إلا أن أعترف و أفتخر بأني كنت أحد طلابكم.

فلكم مني كل الشكر والتقدير، داعياً الله أن يوفقكم ويجزيكم خير الجزاء.

كما أشكر اللجنة الموقرة التي قبلت مناقشة هذا العمل المتواضع.

كما أشكر جميع أساتذة قسم العلوم السياسية بالمسيلة، فلولا مجهوداتكم لما تمكنا من مواصلة النجاح وعلى عطائهم وإخلاصهم في تقديم كل ما هو مفيد فشكراً لكم ملء الأرض حباً وكرماً.

كما لا أنسى شكر الزملاء في قسم العلوم السياسية على الدعم والتشجيع وكل من ساعدني من قريب أو بعيد.

إهــداء

إلى روح والدي الراحل الذي غاب جسده وبقيت ذكراه تسكنني نورا يضيء

عتمات الطريق وهمسا يبعث الطمأنينة في لحظات التردد

إلى أمي زهرة عمري وظل قلبي التي علمتني أن الصبر مفتاح الأمل وأن الحب

دعاء لا ينقطع

إلى عائلتي التي احتضنت ضعفي وشجعت خطاي كنتم دائما نبض الإنجاز

وسر التقدم

إلى زملائي الذين كان لوقوفهم الصادق أثرا لا ينسى في هذه المسيرة أنتم

الحبر الذي يكتمل به هذا السطر

مُقَدّمَـــــــــةٌ

مقدمة

يشهد العالم تقدماً تكنولوجياً وتقنياً هائلاً، ونوعاً جديداً من التسلح لم تعرفه العصور السابقة من قبل، وهذا بعد الثورة المعلوماتية واتساع نطاق استخدامها في شتى مجالات الحياة، المدنية والعسكرية، وخاصة للأغراض العسكرية، فهي بمثابة نقطة التحول في فن الحرب وفي إدارة الصراع الدولي وتغيراً في مفهوم الأمن العالمي.

وأصبح الفضاء السيبراني ساحة للتفاعلات، وبروز العديد من الأنماط التوظيفية له، سواء على صعيد الاستخدامات ذات الطبيعة المدنية أو العسكرية، الأمر الذي جعل هذا الفضاء مجالاً للصراعات المختلفة سواء للفاعلين من الدول أو من غير الدول لحيازة قدر من النفوذ والتأثير السيبراني.

وفي هذا السياق تبلورت ظاهرة الحروب السيبرانية (Cyber wars)، التي اتسمت بخصائص مختلفة عن نظيراتها التقليدية، من حيث طبيعة الأنشطة العدائية، والفواعل، والتأثير في بنية الأمن العالمي. وعبرت تلك الحروب عن نمطين من القوة (الناعمة والصلبة) في عملية توظيف التفاعلات في الفضاء السيبراني، مما يعكس تنامي القدرات والتهديدات المتصاعدة لأمن البنية التحتية الكونية للمعلومات، وأصبح من الصعب حصرها أو تطوير استراتيجيات محكمة لمواجهتها بشكل كامل، خاصة مع تعدد أشكال التهديدات ومصادرها وتطورها المتسارع والمستمر.

وعلى إثر هذه الحروب السيبرانية كتهديد جديد معقد ومتشابك، أصبح تحدياً أمنياً على جميع مستوياته المدنية والعسكرية، وأسقطت مفهوم السيادة والحدود الجغرافية السياسية والثقافية بين الدول، خاصة مع اختراق المواقع الحكومية الرسمية والتجسس المعلوماتي على الدول.

كما أثرت ثورة الاتصالات وتكنولوجيا المعلومات على الشؤون العسكرية وتطورها، وبات الصراع اليوم يتخذ شكل الصراع الرقمي في الفضاء السيبراني. ويمكن تفسير هذا النوع من الصراع بتوظيف استراتيجية الاقتراب غير المباشر لـــ "ليدل هارت"[1]، وتفيد هذه النظرية في فهم جوهر هذا الأسلوب الجديد للحروب السيبرانية التي تواكب التطور التكنولوجي، وكذا امتداداً للاستراتيجية غير المباشرة، حيث تحولت المواجهة من مواجهة بالأسلحة التقليدية إلى مواجهة غير مباشرة بأسلحة رقمية بحتة، وهذا ما يتناسب مع دراستنا لهذا الموضوع.

لمواجهة الحروب السيبرانية، تسعى الدول للحفاظ على بنيتها وأجهزتها الحيوية التقنية الإلكترونية والدفاع عنها وفق استراتيجية سيبرانية قوية، ممثلة في الأمن السيبراني، نتيجة تأثير التكنولوجيا الحديثة لا

[1] المفاهيم النظرية: استراتيجية الاقتراب غير المباشر، مقتبس من الموقع الإلكتروني: http://www.mouquatel.com.

سيما الفضاء السيبراني على الأمن العالمي. ومن هنا نوضح في دراستنا مفهوم الفضاء السيبراني والتحولات النوعية في المفاهيم كالأمن والقوة والصـــراع، والتطرق إلى الحروب الســـيبرانية والأمن الســـيبراني، وأبرز التحديات التي تقف عائقاً أمام الأمن العالمي والســـيبراني، ثم نعرج للجوانب القانونية والتقنية تحت مظلة القانون الدولي، كآلية لمواجهة هذه الحروب الســـيبرانية والتكتيك القادم في طبيعة الحرب في القرن الحادي والعشرين.

ولقد ركزنا في الدراسة على مصطلح "السيبرانية" بدلاً من "الإلكترونية" لضرورة البحث والتناسق في الدراسة لهذا الموضوع.

أولاً: أهمية الدراسة:

تأتي أهمية هذه الدراسة " التطورات التكنولوجية والحروب السيبرانية تحديات للأمن القومي والدولي"، ومن أهمية موضوع الفضاء السيبراني الافتراضي، ومختلف الهجمات السيبرانية والتي يتلقاها هذا الفضاء، وأصبحت المهدد الأول للدول والجماعات والأفراد بالدمار والانهيار، وخلق صراعات دولية فيما بينها، خاصة أن جل المجتمعات الحديثة لم تعد تســتطيع الاســتغناء عن هذه التكنولوجيا. مما يجعل الحروب الســيبرانية والأمن السيبراني جزءاً أساسياً ومهماً للأمن القومي للدول، بالإضافة إلى الجهود الإقليمية والدولية سواء من الجانب القانوني أو التقني لمجابهة المخاطر السيبرانية.

كذلك، يعد التركيز على الفضـــاء الســـيبراني في الدراســـات الأكاديمية مهماً جداً، حيث يعتبر حقلاً دراسياً جديداً في مجالات الدراسات الأمنية، وأن الحروب السيبرانية هيموضوع العصر، والأمن السيبراني أولوية ضرورية في حماية الأمن القومي للدول، وهذا الموضوع يلقى اهتمام ودراسات واسعة فيه.

ثانياً: أهداف الدراسة:

نسعى من خلال دراستنا لهذا الموضوع إلى الوصول للأهداف التالية:

- إبراز وتوضيح مفاهيم جديدة في الفضاء السيبراني.
- معرفة مدى تأثير الفضاء السيبراني في التحولات الدولية: الأمن – القوة – الصراع.
- التعرف على الفضاء السيبراني والحروب السيبرانية والأمن السيبراني.
- معرفة تحديات الحروب السيبرانية على متغير الأمن العالمي.
- تقييم مدى فاعلية القوانين وجهود الدول في مواجهة الحروب السيبرانية وتأثيرها على الأمن العالمي.

ثالثا : أسباب اختيار الموضوع

- **أسباب ذاتية:**
  - الاهتمام بالقضايا الأمنية الدولية الحديثة و خصوصا تلك المتعلقة بالتكنلوجيا و الفضاء السيبراني.
  - الرغبة في التخصص في مجال الامن السيبراني ضمن حقل العلاقات الدولية لما له من أهمية متزايدة في السياسات العالمية.
  - الدافع المعرفي لفهم التحولات الجيوسياسية الناتجة عن التقدم التكنلوجي و تأثيرها على مفاهيم السيادة و الصراع.
- **أسباب موضوعية:**
  - حداثة الموضوع و راهنيته : اذ يمثل ميدان الحروب السيبرانية أحد أبرز التحديات الجديدة للأمن القومي و الدولي.
  - توسع مفهوم الأمن في أدبيات العلاقات الدولية ليشمل الفضاء الرقمي و التهديدات غير التقليدية.
  - الحاجة الى تحليل السياسات الدولية تجاه الفضاء السيبراني خاصة في ظل غياب أطر قانونية ملزمة أو توافق دولي حول قواعد الاشتباك الرقمي.
  - الاسهام في بلورة توصيات واقعية لصناع القرار حول كيفية مواجهة التهديدات التكنولوجية ضمن مقاربة أمنية حديثة.

رابعا : أدبيات الدراسة:

1- كتاب "**السـيبرانية هاجس العصـر**"، من تأليف منى الأشـقر جبور، المركز العربي للبحوث القانونية والقضائية، دراسات وأبحاث، جامعة الدول العربية.

تناولت الكاتبة في إطار جهود جامعة الدول العربية أهمية موضوع الأمن السيبراني والحاجة الماسة إلى التعاون لتحقيقه، على مستوى مركز القرار العربي، وكذلك مناقشة المسائل المتعلقة بالأمن السيبراني ومختلف جوانبه الاقتصادية والاجتماعية والقانونية والتقنية، وضرورة إرساء قواعد مرنة تسمح بمواكبة تحديات الاختراقات السيبرانية ومخاطرها، كما تبرز دور جهود المنظمات الدولية والإقليمية لا سيما الأمم المتحدة والاتحاد الأوروبي وجامعة الدول العربية في تأمين وحماية الفضاء السيبراني.

2- "**الهجمات السـيبرانية: أنماط وتحديات جديدة للأمن العالمي**"، المركز العربي، عادل عبد الصـادق، الموسـوعة الجزائرية للدراسـات السـياسـية والاسـتراتيجية، العدد 18686، تاريخ النشـر: 27/11/2019يناقش الكاتب مدى تحول الفضـاء السـيبراني إلى سـاحة جديدة في العلاقات الدولية، وبروز أنماط توظيفية له، وكذلك اسـتخدام الفضـاء السـيبراني في المجالات العسـكرية والمدنية، مما يجعله سـاحة لصـراعات مختلفة. ومن هنا تبلورت ظاهرة الحروب السـيبرانية "Cyber War"، والتي تميزت عن نظيراتها التقليدية من حيث طبيعة الأنشطة والأنماط والفواعل، والتحديات التي يواجهها الأمن العالمي.

3- "**الحروب السـيبرانية في العصـر الرقمي: حروب ما بعد كلاوزفيتش**"، زينب شـنوف، المجلة الجزائرية للأمن والتنمية، العدد 02، المجلد 9، جويلية 2020.تطرقت الكاتبة في مقالها إلى نمط الحروب في العصـر الرقمي، والتحول في المفهوم الكلاسـيكي التقليدي للحرب، ويهدف المقال إلى تقديم تحليل معمق للحرب السيبرانية، وكيف ساهمت في تغيير مفهوم الحرب في العصر الرقمي، وكذلك الاستراتيجيات الكافية لمواجهة الحرب السيبرانية.

4- كتاب " **Cyber War: The Next Threat to National Security and What to Do About It"، Richard A. Clark & Robert Knake، Harper Collins، 2010.**

يتناول الكاتبان مصطلح الفضاء الإلكتروني، وخصائص الحروب السيبرانية في الفضاء السيبراني، واستخدام الإنترنت كسلاح للحرب الجديدة، ودورها في تطوير القدرات الحربية للدول في الفضاء السيبراني. كما يعرجان على أن الولايات المتحدة الأمريكية أنشأت قيادة عسكرية تعرف بقيادة حرب الفضاء السيبراني، وتعتبر روسيا والصين تهديداً لها في هذا المجال. وفي الأخير، يبرز موقف الولايات المتحدة بشأن ضبط التسلح السيبراني، والتفكير في مواجهة التهديدات السيبرانية من خلال الاتفاقيات الدولية.

خامسا: إشكالية الدراسة وتساؤلاتها:

أفضت التحديات الناجمة عن التطور التقني والتكنولوجي، جراء ثورة المعلومات الهائلة واتساع نطاق اسـتعمالها في مختلف مجالات الحياة، إلى بروز تحولات كبيرة على مسـتوى موضـوع ونوعية التهديدات والصـراعات الدولية، والتي أصـبح ما يُعرف بالحروب السـيبرانية إحدى أهم تجلياتها. من هذا المنطلق تبرز شرعية طرح التساؤل المركزي التالي:

إلى أي مدى تمثل الحروب السـيبرانية تهديداً فعلياً للأمن القومي والدولي في ظل التطورات التكنولوجية الحديثة، وما مدى نجاعة الجهود الوطنية والدولية في مواجهتها؟

والإجابة عن هذا التساؤل المركزي تتطلب طرح عدة تساؤلات فرعية، وهي:

1- كيف أثر الفضاء السيبراني على مفاهيم الأمن والقوة والصراع؟

2- ما هي الحروب السيبرانية وأنماطها؟

3- ما هي تحديات الحروب السيبرانية على الأمن العالمي؟

4- ما هي الجهود الدولية وآليات مواجهة الحروب السيبرانية؟

سادسًا: فرضيات الدراسة:

- إن معظم دول العالم تعتمد على التكنولوجيا والأنترنت وإدارتها استخدامها في شتى المجالات الحيوية، بحيث لا يمكن الاستغناء عنها. وفي ظل هذا التطور الهائل، ظهرت الحروب السيبرانية وانتشرت خطورتها وسرعتها في التدمير، مما شكلت تحدياً للأمن العالمي.
- سباق التسلح السيبراني زاد من خطورة التهديدات السيبرانية.
- تبرز أنماط جديدة للصراع نتيجة تأثير الحروب السيبرانية.
- الأمن السيبراني سياسة حتمية للدول واستراتيجية جديدة لحماية بنيتها التحتية وأنظمة المعلومات.
- زيادة التنسيق والتعاون المتبادل بين الدول في الفضاء السيبراني يقلل من مخاطر التهديدات السيبرانية.

سابعاً: المجال المكاني والزماني للدراسة:

أ- المجال الزماني:

شملت الدراسة في مجالها الزمني مراحل عدة، بداية من مرحلة ما بعد 11 سبتمبر 2001م، والتي كانت بداية التحولات وتغير المفاهيم بسبب ظهور التهديدات السيبرانية على المستوى الدولي، كظهور الفيروسات والتجسس والاختراق وسرقة المعلومات. ولعل أبرز حدث في هذا الشأن الهجمات السيبرانية على دولة استونيا سنة 2007م من طرف روسيا، والتي عطلت كل البنى التحتية والأجهزة.

ب- المجال المكاني:

الفضاء السيبراني كبعد جديد في العلاقات الدولية، وساحة معارك لحروب العصر والمستقبل.

ثامناً: المنهج المتبع في الدراسة:

1- المنهج الوصفي: يعتبر هذا المنهج من أنسب المناهج وأكثرها استخداماً في الظواهر الإنسانية والاجتماعية، وفي ظل معرفة مسبقة ومعلومات كافية حول الظاهرة من طرف الباحث. كما يدرس الظاهرة كما هي في الواقع. لهذا استعملنا المنهج الوصفي التحليلي كأسلوب تحليلي مرتكز على معلومات كافية ودقيقة عن الحروب السيبرانية بالخصوص والفضاء السيبراني عامة، ووصف الظاهرة وتحليلها في الوقت الراهن، والعوامل المؤثرة فيها، ثم استخراج الاستنتاجات ذات الدلالة والمغزى بالنسبة لمشكلة البحث وتقديم عدد من التوصيات.

2- منهج تحليل المضمون: يعتبر اتصالاً غير مباشر في دراسة الظاهرة، فلا يقتصر على الجوانب الموضوعية فقط، وإنما الجوانب الشكلية أيضاً، ونتائجه قابلة للتعميم. وبهذا اعتمدنا في دراستنا على هذا المنهج، وتفسير مضامين أهم الوثائق الرسمية والاتفاقيات الدولية والإقليمية لمواجهة مشكلة الحروب السيبرانية وتحليلها تحليلاً متكاملاً، في سياقها العام وظروفها الموضوعية المحيطة بها.

تاسعا: شرح المفاهيم.

- **الفضاء السيبراني (Cyberspace):** مصطلح حديث ظهر في العقود الأخيرة نتيجة للثورة التكنولوجية، وهو ذلك المكان الافتراضي الذي أوجدته تكنولوجيا المعلومات والاتصالات وفي مقدمتها الإنترنت. ويرتبط الفضاء السيبراني ارتباطاً وثيقاً بالعالم المادي عبر البنى التحتية المختلفة والأنظمة المعلوماتية[1].

- **الهجمات السيبرانية (Cyber Attacks):** هي فعل يقوض من قدرات وظائف شبكة الكمبيوتر، لغرض قومي أو سياسي، من خلال استغلال نقطة ضعف ما تمكن من التلاعب بالنظام[2].

- **الجريمة السيبرانية (Cyber Crime):** تعتبر إساءة استخدام تكنولوجيا المعلومات والاتصالات من طرف المجرمين، وذلك على أنها جرائم انترنت[3].

---

[1] حمزاوي ميلود، مدخل مفاهيمي للأمن السيبيري، الموسوعة الجزائرية للدراسات السياسية والاستراتيجية، على المواقع تاريخ النشر 2019.08.19، اطلع عليه يوم: 2020/03/19 https://www.politics-dz.com.

[2] رغدة البهي، الردع السيبراني: المفهوم والإشكالات والمتطلبات، الموسوعة الجزائرية للدراسات السياسية والاستراتيجية، على المواقع تاريخ النشر 2019.11.27، اطلع عليه يوم: 2020/03/20 https://www.politics-dz.com

[3] يوسف بوغرارة، الأمن السيبراني: الاستراتيجية الجزائرية للأمن والدفاع في القضاء السيبيري، مجلة الدراسات الأفريقية وحوض النيل (المركز الديموقراطي العربي)، العدد 03، المجلد 01، سبتمبر/أيلول 2018، ص1

– **الأمن السيبراني (Cyber Security):** هو مجموعة من المهمات، مثل تجميع وسائل وسياسات وإجراءات أمنية، ومبادئ توجيهية، ومقاربات لإدارة المخاطر، وتدريب وممارسات فضلى وتقنيات، يمكن استخدامها لحماية البيئة السيبرانية وموجودات المؤسسات والمستخدمين[1].

– **الاستراتيجية السيبرانية (Cyber Strategy):** هي تطوير وتوظيف القدرات اللازمة للعمل في الفضاء السيبراني، ومتكاملة مع المجالات العملياتية الأخرى، لتحقيق الأهداف عبر عناصر القوة الوطنية، وتعتمد على الوسائل والطرق وتوفير الموارد والتكاليف لمواجهة المخاطر[2].

عاشرا: صعوبات الدراسة:

كأي بحث من البحوث العلمية، يتصادف فيه الباحث جملة من الصعوبات وعوائق تعترض إنجازه بنجاح، ومن بين هذه الصعوبات نذكر منها:

– قلة المصادر والمراجع في الدراسات المستقبلية باللغة العربية، ونقص الترجمة خصوصاً في هذا الموضوع.

– صعوبة مرتبطة بحداثة الموضوع، وقلة الدراسات المباشرة والمرتبطة به.

– صعوبة الإحاطة بكل جوانب هذا الموضوع، نظراً لحداثته وتسارع الأحداث والتطورات فيه.

– طبيعة العمل الوظيفي لم تسمح بتوفير الوقت الكافي لإنجاز هذه المذكرة، فكان عائقا امامنا في البحث.

إحدى عشر: تفصيل خطة الدراسة:

تم تقسيم الدراسة إلى ثلاثة فصول أساسية:

تناولنا في الفصل الأول، المعنون بالإطار النظري والمفاهيمي للدراسة، واحتوى على ثلاثة مباحث المبحث الأول تطرقنا فيه للفضاء السيبراني والتحول في المفاهيم (الأمن والقوة والصراع). أما المبحث الثاني تكلمنا فيه عن مفهوم الحروب السيبرانية المبحث الثالث خصص للأمن السيبراني.

أما فيما يخص الفصل الثاني، الذي عنوانه الحروب السيبرانية وتحديات الأمن العالمي، فهو يضم ثلاثة مباحث، تكلم المبحث الأول عن أبرز التهديدات السيبرانية، والتي شكلت تحدياً أمنياً على جميع

[1]ITU, Cyber Security, Geneva: International Telecommunication Union (ITU), 2008

[2]زينب شنوف، الحرب السيبرانية في العصر الرقمي: حروب ما بعد كلاوز فيتش، المجلة الجزائرية للأمن والتنمية، العدد 02، المجلد 09، الصفحة 92

الأصـعدة. وقد تناولنا في المبحث الثاني تداعيات الحروب السيبرانية على الأمن العالمي، أما المبحث الثالث فتناولنا أبرز الحروب السيبرانية ودرجة تأثيرها.

وكان الفصـل الثالث آخر فصـل للدراسـة بعنوان "آليات مواجهة الحروب السـيبرانية"، سـواء المتعلقة بالجانب القانوني أو التقني، ويحتوي هو كذلك على ثلاثة مباحث المبحث الأول الجهود الوطنية والإقليمية والدولية لتأمين الفضـاء السـيبراني وقد تناول المبحث الثاني المسؤولية الدولية للحروب السـيبرانية أما المبحث الثالث والأخير فتم تخصيصه لإستراتيجية السيبرانية للدول للدفاع عن نفسها تحت مظلة القانون الدولي.

الفصل الأول

الإطار النظري

و المفاهيمي

للدراسة

تمهيد :

أدى التقدم التكنلوجي السريع و لا سيما في مجال الاتصالات و تكنلوجيا المعلومات إلى نشوء فضاء جديد يعرف بالفضـــاء الســيبراني، و الذي أصــبح يلعب دورا محوريا في إعادة تشــكيل مفاهيم الامن و القوة والصــراع على المســتوى العالمي، فقد فرض هذا الواقع الرقمي تحولات عميقة على طبيعة التهديدات الأمنية وغير من أدوات و أســاليب ممارســة القوة، كما أدى الى بروز أنماط جديدة من الصــراع لا ترتكز فقط على البعدين العسكري أو الجغرافي، و من هذا المنطلق يتناول هذا الفصل الجوانب الأساسية لفهم هذه التحولات.

المبحث الأول: الفضاء السيبراني والتحول في المفاهيم.

لقد تمخض عن ثورة المعلومات وظهور الأنترنت بروز بيئة جديدة وهي الفضاء السيبراني (Cyber space)، إضـافة الى المجالات الأربعة البر والبحر والجو – والفضـاء، وتأثيرها على النظام الدولي، وكان الدور للمجال الخامس في تحول جديد للأمن والقوة والصراع.

المطلب الأول: الفضاء السيبراني والتحول في الأمن العالمي.

أولاً: مفهوم الفضاء السيبراني:

ظهر مصـطلح الفضـاء السـيبراني في ثمانينيات القرن الماضـي في احدى روايات الخيال العلمي للكاتب الأمريكي – الكندي المشـهور وليام جيبسـون، حيث يعتمد هذا المجال الافتراضـي على نظم الكومبيوتر، وشبكات الأنترنت ومخزون هائل من المعلومات والبيانات، فيتم التواصل بالشبكات عبر الهواتف وأجهزة الحواسيب وغيرها دون التقيد بالحدود الجغرافية[1].

" الفضاء السيبراني مجال افتراضي من صنع الإنسان يعتمد على نظم الكومبيوتر وشبكات الأنترنت وكم هائل من البيانات والمعلومات والاجهزة[2] ".

هناك من عرف الفضاء السيبراني بوصفه الذراع الرابعة للجيوش الحديثة[2] ، وهناك من يرى أنه البعد الخامس للحرب، وهذا تعريف يحصـر الفضـاء السـيبراني في المجال العسـكري فقط دون التطرق للمجالات الأخرى.

وعرفته **الوكالـة الفرنسـية لأمن أنظمـة الإعلام** (ANSSI)، وهي وكالـة حكوميـة مكلفـة بـالدفـاع السيبراني الفرنسي على أنه: " فضاء التواصل المشكل من خلال الربط البيني العالمي لمعدات المعالجة الآلية للمعطيات الرقمية[3]".

كما يفهمه الأمريكيون على أنه " مجال شامل على مستوى البيئة الرقمية يتشكل من شبكات مرتبطة ومتواصـلة بينها بالتقنيات وتكنولوجيات الإعلام بما فيها الأنترنت وشـبكات الاتصـال، والحواسـيب.. الدارات المبرمجة، وسائل الرقابة[4] ..."

[1]ربيع محمد يحي،إسرائيلوخطوات الهيمنة على ساحة الفضاء السيبراني في الشرق الأوسط، رؤى استراتيجية، المجلد الأول، العدد 3،2003 ص 67.
[2]عباس بدران، الحروب الإلكترونية:الاشتباك في عالم متغير مركز دراسات الحكومة الإلكترونية، بيروت 2010، ص4
[3]Olivier KEMPF, Introduction à la Cyber stratégie, Paris, Economica,2012, P9
[4]بلعيد لطفي أمين الفضاء السيبراني، هندسة وفواعل المجلة الجزائرية للدراسات السياسية العدد الخامس 2016، ص 151-152.

وجاء في تعريف الاتحاد الدولي للاتصالات للفضاء السيبراني بأنه " المجال المادي وغير المادي الذي يتكون وينتج عن عناصر هي: أجهزة الكومبيوتر الشبكات البرمجيات حوسبة المعلومات المحتوى، معطيات النقل والتحكم، ومستخدمو كل هذه العناصر[1] ".

وعليه يمكن القول بأن: " الفضاء السيبراني هو مجال افتراضي في بيئة تفاعلية حديثة، تشمل عناصر مادية وغير مادية مكونة من مجموعة أجهزة رقمية، وأنظمة الشبكات والبرمجيات، والمستخدمين سواء مشغلين أو مستعملين ".

وفي النهاية يبقى مفهوم الفضاء السيبراني مسألة نسبية، وذلك على حسب فهم وأدراك كل دولة أو هيئة، وعلى حسب قدرة واستراتيجية الدول في مواجهة المخاطر والتهديدات في هذا الفضاء الغامض المعقد.

ثانياً: الفضاء السيبراني والتحول في الأمن العالمي.

بدأ التركيز على الفضاء السيبراني كبعد أمني جديد بفعل أحداث دولية، بعد أحداث 11 سبتمبر 2001، بعدما استخدمته تنظيم القاعدة كساحة قتال ضد الولايات المتحدة الأمريكية، وفي عام 2007 برز بوضوح دور الفضاء السيبراني كمجال جديد في العمليات العدائية في الصراع بين إستونياوروسيا، وفي عام 2008 في الحرب بين روسيا وجورجيا، وجاء الهجوم السيبراني بفيروس ستاكسنت على برنامج إيران النووي عام 2010، ليمثل نقلة مهمة في مجال الأسلحة السيبرانية[2].

ولقد لعبت شبكة التواصل الاجتماعية دورا سياسيا وهو ما تجلى في الثورات العربية مطلع عام 2011، فإنها مثلت نقطة هامة في الاهتمام الدولي بأمن الفضاء السيبراني، لتنتقل هاته الاحتجاجات الى البلدان الديمقراطية كبريطانيا والولايات المتحدة والتي عملتا على احتوائها والسيطرة عليها في محاولة وسعي الجيوش النظامية واستغلال تفوقها التقني والعسكري والإعلامي الكاسح لحسم الحرب بسرعة وتجنب السكان فظائع وآلام المواجهة. وكان الهدف من هاته الاحتجاجات عبر الفضاء السيبراني هو شحن الرأي العام وإسقاط النظام من الداخل بدلا من استخدام القوة العسكرية الخارجية مثل ما جرى للعراق.

لقد فرض الفضاء السيبراني إعادة التفكير في مفهوم الأمن، وتمكن الدولة من تأمين وحماية منشآتها الحيوية، والبنى التحتية والمعلوماتية من أي هجوم عسكري أو إرهابي من خلال الاستخدام السيء لتكنولوجيا الاتصال والمعلومات[3].

[1]The International Telecommunication Union, ITU Toolkit for Cyber-crimelegislation, Geneva, 2010, P 12

[2]عادل عبد الصادق، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي والإنساني، وحدة الدراسات المستقبلية، مكتبة الإسكندرية، مصر، 2012، ص 12.

[3]Martin C.libicki, conquest in cyberspace: National Security and information warfare (New York :Cambridge University Press, 2007) P. 1-14

وتكمن العلاقة بين الفضاء السيبراني والأمن العالمي في اتساع قطاع مستخدمي وسائل الاتصال وتكنولوجية المعلومات في العالم، وتبني الحكومات الإلكترونية من جانب العديد من الدول وربطها بمصالحها القومية والاستراتيجية، فهي اليوم في تزايد مع إمكانية التعرض لمصالح الاستراتيجية من أخطار وتهديدات سيبرانية، وتصبح مصدر وأدوات جديدة للصراع الدولي المتعدد الأطراف، ودورا فيتغذية التوترات الدولية. وبروز فاعلين من غير الدول، وتغير طبيعة الاعتبارات الجغرافية والجيوسياسية مع التطورات المتسارعة في وسائل الاتصالات[1].

إن واقع البيئة الدولية الجديدة يفرض على الدول أن تبحث في أولوية الأمن السيبراني، واستراتيجية توفر وحماية المعلومات من مخاطر التهديدات السيبرانية، التي تغير من مضامين الأمن العالمي، وفي نفس الوقت فتح الباب أمام التعاون ومواجهة الأخطار المشتركة العابرة للحدود[2].

المطلب الثاني: الفضاء السيبراني والتحول في القوة

أحدث التطور التكنولوجي والتقني تحولا في مفهوم القوة، ومنه دخل المجتمع الدولي مرحلة جديدة تلعب فيه الهجمات السيبرانية دورا أساسيا في تنظيم القوة أو الاستحواذ على عناصرها الأساسية، وأصبح التفوق في مجال الفضاء السيبراني عنصرا حيويا في تنفيذ عمليات ذات فاعلية في الأرض وفي الجو والفضاء واعتماد القدرة القتالية في الفضاء السيبراني على نظم التحكم والسيطرة[3].

ودخل الفضاء السيبراني ضمن المحددات الجديدة للقوة وهي القوة السيبرانية (Cyber power) من حيث طبيعتها وأنماط استخدامها وطبيعة الفاعلين، مما انعكس على قدرات الدول وعلاقاتها الخارجية، وترتبط هذه الخصائص الجديدة للقوة " بأنها مجموعة الوسائل والطاقات والإمكانيات المادية وغير المادية، المنظورة وغير المنظور التي بحوزة الدولة، يستخدمها صانع القرار في فعل مؤثر يحقق مصالح الدولة، وتؤثر في سلوك الوحدات السياسية الأخرى[4]".

ويعد جوزيف س ناي (Joseph S Nye) من أبرز المهتمين بالقوة السيبرانية، حيث يعرفها بأنها: "القدرة على الحصول على النتائج الموجودة من خلال استخدام مصادر المعلومات المرتبطة بالفضاء السيبراني، أي أنها القدرة على استخدام الفضاء السيبراني لإيجاد مزايا للدولة، والتأثير على الأحداث المتعلقة بالبيئات التشغيلية الأخرى وذلك عبر أدوات سيبرانية". كما يوضح جوزيف. س ناي أن مفهوم القوة السيبرانية

[1] عادل عبد الصادق، نفس المرجع، ص 17
[2] عادل عبد الصادق، نفس المرجع، ص 17
[3] Arsenio T. Gumahad, Cyber troopes and Netuvar: the profession of Arms in the information Age (Alabama Air university Air war college, 1996) 57-156
[4] جوزيف ناي ، المنازعات الدولية ، مقدمة للنظرية والتاريخ، ترجمة أحمد أمين الجمل، وحمدي كامل ، الجمعية المصرية لنشر المعرفة والثقافة العالمية ، القاهرة ، 1997، ص 82.

يشـــير الى " مجموعة الموارد المتعلقة بالتحكم والســـيطرة على أجهزة الحاســـبات والمعلومات والشـــبكات الإلكترونية والبنية التحتية المعلوماتية والمهارات البشرية المدربة للتعامل مع هذه الوسائل[1]".

ولقد حدد جوزيف ناي ثلاث أنواع من الفاعلين الذين يمتلكون القوة السيبرانية "Cyberpower[2]":

1- **الدولة:** والتي لديها قدرة كبيرة على تنفيذ الهجمات السيبرانية وتطوير البنية التحتية وممارسة السلطات داخل حدودها.

2- **الفاعلون من غير الدول:** ويستخدم هؤلاء الفاعلون السيبرانيون القوة السيبرانية لأغراض هجومية بالأساس، إلا أن قدرتهم على تنفيذ أي هجوم يتطلب مشاركة ومساعدة من طرف أجهزة استخباراتية متطورة، وهذا لا يمنعهم من استهداف واختراق الأنظمة الدفاعية.

3- **الأفراد (القراصنة):** الذين يمتلكون معرفة تكنولوجية عالية والقدرة على توظيفها، مما يصعب معرفة هوياتهم، وصعوبة ملاحقتهم.

كما يمكننا التفصيل أكثر بخصوص الفاعلين من غير الدول كالتالي[3]:

- **الشركات متعددة الجنسيات:** تمتلك بعض الشركات قدرة تفوق الدول، ولكن تنقصها الشرعية التي مازالت حكرا على الدول، فخوادم شركات مثل: جوجل Google وفيسبوك Facebook وميكروسوفت Microsoft، تمتلك قواعد بيانات عملاقة بحيث تستطيع أن تؤثر في اقتصاديات الدول وثقافة المجتمعات وتوجهاتها.

- **المنظمات الإجرامية:** تقوم هذه المنظمات الإجرامية بعمليات القرصنة السيبرانية، وسرقة المعلومات واختراق الحسابات البنكية وتحويل الأموال، كما توجد سوق سوداء على الأنترنت المظلم Darkinternet لتجارة المخدرات والأسلحة والبشر، حيث تكلف هذه الجرائم مليارات الدولارات سنويا.

- **الجماعات الإرهابية:** تعد من أبرز الفواعل الدولية، خاصة بعد أحداث 11 سبتمبر، حيث تستغل الفضاء السيبراني في عمليات التجنيد والتعبئة والدعاية وجمع الأموال والمتطوعين، كما تحاول جمع المعلومات حول الأهداف العسكرية، وكيفية التعامل مع الأسلحة وتدريب المجندين، إلا أنها لم تقم بهجوم سيبراني حقيقي على منشآت البنية التحتية للدول.

ولقد أصبحت القوة السيبرانية (Cyber power) حقيقة أساسية في العالم بكل مظاهرها المتنوعة من دعم ومساندة العمليات الحربية والقوة الاقتصادية والسياسية، وطبيعة النظام الدولي، وأعطت دفعا رئيسيا في تدعيم القوة الناعمة للدول، حيث بات الفضـــاء الســـيبراني مســـرحا للهجمات الســـيبرانية، ونشـــر المعلومات المضللة، والحرب النفسية، مما دفع بالدول إلى الزيادة في الإنفاق لتأمين وحماية بنيتها التحتية، وبالتالي القوة السيبرانية لها تأثير في صنع القرار في النظام الدولي.

[1] J- Joseph S Nye JII, Cyber power , Harvard Kennedy School,2010,P03,4 Ibid ,P 04

[2] Joseph S. Nye JR , Ibid , P10

[3] إيهاب خليفة ، القوة الإلكترونيةوأبعاد التحول في خصائص القوة ، مكتبة الإسكندرية ، مصر ، 2014، ص 33-42.

المطلب الثالث: الفضاء السيبراني والتحول في طبيعة الصراع الدولي.

لقد خلقت شبكات الاتصالات والمعلومات، مساحات وعلاقة تفاعلية بين الفضاء السيبراني والصراع في الواقع الافتراضي، وبرزت فضاءات جديدة للصراع بأدوات مختلفة وأنماط جديدة تختلف عن الصراعات التقليدية، وكان ذلك بعد أحداث 11 سبتمبر 2001، فكان الفضاء السيبراني ساحة للصراع والقتال بين تنظيم القاعدة والولايات المتحدة الأمريكية، وفي عام 2007 جرت العمليات العدائية بين إستونيا وروسيا، وهو ما حدث أيضا في عام 2008 في الحرب بين روسيا وجورجيا وجاء الهجوم السيبراني بفيروس ستاكسنت Stuxnet على برنامج إيران النووي عام 2012 ، ليبرز قوة الأسلحة السيبرانية في الصراعات الدولية[1].

ولعل ما يعزز انتشار الأنشطة غير السلمية في الفضاء السيبراني[2]:

1. ارتباط العالم المتزايد بالفضاء السيبراني وزيادة خطر تعرض البنية التحتية الكونية للمعلومات لهجمات سيبرانية.
2. استخدام الفاعلين من غير الدول للفضاء السيبراني لتحقيق أهداف وتأثير ذلك على سيادة الدولة.
3. انسحاب الدولة من قطاعات استراتيجية لصالح القطاع الخاص.
4. إشكالية تعامل الدول مع الشركات التكنولوجية متعددة الجنسيات، والتي أصبحت تفوق قدراتها، مثل مواقع التواصل الاجتماعي كالفيسبوك وتويتر واليوتيوب الذين أصبحوا فاعلين دوليين بامتياز.

وبالتالي أصبح الفضاء السيبراني ساحة جديدة للصراع بشكله التقليدي ولكنه ذو طابع سيبراني يعكس النزاعات التي تخوضها الدول أو الفاعلين من غير الدول على خلفيات دينية أو عرقية أو أيديولوجية أو اقتصادية أو سياسية، ويتمدد الصراع السيبراني بداخله شبكات الاتصال والمعلومات متجاوزا الحدود التقليدية وسيادة الدول.

وأن التطور الذي فرضه الفضاء السيبراني، انعكس على المجتمع الدولي في التفكير في حركة وديناميكية الصراع والأمن، خاصة في ظل تزايد الاعتماد المتبادل ليظهر بما يعرف بـ (عصر القوة النسبية)، وعجز ((القوة العسكرية))، عن تأمين الأهداف السياسية المترتبة عليها، مما خلق آثار استراتيجية على مستوى توازنات النظام الدولي[3].

ويعد الصراع اليوم تصفية للخلافات بشتى أنواعها، والذي من ورائه دوافع سياسية، ويأخذ شكلا عسكريا، يتم استخدام فيه قدرات هجومية ودفاعية عبر الفضاء السيبراني، والهدف منه هو إفساد النظم

[1] سليم دحمان،أثر التهديدات السيبرانية على الأمن القومي، الولايات المتحدة أنموذجا، مذكرة مقدمة لنيل شهادة ماستر أكاديمي، كلية الحقوق والعلوم السياسية، قسم العلوم السياسية، جامعة المسيلة، 2017/2018، ص 27.
[2] عادل عبد الصادق، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي، سلسلة أوراق، العدد (23)، مكتبة الإسكندرية، مصر، 2016، ص 17-18.
[3] عادل عبد الصادق، مرجع سابق، ص 38.

المعلوماتية والشبكات والبنية التحتية من قبل فاعلين داخل المجتمع المعلوماتي، أو من خلال التعاون ما بين قوى أخرى لتحقيق أهداف سياسية[1].

ويشهد الصراع السيبراني الدولي اليوم، صراعا وتنافسا حول الاستحواذ على التقدم التكنولوجي والسيطرة على الأنترنت، والمواقع والتحكم بالمعلومات والعمل على اختراق الأمن القومي للدول، بدون استخدام طائرات أو متفجرات أو حتى انتهاك الحدود السيادية، وهذا ما أثر على طبيعة العلاقات الدولية.

ويوجد صراع سيبراني ذو طبيعة ناعمة، حول الحصول على المعلومات والتأثير في المشاعر والأفكار وشن حرب نفسية إعلامية.

ويمكن أن يستخدم الفضاء السيبراني كوسيلة من وسائل الصراع داخل الدولة، بين مكوناتها على أساس طائفي أو اقتصادي أو ديني، وبالتالي الفضاء السيبراني يعد أكثر بيئة مناسبة للصراعات المعلوماتية.

[1]Dunn. Information Age Conflicts.2-6

المبحثالثاني: الحروب السيبرانية وأسلحتها

مع الاعتماد المتزايد في حياتنا اليومية على الأنظمة المعلوماتية والأجهزة المتصلة بالشبكات العالمية وبالأنترنت، يزداد عدد المتصلين بالفضاء السيبراني وتزداد التهديدات والحروب السيبرانية والتي هي تعتبر هاجس العصر.

المطلبالأول: مفهوم الحرب السيبرانية

تغيرت الحروب ولم تعد تعتمد على جيوش عسكرية وأسلحة قتالية، بل أصبحت الحروب السيبرانية بديلا لتلك الحروب التقليدية، وذلك لسرعتها ودقتها في تنفيذ العمليات العسكرية وتعتبر من أدوات الحرب الشاملة.

هناك إجماع واسع على أنه لا يوجد تعريف محدد ودقيق لمفهوم الحرب السيبرانية الآن، وعلى الرغم من ذلك، فقد اجتهد عدد من الخبراء ضمن اختصاصاتهم في تقديم تعريفات تحيط بهذا المفهوم.

أولاً: فالحرب جاء في لسان العرب، أن الحرب: نقيض كلمة سلم، ورجل حرب أي شجاع، الحرب: أن يسلب الرجل ماله، والحارب: الناهب[1].

وفي موسوعة (لاروس) الحرب هي: صراع قوة بين شعبين أو بين فريقين من بلد واحد، أو بين متصارعين يريد كل واحد منهما الحصول بالقوة على شيء لم يستطع الحصول عليه بطرق أخرى، ويحدث هذا بقيام دولة بتحقيق أطماعها، وتقوم الثانية بالدفاع عن مصالحها[2].

وفي قاموس (الروبير) الحرب صراع مسلح بين مجموعات اجتماعية أو بين دول. وهي عبارة عن ظاهرة اجتماعية أبدية تتميز بالاحتقار والوحشية والخوف والكراهية. كما أنها ظاهرة تاريخية محددة في إطار الزمان والمكان[3].

وكما وردت الحرب في الموسوعة السياسية على أنها "ظاهرة استخدام العنف والإكراه كوسيلة لحماية مصالح، أو لتوسيع نفوذ، أو لحسم خلاف حول مصالح أو مطالب متعارضة بين جماعتين من البشر.

ثانياً: فالسيبرانية مأخوذة من (سيبر – Cyber)، ونعني صفة لأي شيء مرتبط بثقافة الحواسيب أو تقنية المعلومات أو الواقع الافتراضي، فالسيبرانية تعني فضاء الأنترنت[4].

---

[1]العلامة ابن منظور، لسان العرب، المجلد الأول، دار لسان العرب، بيروت.

[2]Grand Larousse Encyclopédique, tome cinquième librairie Larousse Paris ,1979.

[3]Le Robert, dictionnaire, alphabétique et analogique de la langue française, tom troisième, société lanouveaulivre, paris ,1978

[4]الكيالي عبد الوهاب، الموسوعة السياسية، الجزء الثاني، المؤسسة العربية للدراسات والنشر، الطبعة الأولى،بيروت، 1981.

يقول جيفري كارل مؤلف كتاب Inside cyber warfare " أنه باستطاعة أي دولة أن تتبنى حربا إلكترونية على دولة أخرى، خاصة على أنظمة الجيوش في العالم، وأصبحت متصلة بالأنترنت وتفتقد كل عوامل الأمان المطلق، ولا يقتصر الأمر على الدول، ولكن حتى الأفراد باستطاعتهم شن هجمات تسبب كوارث لدى العديد من الدول[1] ".

ويوضح جيفري أن تاريخ الهجمات السيبرانية يرجعه البعض إلى القرن التاسع عشر باختراق شيفرة مورس 1840، والاتصال السلكي والتلغراف.

ويعرفها بولو شاكريان Paulo Shakarian بأنها "امتداد للسياسة من خلال الإجراءات المتخذة في الفضاء السيبراني من قبل دول أو فاعلين غير دوليين، حيث تشكل تهديدا خطيرا للأمن القومي[2] ".

وتعرف الحرب السيبرانية بأنها " حرب تخيلية أو افتراضية Reality – Virtual ذات طبيعة غير ملموسة، تحاكي الواقع بشكل شبه تام، وهي حرب بلا دماء،إذ أدوات الصراع تكمن بالمواجهات الإلكترونية والبرمجيات التقنية، وجنود من برامج التخريب المحوسبة، وطلقات من لوحات المفاتيح ونقرات المبرمجين[3]".

ويرى بعض القانونيين أن ديناميكيات عمل الحروب السيبرانية تتقارب من ناحية قانونية مع إشاعة الرعب والإرهاب. واستنادا لهذا يمكن تعريف الحروب السيبرانية بأنها "نظام قائم على الرعبالمنتشر في الشبكة العنكبوتية (الأنترنت)، والتي تهدف الى تنفيذ العديد من الأعمال لترويع أمن الأفراد والجماعات والمؤسسات والدول وإرهاقهم اقتصاديا،وإدخالهم في أزمات نفسية واجتماعية ناتجة عما يعرف بالإرهاب الصامت (Silent Terror)[4]".

ووفقا لقرار مجلس الأمن الدولي مؤخرا: "الحرب السيبرانية هي استخدام أجهزة الحاسوب أو الوسائل الرقمية من قبل حكومة أو بمعرفة أو بموافقة صريحة من تلك الحكومة ضد دولة أخرى، أو ملكية خاصة داخل دولة أخرى بما في ذلك الوصول المتعمد أو اعتراض البيانات، أو تدمير البنية التحتية الرقمية، أو إنتاج وتوزيع الأجهزة التي يمكن استخدامها لتخريب النشاط المحلي[5]".

[1] مركز نورس دراسات، الحرب السيبرانية الإلكترونية " نقلة نوعية في الاستراتيجيات العسكرية وأثر ملحوظ على العلاقات الدولية، ص 6.
[2] نفس المرجع، ص 7.
[3] Paulo & Jana Shakarian, Andrew Ruef, Introduction to cyber warfare, A multidisciplinary Approach. Elsevier,2013. P02
[4] مساعد كمال، الحرب الإلكترونية ومستلزمات محاكات الواقع، مجلة الجيش اللبناني على شبكة الأنترنت [http://www.lebarmy.gov.lb/ar/icle/358?issueID=11575253]
[5] عماد سامي، استخدام تكنولوجيا المعلومات في مكافحة الإرهاب، الطبعة الأولى،الإسكندرية Introduction to cyber warfare. A multidisciplinary Approach Elsevier. 2013.P02

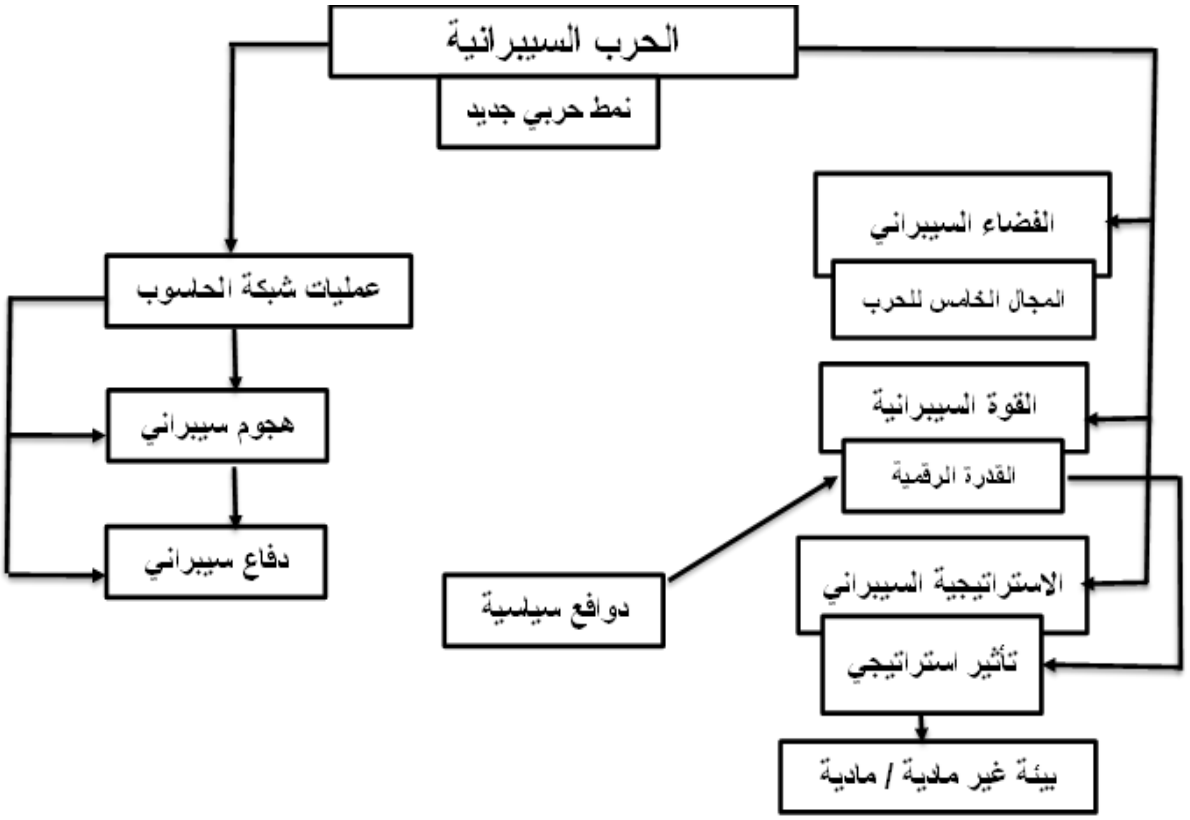
والحروب السيبرانية "هي جزء فرعي من حرب المعلومات التي تنطوي على استخدام ساحة المعارك وإدارة تكنولوجيا المعلومات والاتصالات في السعي لتحقيق ميزة تنافسية على الخصم[1] ".

وتعني " أيضا نشاط متماثل أو غير متماثل، دفاعي أو هجومي على الشبكة الرقمية، من قبل فواعل دولية أو غير دولية، بهدف إلى إلحاق الضرر بالبنية التحتية الحيوية الوطنية، والأنظمة العسكرية[2] ".

كما تختلف الحروب السـيبرانية (Cyberwar) عن الحروب الإلكترونية (Netwar)، كون الحروب السيبرانية نشبت على المستوى العسكري وتدور حول معرفة استراتيجيات تأمين مجتمع أو جيش وأما الحروب الإلكترونية تعني النزاعات السيكولوجية على المستوى المجتمعي التي نشبت من خلال أساليب الاتصالات المختلفة.

أما التعريف الإجرائي للحروب السيبرانية: (أنظر للشكل): "هي حرب نشأت في الفضاء السيبراني، تستخدم التأثير الرقمي الذي تحركه دوافع سياسية، لإجبار الخصم على تنفيذ إدارة الطرف المهاجم، وتعرف أيضا أنها نزاع عسكري في الفضاء السيبراني الذي يمثل مجالا جديدا للحروب".

الشكل رقم (01): مخطط تعريف الحرب السيبرانية



المصدر: زيتوني شنوف، الحرب السيبرانية في العصر الرقمي: حروب ما بعد كلاوزفيتش، المجلة الجزائرية للأمن والتنمية، العدد2، المجلد9، 2020، ص 21

[1]Schreier Fred. (2015). On Cyber warfare . Dcaf Houqon Working Paper. No 7 P10

[2]Mhulwa Res. Cyber warfare versus Information Warfare: Two very Different Concepts. in the site: http// bit.ly/2H94KG3 Ibid.p. 10

ثالثاً: خصائص الحروب السيبرانية

كل المؤشـرات توحي بتغير في نمط الحرب من التقليدية إلى الحرب السـيبرانية مسـتقبلا، وهذا ما تسعى إليه العديد من الجهات نظرا للخصائص العديدة التي تنطوي عليها ومنها[1]:

- **حروب لا تناظرية:Asymmetric** فالتكلفة المتدنية نسبيا للأدوات اللازمة لشن هكذا حروب، يعني أنه ليس هناك حاجة لدول معينة أو منظمة ما لقدرات ضـخمة وتقوم بتصـنيع أسـلحة يجعلها تعتمد بشكل كبير جدا كحاملات الطائرات والمقاتلات المتطورة لتفرض تهديدا خطيرا على دولة ما.
- **يتمتع المهاجم بأفضلية واحدة:** تتميز الحروب السيبرانية بالسرعة والمرونة والمراوغة، وهي بيئة مماثلة بحيث يتمتع المهاجم بأفضلية واضحة وكبيرة على المدافع، ومن الصعب جدا عملية التحصين لوحدها أن تنجح، فالتحصن مع المزيد من عمليات الاختراق وبالتالي المزيد من الضغط.
- **مخاطرها تتعدى استهداف المواقع العسكرية:** لم تعد تنحصر الحروب السيبرانية باستهداف المواقع العسكرية، بل أصبحت تستهدف البنى التحتية المدنية والحساسة في البلدان المستهدفةوهو أمر أصبح واقعيا في ظل القدرة على استهداف شبكات الكهرباء والطاقة وشبكات النقل والنظم المالية والمنشآت النفطية بواسطة فيروس يمكنه إحداث أضرار مادية تؤدي إلى الانفجار أو دمار هائل.
- **تغير الفواعل والأهداف:** أوجدت ثورة المعلومات مجالا خامسا للحرب ليس حكرا على الجهات الفاعلة من الدول فقط، ولكن هناك جهات فاعلة من غير الدول، وفتحت الأبواب لحرب غير متكافئة وغير نظامية، بسـبب التكاليف المنخفضـة نسـبيا، وهذا ما يعكس التحول والتغير في طبيعة الفواعل والأهداف[2].
- **أدوات الحروب السيبرانية:** تعتمد على الحاسوب، وتهدف إلى إلحاق الضرر سواء تقني بالهياكل أو وظيفي أو الأنظمة وحتى الأشخاص، وبصفة عامة تعتمد على الأجهزة والبرامج.

المطلب الثاني: أبرز القطاعات التي تستهدفها الحروب السيبرانية

1- **قطاع الاتصالات والمعلومات:** يشمل جميع شبكات الاتصالات العامة للدولة، وعلى رأسها الأنترنت والحاسبات والشبكات الحكومية والأكاديمية، والتجارية والمدنية، ومحطات البث التلفزي ومن أكبر استقبال الموجات السلكية واللاسلكية، وجميع ما يمكن إدراجه تحت هذا القطاع، لاعتمادها بشكل كامل على وسائل الاتصالات الحديثة[3].

[1]المجال الخامس، الحروب الإلكترونية في القرن الـ 21 (الجزيرة)، نشر يوم: 2011.01.12 على الموقع، اطلع عليه يوم 2025.04.16 - 15:00 http://sobr.aljazeera.net/ac/issues/2011/2122=4346868htm1,1

[2]زينب شنوف، الحرب السيبرانية في العصر الرقمي، حروب ما بعد كلاوزفيتش، المجلة الجزائرية للأمن والتنمية، العدد 02، المجلد 09، جويلية 2020، ص 97.

[3]البدانة ذياب، الأمن وحرب المعلومات، الطبعة الأولى، دار الشروق للنشر والتوزيع، عمان، 2006، ص 37.

ويعتبر هذا القطاع المحرك الرئيسي لجوانب الحوسبة و الحوكمة في أي بلد، وله دور كبير في بناء البنية التحتية والاتصالية للدولة، لذلك فهو يشكل تهديدا كبيرا للأمن القومي لأي دولة، مما يقتضي تقوية هذا القطاع وحمايته من السرقة والتعديل والاستخدام غير الشرعي أو تدمير بنياته بأي شكل كان[1].

وأن هذا القطاع المعقد المتداخل مع جميع القطاعات الاقتصادية والاجتماعية والسياسية والعسكرية والثقافية، أي بجميع مكونات الدولة بشكل واسع وكبير، الأمر الذي جعل الدولة تولي له أهمية كبرى في عصرنا المعلوماتي، ويعتبر جزء من الأمن القومي.

2- **قطاع الأعمال العسكرية والحربية:** شهدت القطاعات العسكرية والحربية تطورات عديدة، مما يجعلها تعتمد بشكل كبير على عنصر المعلومات والرقمنة، وحولتها إلى بناءات تسلح بأجيال جديدة من الأسلحة التكنولوجية والاتصالية، مما زادت في قدرتها وفاعليتها على الدعم اللوجيستي (logistic) والتواصل المعلوماتي والاستخباراتي القائم على توفير عنصر التقنية الحديثة، وبالتالي زاد من الجاهزية والقوة لوسائل والأدوات العسكرية والحربية[2]، لقد ارتبطت المرافق العسكرية ارتباطا وثيقا بالتطورات التكنولوجية الحديثة، لتحدث نقلة نوعية في عالم التسلح اليوم، رافقتها تهديدات أمنية بكشف مآخذ ونقاط ضعف هذه المرافق لتحولها الى هدف من بين الأهداف التي تصوب الحروب السيبرانية بنيرانها عليها، والقطاع العسكري هو نفسه من ينتج هذه النيران أو جزءا منها. لذلك تولي العديد من الدول والحكومات بالصناعة التكنولوجية العسكرية، ما هو جديد في التطور الأمني لهذه القطاعات ورقابتها.

3- **قطاعات الأعمال والأنظمة الحكومية والغير حكومية:** تعد هذه القطاعات عرضة لنيران الحروب السيبرانية، وخاصة ما تعلق بالعمل المدني والإداري، وتقديم الخدمات بشكل خاص فهي اليوم تواجه بتهديدات سيبرانية وبالأخص بين الحكومات أو تلك الشركات التي تعيش التنافس الرقمي[3].

لذلك تعمل الحكومات اليوم على معاينة كافة التحركات التي تتم عبر الفضاء السيبراني، ورصد كل العمليات التي تخرج عن سياق عملها الحكومي من قبل روادها. كما تقوم الشركات بحماية وتأمين كافة إجراءاتها الإلكترونية، وتحليل وضبط تدفق المعلومات إليها، والتنسيق مع القطاع الحكومي، مما يعزز التنمية المستدامة داخل الدولة، كونها تؤمن مسؤولية مجتمعية تجاه الدولة[4]. وأن ضرب الخدمات الإلكترونية للحكومات هو كسر قالبها الأمني ونزع الثقة عنها، وبالتالي خسارتها لجمهورها المتلقي.

---

[1] مرجع سابق، ص 37-38.

[2] بورحلى ريمون، التكنولوجيا الحديثة في المجالات العسكرية، مجلة الجيش اللبناني على شبكة الأنترنت ع 236 (فبراير/ شباط 2005م).
http://www.lebarmy.gov.lb/article.asp?ln=ar\&id=70066 05.04.2025 – 20:00

[3] كلارك ريتشارد نك روبرت، حماية الفضاء الالكتروني في دول مجلس التعاون الخليجي العربية، ط1، ابوظبي،(م ا د ب ا عدد 140، ص 31-32

[4] نفس المرجع السابق ص 32-33

4-**قطاعات المعلومات الإعلامية والمجتمعية:** تلعب الصحافة ووسائل الإعلام والاتصال في تقديم العديد من المعلومات والبيانات للجمهور المتلقي، عبر الوسائل التقنية والرقمية الحديثة، حيث تختزل المسافات والأحداث للأفراد على مدار اليوم على شكل قالب معلوماتي له أهمية كبرى في إبراز ما يجري في العالم[1].

ولقد خطت هاته القطاعات خطوات جبارة بفضل الثورة المعلوماتية والرقمية بحيث اشتركت مع أدوات ووسائل الاتصال والإعلام الإلكتروني (Electronic Media)، والتواصل الاجتماعي والتكنولوجيا الحديثة. فهذا التقدم المتسارع جعلها هدف وبيئة صراع للحروب السيبرانية.

فالحرب الإعلامية (Media War) تعتبر حرب نفسية انعكاسا للحروب التقليدية المادية الموجودة في الواقع[2]، بحيث تحاول التأثير في نفسية الجند والجيش والجمهور المراقب، الأمر الذي يخلق العديد من الآثار النفسية والاجتماعية عليه.

5- **قطاعات الاقتصاد والمال والإعمال:** يولي هذا القطاع الأهمية الكبرى بالمجال السيبراني، وهذا راجع للتحولات الاقتصادية والرأسمالية التي شهدها العالم في عقده الأخير، وتوجه البشرية إلى العمل الاقتصادي والمالي عبر الفضاء السيبراني، والانفتاح الاقتصادي المرتكز على العنصر التكنولوجي، والذي ادخل البشرية في عصر اقتصادي معتمد وقائم على شبكات الأنترنت والرقمنة كالبورصات وصكوك الاكتتاب الإلكتروني والتجارة العالمية (World Trade)، ما يجعلها عرضة للهجمات السيبرانية وإصابتها يكلف الدولة خسائر ضخمة.

المطلب الثالث: أسلحة الحروب السيبرانية

1-**التجسس الإلكتروني (Spyware Information):** تمثل وسائل التجسس التقني والمعلوماتي أحد أشهر وأقدم أسلحة الحروب السيبرانية، وقد تم استخدام هذا السلاح منذ بداية الإنسان لوسائل الاتصال والتواصل[3]. وتتخذ وسائل التجسس المعلوماتي عدة أشكال، منها ما يتم عبر التجسس والتنصت على المعلومات الصادرة من أجهزة الحواسيب، أو الصادرة عن المحطات الطرفية، أو اعتراض المراسلات الإلكترونية الصادرة عن الأقمار الصناعية، والهواتف المحمولة وغيرها من الوسائل التجسس المعلوماتي، ذو الطابع القديم أو الحديث[4].

[1]معالي خالد، أثر الصحافة الالكترونية على التنمية السياسية في فلسطين، رسالة ماجيستير غير منشورة، كلية الدراسات العليا، جامعة النجاح الوطنية، عزة، 2008 ص 11

[2]جاسم جعفر، حرب المعلومات بين ارث الماضي وديناميكية المستقبل، مرجع سابق ص 171

[3]المرجع السابق ص 178

[4]الشهري نوال، حرب المعلومات: في مركز التميز لأمن المعلومات (جامعة الملك سعود)

2-**الاختراق الإلكتروني (Penetration Electronic):** هو عبارة عن إنشـــاء برامج أو نظام إلكتروني يهدف إلى استغلال معلومات الخصم وتدميرها، إضافة إلى إفساد نظامه الحاسوبي والآلي وذلك بهدف التقدم عليه أمنيا وعسكريا واقتصاديا وسياسيا، وقد تكون هذه المواجهة على المستوى الفردي أو المؤسساتي. أو على مستوى الدول[1]. كذلك هناك عدة أشكال للاختراق الإلكتروني لكن لها وظيفة واحدة وهي الدخول في قلب معلومات الخصم، والحصول عليها.

3-**زرع الفيروســـات التقنية في البيئات المعلوماتية:** وهي عبارة عن برامج الكترونية مدمرة تعمل ضمن آلية معينة يحددها صانع هذه البرامج، ولها إشكال وأنواع متعددة تهدف إلى إحداث فوضى في نظام تشغيل الضحية المنوي ضربه واستهدافه إلكترونيا، وتلويث بيئته الإلكترونية وتعطيلها[2].

4-**القرصنة الإلكترونية (Electronic Piracy):** تعتبر القرصنة من أضخم وأشمل الأسلحة السيبرانية المستخدمة عبر الفضاء الرقمي، يشكل هذا السلاح التقني على غالبية وسائل الصراع السيبراني في يومنا هذا، حيث تقوم آلية عمله على تجنيد العديد من الأشـــخاص المؤهلين والقادرين على التعامل مع الحاسوب بخبرة ودراسة عالية جدا تمكنهم من اقتحام مختلف الوسائل الاتصالية، والنظم التكنولوجية من حواسيب وهواتف وموجات وغيرها، ويطلق على هؤلاء الأشخاص المؤهلين باسم الهاكرز (Hackers)[3].

5-**وسائل الإعلام (Media):** تلقى هذه الوسائل إقبالا كبيرا من قبل الجمهور المتلقي، نظرا لسرعة انتشارها وكثرة متابعيها، وتأثيرها على النفس البشرية. دخلت هذه الوســائل عالم الحروب السيبرانية عبر فضـــائيات التلفزة، ومحطات البث المحلي الملتقطة عبر الراديو ومواقع الفيديو الاجتماعي كاليوتيوب (YouTube)، والدبلاج الكاريكاتيري (Dubbing Cartoon)، وغيرها من وسائل الإعلام الأخرى. وتستخدم العديد من الدول هذه الوسائل بشكل كبير خاصة في الخطابات السياسية، وهي سلاح متعدد الأطراف يتم توجيهه إلى دولة أو نظام أو مجموعة بغية تهديدها والتأثير عليها نفسيا ومعنويا[4].

6-**الأقمار الصناعية (Satellites):** هي أسلحة ذات دلالات إستحواذية هدفها السيطرة على أكبر قدر ممكن من المعلومات، وذلك عبر التقاط ملايين الصـــور للهدف وإرســـالها للقاعدة المعلوماتية الموجودة على الأرض، وتعتبر الأقمار الصناعية من أكفئ الوسائل التقنية وأكثرها تعقيدا في حسم المعارك، فهي قادرة على توجيه الصواريخ والقاذفات النارية صوب أهدافها ثم استخدامها في الحرب الباردة[5]. في حين تستخدم الأقمار الصناعية في التشويش على المحطات الفضائية ومنعها من البث بأجندة وأهداف سياسية، هي تعبير

[1] حسين فاروق، فيروسات الحاسوب الألي، عربية للطباعة والنشر، الطبعة الثانية، القاهرة. 1999 ص 7
[2] علوة رأفت، قرصنة الأنترنت، مكتبة التجميع العربي للنشر والتوزيع، الطبعة الأولى، عمان، 2006 ص 23-24
[3] يحي اليحياوي، حرب الاعلام والرقابة، موقع على شبكة الانترنت http://www.elyahyaoui.org
[4] حرب الفضاء والفضاء السيبرانية: صراع أمنية، الموقع: شبكة النبأ المعلوماتية على شبكة الإنترنت، 25 فبراير 2008.
[5] مرجع سابق ص89

جديد عن الحروب السـيبرانية الدائرة في العالم الافتراضـي كبعض التشـويش التي تعرضـت له قناة الجزيرة العربية خلال الثورات العربية.

7-**شـبكات التواصـل الاجتماعي (Social Networks)**: وهي تركيبات اجتماعية تقنية ذات محتوى رقمي، تقوم بربط الحلقات الاجتماعية ببعضـها البعض كالعمل والدين وغيرها، والتي تضـم في طياتها مختلف الفئات العمرية وجميع المسـتويات الاجتماعية والاقتصـادية، وكافة الدرجات الثقافية والتعليمية، وتمثل هذه الشبكة باقة من المواقع ذات النفوذ القوي في العالم ومن أشهرها:

الفيسـبوك Facebook، التويتر Twitter، يوتيوب YouTube البريد الإلكتروني e-mail ، الماسـنجر messenger غوغل بلاس google plus ، المدونات الإلكترونية وغيرها تعد بيئة أكثر تناسـبا وتناغما مع الحروب السـيبرانية، وأكثرها صـراعا باعتبارها سـهلة الوصـول والاسـتخدام والتفاعلية، ولها شـعبية كبيرة ومتطورة وذات طابع اصـطيادي أي يمكن الإيقاع بالضـحايا الإلكترونيين، كما أنها منبر حاشـد للتغيير السياسي[1].

الشكل رقم 02: أشكال الحروب السيبرانية

المصدر: القناة الإخبارية CNBC عربية على الموقع: https://www.cnbcarabic.com

[1]فيصل مراد، التحديات الأمنية الراهنة للأمن القومي الجزائري، رسالة ماجستير منشورة (المدرسة العليا للعلوم السياسية - قسم الدراسات العسكرية والإستراتيجية، 2013/2014. ص02

المبحث الثالث: الأمن السيبراني وأبعاده

يشهد البعد الأمني على وجه الشمول والشؤون الاستراتيجية والعسكرية خصوصاً، بروز تحديات أمنية لا تماثلية منذ نهاية الحرب الباردة، وبروز الفضاء السيبراني كوسيلة ومصدر لأدوات جديدة للصراع الدولي، وباتت هذه التحديات محوراً مهماً في مجال الحفاظ على أمن القومي للدول.

المطلب الأول: مفهوم الأمن السيبراني

يعد مصطلح الأمن من المصطلحات القديمة، واتضحت معالم أصوله الفلسفية عند اليونان فأصل كلمة "Securita" في اللاتينية هو مرادف لغياب العناية، فـ "Sine" متقابلاً بـ "لا" و "cura" تعني "عناية[1]".

إلا أن الأمن كمصطلح يجعل معنيين متعارضين، فيقصد به إما حالة الأمن كمعنى مقصود، أو حالة الأمن من جهة أخرى. فقد عبر عنده في الأصول اليونانية بمصطلح: "Asphaleia" بمعناها الأمن والسلامة؛ والمشتقة من كلمة "Sphallo" والدالة على التعثر والسقوط.

كما أن كلمة "أمن" (Secure) تعني Careless" (se+cura)" أي الحرية من القلق والاضطراب. فقد أشار "Larousse Moderne Dictionary" أن الاستخدام الفرنسي لا يدمج الأمن كإحساس بعدم الخوف، وأشار "فاغر دي دوغلاس Vavere de daugeleas" إلى انفصال أن الأمن يختلف عن اليقين والثقة.

ولكنه يقترب إلى الثقة. أما "Oxford English Dictionary" يمنح الكلمة معنيين: الأول يتجلى في الشروط التي تجعلك في أمان، والثاني يتمثل في الوسائل[2].

أما الجانب اللغوي للأمن، فهو نقيض الخوف أي السلامة. وكلمة "الأمن" لغة مصدر الفعل أمنا أمان وأمنة: أي اطمئنان النفس وسكون القلب وزوال الخوف. ويقال: أمن من الشر، أي سلم منه. وكذلك يقال أمن فلان على كذا أي وثق به وجعله أميناً عليه...يعني الاطمئنان بأن الشيء في حرز وحماية من الخطر[3].

---

[1] يوسف بوقرة، الأمن السيبراني: الاستراتيجية الجزائرية للأمن والدفاع في الفضاء السيبيري، مجلة الدراسات الإفريقية وحوض النيل، المركز الديمقراطي العربي، المجلد الأول، العدد الثالث، 2018. ص105

[2] مرجع سابق ص105

[3] إبراهيم مدكور، المعجم الوجيز: مجمع اللغة العربية، ددن، 1989، القاهرة. ص25

أما المعنى الاصطلاحي والإجرائي للأمن، فهو ذلك الطرف الذي يكتسي طابع الضرورة لنمو الحياة الاجتماعية وتطورها وازدهارها، وذلك للحفاظ على كيان الدولة واستقلالها وسيادتها.

وتتجلى العلاقة التفاعلية بين "الأمن" و"الفضاء السيبراني"، بظهور مصطلح "الأمن السيبراني"، ويعتبر الأمن السيبراني: هو مجموعة الوسائل التقنية والإدارية، التي يتم استخدامها لمنع الاستخدام غير المصرح به على شبكات الكمبيوتر، وسوء استغلال واستعادة المعلومات الالكترونية التي تحتويها بهدف ضمان استمرارية عمل نظم المعلومات، وتأمين وحماية وسرية خصوصية البيانات الخاصة بفواعل الفضاء السيبراني[1].

ترجع المقاربة الإيتيمولوجية لمصطلح "سيبار Syber"، هو لفظ يوناني الأصل مشتق من كلمة "Kybernetes"بمعناها الشخص الذي يدير دفة السفينة، حيث تستخدم مجازاً للمتحدث "governor"، وتم استخدامها من طرف الفلاسفة للتعبير عن الحكم، وتجدر الإشارة إلى العديد من المؤرخين يرجعون أصلها إلى عالم الرياضيات الأمريكي Norbert Wieners 1894-1964، وذلك للتعبير عن التحكم الآلي، فهو الأب الروحي المؤسس للسيبرنيتيقية. مؤلف كتابه الشهير: Cybernetics or control and communication in the Animal and the machine،حيث أشار للسيبرنيتيقية، هي التحكم والتواصل عند الحيوان والآلة، والانسان والآلة وبعد الحرب العالمية الثانية وأزهار الثورة التقنية استبدل استعمال مصطلح الآلة بالحاسوب.

وقد قدمت وزارة الدفاع الأمريكية تعريفاً دقيقاً لمصطلح الأمن السيبراني بأنه: "جميع الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكالها المادية والالكترونية، من مختلف الجرائم كالهجمات، التخريب، التجسس، والحوادث.

واعتبر الإعلان الأوروبي أن معنى الأمن السيبراني: هو قدرة النظام المعلوماتي على مقاومة محاولات اختراق التي تستهدف بياناته. وهذا ما عبر عنه أستاذ الاتصالات بجامعة كاليفورنيا ريتشارد كمرر، حيث عرفه: "عبارة عن وسائل دفاعية من شأنها أن تكشف وتحبط المحاولات التي يقوم بها القراصنة[2]" وبالتالي الأمن السيبراني مفهوم أوسع من أمن المعلومات، أي يهتم بكل ما هو موجود على السايبر، على عكس أمن المعلومات الذي يهتم بأمن المعلومات الفيزيائية (الورقية)[3].

[1] عكاظ، ما هو الأمن السيبراني، 09:42، يوم: 22/06/2020، على الموقع https://www.okaz.com/sa/article/1585526

[2] عناترة بن مرزوق، عمي الدين حريشاوي، الأمن السيبراني كبعد جديد في السياسة الدفاعية الجزائرية، الملتقى الدولي حول سياسات الدفاع الوطني، جامعة قاصدي مرباح ورقلة، كلية الحقوق والعلوم السياسية، 13/01/2017.

[3] مصطفى الطيب، الفرق بين أمن المعلومات والأمن السيبراني، 10:30، 23/06/2020، على الموقع: (https://www.oolom.com/6124)[https://www.oolom.com/6124].

ومن خلال استعراض التعريفات السابقة للأمن والأمن السيبراني، يمكن أن نستخلص ثلاث صفات رئيسة للأمن وهي:

✓**النسبية:** يعني أن الأمن نسبي في العلاقات الدولية، فلا يوجد أمن مطلق يمكن تحقيقه لأن ذلك يعني تهديد أمن الآخرين.

✓**الشمولية:** يعني أن الأمن مفهوم شامل لا يتوقف على عنصر واحد، وإنما يرتبط بمجموعة من الأبعاد السياسية منها والعسكرية والاقتصادية والاجتماعية والثقافية والنفسية.

✓**الديناميكية:** يعني أن الأمن ليس حقيقة ثابتة، ولا يوصف بالجمود بل هو مفهوم مرن، ومتطور يعنى بأشياء مختلفة في أوقات وأماكن مختلفة، بمعنى مسألة الأمن المتغيرة تتأثر بتطور الوضع الداخلي والدولي.

المطلب الثاني: أبعاد الأمن السيبراني.

يعتبر متغير الأمن السيبراني مفهوم ذو أبعاد نسبية أهمها:

1- **البعد العسكري:** كانت البدايات الأولى للإنترنت في البيئة العسكرية، وبعدها انتقلت إلى الأوساط العلمية والأكاديمية وأبحاث تخدم القدرات العسكرية، وتشتمل الميزة النسبية للأمن السيبراني في البعد العسكري، عن طريق قدرة القوة السيبرانية على ربط الوحدات العسكرية ببعضها البعض عبر العالم الافتراضي، وهذا ما يسهل عملية تبادل المعلومات، والذي ينعكس إيجاباً على تحقيق الأهداف العليا للمؤسسة العسكرية، كما توجد في هذا المجال عدة أمثلة توضح البعد العسكري للأمن السيبراني ومدى خطورة الهجمات السيبرانية، وهو ما حصل في جورجيا، واستونيا، وكوريا الجنوبية، وإيران عن بعض الهجمات والاختراقات، والتي أشارت إلى اندلاع صراع مسلح لاحق كذلك الذي وقع بين جورجيا وروسيا، أو بانقطاع الاتصال بالإنترنت في استونيا بين الدولة والمواطنين والتشويش على الإدارات الحكومية[1].

كذلك اختراقات أنظمة المنشآت النووية الإيرانية، والتلاعب بها أدى إلى تهديد الأمن القومي للدولة المعنية في سيناريوهات الهجمات السيبرانية نتائجها كارثية، الأمر الذي يعمل بجدية في تحقيق الأمن السيبراني دون تقاعس أو انتظار وقوع كارثة تكون نتائجها أكثر دراماتيكية[2].

2- البعد السياسي: تتمثل الأبعاد السياسية للأمن السيبراني بشكل أساسي، حق الدولة في حماية نظامها السياسي وكيانها ومصالحها الاقتصادية والسعي إلى تحقيق رفاه شعبها. في حين تؤثر التقنيات في

[1] على الأشقر جسور، السيبرانية هاجس العصر، المركز العربي للبحوث القانونية والقضائية، بيروت، 2017. ص28
[2] على الأشقر جسور، السيبرانية هاجس العصر، المركز العربي للبحوث القانونية والقضائية، بيروت، 2017. ص28

موازين القوى داخل المجتمع نفسه، بحيث أصبح المواطن بإمكانه أن يتحول إلى لاعب سياسي في اللعبة السياسية، وأصبح بإمكانه الاطلاع على خلفيات القرارات السياسية التي تتخذها الحكومة عبر الكم الهائل من المعلومات التي يمكن الوصول إليها أو تم نشرها على الأنترنت[1]. بالقابل هناك تأثير بغض النظر عن صحة السياسات والمبادئ والمواقف والتي يروج لها. فقد استخدم باراك أوباما مثلا: الشبكات الاجتماعية بشكل كثيف خلال حملته الانتخابية. كما تركت التسريبات الوثائقية الدبلوماسية السرية عبر "وكيليكس" أثراً سلبيها على العلاقات بين الدول ومصداقيتها[2].

3- **البعد الاجتماعي:** تعتبر الشبكة الدولية للمعلومات مجالاً مفتوحا لجميع الأفراد، حيث يمكن لجميع المتعلمين السيبرانيين أن يستفيدوا من البنى التحتية والخدمات المتاحة لهم دون تحمل مخاطر أمنية، وهذا يجب التنويه إلى ضرورة التحسيس بأخلاقيات الأمن السيبراني. بالقابل ساهمت جميع فئات المجتمع في تطور الفضاء السيبراني، وذلك بتبادل الأفكار والمعلومات المختلفةوانفتاح المجتمع على الآخر، ويؤسس لتبادل الخبرات والأفكار وتكون حاجات جديدة وأفاق تعاون وتكامل[3]. يضاف إلى ذلك ما تقدمه الأنترنت من امكانات وقدرات، للمجالات العلمية والثقافية والخدماتية، فالمحتويات غير المشروعة وغير مرغوب بها ذات تأثير سلبي على أخلاقيات مجتمع معين، وارتفاع نسبة الممارسات الجرمية، ومن أمثلة ذلك: الاباحية والترويج للإتجاربالممنوعات، والإرهاب، والتجنيد لقضايا تمس الأمن والسلام الدوليين، وعليه لا بد من بناء مجتمع مسؤول ومدرك لمخاطر الفضاء السيبراني، والتعامل معه بعد أدنى من قواعد السلامة مع إدراك العواقب القانونية[4].

4- **البعد القانوني:** يرتب على النشاطات الفردية والمؤسساتية والحكومية في الفضاء السيبراني، نتائج قانونية تمثل في إيجاد القواعد القانونية التي تنظم العلاقات في الفضاء السيبراني، وحل النزاعات التي تنشأ عنها، وقد نشأت أساليب وممارسات عديدة في استخدام تقنية المعلومات، كإنشاء المدونات والمجتمعات على الأنترنت، والحق في حماية ملكية البرامج المعلوماتية، والإبلاغ عن المخالفات والجرائم السيبرانية. وهذا ما أدى إلى ضرورة وجود ترسنة قانونية في المتغيرات الحاصلة. كذلك بروز تحولات جديدة على مستوى جميع المجالات، وتصاعد ازدياد القضايا التي رفعت أمام المحاكم، مما يستدعي إعداد بيئة تنظيمية تشريعية، وبناء ميثاق لمكافحة الجرائم السيبرانية والحكم[5].

5. **البعد الاقتصادي:**يرتبط الأمن السيبراني ارتباطاً وفقاً بالاقتصاد، فقد توسع استخدام تقنيات المعلومات والاتصالات ما أتاح وعزز التنمية الاقتصادية للعديد من البلدان وفرص الاستخدام التي تقدمها

[1]نفس المرجع السابق ص28
[2]نفس المرجع السابق ص29
[3]نفس المرجع السابق ص29
[4]نفس المرجع السابق ص29
[5]بأرة سمير، الدفاع الوطني والسياسات الوطنية للأمن السيبراني في الجزائر: الدور والتحديات، المنتقى الدولي حول سياسات الدفاع الوطني، جامعة قاصدي مراد ورقلة، كلية الحقوق والعلوم السياسية، 31/01/2017. ص 229-231

الشركات الدولية الكبرى، ولا ننسى حلول عصر املال الالكتروني ضمن بيئة تنمية متحركة كوجود المحفظة الالكترونية، وإصدار البطاقات التي تسمح بالدفع الالكتروني[1].

المطلبالثالث: أساسيات الأمن السيبراني كرافد جديد.

يجب أن تسهم الحلول الأمنية في الوفاء بمعايير الأمن الأساسية، مثل التوافر والسلامة والسرية.

1- التوافر Availability: لتأمين توافر النظم والخدمات والبيانات، يجب تحديد الأحجام المناسبة لنظم البنية التحتية، وأن تتوافر لها الأعداد الاحتياطية البديلة الضرورية. يضاف إلى ذلك أنه يجب توفير الإدارة التشغيلية للموارد والخدمات. ويقاس التوافر على أساس الفترة الزمنية التي تكون الخدمة في حالة تشغيل، كما أن الحجم المحتمل للأعمال التي يمكن تناولها أثناء فترة توافر الخدمات، هو الذي يحدد قدرة المورد (الشبكة) مثلاً، وثمة ارتباط شديد بين التوافر ويسر النفاذية (Accessibility)[2].

2- السلامة**Integrity: إن**المحافظة على استقامة البيانات، أو معالجة الخدمات يعني وقابتها من التعديل العارض أو المقصود من التلاعب أو التدمير، وهذا لضمان الدقة وبقاء ما صحيحة دون التلاعب. ويعتبر السبيل الوحيد لضمان وسلامة البيانات، وهو حماية تلك البيانات المعمول بها من أساليب اقتناص المعلومات عن طريق تحويل مصدرها الأصلي (tapping Techniques)، والتي يمكن استخدامها لتعديل المعلوماتالمعترضة، ويمكن توفير هذه الحماية بواسطة آليات أمن مثل[3]:

- مراقبة صارمة على النفاذ
- تشفير البيانات
- الحماية من الفيروسات والديدان أو أحصنة طروادة.

3. السرية: **Confidentiality**ويقصد بذلك الحفاظ على سرية المعلومات، المعاملات، والخدمات، أو الإجراءات التي تجري في الفضاء السيبراني، وهي تتضمن حماية المواردوالافشاء غير المرخص به. كما يمكن تنفيذ السرية عن طريق مراقبة النفاذ والتشفير. كما يساعد التشفير على حماية سرية المعلومات أثناء الإرسال أو التخزين وتحويلها بشكل غير مفهوم لأي شخص لا يمتلك وسائل فك هذا التشفير[4].

[1] على الأشقر جسور، السيبرانية هاجس العصر، المركز العربي للبحوث القانونية والقضائية، بيروت، 2017. ص28

[2] Andrew Mclean, Electronic money regulation 2011(EMR2011) & the payment service Regulation 2009.

[3] الاتحاد الدولي للاتصالات، دليل الأمن السيبراني للبلدان النامية، مكتب تنمية الاتصالات، طبع في جنيف سويسرا، 2006. ص22

[4] نفس المرجع السابق ص22

الشكل رقم 03: جدول أساسيات الأمن السيبراني.

يجب على النظام	أهداف الأمن	أدوات الأمن
يكون الاستخدام	• التوافر • الاستدامة • الاستمرار • الثقة	• تحديد الأبعاد • هامش احتياطي • تدابير التشغيل والمؤازرة
العمل بضرورة سلمية	• أمن التشغيل • الإعتمادية • المتانة • الإستمرارية • الصواب	• التصميم • الأداء • **علم تصميم الآلات بما يناسب الجسم البشري** • نوعية الخدمة • صيانة التشغيل
توفير النفاذ للكيانات المرخص لها (بينما يمنع للكيانات الغير مرخص لها)	• السرية • السلامة (لا تغييرات)	• التحكم في النفاذ • الإستقان • مراقبة الإخطاء • التأكد من التماسك • التشفير
التحقق من الإجراءات	• عدم الرفض • اليقين (بعيد عن الشك) • عدم الممارة	• شهادة التصديق • التسجيل، إمكانية الإقتفاء • التوقيع الإلكتروني • آلية البرهان

المصدر: الاتحاد الدولي للاتصالات، دليل الأمن السيبراني للبلدان النامية، مكتب تنمية الاتصالات، جنيف، سويسرا. 2016، ص 23

خلاصة الفصل :

في نهاية الفصل الأول، استخلصنا أن الفضاء السيبراني ساحة عالمية عابرة لحدود الدول. ولعب دورا أساسيا في تنظيم القوة، أو الاستحواذ على عناصرها الأساسية في العلاقات الدولية. كما فرضت الثورة التكنولوجية مجموعة من التحديات والتهديدات الأمنية الجديدة والتي تسعى بالحروب السيبرانية، مما غيرت أنماط الحياة وحدود العلاقات. وبيئة استراتيجية جديدة برزت فيها أشكال من الصراعات في الساحة الدولية

وأن الأمن السيبراني على مستوى العالم بات بشكل جزءا أساسيا في السياسة الأمنية للدول بحيث أصبح لدى صناع القرار أولوية في سياساتهم الدفاعية. وسيطر الأمن السيبراني على عقائد جيوش العالم

الفصل الثاني
الحروب السيبرانية وتحديات الأمن العالمي

تمهيد :

أفرز التوسع المتسارع في استخدام الفضاء السيبراني جملة من التهديدات و التحديات الأمنية غير التقليدية، و التي أصبحت تشكل مصدر قلق متزايد للمجتمع الدولي، فقد أضحت الحروب السيبرانية أداة استراتيجية تعتمدها الدول و الجهات الفاعلية في الساحة الدولية لتحقيق أهدافها السياسية و العسكرية والاقتصادية، بعيدا عن أساليب المواجهة المباشرة، في هذا السياق يتناول هذا الفصل أبر هذه التهديدات السيبرانية مع التركيز على طبيعتها و مصادرها، كما يستعرض تداعياتها على الامن القومي و الدولي

و يختتم هذا الفصل بعرض أهم الحروب السيبرانية و درجة تأثيرها.

المبحث الأول: أبرز التهديدات السيبرانية.

لقد أثرت التهديدات السيبرانية على الأمن العالمي، وهذا نتيجة الاستخدام الكبير لتكنولوجيا المعلومات والاتصالات، مما أدى إلى بروز جرائم سيبرانية، وإرهاب سيبراني، إلى أن ظهرت حروب سيبرانية فشكلت تحديا أمنيا عالمها، ومن أبرز التهديدات السيبرانية هي كالآتي:

المطلب الأول: الجريمة السيبرانية.

أصبح الفضاء السيبراني بيئة جديدة للمجرمين السيبرانيين، وصنع عدة جرائم تسعى "الجريمة السيبرانية" والتي تشمل الفرصة، والاحتيال، والتخريب، والابتزاز، والتهديد وغيرها.

أولا: مفهوم الجريمة السيبرانية:

إن المفهوم الضيق للجريمة السيبرانية هي "جريمة الكمبيوتر"، وأي تصرف غير قانوني موجه ضد الجهاز، أو المعلومات التي تحتويه.

أما المفهوم الواسع في "الجريمة المتصلة باستخدام الكمبيوتر"، أي تصرف غير قانوني يرتكب باستخدام تقنيات المعلومات والاتصالات، بما فيه حيازة مواد ممنوعة أو توزيعها أو عرضها[1].

كما تعرف على أنها "مجموعة الأعمال غير القانونية التي تتم عبر معدات، أو أجهزة إلكترونية أو شبكة الأنترنت، أو بث عبر محتوياتها، وهي ذلك النوع من الجرائم التي تتطلب الإلمام الخاص بتقنيات الحاسب الآلي، ونظم المعلومات لارتكابها أو التحقيق فيها ومقاضاة فاعليها"[2].

وكذلك "في سلوك غير المشروع أو المنافي للأخلاق، أو غير المسموح به والمرتبط بالشبكات المعلوماتية العالمية"[3].

وعرفتها رابطة كبار الشرطة بأنها "تنطوي على استخدام الكمبيوتر، أو الأنترنت بشبكات تكنولوجية لتسهيل ارتكاب الجريمة"[4]. وبالتالي الجريمة السيبرانية هي إساءة استخدام تكنولوجيا المعلومات والاتصالات من طرف المجرمين، وذلك على أنها جرائم أنترنت.

[1] على الأشقر جسور، السيبرانية هاجس العصر، المركز العربي للبحوث القانونية والقضائية، بيروت، 2017 ص50.
[2] عبد الفتاح مراد، جرائم الحاسوب والإنترنت، دار الكتب والوثائق المصرية، الطبعة الأولى، الإسكندرية ص38.
[3] يوسف بوقرة، الأمن السيبراني: الاستراتيجية الجزائرية للأمن والدفاع في الفضاء السيبيري، مجلة الدراسات الإفريقية وحوض النيل، المركز الديمقراطي العربي، المجلد الأول، العدد الثالث، 2018 ص 105.
[4] صالح بن علي بن عبد الرحمان الربيعة، الأمن الرقمي وحماية المستخدم من مخاطر الإنترنت، هيئة الاتصالات وتقنية المعلومات ص 09.

ثانيا: خصائص الجريمة السيبرانية:

إن الميزة التي ميزت الجريمة السيبرانية عن الجريمة التقليدية بعدة خصائص وهي ارتباطها بالأنترنت، ونذكر منها:

- جريمة عابرة للحدود، فهي تستفيد من خصائص الفضاء السيبراني.
- ترتكب عبر الأنترنت، وبالتالي هي حلقة وصل بين أطراف الجريمة.
- صعوبة إثبات الجريمة السيبرانية، وهذا نظراً لصعوبة تتبع مصدر الجريمة والتخفي وتزوير الهوية.
- ذكاء المجرمين والتطور التكنولوجي.
- مرتبطة بفضاء سيبراني معقد ومتشابك.
- قلة التبليغات عن الجرائم السيبرانية، بسبب الخوف والتشهير وفقدان السمعة، أو عدم القدرة على اكتشاف الجريمة إلا بعد وقت طويل من حدوثها.

ثالثا: المجرمون السيبرانيون

يملك المجرمون السيبرانيون في أغلب الحالات معلومات وتكنولوجيا أكثر تقدمها من ضحاياهم، مما يعطي أفضلية للمهاجم من المدافع عن أنظمة الكمبيوتر، ومن أجل الاعتداء على أمن الشبكة والأنترنت يقوم المهاجم باستغلال نقاط الضعف، أو الثغرات الأمنية في أي نظام معلوماتي.

وقد يكون الدافع الخفي للمجرمين السيبرانيين، متصلا بعوالم سياسية واجتماعية وتقنية ومالية، أو بالحكومة...وتكون مرتبطة بعصابة أو جماعة "الهاكرز"[1]Hackers.

ويختلف نوع المجرمين السيبرانيين في بناء أهدافهم ودوافعهم، فمنهم من يبحث عن التسلية والمعرفة، واكتشاف عمل الأنظمة والخدمات والوظائف التي تقوم بها. ومنهم كذلك من يثبت قدراته الفكرية والتقنية، في حين يبحث البعض عن الانتقام والابتزاز وإلحاق الضرر بالغير، والاعتداء على الأنظمة السياسية والأمنية والاجتماعية[2].

رابعا : أهم الجرائم السيبرانية:

هناك عدة طرق مختلفة لاستغلال الإمكانيات التي تتيحها تكنولوجيات الأنترنت، فهي تقوم في أغلب الأحيان على الخداع والاحتيال. ويمكن اعتبار العمل الجرمي قانوناً جريمة سيبرانية عندما يستهدف الهجوم[3]:

– باتت الجرائم السيبرانية في تطور واستهداف العديد من المواقع على الأنترنت في المستقبل، ولعل أشهر الجرائم السيبرانية هي إطلاق الفيروسات لما تسببه من خسائر اقتصادية، فقد تسبب فيروس "تميدا"

[1] الاتحاد الدولي للاتصالات، دليل الأمن السيبراني للبلدان النامية، مكتب تنمية الاتصالات، طبع في جنيف سويسرا، 2006 ص 35.
[2] على الأشقر جسور، السيبرانية هاجس العصر، المركز العربي للبحوث القانونية والقضائية، بيروت، 2017 ص52.
[3] على الأشقر جسور، السيبرانية هاجس العصر، المركز العربي للبحوث القانونية والقضائية، بيروت، 2017 ص50.

على سبيل المثال في خسائر قدرت 530 مليون دولار للاقتصاد المركزي وكشف تقرير لمكتب التحقيقات الفيدرالي المركزي FB1 أن الخسائر المالية تجاوزت 3.5 مليار دولار في عام 2019 بسبب الجرائم السيبرانية[1].

– كما أن هناك عدة جرائم مصحوبة بالإرهاب مثل التجسس السيبراني، والقرصنة، والجرائم المنظمة، والمواقع التحريضية ضد المعتقدات الدينية، ومواقع متخصصة في القذف وتشويه سمعة الأشخاص والمواقع الإباحية، وتزوير البيانات، وغسيل الأموال، وانتحال شخصية، والأغراق بالرسائل والحواسب الآلية، والاقحام والتسلسل[2].

– **أمن المعلومات:** أي مصداقيتها وتوافرها وصحتها، وتندرج في هذا الإطار عمليات اختراق الأنظمة، عبر سرقة كلمة السر، أو التصيد، أو التضليل والاحتيال، ضف إلى ذلك عمليات سرقة البيانات وتدميرها.

– **الملكية الفكرية:** والتي تدخل فيها سرقة البرامج والقرصنة، والاستعمال غير الشرعي لإنتاج محمي للملكية الفكرية.

المطلب الثاني: الإرهاب السيبراني

ظهر الإرهاب السيبراني كتهديد أمني جديد هدفه نشر الخوف والرعب، باستخدام التقنيات الحديثة

أولاً: إن إرهاب الأنترنت مرتبط بطريقتين هماً:

– ممارسة الأعمال التخريبية عبر شبكات الحاسوب والأنترنت.

إن الأنترنت أصبحت منبر الجماعات والأفراد، لنشر وسائل الكراهية والعنف، والاتصال ببعضهم البعض وبمؤيديهم والمتعاطفين معهم.

عرف جيمس لوس (James Lewis) الإرهاب السيبراني بأنه "استخدام أدوات شبكات الحاسوب في تدمير أو تعطيل البنى التحتية الوطنية المهمة مثل: الطاقة، والنقل، أو بهدف ترهيب الحكومة والمدنيين"[3].

وعرف الإرهاب السيبراني على أنه "الإرهاب الذي يعرف في الفضاء السيبراني ... ويفهم بدوره على أنه الاستخدام المنظم للعنف من أجل تحقيق أهداف سياسية"[4].

وهناك من صنف هجمات 11 سبتمبر كأول إرهاب سيبراني، وكانت بداية ظهور هذا المصطلح.

[1]يمكن الاطلاع على موقع الأنترنت: http://www.computer-word.com/security-topics/security/vuris

[2]Todd Amegilt, the dark fruit of globalization: hostile use of the internet, Carlisle barracks, PAUS .Army College, 2005 p 16

[3]Alix Desforges, cyber terrorisme: quel perimetre?, fiche de L'irsem n 11,2011, p03

[4]الاتحاد الدولي للاتصالات، دليل الأمن السيبراني للبلدان النامية، مكتب تنمية الاتصالات، طبع في جنيف سويسرا، 2006 ص 34

ثانيا: وسائل الإرهاب السيبراني.

1- **البريدالإلكتروني:** يعد من أبرز وسائل الإرهاب السيبراني، حيث يستخدم البريدالإلكتروني في التواصل بين الإرهابيين، وتبادل المعلومات معهم.

2- **إنشاء مواقع الأنترنت:** لقد سهلت على المنظمات والجماعات الإرهابية توسيع أنشطتهم من خلال تبادل الآراء والأفكار والمعلومات.

3- **اختراق وتدمير المواقع:** تتم عملية الاختراق السيبراني عن طريق تسريب البيانات الرئيسية والرموز الخاصة ببرامج شبكة الأنترنت، وتدمير المواقع وهو الدخول غير المشروع بهدف التخريب ونشر رسائل تشيد بالإرهاب[1].

المطلب الثالث: أنماط التهديدات السيبرانية.

تقسم التهديدات السيبرانية التي تواجهها الدول والأفراد إلى أربعة أنماط رئيسة وهي[2]:

1- هجمات الحرمان من الخدمة Denial of service(DOS):

حيث يتم إطلاق خدمة كبيرة من الطلبات على خوادم الضحية بصورة تفوق قدرة الخادم، أو الجهاز على معالجتها والاستجابة لها، مما يؤدي إلى توقفه بصورة جزئية أو كلية أو إبطاء عمله، وهذا ما يسبب ضرر للمستخدم النهائي، وهو هجوم يهدف إلى إيقاف قدرة الهدف على تقديم الخدمات المعتادة، وذلك عن طريق اختراق جهاز الحاسب الآلي المقدم للخدمة (server[3])، وهي تستعمل كثيرا ضد مواقع الأنترنت أو البنوك أو المؤسسات من أجل التأثير عليها أو لدفع فدية مالية.

2- إتلاف المعلومات أو تعديلها:

ويقصد به الوصول إلى معلومات الضحية عبر شبكة الأنترنت أو الشبكات الخاصة والقيام بعملية تعديل البيانات الهامة دون أن يكتشف الضحية ذلك. فالبيانات تبقى موجودة لكنها مضللة قد تؤدي إلى نتائج كارثية، خاصة إذا كانت خطط عسكرية أو خرائط سرية.

3- التجسس على الشبكات:

ويقصد بذلك الوصول غير المصرح، والتجسس على شبكات الخصم دون تدمير أو تغيير في البيانات، والهدف منه الحصول على معلومات قد تكون خطط عسكرية، أو أسرار حربة، سياسية، اقتصادية، مالية، مما يؤثر سلبا على مهام الخصم.

---

[1] عبد الرحمان بن عبد الله المسند، وسائل الإرهاب الإلكتروني وحكمها في الإسلام وطرق مكافحتها على الموقع:
http://shemela.ws/browse.php/book-1244/page-20 تاريخ الاطلاع: 2020.05.01

[2] محمد مختار: "هل يمكن للدول أن تتجنب مخاطر الهجمات الألكترونية؟، مفاهيم المستقبل،(م م أ ت)، العدد السادس، 2015، ص 5-6

[3] انوران شفيق، اشكال التهديدات الالكترونية، المركز الأوروبي لدراسات مكافحة الإرهاب والاستخبارات ECC 29 يناير 2020
https://www.europarabet.com/?p=34807

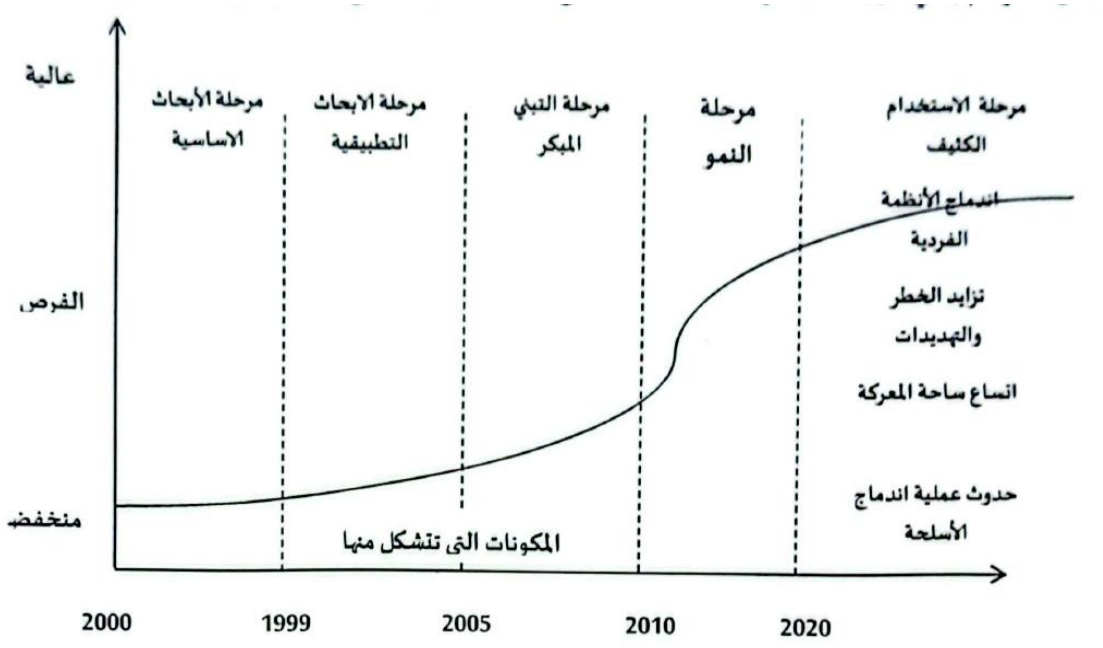
4- تدمير المعلومات:

في هذه الحالة يتم مسح وتدمير كامل لأصول المعلومات، والبيانات الموجودة على الشبكة ويصطلح عليه "تهديد لسلامة المحتوى". ويعني بها إحداث تغيير في البيانات سواء الحذف أو التدمير من قبل أشخاص غير مخولين.

وهناك عدة أنواع لمخاطر التهديدات السيبرانية منها[1]:

- التعرض لسرية الاتصالات التي تطال البريد الإلكتروني، والدخول إلى الأنظمة والملفات دون إذن، وهذا يعتبر اعتداء على الحريات والحقوق الشخصية.
- التلاعب بالمعلومات الموجودة في نظام معين، وتشويهها أو إتلافها، سواء عبر الاختراق أو نشر الفيروسات.
- الجرائم العادية التي تستخدم الأنترنت كالسرقة، والغش وسرقة الهويات، والاعتداء على الملكية الفكرية وغيرها.
- الجرائم التي تندرج في إطار الجريمة المنظمة، والتي تهدد أمن الأفراد والدول، كتبييض الأموال والإرهاب،... إلخ.

شكل 04: رسم بياني لتزايد المخاطر الأمنية للشبكات مع تطور مراحل النضج التكنولوجي



المصدر: عبد الصادق عادل، أسلحة الفضاء الالكتروني في ضوء القانون الدولي الانساني، وحدة الدراسات المستقبلية، سلسلة أوراق، العدد23مكتبة الاسكندرية، ص 70.

[1] على الأشقر جسور، السيبرانية هاجس العصر، المركز العربي للبحوث القانونية والقضائية، بيروت، 2017 ص353

المبحث الثاني: تداعيات الحروب السيبرانية على الأمن العالمي

لقد أصبح التعامل الحالي في الفضاء السيبراني عبر شبكة الإنترنت، والت بنيتها الأساسية هي التقنيات الحديثة، والحاسوب هو القاعدة الأساسية لهذا الفضاء، مما تسبب في بروز تهديدات سيبرانية فشكلت تحدياً أمني عالمي، وسيبراني خاص.

المطلب الأول: تصاعد تأثيرات الحروب السيبرانية

تختلف الحروب التقليدية عن الحروب السيبرانية، فالأولى مادية ومفهوم يستخدم لوصف مجموعة متنوعة وهائلة من الظروف والسلوكيات، وبداية من حالة النزاع المسلح بين الدول مثل (الحرب العالمية الثانية)، ووصولاً إلى الحروب الرمزية. أما الثانية فمصطلح يستخدم لوصف كل شيء متعلق بحملاتالتخريب وتعطيل الأنترنت، وصولاً إلى حالة الحرب الفعلية باستخدام الرسائل الإلكترونية، ولها ثلاث معالم رئيسية[1]:

1- الحروب السيبرانية تهدف إلى مآرب سياسية محددة.
2- الحروب السيبرانية دائما "**وحدة عنف**" أساسية.
3- الحروب السيبرانية تمتلك فضاءً مستضيفاً لها، وهو الفضاء السيبراني كما أن الحروب التقليدية فضاؤها البر، والبحر، والجو.

وحالياً تحاول الولايات المتحدة الأمريكية الوصول بالحروب السيبرانية إلى مستوى الحروب المادية من حيث طبيعة التأثير والنتائج، وأصبح هدفها أن تحقق الهجمات السيبرانية قدراً كبيراً من الدمار، والضرر المادي، وإذا راجعنا الهجمات السيبرانية الأكثر شهرة على مستوى العالم، والتي استهدفت مؤسسات عسكرية أو حكومية. يتضح أنها تهدف بالأساس إلى الحصول على معلومات سرية أو منع الحكومة من الولوج إلى مواقعها الإلكترونية، أو السيطرة عليها[2].

ولقد استطاعت وكالة الاستخبارات الأمريكية والإسرائيلية تصميم فيروس "**ستكسنتStuxnet**"، يعمل على اختراق وتعطيل المنشآت النووية الإيرانية، وقد كان هذا الهجوم دقيقاً إلى درجة تحديد عدد أجهزة الطرد المركزي، وبالتالي تم تعطيل هذه الأجهزة بمهارة فائقة، وجعل سرعة الدوران متفاوتة مما أدى إلى انهياره.

وفي سياق آخر نرى المنافسة الأمريكية الصينية قد ترتقي إلى مرحلة "حرب سيبرانية باردة"، وهو ما يعني دخول البلدين في مرحلة سباق تسلح سيبراني جديد قد يؤدي في النهاية إلى خسائر وأضرار قد تلحقبالبلدان إلى نشوب حرب باردة، وانقسام أيديولوجي بين الغرب والصين[3].

---

[1] نحوي السودة، بحث الفضاء السيبراني، مؤتمر حرب الفضاء السيبراني، تاريخ النشر: 05/05/2014، على الموقع: [https://seconf.wordpress.com]
[2] نفس المرجع على لموقع : [https://seconf.wordpress.com]
[3] نفس المرجع 1

ومع انتشار "فيروس كورونا" COVID 19 في 200 دولة في العالم، زاد عمل القراصنة باستغلال الأزمة الوبائية وتحقيق أهداف شخصية، وهذا مع توجه الكثير من الشركات والمؤسسات للدول لتبني نمط العملعن بعد والتعليم عن بعد، وزيادة الاستهلاك والاعتماد على الإنترنت والأدوات الرقمية، وأصبحت هاته البيئة جاذبة لكثير من قراصنة المعلومات وممارسة هوايتهم المفضلة في الاختراق أكثر من ذي قبل.

المطلب الثاني: مخاطر تهديد الأمن السيبراني لأمن الدول

للإرهاب السيبراني تداعيات خطيرة على الأمن القومي للدول، ونذكر منها ما يلي:

1- تهديد أمني سياسي:

تعمل المنظمات الإرهابية على إلحاق الضرر وشل أنظمة القيادة والسيطرة على الاتصالات، أو تعطيل أنظمة الدفاع الجوي، بالإضافة إلى اختراق البريد الإلكتروني لرؤساء وكبار المسؤولين للدول والشخصيات السياسية، ونشر رسائل مضللة. ففي عام 2010 قامت مجموعة "ويكيليكس" بتسريب وثائق تحتوي معلومات سرية متداولة بين الإدارة الأمريكية وقنصلياتها الخارجية بدول العالم[1]، وفي مارس هاجمت مجموعة "سايبر بيركوث" الأوكرانية المواقع الإلكترونية لحلف الناتو مما أدى إلى تعطيل مواقع الحلف لمدة ساعات.

وأقرت وحدة الجرائم السيبرانية الأمريكية في أوت 2014 بأن قراصنة أجانب تمكنوا من اختراق حسابات تابعة للهيئة الأمريكية لتنظيم الأنشطة النووية.

كما أكدت صحيفة نيوز تايمز في تقرير لها يوم 2015/04/26 أن قراصنة روس اطلعوا على رسائل الكترونية للرئيس الأمريكي باراك أوباما وتعامله مع موظفيه داخل البيت الأبيض[2]. وهذا يعد تهديداً خطيراً للأمن القومي الأمريكي.

أما أمنيا تعمل الجماعات الإرهابية على التسلل الإلكتروني إلى الأنظمة الأمنية في دولة ما، وشل وفك الشفرات السرية للتحكم في تشغيل منصات إطلاق الصواريخ الاستراتيجية والأسلحة الفتاكة، وتعطيل مراكز القيادة والسيطرة العسكرية ووسائل الاتصال للجيوش، بهدف عزلها عن قواتها، والنفاذ إلى النظم العسكرية واستخدامها لتوجيه الجنود إلى نقطة غير آمنة قبل قصفها أو تفجيرها[3].

2- تهديد اقتصادي:

تقوم المنظمات الإرهابية باختراق النظام المصرفي، وإلحاق الضرر بأعمال البنوك أو أسواق المال، وتعطيل عملية التحويل المالي، ومن أمثلة ذلك قيام مجموعة "هاكرز" المحترفين بسرقة بيانات بطاقات

[1] أيوب خليفة والأمن المعلوماتي: لماذا تضاددت التهديدات الإلكترونية مع انتشار كورونا؟، الموسوعة الجزائرية للدراسات السياسية والإستراتيجية، العدد 4868، يوم: 10/04/2020.

[2] هاجر حسونة، الإرهاب الإلكتروني.. ها يتجول في المصير الجديد الأول في العالم، نشر يوم: 04/05/2015، على الموقع: اطلاع عليه يوم 07/05/2020. [https://alakhbaronline.net/articles/1430728333185670700]

[3] عبد الله بن فهد العجلان، مرجع سابق، ص 22

الائتمان من بعض أكبر مراكز التسويق الإلكتروني للدولة، وخصم ملايين الدولارات من أصحاب تلك البطاقات لتوفير تمويل الإرهابية في الدول التي يتم بيع السندات فيها[1].

وأكدت شركة "كاسبر سكي" الرائدة في مجال الأمن المعلوماتي أن مجموعة "الهاكرز" تمكنوا من السيطرة على حسابات مصارف عالمية، وسرقة نحو مليار دولار[2].

3- تهديد اجتماعي:

توجه المنظمات الإرهابية رسائلها للإعلام والجمهور الخاص بالمجتمعات، والتي تقوم بترويعها وإرهابها وذلك بهدف شن حملات وحرب نفسية ضد الدول، فهي تعرض أفلام مرعبة للرهائن والأسرى أثناء إعدامهم مما يؤثر على المدنيين، بشكل أساسي على كرامة الإنسان والسلامة الشخصية، والتحرش والملاحقة، أو الترصد، ومع زيادة الاستعمال والإدمان أدى تدريجيا إلى انفصال البشر عن محيطهم الاجتماعي البشري، وهو ما يفقد العلاقات الإنسانية مرونتها التقليدية.

المطلب الثالث: مخاطر الحروب السيبرانية على الأمن العالمي

تسببت الحروب السيبرانية ببروز عدة مخاطر وتداعيات على تفاعلات السياسة الدولية، ويمكن طرح أبرزها على النحو الآتي[3]:

1- تصاعد المخاطر السيبرانية:

خاصة مع قابلية المنشآت الحيوية (مدنية وعسكرية) في الدول للهجوم، الأمر الذي يؤثر في وظائف تلك المنشآت، وبالتالي فإن التحكم في تنفيذ هذا الهجوم يعد أداة استراتيجية.

2- تعزيز القوة وانتشارها:

عمل الفضاء السيبراني على إعادة تشكيل قدرة الأطراف المؤثرة، و أدى إلى عملية انتشار القوة بين فاعلين متعددين.

3- عسكرة الفضاء السيبراني:

حيث برز في الأطر عدة اتجاهات ونذكر منها: التطور في مجال سياسات الدفاع والأمن السيبراني لدى الأجهزة المعنية، وتصاعد القدرات في سباق التسلح السيبراني، وتبني سياسات دفاعية سيبرانية لدى الأجهزة المعنية بالدفاع والأمن في الدول، وتزايد الاستثمار في مجال الحروب السيبرانية داخل الجيوش الحديثة.

---

[1] أيمن حسين، مرجع سابق

[2] هاجر حسونة، مرجع سابق

[3] عادل عبد الصادق، الهجمات السيبرانية: أنماط وتحديات جديدة للأمن العالمي، الموسوعة السيبرانية الجزائرية، العدد 18601، يوم: 27/11/2019، على الموقع: (https://www.politics-dz.com) [https://www.politics-dz.com].

4- إدماج الفضاء السيبراني ضمن الأمن القومي:

بدأت الدول بتحديث جيوشها وتشكيل وحدات متخصصة في الحروب السيبرانية وإقامة هيئات وظيفية للأمن والدفاع السيبراني، بالإضافة إلى القيام بالتدريب وإجراء مناورات لتعزيز الدفاعات السيبرانية.

5- الاستعداد لحروب المستقبل:

وهو ما نلاحظه اليوم من تبني العديد من الدول استراتيجية حرب للمستقبل، وترى الدول الكبرى أن من يحدد مصير تلك المعركة المستقبلية ليس من يملك القوة فقط، وإنما القادر على شل القوة والتشويش على المعلومة[1].

هناك تحديات ومخاطر جديدة نابعة من أنشطة عبر الإنترنت، والتي يمكن ممارستها وتوجيهها عبر جميع أنحاء العالم بشكل غير مضبوط، دون وجود إطار واضح لمساءلة الأفراد القائمين على هذه الأنشطة.وكذلك يصعب في الفضاء السيبراني تمييز مبدأ "الحرب العادلة" ، كما في الأنشطة المدنية والسياسية والعسكرية.

ويوضح الكاتبان الأمريكيان "بيتر سينجرو والان فريدمان" من خلال استخدام دراسات الحالة، كيف يتمكن المجرمون وقراصنة الكمبيوتر والحكومات على حد سواء من الاستفادة من نقاط الضعف البشرية، والتقنية للوصول إلى أجهزة الكمبيوتر الأخرى و والقيام بهجمات سيبرانية، فالخطأ البشري هو جزء رئيسي من اختراق أنظمة الأمن السيبراني، كما أن الخطأ الفردي يمكن أن يكون كافيا لمنح فرص الوصول إلى شبكات بأكملها، بالإضافة إلى الشبكات الحكومية، والصناعية، والمؤسسات العسكرية، وذلك في الوقت الذي يصعب فيه تتبع أصول مطورو البرمجيات الخبيثة، أو الهجوم السيبراني المباشر والكشف عن هويته[2].

[1] سليم دحمان، أثر التهديدات السيبرانية على الأمن القومي: العلاقات المتحدة أنموذجاً، مذكرة مقدمة لنيل شهادة ماستر أكاديمي، كلية الحقوق والعلوم السياسية، قسم العلوم السياسية، جامعة المسيلة، 2017/2018، ص 51.

[2] نحوي السودة، بحث الفضاء السيبراني، مؤتمر حرب الفضاء السيبراني، تاريخ النشر: 05/05/2014، على الموقع: [https://seconf.wordpress.com]

المبحث الثالث: أبرز الحروب السيبرانية ودرجات تأثيرها

لقد خلق الفضـــاء الســـيبراني جيل جديد من الحروب، والتي كانت نتيجة التطور التكنولوجي والتقني وتوظيفها في جميع المجالات، وهذا الاتساع والتطور المستمر خلق حروب سيبرانية وعلى قدر درجة تأثيرها استطاعت اختراق سيادة الدول، أو تعطيل قطاعاتها الحيوية أو تدمير شبكاتها.

المطلب الأول: الحرب السيبرانية الباردة المنخفضة الشدة

يتم استخدام الفضاء السيبراني كساحة للصراع منخفض الشدة، فهو صراع مستمر بين فاعلين متنازعين وذو طبيعة ممتدة ودائمة النشاط العدائي الغير سلمي، بخلاف أنه عميق الجذور ونواحي متعددة ثقافية، اقتصادية، اجتماعية، وعادة ما يتم اللجوء إلى القوة الناعمة للحروب السيبرانية في مثل هذه الصراعات[1].

وللحرب السيبرانية الباردة وسائل عدة، منها الحروب النفسية، و الاختراقات المتعددة، والتجسس وسرقة المعلومات، وشن حرب الأفكار والتنافس بين الشركات التكنولوجيا العالمية، وأجهزة الاستخبارات الدولية، ويتجلى هذا النمط من الحروب في الصراعات السياسية ذات البعد الاجتماعي الديني الممتد مثل: الصراع العربي الإسرائيلي، أو الصراع الهندي الباكستاني، أو الصراع بين الكوريتين الشمالية والجنوبية .كذلك هناك حروب تشتها جماعات دولية للقرصنة للتعبير عن مواقف سياسية أو حقوقية مثل: جماعة "ويكيليكس" و "أونيموس" وكذلك في الأزمات الدولية كالتوتر بين إستونيا وروسيا في عام 2007، وكذلك الاختراقات المتبادلة بين الصين والولايات المتحدة الأمريكية، والصراع بين إيرانوإسرائيل مثل شن هجمات فيروس "ستكسنت" ضد المنشآت النووية الإيرانية بالتعاون مع الولايات المتحدة الأمريكية في نوفمبر 2010[2].

وقد تعرضت روسيا للاتهام بالقرصنة في الانتخابات الرئاسية الأمريكية الأخيرة، وذم المرشح الجمهوري "دونالد ترامب" في مواجهة منافسته الديمقراطية هيلاري كلينتون والتسلل إلى خوادم البريد الإلكتروني للجنة الوطنية الديمقراطية، كما تم اختراق البريد الإلكتروني الخاص بجون بوديستا رئيس الحملة الانتخابية الرئاسية لهيلاري كلينتون، وعلى إثرها تم طرد 35 دبلوماسياً روسياً[3].

كما قامت روسيا بشن هجمات سيبرانية على النرويجوالتشيك، وبريطانيا، مما دفع الدول الأخيرة الى إعلان أنها قادرة على الرد بالمثل وقد تعرض العالم لعدد من الهجمات مثل هجمات فيروس "شمعون 2" ضد السعودية من طرف إيران وشن الهجوم على المنشآت النفطية في المنطقة الخليج، وتدمير 35 ألف جهاز

---

[1] عادل عبد الصادق، الهجمات السيبرانية أنماط وتحديات جديدة للأمن العالمي، الموسوعة السيبرانية الجزائرية، العدد 18601، يوم: 27/11/2019، على الموقعhttps://www.politics-dz.com. 15:30-15.03.2025

[2] عادل عبد الصادق، نفس المرجع.

[3] رفيدة البري، الدرع السيبراني: المفهوم والإشكالات والمنظمات، الموسوعة الجزائرية لدراسات السياسية والإستراتيجية، العدد 4741، نشر يوم: 27/11/2019، على الموقع.https://www.politics-dz.com. الاطلاع :16:00-15.03.2025

كمبيوتر في شركة النفط "أرامكو" لتخريب صادرات النفط وهجوم فيروس "وينا كراي" في عام 2017، والذي أتى به كوريا الشمالية[1].

المطلب الثاني: الحرب السيبرانية متوسطة الشدة.

يتجلى هذا الصراع في الفضاء السيبراني إلى الساحة الدولية موازياً لحرب تقليدية دائرة على الأرض، ويكون ذلك تعبيراً عن وحدة الصراع القائم بين الأطراف، كما أنه يمهد لعمل عسكري وهنا تدور الحروب في الفضاء السيبراني عن طريق اختراق المواقع وتخريبها، وشن حرب نفسية ضد الخصوم، ويستمد هذا النوع من الحروب السيبرانية قوته من قوة أطرافه، وارتباطها بعمل عسكري تقليدي في ظل بعض التقديراتإلى أن تكلفة هذه الحروب قد تشكل أربعة أضعاف من إنفاق نظيراتها التقليدية، كما تقدر تكلفة تمويل حرب كاملة سيبرانية بتكلفةدبابة.

وتاريخياً تم استخدام الحروب السيبرانية متوسطة الشدة في هجمات حلف الناتو NATO في عام 1999 على يوغوسلافيا، حيث استهدفت الهجمات تعطيل شبكات الاتصالات للخصوم[2].

وأيضا برزت خلال الحرب بين (حزب الله وإسرائيل) عام 2006، وكذلك بين (جورجيا وروسيا) في عام 2008، والمواجهات بين حركة المقاومة الفلسطينية (حماس) وإسرائيل في عام 2008-2012.

المطلب الثالث: الحروب السيبرانية مرتفعة الشدة.

ينشأ هذا النمط في الفضاء السيبراني منفرداً، ومتوازياً مع الأعمال العسكرية التقليدية، ولم يشهد العالم هذا النوع من الحروب، وإن كانت احتمالات حدوثها واردة في المستقبل مع تطور القدرات التكنولوجية، واتساع الاعتماد بين الدول والفاعلين من غير الدول على الفضاء السيبراني.

وينطوي هذا النوع من الحروب على سيطرة البعد التكنولوجي على إدارة العمليات الحربية، حيث يتم استخدام الأسلحة السيبرانية (الإلكترونية) ضد منشآت العدو، وكذلك اللجوء إلى الروبوتات الآلية Robots Automation في الحروب بدون طيار Drone، والتي فرضت نفسها في الآونة الأخيرة كسلاح فعال متعدد المهام في المعارك الحربية. وسعت الدول لامتلاكها وذلك لأهميتها في توجيه ضربات موجعة للعدو بتكلفة منخفضة وإدارتها عن بعد بخلاف تطوير القدرات في مجال الدفاع والهجوم السيبراني في الاستحواذ على القوة السيبرانية.

[1] عادل عبد الصادق، مرجع سابق.

[2] Robert MC Muller. Was Stuxnet built to a hack Iran nuclear program.

وفي هذا السياق يتم أيضاً استخدام الفضاء السيبراني للاستعداد لحرب المستقبل، وهذا بقيام الدول بتدريبات على توجيه ضربة أولى لحواسيب العدو، واختراق العمليات العسكرية عالية التقنية، والبنية التحتية المعلوماتية، والهدف من هذا هو تحقيق "الهيمنة السيبرانية الواسعة" بشكل أسرع في حالة نشوب صراع[1].

ولقد شهدت الأسلحة في هذا المجال تطورا أكبر في قدرتها على التأثير في الخصوم، مثل أسلحة الميكروويف عالية القدرة، وهو ما قامت به إسرائيل وبالتعاون مع الولايات المتحدة الأمريكية بشن هجمات فيروس "ستكسنت" ضد المنشآت النووية الإيرانية في عام 2010.

[1]Florian Bieber, cyber war or sideshow the internet and the Balkan wars, current history, 99, no, 635, (Mars 2000): :124128, online e-article, in the site
http://search.proquest.com/docview/200751259accountid=7180] .2

الشكل (05) : أبرز الهجمات السيبرانية و خصائص تحديد مصادرها

الحادث	السنة التي بدأت بها	التأثير	تحديد المصدر في النطاق العام
مختبر لورنس بيركلي الوطني (الولايات المتحدة)	1986	اختراق بيانات حساسة واستخراجها	محاكمة جنائية في ألمانيا الغربية، 1990
تايتن ران (Titan Ran) (الولايات المتحدة)	2003	استخراج بيانات حساسة من منظمات تشمل وكالة ناسا (NASA)، ولوكهيد مارتن ومختبرات ساندیا الوطنية (Sandia Laboratories National) ومكتب التحقيقات الفيدرالي فضلا عن وزارتي الدفاع الأمريكية والبريطانية Lockheed Martin	عزته الحكومة والمصادر الخاصة في وسائل الإعلام بدرجة كبيرة إلى الصين في عام 2005 وهو ما عارضته الدولة الصينية.
هجمات القطع الموزع للخدمة الإستونية (إستونيا)	2007	هجمات قطع موزع للخدمة واسع النطاق على المو اقع الإلكترونيةالإستونية في إطار التوترات مع روسيا	اتهمت الحكومة الإستونية جهات فاعلة حكومية روسية ألقت روسيا باللائمة على حركة شبابية مؤيدة للكرملين وليس على جهات فاعلة ترعاها الدولة
دودة ستكسنت(إيران)	2010	أضرار مادية بأجهزة الطرد المركزي الإير انية أصيبت بها أجهزة الكمبيوتر عالميا	عزي بالدرجة كبيرة إلى الولايات المتحدة وإسر ائيل، تسريبات من قبل مسؤولين أمريكيين

هجمات القطع الموزع للخدمة على المصارف الأمريكية (الولايات المتحدة)	2012	هجمات القطع الموزع للخدمة على أكثر من 46 من المؤسسات المالية في الولايات المتحدة	تصورواسع لرعاية الدولة الإير انية، تسريبات أولية من الحكومة الأمريكية وفي نهاية المطاف اتهام الجهات الفاعلة الحكومة الإير انية في أذار(مارس) 2016
أرامكو السعودية (السعودية)	2012 و2016	مسح 35000 جهازكمبيوتر تابع لأرامكو السعودية أو تدميرها: هجوم مماثل في أواخر عام 2016	في عام 2012 ربط مسؤولون أمريكيون الهجوم بإيران في وسائل الإعلام
حساب وكالة أسوسيتد برس (Associated Press) على تويتر (Twitter) (الولايات المتحدة)	2013	قرصنة وكالة أسوسيتد برس على تويترونشر تغريدة كاذبة عن هجوم على البيت الأبيض ما أدى إلى هبوط حاد في أسعار الأسهم	تبني الجيش السوري الإلكتروني Syrian Electronic Army الهجوم
البيت الأبيض ووزارة الخارجية (الولايات المتحدة)	2014	اختراق كبير لأنظمة الكمبيوتر غير السرية	عزي بدرجة كبيرة روسيا ولكن لم تحدد الحكومة الأمريكية رسميا المصدر
سوني بكتشرز(Sony Pictures) (الولايات المتحدة)	2014	سرقة بيانات حساسة وتسريبها تعطيل كبير لأعمال	عزاها الرئيس الأمريكي إلى جهات فاعلة حكومية كورية الشمالية في كانون الثاني (ديسمبر) 2014 وعزتها عملية أوبريشن بلوكبوستر (operation blockbuster) إلى مجموعة لازاروس (Lazarus) في عام 2016
غيت هاب (GitHub)(الولايات المتحدة)	2015	هجوم قطع موزع للخدمة كبيرومتواصل على موقع التعاون لتطوير البرمجيات	عزته الشركات الخاصة والباحثون بدرجة كبيرة إلى جهات فاعلة حكومية صينية

قناة TV5 Monde (فرنسا)	2015	تعطيل القناة التلفزيونية لمدة 18 ساعة، أدى الحادث المموه إلى الإلقاء باللائمة على داعش	عزته شركة فاير أي لمجموعة القرصنة الروسية APT28 في حزيران (يونيو) 2015
المكتب الأمريكي لإدارة شؤون الموظفين (الولايات المتحدة الأمريكية)	2015	استخراج 21.5 مليون سجل خاص بموظفي حكومة الولايات المتحدة	عزى بدرجة كبيرة إلى الصين علما أن الحكومة الأمريكية لم تحدد رسميا المصدر
البرلمان الألماني (ألمانيا)	2015	استخراج ونشر 2420 ملفا حساسا ينتمي للاتحاد الديمقراطي المسيحي الألماني (Democratic Union Christian)	عزاه المكتب الفيدرالي لحماية الدستور(BFV) لمجموعة APT28 في وسائل الإعلام في أيار(مايو) 2016
شبكة الكهرباء الأوكرانية (أوكرانيا)	2016	انقطاع الطاقة لساعات متعددة في محطات توزيع الطاقة الإقليمية وقطع الكهرباء عن 225000 مستهلك	اتهم مسؤولون أوكرانيون روسيا، أشارت شركات خاصة إلى جهات فاعلة حكومية محتملة أو مبرمجين إلكترونيين
اللجنة الديمقراطية الوطنية (DNC) (الولايات المتحدة)	2016	استخراج وثائق خاصة باللجنة الديمقراطية الوطنية والحملة الانتخابية ونشرها، تدخل بالانتخابات الرئاسية الأمريكية في عام 2016	عزته شركة كراود ستر ايك (CrowdStrike) حزيران -يونيو 2016 وتقرير مكتب الاستخبارات القومية الأمريكي كانون الثاني (يناير) 2017 إلى جهات فاعلة في الحكومة الروسية

الناطور المركزي في بنغلاديش	2016	سرقة مبلغ 81 مليون دولار من حساب البنك المركزي في بنغلاديش لدى البنك الاحتياطي الفيدرالي في نيويورك باستخدام نظام جمع الاتصالات السلكية واللاسلكية بين المصارف على مستوى العالم في الميدان المالي المصرفي (SWIFT).	ربطه تقرير شركة سيمانتيك بمجموعة لازاروس في أيار (مايو) 2016، وربطه تقرير وكالات الاستخبارات الأمريكية بدولة كوريا الشمالية وفقاً لوسائل الإعلام في آذار (مارس) 2017.
موساك فونسيكا (Mossack Fonseca)	2016	تسريب 11.5 مليون وثيقة تمثل أكثر من 214,488 كياناً خارجياً أدت إلى تهم عديدة بالتهرب الضريبي والفساد.	لم يحدد مصدر حتى تاريخه؛ نشطاء محتملون من القراصنة الإلكترونيين أو عملية داخلية.
دين (Dyn) (الولايات المتحدة)	2016	هجوم قطع موزع للخدمة باستخدام شبكة مصابة من أجهزة إنترنت الأشياء استهدف مزود نظام أسماء النطاقات دين وعطل عدداً كبيراً من المو اقع الإلكترونية.	لم يحدد المصدر رسمياً؛ عزي بدرجة كبيرة إلى منظمة قرصنة ناشطة مثل أنونيموس (Anonymous) أو نيو وورلد هاكرز (New World Hackers) أو سباين سكواد (Spain Squad)
و اناكراي (عالمياً)	2017	هجوم برنامج فدية مال قطاعي الرعاية الصحية والنقل والبنية التحتية للاتصالات في جميع أنحاء العالم.	لم يحدد المصدر رسمياً؛ ربطته بعض الشركات الخاصة بمجموعة لازاروس ألقت روسيا باللائمة على الولايات المتحدة لابتكارها برمجية (إكسبلويت) القادرة على تدمير برنامج و اناكراي

المصدر: مؤسسة ميكروسفت، نشرته مؤسسة راند RAND على موقعها الالكتروني

www.rand.org/t/RR20181

خلاصة الفصل:

نستخلص في نهاية هذا الفصل أن الحروب السيبرانية اليوم تشكل تحديات أمنية جديدة على الأمن العالمي، والأمن السيبراني بالخصوص، وأنها حرب خفية تقاد في الظل وعبر شاشات الحواسيب، وفرضت سيطرة عالمية جديدة، سلاحها الإنترنت، وفضاؤها قائم على التكنولوجيا، اقتحمت الأنظمة الإلكترونية، وانتهكت البيانات الشخصية، ونسفت العمل العسكري، واستهدفت السياسة والاقتصاد والمجتمع، فخرقت الحدود الجغرافية واعتدت على سيادة الدول، وبالتالي هي حروب لا يرى فيها المهاجم المدافع عدو مجهول، وأننا اليوم أمام أخطر حروب العالم، إنها القوة الجديدة، وبات الصراع في هذا الفضاء ساحة مفتوحة المعارك بين كل اللاعبين سواء من دول أو من غير الدول، ويرى الأكاديميون أن الحروب السيبرانية قد تكون حروب المستقبل.

الفصل الثالث

آليات مواجهة الحروب السيبرانية

تمهيد

أمام التنامي السريع للحروب السيبرانية و تزايد تهديداتها للامن القومي و الدولي، برزت حاجة ملحة لتبني آليات فعالى لمواجهتها و الحد من آثارها، فقد باتت الهجمات السيبرانية تشكل تحديا متزايدا للدول، لا سيما في ظل ضعف الحدود التقليدية لهذا النوع من الحروب و اعتمادها على أدوات تكنلوجية يصعب تتبعها أو ردعها بالوسائل التقليدية.

يتناول هذا الفصل السب التي اعتمدتها الدول و المنظمات الدولية لمواجهة الحروب السيبرانية، من خلال استعراض الجهود الوطنية و الدولية المبذولة في هذا المجال إضافة الى تسليط الضوء على طبيعة الاستراتيجيات السيبرانية المعتمدة كوسيلة للردع و التامين الرقمي.

المبحث الأول: جهود الدول لمواجهة الحروب السيبرانية.

تعد ساحة الفضاء السيبراني اليوم أرضية للتفاعلات الدولية والحروب السيبرانية بين الدول، والتي تحدق بالمجتمع والدولة، نتيجة سهولة الهجوم وصعوبة الدفاع، وفي هذا الإطار تحاول العديد من الدول بذل الجهد في تطوير قدراتها والإجراءات الكافية لحماية بنيتها التحتية المعلوماتية، سواء في الجانب التقني أو الجانب القانوني.

المطلب الأول: الجهود الوطنية لتأمين الفضاء السيبراني.

أولاً: وضع التشريعات الوطنية للأمن السيبراني

وضعت العديد من الدول قوانين ونصوص تشريعية لمواجهة الحروب السيبرانية، وهذا بعد أن ظهر جلياً مدى خطورتها والخسائر الناتجة عنها، وأجمع الكل على أن هذه الحروب أو التهديدات ما هي إلا تعدي على الآخرين وعلى الممتلكات الخاصة والعامة للأنظمة بواسطة استخدام التقنية، وكان الجزء الأكبر من هذه القوانين عقوبات رادعة[1].

وتعتبر الولايات المتحدة الأمريكية في تشريعاتها حول الأمن السيبراني، من أهم المبادرات في العالم التي تعالج مشكلة التهديدات، وذلك بربطها مباشرة بالإرهاب.

بالإضافة إلى أن معظم الدول الأوروبية، والأسيوية، والعربية، وغيرها من دول العالم التي أضافت إلى قانونها الجزائي ملحقاً خاصاً لمكافحةالجريمة السيبرانية (مثل الجزائر)، ويمكن ذكر ثلاث دول عربية فقط سنت قوانين مستقلة لمكافحة الجرائم السيبرانية، وهي (السعودية، عمان، الإمارات العربية المتحدة)، هذه الأخيرة تعتبر رائدة في إصدار التشريعات التي تخص الأمن السيبراني، حيث صدر قانون مكافحة الجرائم السيبرانية عام 2012، ثم تم تعديله في عام 2016، وقد دعم بمجموعة من السياسات التنظيمية والمعايير الفنية اللازمة لحماية النظم الحساسة والبنية التحتية والبيانات، فضلاً عن حماية المستخدمين[2].

ثانياً: تشكيل هيئات وطنية للأمن السيبراني.

من المعروف أن الحروب السيبرانية لا تفرق بين ما هو مدني وعسكري، بدأت الدول في تشكيل هيئات مختصة في تأمين السيبراني، وتكون مهمتها:

- ✓إعداد استراتيجية وطنية للأمن السيبراني،والسهر على تنفيذها.
- ✓ وضع السياسات وآليات الحوكمة والإرشادات المتعلقة بالأمن السيبراني وتعميمه.
- ✓وضع أطر إدارة المخاطر المتعلقة بالأمن السيبراني.
- ✓وضع أطر الاستجابة للحوادث والاختراقات.

---

[1]حسين بن احمد الشهري، الإرهاب الالكتروني – حرب الشبكات- المجلة العربية الدولية للمعلوماتية 2015 ص19

[2]فاروق حاتم، الإمارات تتقدم في إصدار تشريعات الأمن السيبراني، جريدة الاتحاد.على الرابط

http://www.alittihad.ae/details.php?id=66522&y=2017&article=full تاريخ النشر 2017/11/08 تاريخ الاطلاع:2020/07/05

✓وضع السياسات والمخاطر الوطنية للتشفير.

✓رفع مستوى الوعي بالأمن السيبراني.

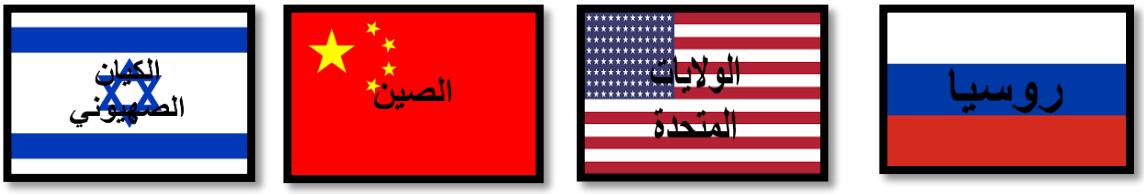
ثالثاً: بناء الجيوش السيبرانية

لقد نتج عن التطور السريع للتكنولوجيا، قوة جديدة في الفضاء السيبراني والحروب الخفية، عبر شاشة الحاسوب، شكلت تحدياً لمفاهيم جديدة للأمن القومي للدول، وأصبح الدفاع عن البنية التحتية المعلوماتية ذات الأهمية القصوى، وعليه سعت معظم الدول إلى تشكيل جيوشسيبرانية ورصدت لها ميزانيات ضخمة لتطوير هذا المجال الحساس والمهم، وهدفها هو الهجوم والدفاع والحماية.

وحسب الوكالة الروسية للاستشارات الأمريكية "زيكوريون" فإن الولايات المتحدة الأمريكية تنفق أكثر من أي بلد في مجال الفضاء السيبراني، فوزارة الدفاع لديها ميزانية ضخمة سنوية تقدر بـــ 07 مليارات دولار للأمن السيبراني، وعدد الموظفين المختصين يبلغ أكثر من 9000 موظف، وتنفق كل من الصين والمملكة المتحدة سنويا 1.5 مليار دولار و 450 مليون دولار، على التوالي.

وخصصت كوريا الشمالية نحو 20% من الميزانية العسكرية للأمن السيبراني ويحتل الجيش السيبراني الروسي المرتبة الخامسة في العالم، وتظهر التقارير أن قوات الأمن السيبراني الروسية وصلت إلى 1000 موظف، وتخصص وزارة الدفاع الروسية حوالي 300 مليون دولار سنوياً على مثل هذه الأنشطة[1].

وحسب القناة الاخباريةCNBC عربية فإن أقوى قدرات العالم في الفضاء السيبراني:



الوحدة العسكرية الالكترونية Cyber command مجموعة شنغهاي تلبيوت

المطلب الثاني: الجهود الدولية السلمية لتأمين الفضاء السيبراني

أولاً: الحد من سباق التسلح السيبراني

يلعب التسلح أهمية استراتيجية في توازن القوى على المستوى العالمي، في ظل بيئة مبنية من المصالح ويسودها الشك والغموض. وتدمير تلك المصالح بسرعة الضوء، وهو ما يحمل خطورة عسكرة الفضاء السيبراني، الأمر الذي جعل كثيرا من الدول تتبنى استراتيجية الحروب السيبرانية كحرب للمستقبل. وأن النصر في المعركة حليف من يقدر على شل القوة والتشويش على المعلومة .

[1]أفضل خمسة جيوش الكترونية في العالم، مركز الدراسات .

لقد بدأ سباق تسلح خطير لتطوير الأسلحة السيبرانية، وكانت بداية ظهورها بحسب المختصين في الصراع الروسي – الإستوني، والروسي – الجورجي، والتطور البارع مع فيروس "ستكسنت" الموجه ضد المنشآت النووية الإيرانية، والذي اهتمت بتطويره إسرائيل والولايات المتحدة الأمريكية.

واتجهت الدول لتعزيز قدراتها السيبرانية سواء في مجال الدفاع أو الهجوم أو الردع، إضافة إلى حماية بنيتها التحتية المعلوماتية، وهذا من خلال السعي إلى امتلاك التكنولوجيا وأنظمة عمل على تحقيق التفوق التقني.

وعليه فإن مشكلة سباق التسلح السيبراني تكمن في تحديد ماهية الأسلحة، وعدم السماح للمجتمع الدولي أن يمتلك تلك الأسلحة والتقدم في مجالها.

وحسب جوزيف ناي انه يمكننا أن نتعلم من تاريخ العصر النووي، في حين أن التكنولوجيات السيبرانية والنووية تختلفان اختلافا كبيرا، فإن العملية التي يتعلم المجتمع من خلالها التعامل مع تكنولوجيا شديدة التعطيل تظهر تشابها مفيدا. ولقد استغرق عقدين من الزمن للوصول إلى اتفاقيات تعاونية في العصر النووي وفي المجال السيبراني اقترحت روسيا عام 1999 معاهدة للأمم المتحدة لحظر الأسلحة الإلكترونية والمعلوماتية (بما في ذلك الدعاية)، ثم واصلت مع الصين وغيرها من أعضاء منظمة شانغهاي للتعاون، من أجل اتفاقية عامة منبثقة عن الأمم المتحدة .

اعتبرت الولايات المتحدة الأمريكية هذه الاتفاقية محاولة للحد من القدرات الأمريكية، ولا تزال تعتبر هذه الاتفاقية مظلة ولا يمكن التحقق منها، واتفقت الولايات المتحدة الأمريكية وروسيا وعدد من الدول على أن يعين الأمين العام للأمم المتحدة مجموعة من الخبراء الحكوميين والتي اجتمعت في عام 2004.

ولقد أسفرت أعمال تلك المجموعة في البداية عن نتائج هزيلة، ولكن بحلول جوان 2015 أصدرت تقريراً أقرته مجموعة العشرين بقضيبوضع معايير للحد من الصراع وأخرى لبناء الثقة .

وعلى الرغم من صعوبة عملية الرقابة والتفتيش على الأسلحة السيبرانية، فإن السعي نحو الحد من انتشار هذه الأسلحة، يتطلب وجود إطار دولي تشارك فيه العديد من الدول والجماعات عبر العالم إلى جانب وجود إطار قانوني دولي يحدد الالتزامات والواجبات لجميع الفاعلين في هذا الفضاء.

ثانياً: قانون (دليل) تالين:

هناك صعوبة في الحد من سباق التسلح السيبراني من جهة، وقصور القانون الدولي في هذا المجال، نتيجة عدم وجود أساس قانوني ينظم اللجوء إلى الحروب السيبرانية من جهة أخرى، تم إبرام صك قانوني عام 2013 يدعى "دليل تالين" الذي أعدته مجموعة من الخبراء في القانون الدولي بدعوة من حلف شمال الأطلسي NATO قصد دراسة مدى إمكانية تطبيق قواعد النظام الدولي الإنساني على الحروب السيبرانية، وذلك إثر الهجوم السيبراني الشامل على إستونيا عام 2007 من طرف روسيا [1].

ويحتوي دليل "تالين" على 95 قاعدة قانونية إرشادية، لعمل أو سلوك الدول في سياق الحرب السيبرانية (الإلكترونية)، وصدر الإصدار الثاني في العام 2017، ويحتوي على 154 قاعدة، ليشكل مستوى أكثر اتساعاً لمعالجة العمليات الإلكترونية، ومراجعة وحسم لنقاط عدم الاتفاق في الإصدار الأول[2] .

وتتمثل تحدياته الرئيسية في ضمان توجيه الهجمات ضد الأهداف العسكرية فقط، وتوخي الحذر لحقن دماء المدنيين وحماية البنية التحتية المعلوماتية لحياتهم، وهذا لوجود فضاء سيراني واحد تتقاسمه الجيوش المسلحة والجيوش السيبرانية مع باقي المستخدمين المدنيين. كما يجب التركيز على أهم النقاط الحساسة المرتبطة بالحروب والهجمات السيبرانية، سواء تنفذها دول أو من غير الدول، وكيفية إدارة الحروب السيبرانية والصراع في الفضاء السيبراني، بالإضافة إلى مراعاة القانون الدولي الإنساني كمبدأ التمييز، والشرعية في استهداف المقاتلال سيبراني بالوسائل العسكرية المادية كالطائرات العسكرية بدون طيار Drones.

ويعتبر دليل "تالين" الهجوم السيبراني على أنه "عملية إلكترونية سواء هجومية أو دفاعية يتوقع أن تسبب في إصابة أو قتل أشخاص أو الإضرار بأعيان أو تدميرها". ولكن لم يتفق الخبراء حول "الضرر" بحسب إقرار كل بلد بحجم الأضرار التي تبرر خوض الحرب. وهو ما يعرف بمبدأ الحق في اللجوء إلى الحرب " jus in bellum" بشرط تكون مشروعة وعادلة. لكن تضفي عليها صفة الشرعية [3].

ثالثاً: الاتفاقيات الإقليمية والدولية لأمن الفضاء السيبراني.

نظراً لخطورة وسرعة التهديدات السيبرانية ومواكبة مع تطورها، تتطابق الاتفاقيات الإقليمية والدولية معها، ونذكر عدد من المبررات منها[4]:

[1] [1]جوزيف س.ناي، التحكم في الصراع السيبراني، مدونات الجزيرة، على الرابط : http://blogs.aljazeera.net/blogs/2017

[2] سعيد درويش، ماهية الحرب الألكترونية في ضوء قواعد القانون الدولي، حوليات جامعة الجزائر 1 العدد 29 ص119.

[3] عمر شهرزاد، الإدارة الدولية للتهديدات اللاتماثلية- الأمن السيبراني انموذجا، محاضرة مقدمة لطلبة السياسة الدولية، ماستر 2 ، الموسوعة الجزائرية للدراسات السياسية والاستراتيجية، العدد 10831 تاريخ النشر: 2019/11/27

[4]اللجنة الدولية للصليب الأحمر، ماهي القيود التي يفرضها قانون الحرب على الهجمات السيبرانية على الرابط

- في عام 2002 وضـــعت مجموعة بلدان الكومونولث قانوناً نموذجياً لمكافحة الجريمة الســيبرانية بالإضافة إلى قانون الإثبات الرقمي.
- في عام 2009 بادرت المجموعة الاقتصادية لغرب إفريقيا، إلى إصدار توصية لمكافحة الجريمة السيبرانية.
- في عام 2011 الاتفاقية العربية لمكافحة الجرائم التقنية المعلوماتية، قصـــد تعزيز التعاون بين الدول العربية لمكافحة الجرائم السيبرانية والحفاظ على أمنها وسلامة مجتمعاتها.
- في عام 2001 شـكلت اتفاقية بودابســت بكتلالمجموعة من الخبراء الأوروبيين وغير الأوروبيين كالولايات المتحدة، وأفريقيا الجنوبية، واليابان، والتي عملت ضـــمن مجموعة لمكافحة الجريمة في الفضـــاء الســيبراني، ودخلت حيز التنفيذ في تموز 2004 وتعتبر هذه الاتفاقية أداة اقليمية ملزمة لمكافحة الجريمة السيبرانية، ولقد شددت على تحسين تقنيات التحقيق والبحث، وزيادة التعاون بين الدول[1].
- أما على المســتوى الدولي، فقد لعبت هيئة الأمم المتحدة عبر القرارات الصـــادرة عنها التي تدعم الأمن والسلام في الفضاء السيبراني، وتوعية الوعي العالمي للأمن السيبراني دوراً في جذب انتباه دول الأعضاء إلى أهمية التحديات السيبرانية.

ومن أهم قرارات الهيئة[2]:

- قرار صادر سنة 1990: حول قانون جرائم المعلوماتية.
- قرار صادر سنة 1991: حول مكافحة الاستخدام الجرمي لتقنيات المعلومات والاتصالات.
- عام 2001: إنشـــاء "مجموعة الخبراء الحكومية" GGE، بدأت عملها في 2004 لمناقشـــة الأخطار القائمة والمحتملة في مجال أمن المعلومات، والإجراءات الممكنة لوضـع الأسس الدولية التي تهدف إلى تقوية نظم الاتصالات والمعلومات العالمية.
- في العام 2003: صدر قرار خاص بالأمن السيبراني، ركز فيه على مكافحة الجريمة السيبرانية.
- في العام 2010: صـدر قرار حول الأمن السـيبراني، وملحق حول ضـرورة أن تلجأ الدول لمعرفة تناسب أطرها التشريعية وقدرتها على مكافحة الجريمة السيبرانية[3].

نظراً لخطورة وسـرعة التهديدات السـيبرانية ومواكبة مع تطورها، تتطابق الاتفاقيات الإقليمية والدولية معها، ونذكر عدد من المبررات منها[4]:

[1] سعيد درويش، ماهية الحرب الألكترونية في ضوء قواعد القانون الدولي، حوليات جامعة الجزائر 1 العدد 29 ص133.
[2] علي الأشقر جسور، السيبرانية هاجس العصر، مرجع سابق ص 103
[3] عادل عبد الصادق، الإرهاب الالكتروني في العلاقات الدولية: نمط جديد وتحديات مختلفة، مركز الأهرام للدراسات السياسة والاستراتيجية، القاهرة 2009 ص 334
[4] اللجنة الدولية للصليب الأحمر، ماهي القيود التي يفرضها قانون الحرب على الهجمات السيبرانية على الرابط

في عام 2002 وضعت مجموعة بلدان الكومونولث قانوناً نموذجياً لمكافحة الجريمة السيبرانية بالإضافة إلى قانون الإثبات الرقمي.

في عام 2009 بادرت المجموعة الاقتصادية لغرب إفريقيا، إلى إصدار توصية لمكافحة الجريمة السيبرانية.

في عام 2011 الاتفاقية العربية لمكافحة الجرائم التقنية المعلوماتية، قصد تعزيز التعاون بين الدول العربية لمكافحة الجرائم السيبرانية والحفاظ على أمنها وسلامة مجتمعاتها.

في عام 2001 شكلت اتفاقية بودابست بكتل المجموعة من الخبراء الأوروبيين وغير الأوروبيين كالولايات المتحدة، وأفريقيا الجنوبية، واليابان، والتي عملت ضمن مجموعة لمكافحة الجريمة في الفضاء السيبراني، ودخلت حيز التنفيذ في تموز 2004 وتعتبر هذه الاتفاقية أداة اقليمية ملزمة لمكافحة الجريمة السيبرانية، ولقد شددت على تحسين تقنيات التحقيق والبحث، وزيادة التعاون بين الدول[1].

أما على المستوى الدولي، فقد لعبت هيئة الأمم المتحدة عبر القرارات الصادرة عنها التي تدعم الأمن والسلام في الفضاء السيبراني، وتوعية الوعي العالمي للأمن السيبراني دوراً في جذب انتباه دول الأعضاء إلى أهمية التحديات السيبرانية.

ومن أهم قرارات الهيئة[2]:

- قرار صادر سنة 1990: حول قانون جرائم المعلوماتية.
- قرار صادر سنة 1991: حول مكافحة الاستخدام الجرمي لتقنيات المعلومات والاتصالات.
- عام 2001: إنشاء "مجموعة الخبراء الحكومية" GGE، بدأت عملها في 2004 لمناقشة الأخطار القائمة والمحتملة في مجال أمن المعلومات، والإجراءات الممكنة لوضع الأسس الدولية التي تهدف إلى تقوية نظم الاتصالات والمعلومات العالمية.
- في العام 2003: صدر قرار خاص بالأمن السيبراني، ركز فيه على مكافحة الجريمة السيبرانية.
- في العام 2010: صدر قرار حول الأمن السيبراني، وملحق حول ضرورة أن تلجأ الدول لمعرفة تناسب أطرها التشريعية وقدرتها على مكافحة الجريمة السيبرانية[3].

كما بذلت عدة جهود وبدعم من الاتحاد الدولي للاتصالات لإقرار مجموعة من المعايير والقواعد التي تضمن الاستخدام الآمن في المجال السيبراني.

لكن تبقى هذه الجهود رغم قيمتها غير كافية وغير ملزمة لعدم إلزاميتها القانونية، خاصة مع سيطرة الدول المتقدمة، وعلى رأسها الولايات المتحدة الأمريكية على الإنترنت.

---

[1] سعيد درويش، ماهية الحرب الألكترونية في ضوء قواعد القانون الدولي، حوليات جامعة الجزائر 1 العدد 29 ص133.

[2] علي الأشقر جسور، السيبرانية هاجس العصر، مرجع سابق ص 103

[3] عادل عبد الصادق، الإرهاب الالكتروني في العلاقات الدولية: نمط جديد وتحديات مختلفة، مركز الأهرام للدراسات السياسة والاستراتيجية، القاهرة 2009 ص 334

المطلب الثالث: التعاون الدولي لمواجهة الهجمات السيبرانية.

بذل المجتمع الدولي العديد من الجهود لحظر استخدام أسلحة الدمار الشامل، والتقدم في شأن المناطق الخالية من الأسلحة النووية، وكانت كذلك حتمية العلاقة بين الأسلحة والتقدم التكنولوجي، والتي أفرزت ثورة في الشؤون العسكرية، وظهور أسلحة الفضاء السيبراني وأصبحت لها أضرار هددت الأمن السيبراني.

ولقد طالت التهديدات السيبرانية الطابع المدني، مما استدعى الحاجة إلى تضافر الجهود الدولية من أجل العمل على تعزيز الأمن والحماية للفضاء السيبراني الإيجابي على السيادة الدولية، كإسهام تلك الاتفاقيات التي تحد من انتشار الأسلحة النووية، والكيميائية، والبيولوجية، حيث تسهم تلك الاتفاقيات في حال تطبيقها على الفضاء السيبراني والأسلحة التي يمكن أن تستخدم فيه، من خلال وضع قيود على استخدامها وتوزيعها وإنشائها وتطويرها[1].

ويجب على الدول أن توافق على خضوع الهجمات السيبرانية إلى القانون الجنائي الدولي ومحكمة العدل الدولية، رغم مواجهة تلك الاتفاقيات من تحديات جعلت الدول ترفض الموافقة على الاتفاقيات، على أساس أنها قيود تحد من قدرتها في تطوير الأسلحة الهجومية، في حال تعرضها للهجوم السيبراني، وأن الاتفاق يشمل الدول دون أطراف أخرى كالمنظمات الإرهابية والإجرامية التي لا تخضع لكل تلك القيود[2].

ومن ناحية أخرى أصبحت هناك صعوبة في الفصل بين الاستخدام المدني والعسكري، وهذا يتطلب على الدول من أجل تحقيق الأمن السيبراني الجماعي الدولي، أن يوجد ثقافة عالمية بأن السلام أمر غير قابل للانقسام أو التجزئة، وأن يكون النظام حيادياً وموضوعياً، وأن توجد قوة عسكرية رادعة للمخالفين لذلك النظام، كل هذا مع احترام حرية الأفراد وانتماءاتهم المتنوعة، وضرورة تشكيل تحالف عالمي لتعزيز السياسات المؤسسية التي تربط ما بين الأفراد والدول[3].

ولكي يتم خضوع الفضاء السيبراني للقانون الدولي، فلا بد من تغيير تنظيمي قانوني وسياسي وأمني وقائي شامل، وإطلاق حوار دائم يفرق بين الجريمة السيبرانية والإرهاب السيبراني، وما يمكن أن يدخل ضمن الاستخدام السلمي وأن يتم التمييز بينهما.

و لكي يتم التوصل إلى نظام قانوني عالمي يحكم الفضاء السيبراني يجب أن يتم تحديد[4] :

- ماهية وكيفية التغلب على العمليات العسكرية باستخدام هجمات الفضاء السيبراني.
- أن تكون الاتفاقية قادرة على تحقيق التوازن بين مبدأين أساسيين هما: مبدأ الضرورة العسكرية ومبدأ احتمالية الوقوع.
- التمييز بين الأهداف العسكرية والمدنية.

[1] على الأشقر ، مرجع سابق ص 104

[2] عادل عبد الصادق، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي، سلسلة أوراق، العدد 23، مكتبة الإسكندرية، مصر، 2016 ص152

[3] نفس المرجع ص 153

[4] المرجع السابق ص 153.

- التصديق على هذه المعاهدة من المحكمة الجنائية الدولية، حتى يتم تفعيل القانون الدولي لكي يتلاءم مع تلك الظاهرة.
- وسائل المنع أو الوقاية التي تستخدم في تطبيق أحكام القانون الدولي لصالح الضحايا أو يتم تطبيقها تطبيقا سلميا.
- وسائل الرقابة: وهي وسائل الإشراف المتواصل بما يتضمن الإلتزام السليم عند تطبيق الأحكام التي تتكفل بمصلحة الضحايا.
- العقوبات: وهي جزء لا يتجزأ من أي نظام قانوني سليم وذلك بسبب قيمتها الرادعة.
- ضرورة البحث عن وسائل أخرى كالأبعاد الاقتصادية والأمنية والثقافية.

جدول رقم (06): الدعامات الخمسة التي يرتكز عليها برنامج الأمن السيبراني العالمي.

	التدابير القانونية	التدابير الفنية	التدابير التنظيمية	
التعاون الدولي	تشمل الأهداف: وضع استراتيجيات لاستحداث تشريع نموذجي لمكافحة الجريمة السيبرانية قابل للتطبيق والاستخدام المتبادل عالميا	تشمل الأهداف: تقديم مقترحات لوضع إطار للحوار والتعاون والتنسيق على الصعيد الدولي	تشمل الأهداف: وضع استراتيجيات لإيجاد هياكل تنظيمة وسياسات عامة بشأن الجريمة السيبرانية والرصد والإنذار والاستجابة للحوادث ونظام هوية رقمي تنوعي عالمي	**4**
بناء القدرات	تشمل الأهداف: وضع استراتيجيات عالمية لبناء القدرات البشرية والمؤسسية في المجالات	تشمل الأهداف: وضع استراتيجيات لاستحداث إطار عالمي للبروتوكولات والمعايير وخطط الاعتماد الخاصة بالبرمجيات والمعدات في مجال الأمن		**5**
	1	**2**	**3**	

المصدر : أخبار الاتحاد الدولي للاتصالات،2010/10، على الموقع
www.itu.int/net/itunews/issues/2010/10dpf201010_39-ar

المبحث الثاني: المسؤولية الدولية للحروب السيبرانية.

تعد المسؤولية الدولية من أهم موضوعات القانون الدولي في الوقت الحاضر، وهذا نظراً لتأثيراتها البالغة في التطورات العلمية الحديثة على العلاقات الدولية، وما نتج عنها من تحديات جديدة أدت إلى ضرورة معالجتها بطريقة جديدة تتلاءم مع طبيعتها في ظل قانون دولي منظم.

المطلب الأول: أركان المسؤولية الدولية.

يفرض القانون الدولي التزاماته على أشخاصه الخاصون ومنهم الدول، أما القانون الداخلي يفرض على شخص. فالدولة التي تقوم بأي فعل يحدث ضرراً يصيب دولة أخرى أو عدة دول. فتتحمل الدولة التي أحدثت ذلك الضرر، أو تسببت في إحداثه، تبعاً للمسؤولية الدولية عن ذلك الفعل، فالحروب أو الهجمات السيبرانية يقوم بها أشخاص يخضعون للقانون الدولي، وتؤدي إلى ضرر وبذلك تكون الهجمات السيبرانية مستوفية شروط قيام المسؤولية السيبرانية، لكن نقص القواعد القانونية، وصعوبة الأدلة والإثبات لمصدر الهجمة يتعذر ذلك. ومن بين أركان المسؤولية الدولية نذكر ما يلي[1]:

1- نسبة الفعل إلى الدولة:

الفعل الضار هو الذي يفرض وجود المسؤولية، لأنه يستند إلى الدولة لا إلى شخص لا تقوم المسؤولية بمواجهته، كما يجب أن تكون الدولة كاملة السيادة، وهذا لكي تسأل عن أعمال سلطاتها الثلاث: التشريعية والتنفيذية والقضائية، وفي حالة الهجمات السيبرانية التي تستهدف البنى التحتية للدولة، سواء من طرف الدولة القومية، أو المنظمات الحكومية، إقليمية أو عالمية، وهنا يلصق الفعل بالدولة وتكون مسؤولة عن أفعال رعاياها في حالة التقصير.

2- أن يكون الفعل غير مشروع دولياً:

أجمع فقهاء القانون الدولي على أن الفعل غير المشروع هو الذي يتضمن مخالفة قواعد القانون الدولي، ومبادئه العامة، وهو سلوك منسوب إلى الدولة بالقيام بفعل، أو الامتناع عن القيام بالفعل، فمعيار المشروعية هو معيار دولي موضوعي، وأن الهجمات السيبرانية تعتبر مخالفة لقواعد القانون الدولي، لأنها تسبب أضرار مادية وبشرية كبيرة، وهذا مخالف لمقاصد الأمم المتحدة.

3- الضرر:

بعد هذا العنصر من أهم عناصر المسؤولية، لأنه إذا انعدم الضرر انعدمت المسؤولية، فهناك ضرر مادي وغير مادي، وضرر مباشر وغير مباشر، فنجد الضرر الذي خلفه الهجوم السيبراني على المفاعلات النووية الإيرانية والهجمات على البنوك ، وسرقة المعلومات كلفت تريليون دولار سنويا لكن رغم توافر أركان المسؤولية الدولية إلا أنه يصعب الكشف عن هوية الفاعلين.

[1] ياسين طلال السعدي، محمد عدي عنابا، المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر، مجلة الرفادة للبحوث والدراسات الإنسانية، العدد 01، المجلد 19، 2019 ص88

المطلب الثاني: الوصف القانوني للحروب السيبرانية.

القانون الدولي هو الذي يحكم أنشطة الدولة أينما كانت بما في ذلك الفضاء السيبراني، وأصبح العالم يواجه هجمات وحروب سيبرانية دولية جديدة، مما هدد أحد المبادئ الرئيسة للدول في القانون الدولي، وهو احترام سيادة الدول وعدم التدخل في شؤونها، والذي نصت عليه الفقرة الرابعة من المادة الثانية لميثاق الأمم المتحدة، وهذا نتيجة تسريب معلومات أمنية سرية عن حكومات الدول، وإمكانية إلحاق الضرر بالمدنيين، تعطيل أو تدمير المؤسسات والمنشآت الحيوية وشلها، كالمطارات والمستشفيات وشبكات النقل إلخ [1]...

ولهذا فقد اعتبر القانون الدولي الإنساني الحروب السيبرانية بأنها هجوم سواء كانت دفاعية أو هجومية، قد يتسبب في إصابة أو قتل الأشخاص أو تدمير وشل المنشآت[2]. هذا الوضع مناسب ويفيبالغرض، لكن يصعب على القانون التمييز في الهجمات السيبرانية ومصدرها، وبالتالي السؤال الذي يطرح هو أي نموذج قانوني يجب أن يضم إطاراً للهجمات السيبرانية؟ فهذا الطرح يثير بنقاش كبير ومحل اختلافات في مجال الحقوق القانونية والمسؤوليات التي تنتج عن الهجمات السيبرانية[3].

وأن مشروعية الأسلحة الجديدة تصب في مصلحة كافة الدول، حيث يساعدها في ضمان توافق سلوك قواتها المسلحة مع الالتزامات الدولية، إذ تلزم المادة الستة والثلاثين من البروتوكول الإضافي الأول لعام 1977م، كل دولة من الدول الأطراف التحقق من امتثال أي أسلحة جديدة تقوم بنشرها، أو تدرس نشرها لقواعد القانون الدولي الإنساني.

كما طالبت الدول الأطراف في اتفاقية "جنيف" أثناء المؤتمر الدولي الثامن والعشرين للصليب الأحمر والهلال الأحمر المنعقد عام 2003م، بأن تخضع جميع الأسلحة الجديدة ووسائل الحرب الجديدة وأساليبها للاستعراض الدقيق والمتعدد التخصصات". وذلك لضمان أن يخضع تطور التكنولوجيا للحماية القانونية المكفولة، وبعد استخدام العمليات السيبرانية أثناء النزاعات المسلحة، مثال جيد على هذا التطور التكنولوجي[4].

المطلب الثالث: التكييف القانوني للحروب السيبرانية.

لا يزال لمفهوم الحروب السيبرانية اختلافاً بيناً، وهذا ما أدى إلى أكبر تحدي يواجه القانون الدولي ويتجسد ذلك في ضرورة تكييف القوانين والبحث في مصدر التكييف وأساسه، والمعضلة الأمنية ستكون كبيرة فيها لو تم الإقرار بوجود فراغ قانوني، أي عدم وجود قواعد قانونية محددة تنظم الحروب السيبرانية أو الهجمات،

[1] ياسين طلال السعدي، محمد عدي عنابا، المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر، مجلة الرفادة للبحوث والدراسات الإنسانية، العدد 01، المجلد 19، 2019 ص87

[2] Philip levitz,the law of cyber Attack, 2012 vol 100 p833

[3] ياسين طلال السعدي، محمد مرجع سابق ص87

[4] احمد العبسي القنلاوي، الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق المحلي للعلوم القانونية والسياسية، العدد الرابع، الصنة الثامنة 2016 ص627

والسـؤال الذي يطرح هو: هل توجد قواعد واجبة التطبيق في ظل تزايد مخاطر الحروب السـيبرانية المهددة للأمن والسلم الدوليين؟[1]

ويرى المختصون بذات الصلة في هذا الموضوع، أن المبادئ والقواعد التي أرساها القانون الدولي الإنساني تنطبق على تلك الهجمات، وهناك من يرى العكس لأنها ذات صـلة باسـتخدام وسـائل وطرائق القتال، ولم تكن الوسائل الإلكترونية تستخدم لأغراض عسكرية، ما يعني أنها غير مقننة أصلاً[2].

وأن تكييف استخدام الحروب السيبرانية يدور في فرضيتين اثنتين، الأولى في عدم القدرة على إثبات الدليل المادي الناجم عن اسـتخدام الهجمات أو الحروب السـيبرانية. وهو العائق الأكبر الذي يواجه المختصـون، على عكس طرق ووسائل القتال المعروفة، والتي لها أثر مادي ملموس مباشر أو غير مباشر بعد الهجوم، كالدمار أو التعطيل الكلي أو الجزئي للمنشآت المدنية أو العسكرية، أو القتل والجرح الذي يصيب المقاتلين أو المدنيين[3].

أما الفرضـية الثانية فعلى العكس، إذ تثبت أن الحروب السـيبرانية قد تؤدي إلى آثار مادية ملموسـة على المستويات الاقتصادية والأمنية والعسكرية كافة[4].

فخطورة الحروب السـيبرانية لم تُحدد آثارها في ضـوء الاتفاقيات الدولية إما بالحظر أو التقييد، وبالتالي يمكن أن تطال آثار الحروب السـيبرانية وتؤدي إلى الدمار الشـامل لنواحي الحياة، وأن تكتم الدول المتقدمة وتفردها باستخدام الحروب السيبرانية، لأنها لا تحبذ من يطرح هذا الموضـوع في المنابر الدولية، لأنها هي المهيمنة على هذا القطاع الحيوي الهام الذي يخدم مصالحها ويديم أمنها القومي.

ونرى تأخر الدول في التوصل إلى اتفاقية دولية معنية بالحروب أو الهجمات السيبرانية، يعود بالذاكرة إلى الوراء، ما حصـل في موضـوع تأخر تنظيم حظر انتشـار الأسـلحة النووية لعام 1968 م، واتفاقية الحظر الشامل للتجارب النووية عام 1996 م.

ومن خلال ما تقدم يبدو أن العائق في تكييف الهجمات السـيبرانية بإحدى وسـائل وطرق القتال، إنما يعود لصـالح بعض القوى الرائدة في مجال اسـتخدامها، بالإضـافة إلى قدرة الأنظمة الإلكترونية في تحويل تلك الاستخدامات إلى برامج عدائية، وتحقيق أهداف سياسية.

[1] نفس المرجع السابق ص 628

[2] Emily hastam. Information warfare: technological changes and international law, journal of conflict and security law vol5 200 p 157

[3] Michael shmit, bellum American: the law of armed conflict into the next millenuim: newpost naval war college 1998 p 408

[4] احمد العبسي القنلاوي، مرجع سابق ص 629

المبحث الثالث: الإستراتيجية السيبرانية.

نظراً لخطورة الحروب السيبرانية وتحدياتها على الأمن القومي للدول، أصبح من الضروري وضع استراتيجية سيبرانية قوية دفاعية فعالة لحماية البنية التحتية المعلوماتية، ومواجهة هذه الحروب.

المطلب الأول: الدفاع السيبراني.

عموماً يشمل الدفاع السيبراني على ثلاث فئات متكاملة:

الدفاع السيبراني الاستباقي:

ويتمثل في الأنشطة التي تحمي البيئة السيبرانية بكفاءة عالية وتحافظ على البنية التحتية السيبرانية، والوظائف المهمة، من خلال الابتكار وتعزيز الفعل السريع أسرع من المنافسين الاستراتيجيين، وحماية الشبكات والأنظمة والبيانات، بالإضافة إلى مواكبة التهديدات والتكنولوجيات سريعة التطور في الفضاء السيبراني، والحفاظ على الأمن السيبراني من خلال تعزيز قدرة الدول، وبالتنسيق مع الحلفاء والشركاء على ردع ومعاقبة أولئك الذين يستخدمون الأدوات السيبرانية لأغراض ضارة.

الدفاع السيبراني النشط:

يوقف أو يحد من أضرار الهجوم السيبراني، وردع الأنشطة السيبرانية الضارة، باستخدام جميع أدوات القوة الوطنية لردع الأعداء عن القيام بأي نشاط ضار بالفضاءالسيبراني، وإعطاء الأولوية لتأمين معلومات وزارة الدفاع، كما يجب على الدولة حماية شبكاتها من خلال هيئاتها التشريعية. ليس أي ثغرات قائمة في قانون الإنترنت، وفهم طبيعة التهديدات فلا يمكن للمقاومة بشكل فعال دون فهم الخطر.

الدفاع السيبراني التفاعلي:

يعمل على استعادة الفعالية، أو الكفاءة بعد الهجوم السيبراني الناجح، وهذه الفئات تشكل سلسلة متصلة من أنشطة الأمن السيبراني التي تحدث بشكل مستمر وفي وقت واحد على الشبكات، ووضع سياسات لأمن المعلومات ومراجعتها بشكل دوري. زد على ذلك هيمنة التصعيد Escalation Dominance، من خلال القدرة على الجمع بين الوسائل السيبرانية، والأدوات العسكرية الأخرى للقيام بحرب أسلحة مشتركة.

وهذا النوع من الدفاعات تبنته الولايات المتحدة الأمريكية بعد 11 سبتمبر، وأجازت فيه أعمال دفاعية ضد أي خطر محدق بها. كما قامت إيران وكوريا الشمالية أيضاً بالاعتراف بهذا النوع من الدفاعات.

ولكن على الصعيد الدولي فقد امتنعت محكمة العدل الدولية عن إبداء رأي في هذا النوع من الدفاع بالرغم من أنها في قضائها سابقاً كانت تجعل التحقق من الهجوم ووقوعه شرطاً أساسياً لثبوت الحق في الدفاع[1].

[1] زينب شنوة، الحرب السيبرانية في العصر الرقمي حروب ما بعد كلافويتشن، المجلة الجزائرية للأمن والتنمية، العدد 02، المجلد 09، جويلية 2020 ص 101

المطلب الثاني: مشروعية الرد على الهجوم السيبراني

نص المبدأ الثامن عشـــر (18) المتعلق بمجلس الأمن الدولي أن لمجلس الأمن الدولي أن يقرر وفقاً للفصل السابع إن كان أي نشاط سيبراني يمكنه أن يهدد الأمن الدولي، أو يشكل عملاً من أعمال العدوان، كما أجاز المبدأ الخامس والتسعون (95) لمجلس الأمن الدولي أن يتحرك بموجب الفصل السابع من ميثاق الأمم المتحدة، في حالة الحرب السيبرانية أيضاً، لا سيما إذا خرقت دولة من الدول السلم والأمن الدوليين، أو لم تلتزم بواجب الحياد في أي حرب سيبرانية[1].

وفي هذا الصـدد، فإن دليل "تالين" يمنح الحق بشـن الهجوم المسـلح بعد الاعتداء، وهذا بعد أن أصـبحت الحروب السـيبرانية تندلع ضـمن سـاحات رقمية في عالم افتراضـي، مما قد تسـبب هذه الحروب في احتدام الصـراع ويتحول سريعاً إلى حرب حقيقية بالقنابل والصـواريخ، لأن القادة العسكريين يمكن أن يفسروه بدعوة إطلاق أول ضربة استباقية في الحرب السيبرانية.

وحتى يكون هذا الرد قانونيا ينطبق عليه صـــفة الدفاع الشـــرعي، وبالتالي على الدولة المعتدى عليها أن تنوي الرد أن تحسـب المنفعة التي تكمن في هذا الهجوم العسـكري مقابل الهجوم السـيبراني الذي تعرضـت إليه أنظمتها والمنشـآت التابعة لها[2]. فالمادة (48) من الملحق الإضـافي— لاتفاقية "جنيف" تحدد الأهداف التي تسـتطيع الدولة اسـتهدافها، وفي الأهداف العسـكرية حصـرا، ومنعت اتفاقية "لاهاي" الرابعة تدمير أو مصـادرة ممتلكات المدنيين، وبالتالي انتهاك هذه القوانين يعتبر جريمة دولية، يعاقب عليها في اتفاقية "روما" المنشئة للمحكمة الجنائية الدولية[3].

ويرى فقهاء القانون الدولي أن حالة التناسـب تعرض مصـالح وأرواح المدنيين للخطر، ويتسـبب الهجوم السـيبراني بتعطيل الأنظمة للبنية التحتية كالمسـتشـفيات والمطارات، وهذا يتنافى مع مبادئ القانون الدولي الإنساني[4].

لذا يجب على الدولة اســـتخدام القوة في الرد على الهجوم الســـيبراني أن تميز بين الأهداف العســـكرية والأهداف الحكومية الأخرى (المدنيين والمقاتلين)، دون تدمير المنشـــآت الحيوية لدولة المعتدية، ولا تهاجم مصالح المدنيين تطبيقا لمبدئ المساواة الإنسانية.

المطلب الثالث: مصير سيادة الدول في ظل الحروب السيبرانية.

تعد فكرة الســـيادة والاعتراف بها للدول من المبادئ المتفق عليها في ميثاق الأمم المتحدة والاتفاقيات الدولية، ومنه السـيادة في حق الدولة أن تسـيطر على إقليمها وتتمتع بمباشـرة سـلطتها عليه، ومع التطور التكنولوجي والتقني وتطور شبكات الاتصـال في الفضـاء السيبراني، وأصـبح فضـاء ومسرحا لبروز تحديات

[1] يحي الزهراني، مرجع سابق ص241

[2] Oren gross, Cyber Responsilbility to Protect legal Obligation of States Directly Affected by Cyber incident, Cornell international law journal, vol 48 p 504-510

[3] Mecheal Gervais, Cyber Attack an Law of wars, Berkeley Journal of international Law,vol30 2012 p 560

[4] ليث ناجح محمد ، موقف القانون الدولي من الهجمات الالكترونية ، مجلة كلية القانون والعلوم السياسية، جامعة كركوك، العدد 24 المجلد 7 جامعة كركوك 2018 ص20

جديدة أمام سيادة الدولة فظهرت الحروب السيبرانية، والتي لا تعترف بالحدود الجغرافية، وباتت الأطراف الدولية تتنازع وتتسابق على تطوير قدراتها الهجومية والدفاعية ضمن شكل جديد من أشكال سباقات التسلح[1].

وفي ظل هذه المتغيرات تغير المفهوم التقليدي للسيادة، وأصبح ما يعرف اليوم بالسيادة الرقمية، وهو التي تبسط الدولة سيطرتها وولايتها القضائية على الفضاء الرقمي المتمثل بالإنترنت التي تجتاز حدود الدولةبالتالي وضع الدولة أمام تحدي حقيقي إذ لا تستطيع الدولة فرض سيطرتها على مواطنيها في الفضاء السيبراني.

وتعتبر الشبكات أداة جديدة وهامة وقادرة على تخطي الحدود الجغرافية، وتخطي كل حاجز أمني بكل سهولة، وإيصال أي معلومة إلى مكان بسرعة لم يكن لأحد أن يتخيلها، فأصبحت سببا في اضمحلال الحدود الجغرافية في الفضاء السيبراني، وما نتج عنها من مخاطر وصعوبات في التصدي لها.

وكذلك تضاعف الانتماءات الوطنية مما يثير التساؤل بشأن نطاق سيادة الدولة، لتشعر الدول بضرورة معالجة مشاكل السيادة لتجنب المخاطر المستقبلية سواء على الصعيد الوطني أو الدولي، فقامت أغلبها بتعديل تشريعاتها الوطنية والتنسيق مع دول أخرى بإبرام اتفاقيات لاستيعاب الجرائم السيبرانية وتتبع مصادرها والقوانين الردعية لها، وذهب الخبراء في حلف شمال الأطلسي إلى تأكيد منع استخدام البنى التحتية السيبرانية الواقعة في إقليم الدول التي تخضع لسيطرتها الكاملة، في نشاطات تمس الحقوق السيادية للدول الأخرى[2].

ويمكن القول أن مصير ومستقبل سيادة وأمن الدول مرتبط بمدى سيطرتها على البنية التحتية السيبرانية بشكل كامل، حتى ولو كانت واقعة في إقليم دولة أخرى، لأن الحروب السيبرانية تمثل خرقاً لسيادة الدولة وإحداث أضرار مدمرة.

[1] احمد عيسى الفتلاوي، زهراء عماد محمد ، تكييف الهجمات السيبرانية في ضوء القانون الدولي ، مجلة الكوفة. العدد 44 الجزء الأول، 2018 ص 58

[2] احمد عيسى الفتلاوي، زهراء عماد محمد ، تكييف الهجمات السيبرانية في ضوء القانون الدولي ، مجلة الكوفة. العدد 44 الجزء الأول، 2018 ص 58

خلاصة الفصل:

نستخلص في هذا الفصل أنّ الدول بذلت ما في وسعها من الجهود (الوطنية والإقليمية والدولية)، لمواجهة مجابهة الحروب السيبرانية ومخاطرها، وأسهمت تلك الاتفاقيات والتعاون الدولي في وضع قيود في استخدام التكنولوجيا في رحم الفضاء السيبراني. دون أحداث أضرار سواء مادية أو معنوية على المدنيين، لكن رغم كل هذه الجهود المبذولة، إلاّ أنّها لا تزال (التهديدات السيبرانية) هاجسا بالنسبة للمجتمعات والدول. لذا لا بد من إرادة قوية من طرف الدول وخاصة الدول الرائدة في هذا المجال واستراتيجية سيبرانية شاملة تقف أمامها، بغية الوصول إلى تحقيق فضاء سيراني سلمي وآمن.

خاتمة

خاتمة

كان للتطور التكنولوجي وثورة المعلومات والاتصـــال دور كبير في تطوير المجتمعات والدول، وفي تشكيل فضاء سيبراني ازداد الاعتماد عليه من طرف الدول والمجموعات والأفراد، وأصبح هذا الفضاء يعتمد عليها في جميع المجالات السياسية والاجتماعية والاقتصادية والعسكرية.

وأحدث هذا الفضـاء تغييرات جذرية في مفاهيم العلاقات الدولية كمفهوم الأمن والقوة والصـراع حيث برز الأمن السـيبراني وتغيرت القوة بين الفاعلين. وتحول الصـراع إلى صـراع سـيبراني. وأصـبحت الحروب السيبرانية تطفو على السطح كتهديد للأمن العالمي. وعليه دعت الضـرورة إلى تطوير مفهوم الأمن لمواجهة الحروب السـيبرانية، حيث جاء الأمن السـيبراني كرد فعل على هذه التهديدات، والتي مسـت جميع مجالات الحياة المختلفة العســكرية والمدنية. فالاعتماد المتزايد على التكنولوجيا والاتصـــالات يوما بعد يوم، زاد في التعرض إلى تهديدات ســيبرانية بالغة الخطورة، وبالتالي يتعرض الأمن القومي لمخاطر كبيرة تهدد اســتقرار الدولة وتماسكها.

هذه الحروب الســيبرانية تنوعت أشــكالها، فبدأت بجرائم ســيبرانية يقوم بها أفراد ومنظمات اجرامية كالاختراق والتجسس وسرقة الأموال، وتطورت لتصل إلى التخويف والإبتزاز عن طريق الشبكات العنكبوتية لتصل إلى صراع بين الدول وتهديد أمنها القومي، حيث ظهر جليا عسكرة الفضاء السيبراني، وإعداد جيوش سيبرانية تتمتع بمهارات وإمكانيات عالية التأثير في شن حروب سيبرانية مدمرة.

وفي ظل تحديات الحروب السيبرانية على الأمن العالمي. سعت الدول والحكومات إلى بذل جهود في تطوير قدراتها، واتخاذ إجراءات وقائية لحماية بنيتها التحتية من أي هجوم ســـيبراني، كما شـــكلت جيوش ســـيبرانية تقوم بمهمة الدفاع والهجوم والحماية. أما في الجانب القانوني فطورت الدول منظومتها القانونية لتتلاءم وتتكيف مع الحروب الســيبرانية والهجمات الجديدة، وبما أن الفضـــاء الســيبراني لا يعترف بالزمان والجغرافية بذلت الدول مســاعي إقليمية ودولية، لوضــع أطر قانونية واتفاقيات دولية لهذا الفضــاء، كاتفاقية بودابست، وجامعة الدول العربية، ولعل من أبرزها دليل تالين عدة مفاهيم خاصة في الفضاء السيبراني.

ولتحقيق الأمن السيبراني المثالي في العالم المادي، لا بد من إرادة سياسية قوية وتعاون دولي مشترك يمكن الوصول إلى الهدف المرجو وهو التقليل من الحروب السيبرانية ومن هجماتها المدمرة لمفاصل الحياة.

وأن مواجهة الحروب السيبرانية الراهنة، أمر ضروري، وأن خطورتها تكون أصعب في المستقبل، لذا فإن تجاهلها اليوم، يعرض الأمن العالمي لخطر دائم.

خاتمة

فالتحدي اليوم هو الاســـتعداد للغد، فالواجب تطوير اســـتراتيجيات المواجهة، والعمل مع بقية الدول والمشاركة في قيم الأمن والاستقرار، واحترام قواعد السلوك الجيد، من أجل فضاء سيبراني سلمي، يعزز الأمن والتقدم والازدهار للجميع.

النتائج والتوصيات:

أولاً: النتائج:

• الفضـاء السـيبراني يعد جديد ويتميز بالغموض والتعقيد، وشـدت تنوع تهديداته. مما يجعل الأمن السيبراني كرافد جديد للأمن القومي، وله أهمية في الاستراتيجية الأمنية للدول.

• التطور التكنولوجي والتقني ســـوف يؤثر تأثيرا كبيرا على الســـلوك الدولي، وهذا نتيجة الاعتمادعلى شـبكات الانترنت والاتصـالات لدى الدول في خدماتها وتطبيقاتها، وما يزيد من التهديدات.

• في عصـرنا الرقمي، أصـبح للفضـاء السـيبراني مجالا جديدا وهاما للتفاعلات الدولية، وقد أحدث تغييرات في مفاهيم القوة والأمن والصـــراع (الحرب)، وظهر فاعلون جدد، وانتشـــرت القوة السـيبرانية بينهم، وازداد الصـراع في الشـبكات، قد يتطور أحيانا لتصـبح حروبا جديدة بأسلحة سيبرانية.

• الفضـــاء الســـيبراني أصـــبح مجالا جديدا هاما في التفاعلات الدولية، وأحدث تغييرات في مفاهيمالأمن والقوة والصراع، وظهر فاعلون جدد، وانتشرت القوة واشتد الصراع أحيانا ليصبح حروبا جديدة في ظل عبر شاشة الحاسوب سلاحها المعلومة، وفضاءها التكنولوجيا.

• الحروب السيبرانية لها طابع تقني خاص، بحيث أنها تهديدات عابرة للحدود وانتهاك سيادة الدول، وعليه تكون المواجهة تقنية بتحديث الجيوش وهيئات الأمن الســـيبراني، ومواجهة قانونية بوضـــع التشـــريعات الوطنية والإقليمية والدولية، والتعاون الدولي من أجل فضـــاء سيبراني سلمي.

• أن الحروب الســـيبرانية من المفاهيم الحديثة التي لا يوجد اتفاق دولي بشـــأن تعريفها، مما يؤدي إلى صعوبة تكييفها، وتحديد المسؤولية الدولية عنها.

• أن هناك سباق للتسلح السيبراني بين الدول، وذلك لرغبة الدول المتزايدة في تعزيز دفاعاتها ضدأي هجوم سيبراني.

• أن الحروب الســـيبرانية ظاهرة عالمية، يصـــعب مواجهتها إلا بالنظر والتعاون بين جميع الدول على المستوى الإجرائي والجنائي.

• أن هناك علاقة تبادلية بين التكنولوجيا والقانون، فالتطورات التكنولوجية تفرض تشـــريعات قانونية تواكب جميع الأصعدة الداخلية والإقليمية والدولية.

• يتوجب على الدول اتخاذ خطوات جديدة للحد من الحروب السيبرانية، دون مراعاة المصالح الدولية للقوى العظمى التي تقف عائقا أمام المساعي والجهود.

• الأمن العالمي يواجه تحديات جديدة، وبالغة الخطورة في المستقبل، إذا لم تتخذ الدول على عاتقها المسؤولية اللازمة، وتبني استراتيجيات شاملة بعيدة الأمد للتقليل من تداعيات الحروب السيبرانية.

• أن هناك جهود وطنية وإقليمية ودولية، في مواجهة الحروب السـيبرانية، وذلك من خلال عقد المؤتمرات والاتفاقيات لمنع الحروب والهجمات والجرائم السـيبرانية، وكل ما يهدد الأمن العالمي.

ثانياً: التوصيات:

• ضـرورة إدماج الأمن السـيبراني في العقيدة الأمنية للدول، لما له من علاقة وطيدة مع قضايا التنمية السياسية والاقتصادية والاجتماعية.

• العمل على تحديث جيوش سـيبرانية بتقنيات عالية للتعامل مع التهديدات السـيبرانية، وأن يكون للمجتمع الدولي دور في العمل على الحفاظ على الطابع السلمي للفضاء السيبراني.

• أهمية إنشـاء لجنة دولية لإدارة الأزمات السـيبرانية من خلال دراسـة الهجمات السـيبرانية والعمل على التحقيق الدولي المستقبلي حول المسؤولية السيبرانية حول تلك الهجمات.

• إنشـاء مركز تدريب لمكافحة الطوارئ المعلوماتية، والعمل على بناء القدرات في مجال الأمن السيبراني.

• أهمية تعزيز التعاون الدولي في مكافحة مخاطر الحروب السـيبرانية، والعمل على تبادل الخبرات، والعمل على تعزيز النظم القضائية.

• أهمية العمل على المسـتوى الدولي في حل الصـراعات الدولية، التي تحدث في الفضـاء السيبراني وانعكاس التوتر على الأرض، ومواجهتها بالطرق السلمية.

• يجب تعديل ميثاق الأمم المتحدة في بعض تصـرفات التي تهدد السـلم والأمن الدوليين، ومنها الحروب والهجمات السيبرانية.

قائمة المصادر والمراجع

أولاً: قائمة المراجع باللغة العربية

أ/ الكتب:

1. الاتحاد الدولي للاتصالات، **دليل الأمن السيبراني للبلدان النامية**، مكتب تنمية الاتصالات، طبع في جنيف سويسرا، 2006.

2. إياد خليفة، **القوة الإلكترونية وأبعاد التحول في خصائص القوة**، مكتبة الإسكندرية، مصر، 2014.

3. بارة سمير، الدفاع الوطني والسياسات الوطنية للأمن السيبراني في الجزائر: الدور والتحديات، الملتقى الدولي حول سياسات الدفاع الوطني، جامعة قاصدي مرباح ورقلة، كلية الحقوق والعلوم السياسية، 2017/01/31.

4. البدانة ذياب، **الأمن وحرب المعلومات**، الطبعة الأولى، دار الشروق للنشر والتوزيع، عمان، 2006.

5. جوزيف ناي، **المنازعات الدولية: مقدمة للنظرية والتاريخ**، ترجمة أحمد أمين الجمل، ومجدي كامل، الجمعية المصرية لنشر المعرفة والثقافة العالمية، القاهرة، 1997.

6. حسين فاروق، **فيروسات الحاسوب الآلي**، عربية للطباعة والنشر، الطبعة الثانية، القاهرة، 1999.

7. د. كيالي عبد الوهاب، **الموسوعة السياسية**، الجزء الثاني، المؤسسة العربية للدراسات والنشر، الطبعة الأولى، بيروت، 1998.

8. صالح بن علي بن عبد الرحمان الربيعة، **الأمن الرقمي وحماية المستخدم من مخاطر الإنترنت**، هيئة الاتصالات وتقنية المعلومات.

9. عادل عبد الصادق، **أسلحة الفضاء الإلكتروني في ضوء القانون الدولي**، سلسلة أوراق، العدد 23، مكتبة الإسكندرية، مصر، 2016.

10. عباس بدران، **الحروب الإلكترونية: الإشتباك في عالم متغير**، مركز دراسات الحكومة الإلكترونية، بيروت، 2010.

11. عبد الفتاح مراد، **شرح جرائم الكمبيوتر والإنترنت**، دار الكتب والوثائق المصرية، الطبعة الأولى، الإسكندرية.

12. علوة رأفت، **قرصنة الأنترنت**، مكتبة التجميع العربي للنشر والتوزيع، الطبعة الأولى، عمان، 2006.

13. عياد سامي، **استخدام تكنولوجيا المعلومات في مكافحة الإرهاب**، الطبعة الأولى، الإسكندرية، دار الفكر الجامعي، 2007.

14. محمد خالد، **الحرب الإلكترونية**، المكتبة العالمية للطبع والنشر، بغداد، 1986.

15. محمد شلبي، **المنهجية في التحليل السياسي**، مطبعة دار هومة، الجزائر، 2007.

16. مركز نورس للدراسات، **الحروب السيبرانية "الإلكترونية"**، نقلة نوعية في الإستراتيجيات العسكرية وأثر ملحوظ على العلاقات الدولية.

17. منى الأشقر جبور، **السيبرانية هاجس العصر**، المركز العربي للبحوث القانونية والقضائية، بيروت، 2017.

18. نهلاالمومني، **الجرائم الإلكترونية**، الطبعة الأولى، عمان.

ب/ المجلات والمقالات:

1. زينب شنوف، **الحرب السيبرانية في العصر الرقمي**: حروب ما بعد كلاوزفيتش، المجلة الجزائرية للأمن والتنمية، العدد 02، المجلد 09، جويلية 2020.

2. سعيد درويش، **ماهية الحروب الإلكترونية في ضوء قواعد القانون الدولي**، حوليات جامعة الجزائر، العدد 29.

3. لطفي أيمن بلغراد، **الفضاءالسيبرانية: هندسة وفواعل**، المجلة الجزائرية للدراسات السياسية، العدد الخامس، 2016.

4. ياسين طلال السعدي، محمد عدي عناب، **المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر**، مجلة الرزقاء للبحوث والدراسات الإنسانية، العدد 01، المجلد 19، 2019.

5. يوسف بوغرارة، **الأمن السيبراني: الاستراتيجية الجزائرية للأمن والدفاع في الفضاء السيبيري**، مجلة الدراسات الإفريقية وحوض النيل، المركز الديمقراطي العربي، المجلد الأول، العدد الثالث، 2018.

ج/ المذكرات والبحوث:

1. إيهاب خليفة والأمن المعلوماتي: **لماذا تصاعدت التهديدات الإلكترونية مع انتشار كورونا؟**، الموسوعة الجزائرية للدراسات السياسية والإستراتيجية، العدد 4868، يوم: 2020/04/10.

2. خالد معالي، **أثر الصحافة الإلكترونية على التنمية السياسية في فلسطين**، رسالة ماجستير غير منشورة، كلية الدراسات العليا، جامعة النجاح الوطنية، غزة، 2008.

3. رغدة البهي، **الردع السيبراني: المفهوم والإشكالات والمتطلبات**، الموسوعة الجزائرية لدراسات السياسية والإستراتيجية، العدد 4741، نشر يوم: 27/11/2019.

4. سليم دحمان، **أثر التهديدات السيبرانية على الأمن القومي: العلاقات المتحدة أنموذجاً**، مذكرة مقدمة لنيل شهادة ماستر أكاديمي، كلية الحقوق والعلوم السياسية، قسم العلوم السياسية، جامعة المسيلة، 2017/2018.

5. عادل عبد الصادق، **الهجمات السيبرانية أنماط وتحديات جديدة للأمن العالمي**، الموسوعة السيبرانية الجزائرية، العدد 18601، يوم: 27/11/2019.

6. عنترة بن مرزوق، محي الدين حرشاوي، **الأمن السيبراني كبعد جديد في السياسة الدفاعية الجزائرية**، الملتقى الدولي حول سياسات الدفاع الوطني، جامعة قاصدي مرباح ورقلة، كلية الحقوق والعلوم السياسية، 13/01/2017.

7. فيصل مراد، **التحديات الإقليمية الراهنة للأمن القومي الجزائري**، رسالة ماجستير منشورة المدرسة العليا للعلوم السياسية – قسم الدراسات العسكرية والإستراتيجية، 2013/2014.

د/ القواميس:

1. إبراهيم مدكور، **المعجم الوجيز**: مجمع اللغة العربية، ددن، 1989، القاهرة.

2. أحمد عطية الله، **القاموس السياسي**، الطبعة الثالثة، دار النهضة العربية، 1968، القاهرة.

3. العلامة ابن منظور، **لسان العرب**، المجلد الأول، دار لسان العرب، بيروت.

هـ/ المواقع الإلكترونية:

1. يورحلي رومون، **التكنولوجيا الحديثة في المجالات العسكرية**، مجلة الجيش اللبناني على شبكة الإنترنت ل ع :236، (فبراير/شباط 2005 م)، http://www.lebarmy.gov.lb/article.asp?ln=ar\&id=70066

2. تاريخ الاطلاع: 01/05/2020 http://shemelaws.ws/browse.php/book/1244/page20

3. **حرب الفضاء والأقمار الصناعية: صراع إستراتيجي جديد**، الموقع: شبكة النبأ المعلوماتية على شبكة الإنترنت، 25 فبراير 2008.

4. عادل عبد الصـــادق، **الهجمات الســـيبرانية: أنماط وتحديات جديدة للأمن العالمي**، الموســـوعة السيبرانية الجزائرية، العدد 18601، يوم: 27/11/2019، على الموقع: https://www.politics-dz.com

5. عبد الرحمان بن عبد الله الســـند، **وســـائل الإرهاب الإلكتروني وحكمها في الإســـلام وطرق مكافحتها.**

6. عكاظ، ما هو الأمن السيبراني، 09:42، يوم: 22/06/2020.

7. فاروق حاتم، **الإمارات تتقدم في إصدار تشريعات الأمن السيبراني**، جريدة الاتحاد.

8. كمال مساعد، **الحرب الافتراضية وسيناريوهات محاكاة الواقع**، مجلة الجيش اللبناني على شبكة الإنترنت.

9. المجال الخامس، **الحروب الإلكترونية في القرن الـ21 (الجزيرة)**، (نشر يوم: 12/01/2011)، على الموقع: اطلاع عليه يوم: 16/04/2020.

10. مصطفى الطيب، **الفرق بين أمن المعلومات والأمن السيبراني**، 10:30، 23/06/2020، على الموقع: https://www.oolom.com/6124

11. نجوى السودة، **بحث الفضاء السيبراني، مؤتمر حرب الفضاء السيبراني**، تاريخ النشر: 05/05/2014، على الموقع: https://seconf.wordpress.com

12. نوال الشهري، **حرب المعلومات: في مركز التميز لأمن المعلومات** (جامعة ملك سعود)، على الموقع: http://coela.edu.sa/index.php/ar/assurance-awarness/articles/47-data-privacy-1263

13. هاجر حسونة، **الإرهاب الإلكتروني.. ها يتحول في المصدر التهديد الأول في العالم**، نشر يوم: 04/05/2015، على الموقع: اطلاع عليه يوم 07/05/2020.
https://alakhbaronline.net/articles/1430728333185670700

14. يحيى اليحياوي، **حرب الإعلام والرقابة**، موقع على شـــبكة الإنترنت: http://www.alyahyari.org

ثانياً: قائمة المراجع باللغة الأجنبية

A/Books:

1. Andrew Mclean, **Electronic money regulation 2011(EMR2011) & the payment service Regulation** 2009.

2. Joseph S Ney JR, **Cyber power**, Harvard Kennedy School, 2010.

3. Asenio T Gumahad, **Cyber tropes and Netuvar**, the profession of Arms in the information Age (Alabama Air University Air war college), 1996, 57-156.
4. Myriam Dunn Cavelty, **Information age Conflicts**: A study of the Information Revolution and changing International Operating Environment.
5. ITU, **Cyber security Geneva, International Telecommunication Union** (ITU), 2008.
6. Martin C. libicki, **conquestion cyberspace**: National Security and information warfare (New York Cambridge University Press, 2007.
7. Olivier KEMPF, **Introduction à la Cyber stratégie**, Paris, Economica, 2012.
8. Paulo & Jana Shakarian, Andrew Ruef, **Introduction to cyber warfare**: A multidisciplinary Approach, Elsevier, 2013.
9. Schreier Fred, (2015)،**On Cyber warfare**, Dcaf Horizon Working Paper, No 7.
10. The International Télécommunication Union, ITU **Toolkit for Cybercrime, législation**, Geneva, 2010.

B/Articles:

1. Fred Schreier, **On Cyberwarfare**, DCAF horizon 2015 Working paper No, 07.
2. Martin C. libicki, **conquestion cyberspace**: National Security and information warfare (New York Cambridge University Press, 2007.

C/Dictionnaires:

1. **Grand Larousse Encyclopédique**, tome cinquième Libraire Larousse, paris, 1979.
2. **Le Robert, dictionnaire**, alphabétique et analogique de la langue française, tom troisième, société la nouveau livre, paris, 1978.

D/Websites:

1. Florian Bieber, **cyber war or sideshow the internet and the Balkan wars**, current history, 99 no 635 (Mars 2000): 124128, online e-article, in the site:
2. http://search.proquest.com/docview/200751259accountid=7180
3. https://www.europarabct.com/?p=34807
4. Mbuthia Rex, **Cyber warfare versus Information Warfare**: Two Very Different Concepts, in the site:

1. http://bit.ly/20H4UKG3lbid.

فهرس
الجداول و الأشكال

فهرس الجداول والأشكال

فهرس
المحتويات

فهرس المحتويات

فهرس المحتويات

الملخص :

تعتبر الحروب السيبرانية من بين التحديات الأمنية المعاصرة في الفضاء السيبراني. وأصبحت واحدة من أهم الصـراعات بين الدول الكبرى. بحيث تسـتهدف القطاعات العسـكرية والمدنية. كالتجسـس والقرصـنة واختراق وزرع الفيروســات. لتعطيل وتدمير البنية التحتية المعلوماتية للدولة كذلك أدت الحروب الســيبرانية لإحداث تحول في مفاهيم الأمن والقوة والصراع في الفضاء السيبراني. الذي يتميز بالتطور السريع. والغموض الشديد. لتشكل تهديداً فعلياً على أمن الدول وهو ما دفع بالأمن السيبراني يشكل صدارة أولويات الأمن القومي للدول. ما طرح الإشكالية: "هل يمكن للحروب السيبرانية أن تشكل تهديداً على الأمن العالمي؟". وفي إثر هذا سارعت الدول إلى بذل الجهود والتعاون على المستوى الإقليمي والدولي. ووضـع آليات قانونية وتقنية. وتبني استراتيجية سيبرانية لمواجهة الحروب السيبرانية والدفاع عن أمنها. وخلق فضاء أمن وسلمي.

الكلمات المفتاحية : الفضـاء السـيبراني. الهجمات السـيبرانية. الجريمة السـيبرانية. الأمن السـيبراني. الاستراتيجية السيبرانية.

Summary

The cyberian wars were considered as one of the main modern security challenges. It became one of the major conflicts between powerful nation. The started targeting both the military and civil field, such as. spy. piracy and lack. They took this conflict to another level, (viruses) to break down and destroy the informational background. The world interested a radical change in some concepts such as: security, power, and conflict, in cyberian field which is characterized by fast progress and obscurity. As a result, this was. considered as a real threat against national security. It led to the cyberian security to be the alpha lion in national security. This made us ask the following question: Can we consider the cyberian wars as a threat against the universal security؟

Nations started doing all their efforts to make cooperation on both regional and national level. They followed technical policies and adopted the cyberian strategies to comfort the cyberian wars and keep peace.

Keywords: Cyberspace, Cyberian Attacks, Cyberian Crime, Cyberian Security, Cyberian Strategy.