جامعة زيان عاشور -الجلفة-
Zian Achour University of Djelfa
كلية الحقوق والعلوم السياسية
Faculty of Law and Political Sciences

قسم العلوم السياسية

الحروب السيبرانية والأمن العالمي التحديات والمواجهة

مذكرة ضمن متطلبات
نيل شهادة الماستر في العلوم السياسية تخصص دراسات أمنية وإستراتيجية

إعداد الطالب :
- ساسوي خالد
- بن حسين محمد

إشراف الأستاذ:
-د. بوسعيد عبد الحق

لجنة المناقشة

-د/أ. بلخيرات حوسين	رئيسا
-د/أ. بوسعيد عبد الحق	مقررا
-د/أ. عصبي حليمة السعدية	ممتحنا

الموسم الجامعي 2020/2019


بسم الله الرحمن الرحيم

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

دونالد رامسفيلد Donald Rumsfuld

-وزير دفاع سابق أمريكي-

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

صون تزو-جنرال وخبير عسكري صيني-

إهداء

إلى من تعهداني بالتربية في الصغر...

وكانا نبراسا يضيء فكري بالنصح والتوجيه في الكبر ...

فوجودهما سبب للنجاة والفلاح في الدنيا والآخرة

«أمي و أبي» حفظهما الله .

إلى من حفزوني في التقدم ، وأسعدوني بالعون ...

إخوتي رعاهم الله .

إلى أصدقائي وجميع طلبة قسم العلوم السياسية .

محمد

إهداء

إلى روح والدي الطاهرة طيب الله ثراه برحمته الواسعة

وإلى أمي الكريمة حفظها الله ورعاها

وإلى جميع أفراد عائلتي الكريمة .

إلى جميع طلبة قسم العلوم السياسية ، وزملائي في العمل .

خـالــد

شكر وعرفان

الحمد لله والشكر لله الذي وفقنا لإتمام هذا العمل المتواضع .

كما نتوجه بالشكر لأهل الفضل فأخص في هذا المقام بالشكر الجزيل الأستاذ الدكتور: "بوسعيد عبد الحق" ، الذي يتميز بالأخلاق والشخصية القوية والشخصية اللطيفة ،

شكرا على مجهوداتك المضنية، فأنت أهل للشكر والتقدير.

كما نشكر اللجنة الموقرة التي قبلت مناقشة هذا البحث المتواضع.

كما نشكر جميع أساتذة قسم العلوم السياسية بالجلفة، فلولا مجهوداتكم لما تمكنا من مواصلة النجاح، وعلى عطائهم، وعلى اخلاصهم في تقديم كل ما رائع ومفيد، فشكرا لكم ملئ الأرض حبا وكرما، فشكري لن يوفيكم حقا ،

ونشكر بكل ود وعرفان الزملاء في قسم العلوم السياسية – تخصص دراسات أمنية واستراتيجية – على الدعم والتشجيع، وكل من ساعدننا سواء من قريب أو بعيد

فهرس المحتويات

فهرس المحتويات

فهرس الجداول

والأشكال

مقدمـــــة

مقدمة:

يشهد العالم تقدما تكنولوجيا وتقنيا هائلا ، ونوعا جديدا من التسلح، لم تعرفه العصور السابقة من قبل وهذا بعد الثورة المعلوماتية، واتساع نطاق استخدامها في شتى مجالات الحياة، المدنية والعسكرية، وخاصة الأغراض العسكرية فهي بمثابة نقطة التحول في فن الحرب وفي ادارة الصراع الدولي وتغيرا في مفهوم الامن 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 مجالا 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 على نمطين من القوة (الناعمة والصلبة) في عماية توظيف التفاعلات في الفضاء السيبراني، مما يعكس تنامي القدرات والتّهديدات المتصاعدة لأمن البنية التّحتية الكونية للمعلومات، وأصبح من الصّعب حصرها أو تطوير استراتيجيات محكمة لمواجهتها بشكل كامل، خاصة مع تعدّد أشكال التهديدات ومصادرها وتطوّر المتسارع والمستمر .

وعلى إثر هذه الحروب السيبرانية كتهديد جديد ، معقدة ومتشابكة تحديًا أمنيا على جميع مستوياته المدنية والعسكريّة ، وأسقطت مفهوم السّيادة والحدود الجغرافية السّياسية والثقافية بين الدول خاصة مع اختراق المواقع الحكوميّة الرسميّة والتجسس المعلوماتي على الدّول.

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

[1]- المفاهيم النظرية لاستراتيجية الاقتراب غير المباشر ، مقاتل من الصحراء ، على الموقع الالكتروني: *http:www.mouquatel.comm-All Rights Reserved*

ولمواجهة الحروب السيبرانية تسعى الدول للحفاظ على بنيتها وأجهزتها الحيوية التقنية والالكترونية والدفاع عنها، وفق استراتيجية سيبرانية قوية متمثلة في الأمن السيبرانية، نتيجة تأثير التكنولوجيا الحديثة لا سيما الفضاء السيبراني على الأمن العالمي، ومنه نوضح في دراستنا لمفهوم الفضاء السيبراني والتحولات التغير في المفاهيم كالأمن والقوة والصراع، والتطرق إلى الحروب السيبرانية و الأمن السيبراني، وأبرز التحديات التي تقف عائقا أمام الأمن العالمي والسيبراني، ثم نعرج الجوانب القانونية والتقنية تحت مضلة القانون الدولي، كآلية لمواجهة هذه الحروب السيبرانية والتكتيك القادم في طبيعة الحرب في القرن الحادي والعشرين.

ولقد ركزنا في الدّراسة على مصطلح "السيبرانية" بدل "الالكترونية" لضرورة البحث والتناسق في الدراسة لهذا الموضوع.

أولا : أهمية الدراسة:

تأتي أهمية هذه الدراسة الموسومة بـ: "**الحروب السيبرانية والأمن العالمي –التحديات والمواجهة**- من 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 تستطيع الاستغناء عن هذه التكنولوجيا ، مما باتت الحروب السيبرانية تهدد الأمن السيبراني الذي أصبح جزءا أساسيا ومهما للأمن القومي للدول، بالإضافة إلى الجهود الإقليمية والدولية سواء من الجانب القانوني أو التقني لمجابهة المخاطر السيبرانية.

كذلك التركيز على الفضاء السيبراني في الدراسات الاكاديمية مهم جدا، بحيث يعتبر حقلا دراسيا جديدا في مجالات الدراسات الامنية، وأن الحروب السيبرانية هي موضوع العصر ، والأمن السيبراني أولوية ضرورية في حماية الأمن القومي للدول وهذا الموضوع يلقى اهتمام ودراسات واسعة فيه.

ثانيا :أهداف الدراسة:

نسعى من خلال دراستنا لهذا الموضوع إلى الوصول للأهداف التالية:

- ابراز وتوضيح مفاهيم جديدة في الفضاء السيبراني.
- مدى تأثير الفضاء السيبراني في التحولات الدولية : الأمن – القوة – الصراع .
- التعرف على الفضاء السيبراني والحروب السيبرانية والامن السيبراني.
- معرفة تحديات الحروب السيبرانية على متغير الأمن العالمي.
- مدى فاعلية القوانين وجهود الدول في مواجهة الحروب السيبرانية تأثيرها على الامن العالمي .

ثالثا :إشكالية الدراسة وتساؤلاتها.

أفضت التحديات الناجمة عن التطور التقني والتكنولوجي، جراء ثورة المعلومات الهائلة واتساع نطاق استعمالها في مختلف مجالات الحياة، إلى بروز تحولات كبيرة على مستوى موضوع ونوعية التهديدات والصراعات والدولية، والتي أصبح ما بات يسمى بالحروب السيبرانية إحدى أهم تجلياتها. من هذا المنطلق تأتي شرعية طرح التساؤل المركزي الآتي:

" كيف يمكن أن تشكل الحروب السيبرانية تهديدا على الأمن العالمي " ؟.

وللإجابة عن التساؤل المركزي نطرح عدة تساؤلات فرعية وهي :

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

2-ماهي الحروب السيبرانية وأنماطها؟ .

3-ماهي تحديات الحروب السيبرانية على الأمن العالمي ؟.

4- ما هي الجهود الدولية وآليات مواجهة الحروب السيبرانية ؟ .

رابعا : فرضيات الدراسة .

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

خامسا : المجال المكاني والزماني للدراسة.

أ – **المجال الزماني :** شملت الدراسة في مجالها الزمني مراحل عدة، بداية من مرحلة ما بعد 11 سبتمبر 2001م، والتي كانت بداة التحولات وتغير المفاهيم بسبب ظهور التهديدات والسيبرانية على المستوى الدولي، كظهور الفيروسات والتجسس والاختراق وسرقة المعلومات، ولعلى أبرز حدث في هذا الشأن الهجمات السيبرانية على دولة استونيا 2007م،من طرف روسيا والذي عطل كل البنى التحتية والأجهزة .

ب – **المجال المكاني**: الفضاء السيبراني كبعد جديد في العلاقات الدولية، وساحة معارك لحروب العصر والمستقبل .

سادسا :المنهج المتبع في الدراسة .

1- **المنهج الوصفي:** يعتبر هذا المنهج من أنسب وأكثرها استخداما في الظواهر الانسانية 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، و العوامل المؤثرة فيها، ثم استخراج الاستنتاجات ذات الدلالة والمغزى بالنسبة لمشكلة البحث وتقديم عدد من التوصيات .
2- **منهج تحليل المضمون:** يعتبر اتصال غبر مباشر في دراسة الظاهرة، فلا يقتصر على الجوانب الموضوعية فقط، وإنما الجوانب الشكلية أيضا، ونتائجه قابلة للتعميم، وبهذا اعتمدنا في دراستنا على هذا المنهج، وتفسير مضامين أهم الوثائق الرسمية والاتفاقيات الدولية والاقليمية لمواجهة مشكلة الحروب السيبرانية وتحليلها تحليلا متكاملا، في سياقها العام وظروفها الموضوعية المحيطة بها .

سابعا: أدبيات الدراسة:

1-كتاب **السيبرانية هاجس العصر**، منى الأشقر جبور، المركز العربي للبحوث القانونية والقضائية، دراسات وأبحاث، جامعة الدول العربية.

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

2-الهجمات السيبرانية: أنماط وتحديات جديدة للأمن العالمي، المركز العربي، عادل عبد الصادق الموسوعة الجزائرية للدراسات السياسية و الاستراتيجية، العدد18686، تاريخ النشر: **2019/11/27**، يناقش الكاتب مدى تحول الفضاء السيبراني إلى ساحة جديدة في العلاقات الدولية، وبروز أنماط توظيفية له، وكذلك استخدام الفضاء السيبراني في المجالات العسكرية والمدنية، مما برزت فيه صراعات مختلفة، ومنه تبلورت

ظاهرة الحروب السيبرانية "Cyber War" ،والتي تميزت عن نظيراتها التقليدية من حيث طبيعة الأنشطة والأنماط والفواعل، والتحديات التي يواجهها الأمن العالمي.

3-الجروب السيبرانية في العصر الرقمي: حروب ما بعد كلاوز فيتش، زينب شنوف، المجلة الجزائرية للأمن التنمية، العدد02،المجلد 9 ، جويلية 2020.تطرقت الكاتبة في مقالها إلى نمط الحروب في العصر الرقمي، والتحول في المفهوم الكلاسيكي التقليدي للحرب، ويهدف المقال إلى تقديم تحليل معمق للحرب السيبرانية، وكيف ساهمت في تغيير تغير الحرب في العصر الرقمي، وكذلك الاستراتيجيات الكافية لمواجهة الحرب السيبرانية .

4-كتاب : Richard A. Clark & Robert Knake , **Cyber Ware: The Next Threat to National Secutity and What to About It , Harper Collins, 2010.**

يتناول الكاتبان مصطلح الفضاء الالكتروني، وخصائص الحروب السيبرانية في الفضاء السيبراني ، واستخدام الأنترنت كسلاح للحرب الجديدة، ودرورها 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 تهديدا لها في هذا المجال، وفي الأخير يبرز موقف الولايات المتحدة موقفها بشأن ضبط التسلح السيبراني، والتفكير في مواجهة التهديدات السيبرانية من خلال الاتفاقيات الدولية .

شرح المفاهيم :

- **الفضاء السيبرانيCyber Space**: مصطلح حديث، ظهر في العود الأخيرة نتيجة للثورة التكنولوجية، وهو ذلك المكان الافتراضي الذي أوجدته تكنولوجيا المعلومات والاتصالات وفي مقدمتها الأنترنت، ويربط الفضاء السيبراني ارتباطا وثيقا 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 المهاجم من التلاعب بالنظام[2]
- **الجريمة السيبرانية Cyber Crime**: تعتبر إساءة استخدام تكنولوجيا المعلومات والاتصالات من طرف المجرمين ، وذلك على أنها جرائم أنترنت[1] .

1- حمزاوي ميلود ، **مدخل مفاهيمي للأمن السيبيري**، الموسوعة الجزائرية للدراسات السياسية والاستراتيجية ،على الموقع:تاريخ النشر :19-08-2019 ، اطلع عليه يوم :https://www.politics-dz.com2020/03/19 . .

2-رغدة البهي ، **الردع السيبراني : المفهوم والاشكالات والمتطلبات**، الموسوعة الجزائرية للدراسات السياسية والاستراتيجية، على الموقع: تاريخ النشر :27-11-2019، اطلع عليه يوم https://www.politics-dz.com2020/03/20 .

- **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[2].
- **الاستراتيجية السيبرانيةCyber 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[3].

صعوبات الدراسة :

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

- قلة المصادر والمراجع في الدراسات المستقبلية باللغة العربية، ونقص الترجمة خصوصا في هذا الموضوع.
- صعوبة مرتبطة بحداثة الموضوع، وقلة الدراسات المباشرة والمرتبطة في هذا الموضوع .
- صعوبة الاحاطة بكل جوانب هذا الموضوع، نظرا لحداثته وتسارع الأحداث والتطورات فيه
- غلق المعاهد والجامعات والمكتبات الخاصة بسبب الوباء العالمي كورونا (Covid-19)، فكان عائقا أمامنا في البحث عن المعلومات.

ثامنا: تفصيل خطة الدراسة.

تم تقسيم الدراسة لثلاثة فصول أساسية:

تناولنا في **الفصل الأول** المعنون بالاطار النظري والمفاهيمي للدراسة، واحتوى على ثلاث مباحث ، المبحث الأول تطرقنا فيه للفضاء السيبراني والتحول في المفاهيم(الامن والقوة والصراع)، أما المبحث الثاني تكلمنا فيه عن مفهوم الحروب السيبرانية، أما المبحث الثالث والأخير من هذا الفصل خصص للأمن السيبراني .

1-يوسف بوغرارة ،**الأمن السيبراني: الاستراتيجية الجزائرية للأمن والدفاع في الفضاء السيبيري**، مجلة الدراسات الأفريقية وحوض النيل (المركز الديمقراطي العربي) ، العدد 03، المجلد01، سبتمبر/أيلول 2018، ص1

2 -ITU, **Cyber Security ,Geneva** : International Télécommunication Union (ITU) , 2008

3--زينب شنوف، **الحرب السيبرانية في العصر الرقمي: حروب ما بعد كلاوز فيتش**، المجلة الجزائرية للأمن والتنمية، العدد02، المجلد09 ،ص92

أما فيما يخص **الفصل الثاني** الذي عنوانه الحروب السيبرانية وتحديات الأمن العالمي، هو الآخر ثلاثة مباحث، تكلم المبحث الأول عن أبرز التهديدات السيبرانية، والتي شكلت تحديا أمنيا عالميا على جميع الأصعدة، وقد تناولنا في المبحث الثاني عن تداعيات الحروب السيبرانية على الأمن العالمي، أما المبحث الثالث تناولنا أبرز الحروب السيبرانية ودرجة تأثيرها .

وكان **الفصل الثالث** كآخر فصل للدراسة بعنوان آليات مواجهة الحروب السيبرانية، سواء المتعلقة بالجانب القانوني أو التقني، ويحتوي هو كذلك على ثلاثة مباحث، المبحث الأول الجهود الوطنية والاقليمية والدولية لتأمين الفضاء السيبراني، وقد تناول المبحث الثاني المسؤولية الدولية للحروب السيبرانية، أما المبحث الثالث والأخير تم تخصيصه للاستراتيجية السيبرانية للدول للدفاع عن نفسها تحت مظلة القانون الدولي .

الفصل الأول

الإطار النظري والمفاهيمي للدراسة

المبحث الأول : الفضاء السيبراني والتحول في المفاهيم .

لقد تمخضي عن ثورة المعلومات وظهور الأنترنت ببروز بيئة جديدة وهي **الفضاء السيبراني** (Cyber space)، اضافة الى المجالات الأربعة البر- والبحر- والجو – والفضاء، وتأثيرها على النظام الدولي . وكان للمجال الخامس في تحول جديد للأمن و القوة والصراع .

المطلب الأول : الفضاء السيبراني والتحول في الأمن العالمي .

أولا : مفهوم الفضاء السيبراني :

ظهر مصطلح الفضاء السيبراني في ثمانينيات القرن الماضي في احدى روايات الخيال العلمي للكاتب الأمريكي –**الكندي المشهور وليام جيبسون**، حيث يعتمد هذا المجال الافتراضي على نظم الكومبيوتر ، وشبكات الانترنت ومخزون هائل من المعلومات والبيانات، فيتم التواصل بالشبكات عبر الهواتف وأجهزة الحواسيب ، وغيرها دون التقيد بالحدود الجغرافية[1].

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

هناك من عرّف الفضاء السيبراني بوصفه الذراع الرابعة للجيوش الحديثة [2]، وهناك من يرى أنه البعد الخامس للحرب، وهذا تعريف يحصر الفضاء السيبراني في المجال العسكري فقط دون التطرق للمجالات الأخرى .

وعرفته **الوكالة الفرنسية لأمن أنظمة الاعلام** (ANSSI)، وهي وكالة حكومية مكلفة بالدفاع 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 ومتواصلة بينيا بالمنشآت وتكنولوجيات الاعلام بما فيها الانترنت وشبكات الاتصال، والحواسيب، الدارات للبرمجة، وسائل الرقابة ..."[4]

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].

1- ربيع محمد يحي ، **إسرائيل وخطوات الهيمنة على ساحة الفضاء السيبراني في الشرق الأوسط** ، رؤى استراتيجية ، المجلد الأول، العدد 3،2003 .ص67.

2- عباس بدران ، **الحروب الالكترونية : الاشتباك في عالم متغير**، مركز دراسات الحكومة الالكترونية ، بيروت،2010، ص4.

3 - Olivier KEMPF, Introduction à la Cyberstratégie, Paris,Economica,2012,P 9.

4- بلغرد لطفي أمين ، **الفضاء السيبراني: هندسة وفواعل**، المجلة الجزائرية للدراسات السياسية ، العدد الخامس ، 2016، ص ص 151-152.

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 وادراك كل دولة أو هيئة، وعلى حسب قدرة واستراتيجية الدول في مواجهة والمخاطر والتهديدات في هذا الفضاء الغامض المعقد .

ثانيا : الفضاء السيبراني والتحول في الأمن العالمي .

بدأ التركيز على الفضاء السيبراني كتهديد أمني جديد بفعل أحداث دولية، إلا بعد أحداث 11سبتمبر 2001، بعدما استخدمته تنظيم القاعدة كساحة قتال ضد الولايات المتحدة الأمريكية، و في عام2007 برز بوضوح دور الفضاء السيبراني كمجال جديد في العمليات العدائية في الصراع بين استونيا وروسيا ، وفي عام 2008 في الحرب بين روسيا وجورجيا، وجاء الهجوم السيبراني بفيروس ستاكسنت على برنامج ايران 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 والاعلامي الكاسح، لحسم الحرب بسرعة وتجنب السكان فظائع وآلام المواجهة، وكان الهدف من هاته الاحتجاجات عبر الفضاء السيبراني هو شحن الرأي العام واسقاط النظام من الداخل بدلا من استخدام القوة العسكرية الخارجية مثل جرى للعراق.

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

وتكمن العلاقة بين الفضاء السيبراني والأمن العالمي في اتساع قطاع مستخدمي وسائل الاتصال وتكنولوجية المعلومات في العالم، وتبني الحكومات الالكترونية من جانب العديد من الدول وربطها بمصالحها القومية والاستراتيجية، فهي اليوم في تزايد مع امكانية التعرض المصالح الاستراتيجية من أخطار وتهديدات سيبرانية، وتصبح مصدر وأدوات جديدة للصراع الدولي المتعدد الاطراف، ودورا في

---

[1] - The International Télécommunication Union, **ITU Toolkit for Cybercrimelégislation**,Geneva,2010,P 12.

[2] - عادل عبد الصادق، **أسلحة الفضاء الالكتروني في ضوء القانون الدولي والانساني**، وحدة الدراسات المستقبلية، مكتبة الاسكندرية، مصر،2017،ص 12 .

[3] - Martin C.libicki ,**conquestion cyberspace :National Security and information warfare** (New York :Combridge University Press, 2007) :1-14

تغذية 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 ان تبحث في أولوية الامن السيبراني، واستراتيجية توفر وحماية المعلومات من مخاطر التهديدات السيبرانية، التي تغير من مضامين الأمن العالمي، وفي نفس الوقت فتح الباب أمام التعاون ومواجهة الاخطار 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 الاساسية ، وأصبح التفوق في مجال الفضاء السيبراني عنصرا حيويا في تنفيذ عمليات ذات فاعلية في الارض 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 والامكانيات المادية وغير المادية، المنظورة وغير المنظور التي بحوزة الدولة . يستخدمها صانع القرار في فعل مؤثر يحقق مصالح الدولة، وتؤثر في سلوك الوحدات السياسية الاخرى [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 الاخرى وذلك عبر أدوات سيبرانية"[3]، كما يوضح **جوزيف.س ناي** أن مفهوم القوة السيبرانية يشير الى " مجموعة الموارد المتعلقة بالتحكم والسيطرة على أجهزة الحاسبات والمعلومات والشبكات الالكترونية والبنية التحتية المعلوماتية والمهارات البشرية المدربة للتعامل مع هذه الوسائل[5]".

---

[1]- عادل عبد الصادق ، نفس المرجع ، ص17.

[2]- عادل عبد الصادق نفس المرجع ،ص 17

[3] - Asenio .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 الحجمل، وبجدي كامل ،الجمعية المصرية لنشر المعرفة والثقافة العالمية، القاهرة ،1997،ص82.

[5] 3- Joseph S.Ney JR, **Cyber power** , Harvard Kennedy School,2010,P03.4 **Ibid** , P 04

ولقد جدد **جوزيف ناي** ثلاث أنواع من الفاعلين الذين يمتلكون القوة السيبرانية " Cyber power [1]" :

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 اي هجوم يتطلب مشاركة ومساعدة من طرف اجهزة استخباراتية متطورة، وهذا لا يمنعهم من استهداف واختراق الانظمة 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[2]:

-الشركات متعددة الجنسيات: تمتلك بعض الشركات قدرة تفوق الدول، ولكن تنقصها الشرعية التي مازالت حكرا علة 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 الاجرامية: تقوم هذه المنظمات الاجرامية بعمليات القرصنة السيبرانية، وسرقة المعلومات واختراق الحسابات البنكية وتحويل الاموال، كما توجد سوق سوداء على الانترنت المظلم Dark internet لتجارة المخدرات والاسلحة والبشر ، حيت تكلف هذه الجرائم مليارات الدولارات سنويا .

-الجماعات الارهابية: تعد من ابرز الفواعل الدولية، خاصة بعد أحداث 11سبتمبر، حيث تستغل الفضاء السيبراني في عمليات التجنيد والتعبئة والدعاية وجمع الاموال 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 للدّول .

ولقد اصبحت القوة السيبرانية (Cyber power) حقيقة أساسية في العالم بكل مظاهرها المتنوعة من دعم ومساندة العمليات الحربية والقوة الاقتصادية والسياسية، وطبيعة النظام الدولي، واعطت دفعا رئيسيا في تدعيم القوة الناعمة للدول، حيث بات الفضاء السيبراني مسرحا للهجمات السيبرانية، ونشر المعلومات المظللة، وحرب نفسية. مما دفع بالدول إلى الزيادة في الإنفاق لتأمين وحماية بنيتها التحتية، وبالتالي القوة السيبرانية لها تأثير في صنع القرار في النظام الدولي.

[1] -1 Joseph S. Nye JR , Ibid , P 10.

[2] - ايهاب خليفة ، **القوة الالكترونية وأبعاد النحول في خصائص القوة** ، مكتبة الاسكندرية ، 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 سبتمبر2001، فكان الفضاء السيبراني ساحة للصراع والقتال بين تنظيم القاعدة والولايات المتحدة الامريكية، وفي عام 2007 جرت العمليات العدائية بين استونيا وروسيا، وهو ما حدث ايضا 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 الصّراعات الدولية[1].

ولعل ما يعزز انتشار الانشطة 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 . اشكالية تعامل الدول مع الشركات التكنولوجية متعددة الجنسيات، والتي اصبحت تفوق قدراتها، مثل مواقع التواصل الاجتماعي كالفيس بوك وتويتر واليوتوب 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 ايديولوجية أو اقتصادية أو سياسية، ويتمدد الصراع السيبراني بداخله شبكات الاتصال والمعلومات متجاوزا الحدود التقليدية وسيادة الدول.

وأن التّطور الذي فرضه الفضاء السيبراني، انعكس على المجتمع الدولي في التفكير في حركة و ديناميكية الصّراع 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

[1]- سليم دحمان ، **أثر التهديدات السيبرانية على الأمن القومي: الولايات المتحدة انموذجا**، مذكرة مقدمة لنيل شهادة ماستر اكاديمي، كلية الحقوق والعلوم السياسية ،قسم العلوم السياسية، جامعة المسيلة، 2018/2017، ص 27.

[2]- عادل عبد الصادق، **أسلحة الفضاء الالكتروني في ضوء القانون الدولي** ، سلسلة أوراق، العدد23، مكتبة الاسكندرية،مصر،2016، ص17-18.

[3]- عادل عبد الصادق ، مرجع سابق، ص 38

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

ويشهد الصراع السيبراني الدولي اليوم، صراعا و تنافسا حول الاستحواذ على التقدم التكنولوجي والسيطرة على الانترنت، والمواقع والتحكم بالمعلومات والعمل على اختراق الامن 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 والافكار وشن حرب نفسية اعلامية.

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

المبحث الثاني : 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.

المطلب الأول : 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 اجماع 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 .

أولا: فالحرب جاء في لسان العرب، أن الحرب : نقيض كلمة سلم، ورجل حرب أي شجاع، الحرب :أن يسلب الرجل ماله ، والحارب : الناهب[2].

[1] - **Dunn . information Age Conflicts :2-6**

[2] - العلامة ابن منظور ، **لسان العرب** ، المجلد الأول ، دار لسان العرب ، بيروت.

وفي موسوعة (**لاروس**) الحرب :هي صراع قوة بين شعبين أو بين فرقتين من بلد واحد، أو بين متصارعين يريد كل واحد منهما الحصول بالقوة على شيء لم يستطيع الحصول عليه بطرق أخرى، ويحدث هذا بقيام دولة بتحقيق أطماعها، وتقوم الثانية بالدفاع عن مصالحها[1].

وفي قاموس (**لوروبير**): 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[2].

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

ثانيا : فالسيبرانية مأخوذة من (**سيبر- Cyber**) ، وتعني صفة لأي شيء مرتبط بثقافة الحواسيب أو تقنية المعلومات أو الواقع الافتراضي ، فالسيبرانية تعني فضاء الانترنت[3] .

يقول **جيفري كارل مؤلف** -كتاب Inside cyber warfare - أنه " باستطاعة أي دولة أن تتبنى حربا الكترونية على دولة أخرى، خاصة على أنظمة الجيوش في العالم، وأصبحت متصلة بالأنترنت وتفتقد كل عوامل الأمان المطلق، ولا يقتصر الامر على الدول، ولكن حتى الافراد باستطاعتهم شن هجمات تسبب كوارث لدى العديد من الدول"[4] .

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 الاجراءات المتخذة في الفضاء السيبراني من قبل دول أو فاعلين غير دوليين، حيث تشكل تهديدا خطيرا للأمن القومي"[5].

وتعرف الحرب السيبرانية بأنها " حرب تخيلية أو افتراضية Virtual – Reality ذات طبيعة غير ملموسة ، تحاكي الواقع بشكل شبه تام ، وهي حرب بلا دماء ، اذ أدوات الصراع تكمن بالمواجهات الالكترونية والبرمجيات التقنية ، وجنود من برامج التخريب المحوسبة ، وطلقات من لوحات المفاتيح ونقرات المبرمجين"[6].

ويرى بعض القانونيين أن ديناميكيات عمل الحروب السيبرانية تتقارب من ناحية قانونية مع اشاعة الرعب والارهاب. واسنادا لهذا يمكن تعريف الحروب السيبرانية بأنها "نظام قائم على الرعب

---

[1] -Grand Larousse Encyclopédique ,tome cinquième ,libraire Larousse ,paris,1979.

[2] - Le Robert , dictionnaire , alphabétique et analogique de la langue française , tom troisieme , société la nou – veau livre , paris ,1978.

[3] - د.الكيالي عبد الوهاب ، **الموسوعة السياسية** ، الجزء الثاني ، المؤسسة العربية للدراسات والنشر ، الطبعة الاولى ، بيروت ، 1981.

[4] - مركز نورس للدراسات ، **الحرب السيبرانية " الالكترونية "** ،نقلة نوعية في الاستراتيجيات العسكرية واثر ملحوظ على العلاقات الدولية ، ص 6.

[5] - نفس المرجع ، ص 7.

[6] -Paulo & Jana Shakarian , Andrew Ruef **, Introduction to cyber warfare , A multidisciplinary Approach** ,Elsevier ,2013, P 02.

المنتشر في الشبكة العنكبوتية (الانترنت) ، والتي تهدف الى تنفيذ العديد من الاعمال لترويع أمن الافراد والجماعات والمؤسسات والدول وارهاقهم اقتصاديا ، وادخالهم في ازمات نفسية واجتماعية ناتجة عما يعرف بالإرهاب الصامت (Silent Terror)[1]".

ووفقا لقرار مجلس الأمن الدولي مؤخرا : "الحرب السيبرانية هي استخدام أجهزة الحاسوب أو الوسائل الرقمية من قبل حكومة أو بمعرفة أو موافقة صريحة من تلك الحكومة ضد دولة أخرى ، أو ملكية خاصة داخل دولة أخرة بما في ذلك : الوصول المتعمد أو اعتراض البيانات ، أو تدمير البنية التحتية الرقمية ، أو انتاج وتوزيع الأجهزة التي يمكن استخدامها لتخريب النشاط المحلي"[2].

والحروب السيبرانية "هي جزء فرعي من حرب المعلومات التي تنطوي على استخدام ساحة المعارك وادرة تكنولوجيا المعلومات والاتصالات في السعي لتحقيق ميزة تنافسية على الخصم "[3].

وتعني "أيضا نشاط متماثل أو غير متماثل، دفاعي أو هجومي على الشبكة الرقمية، منقبل فواعل دولية أو غير دولية، يهدف إلى إلحاق الضرر بالبنية التحتية الحيوية الوطنية، والأنظمة العسكرية "[4].

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

أما **التعريف الاجرائي للحروب السيبرانية: (** أنظر للشكل): "فهي حرب نشأة 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 .

---

[1]- مساعد كمال ، **الحرب الافتراضية وسيناريوهات محاكات الواقع** : مجلة الجيش اللبناني على شبكة الانترنت http://www.lebarmy.gov.lb/article.OSP?Inoor&id=11575253 تموز /يوليو 2006م.

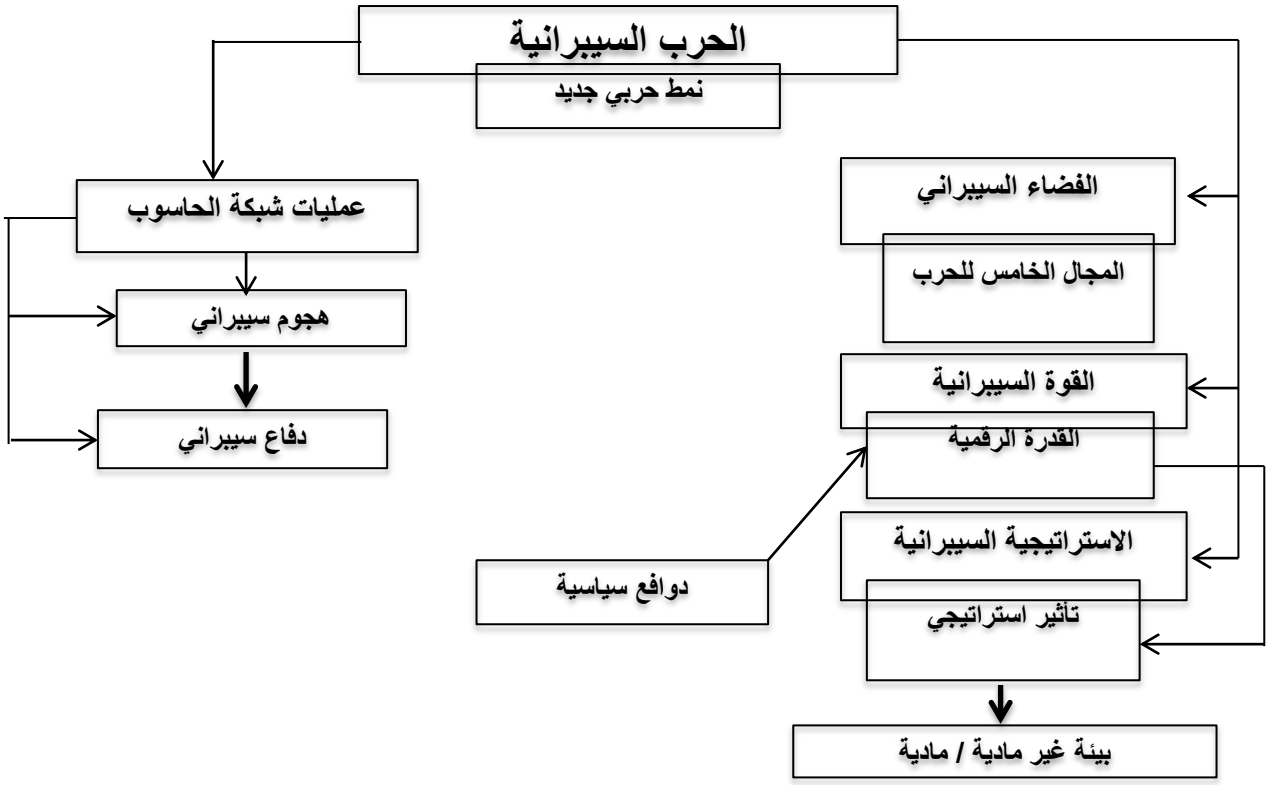
[2]- عياد سامي ، **استخدام تكنولوجيا المعلومات في مكافحة الارهاب** ، الطبعة الاولى ، الاسكندرية **Introduction to cyber warfare , A multidisciplinary Approach** ,Elsevier ,2013, P 02.

[2]- مساعد كمال ، **الحرب الافتراضية وسيناريوهات محاكات الواقع** : مجلة الجيش اللبناني على شبكة الانترنت http://www.lebarmy.gov.lb/article.OSP?Inoor&id=11575253 تموز /يوليو 2006م.، دار الفكر الجامعي ، 2007، ص 65

[3] - Schreier Fred, (2015) , **On Cyber warfare** , Dcaf Horizon Working Paper ,No, 7,P ?16.

[4] - Mbuthia Rex , **Cyber warfare versus Information Warfare** : Two Very Different Concepts , in the site :*http://bit.ly/20H4UKG*3 Ibid. Ibid. ,p,10

الشكل رقم (01) : مخطط تعريف الحرب السيبرانية .



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

ثالثا : خصائص الحروب السيبرانية

كل المؤشرات توحي بتغير في نمط الحرب من التقليدية إلى الحرب السيبرانية مستقبلا، وهذا ما استعى 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 ضخمة وتقوم بتصنيع أسلحة مكلفة 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 التحصن لوحدها أن تنجح . فالتحصن مع المزيد من عمليات الاختراق وبالتالي المزيد من الضغط .
- **مخاطرها تتعدى استهدف المواقع العسكرية:** لم تعد تنحصر الحروب السيبرانية باستهداف المواقع العسكرية، بل اصبحت تستهدف البنى التحتية المدنية والحساسة في البلدان المستهدفة ،

[1]- المجال الخامس .. **الحروب الالكترونية في القرن الـ21 (الجزيرة)** ، نشر يوم : 2011/01/12 على الموقع :*اطلع عليه يوم:2020/04/16*
https://stdies.aljazeera.net/ar/issues/2010/20117212274346868.htlm ≠3

وهو أمر أصبح واقعيا في ظل القدرة على استهداف شبكات الكهرباء والطاقة وشبكات النقل والنظام المالي والمنشآت النفطية بواسطة فيروس يمكنه احداث 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، بسبب التكاليف المنخفضة نسبيا، وهذا ما يعكس التحول والتغير في طبيعة الفواعل والأهداف[1].
- **أدوات الحروب السيبرانية :** تعتمد على الحاسوب، وتهدف إلى الحاق 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 راسها الانترنت والحاسبات والشبكات الحكومية والاكاديمية، والتجارية والمدنية، والمحطات البث التلفزي ومراكز استقبال الموجات السلكية واللاسلكية، وجميع ما يمكن ادراجه تحت هذا القطاع، لاعتمادها بشكل كامل على وسائل الاتصالات الحديثة[2].

ويعتبر هذا القطاع المحرك الرئيسي لجوانب الحوسبة والحوكمة في اي بلد، وله دور كبير في بناء البنية التحية 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 باي شكل كان[3].

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

2-قطاع الاعمال العسكرية والحربية: شهدت القطاعات العسكري والحربية تطورات عديدة، مما يجعلها تعتمد بشكل كبير على عنصر المعلومات والرقمنة، وحولتها الى بناءات تسلح بأجيال جديدة من الاسلحة التكنولوجية والاتصالية، مما زادت في قدرتها وفاعليتها على الدعم اللوجيستي (logistic) والتواصل المعلوماتي والاستخباراتي القائم على توفير عنصر التقنية الحديثة، وبالتالي زاد من الجاهزية و القوة لوسائل والادوات العسكرية والحربية[4]. لقد ارتبطت المرافق العسكرية ارتباطا وثيقا بالتطورات

---

[1]- زينب شنوف، **الحرب السيبرانية في العصر الرقمي**: حروب ما بعد كلاوزفيتش، المجلة الجزائري للأمن والتنمية، العدد02، المجلد 09، جويلية2020، ص97.

[2]- البدانة ذياب ، **الأمن وحرب المعلومات** ، **الطبعة الاولى** ، دار الشروق للنشر والتوزيع ، عمان ، 2006، ص 37 .

[3]- مرجع سابق ، ص 37-38

[4]- بورحلي ريمون ،**التكنولوجيا الحديثة في المجالات العسكرية** ، مجلة : الجيش اللبناني على شبكة الانترنت *ل ع :236 (فبراير /شباط 2005م).* *http://www.lebarmy.gov.lb/article.asp?ln=ar&id=70066*

التكنولوجية الحديثة، لتحدث نقلة نوعية في عالم التسلح اليوم ، رافقتها تهديدات امنية بكشف مآخذ ونقاط ضعف هذه المرافق لتحولها الى هدف من بين الاهداف التي تصوب الحروب السيبرانية نيرانها عليها، والقطاع العسكري هو نفسه من ينتج هذه النيران أو جزءا منها. لذلك تولي العديد من الدول والحكومات بالصناعة التكنولوجية العسكرية، وتقدم كل ما هو جديد في التطور الأمني لهذه القطاعات ورقابتها.

3-قطاعات الاعمال والأنظمة الحكومية وغير الحكومية: تعد هذه القطاعات عرضة لنيران الجروب السيبرانية، وخاصة ما تعلق بالعمل المدني والاداري، وتقديم الخدمات بشكل خاص. فهي اليوم تواجه تهديدات سيبرانية وبالأخص بين الحكومات أو تلك الشركات التي تعيش التنافس الرقمي[1] .

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 اجراءاتها الالكترونية، وتحليل وضبط تدفق المعلومات اليها، والتنسيق مع القطاع الحكومي، مما يعزز التنمية المستدامة داخل الدولة، كونها تؤمن مسؤولية مجتمعية تجاه الدولة[2]. وأن ضرب الخدمات الالكترونية للحكومات هو كسر قالبها الأمني ونزع الثقة عنها، وبالتالي خسارتها لجمهورها المتلقي .

4-قطاعات المعلومات الاعلامية والمجتمعية: تلعب الصحافة ووسائل الإعلام والاتصال في تقديم العديد من المعلومات والبيانات للجمهور المتلقي، عبر الوسائل التقنية والرقمية الحديثة ، حيث تختزل المسافات والاحداث للأفراد على مدار اليوم على شكل قالب معلوماتي له اهمية كبرى في ابراز ما يجري في العالم[3].

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

فالحرب الاعلامية (Media War) تعتبر حرب نفسية انعكاسا للحروب التقليدية المادية الموجودة في الواقع[4]، بحيث تحاول التأثير في نفسية والجند والجيش والجمهور المراقب، الامر الذي يخلق العديد من الاثار النفسية والاجتماعية عليه.

5-قطاعات الاقتصاد والمال والاعمال : يولي هذا القطاع الاهمية الكبرى بالمجال السيبراني، وهذا راجع للتحولات الاقتصادية والرأسمالية التي شهدها العالم في عقده الاخير ، وتوجه البشرية الى العمل

---

[1]- كلارك ريتشارد نك روبرت، **حماية الفضاء الالكتروني في دول مجلس التعاون الخليجية العربية**،ط1،ابوظبي، (م ا د ب ا عدد140،ص31-32.

[2]- كلارك ريتشارد نك روبرت ،مرجع سابق، ص32-33 .

[3]- معالي خالد ،**أثر الصحافة الإلكترونية على التنمية السياسية في فلسطين**، رسالة ماجستير غير منشورة ،كلية الدراسات العليا ، جامعة النجاح الوطنية ، غزة ، 2008م،ص 11 .

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

الاقتصادي والمالي عبر الفضاء السيبراني، والانفتاح الاقتصادي المرتكز على العنصر التكنولوجي، والذي ادخل البشرية في عصر اقتصادي معتمد وقائم على شبكات الانترنت والرقمنة كالبوصات وصكوك الاكتتاب الالكتروني والتجارة العالمية(*World Trade*)، ما جعلها عرضة للهجمات السيبرانية واصابتها يكلف الدولة خسائر ضخمة.

المطلب الثالث : أسلحة الحروب السيبرانية

1-التجسس الالكتروني : (***Spyware information***): تمثل وسائل التجسس التقني والمعلوماتي أجد أشهر وأقدم اسلحة الحروب السيبرانية ، وقد تم استخدام هذا السلاح منذ بداية الانسان لوسائل الاتصال والتواصل[1]. 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 الالكترونية الصادرة عن الاقمار الصناعية، والهواتف المحمولة وغيرها من الوسائل التجسس المعلوماتي، ذو الطابع القديم أو الحديث[2].

2-الاختراق الالكتروني: (***Pénétration Electronic***): هو عبارة عن انشاء برامج أو نظام الكتروني يهدف الى استغلال معلومات الخصم وتدميرها، إضافة الى افساد نظامه الحاسوبي والآلي وذلك بهدف التقدم عيه أمنيا عسكريا واقتصاديا وسياسيا، وقد تكون هذه المواجهة على المستوى الفردي أو المؤسساتي، أو على مستوى الدول[3]. كذلك هناك عدة أشكال للاختراق الالكتروني لكنها لها وظيفة واحدة وهي الدخول في قلب معلومات الخصم، والحصول عليها مستخدمة لأجل ذلك .

3-زرع الفيروسات التقنية في البيئات المعلوماتية : وهي عبارة عن برامج الكترونية مدمرة تعمل ضمن آلية معينة يحددها صانع هذه البرامج، ولها اشكال وأنواع متعددة تهدف الى اجداث فوضى في نظام تشغيل الضحية المنوي ضربه واستهدافه الكترونيا، وتلويث بيئته الالكترونية وتعطيلها[4]

4-**القرصنة الالكترونية** :(**Electronic Piracy**) تعتبر القرصنة من أضخم وأشمل الاسلحة السيبرانية المستخدمة عبر الفضاء الرقمي. يشمل هذا السلاح التقني على غالبية وسائل الصراع السيبراني في يومنا هذا، حيث تقوم آلية عمله على تجنيد العديد من الاشخاص المؤهلين والقادرين على التعامل مع الحاسوب بخبرة ودراية عالية جدا تمكنهم من اقتحام مختلف الوسائل الاتصالية، والنظم التكنولوجية من حواسيب وهواتف وموجات وغيرها، ويطلق على هؤلاء الاشخاص المؤهلين باسم ـ الهاكرز –(Hackers)[5].

---

[1]- مرجع سابق ، ص 178.

[2]- الشهري نوال ، **حرب المعلومات** : في مركز التميز لأمن المعلومات (جامعة ملك سعود) دت-*http://coeia.edu.sa/index.php/ar/assurance awarmess/articles/47-data-privacy-1263-informationwarfare.html*

[3]- حسين فاروق، **فيروسات الحاسوب الآلي** ، ، عربية للطباعة والنشر، الطبعة الثانية، القاهرة ،1999، ص07.

[4]- علوة رأفت، **قرصنة الأنترنت**، مكتبة التجميع العربي للنشر والتوزيع، الطبعة الاولى، عمان ، 2006، ص 23-24

[5]- يحي اليحياوي ،**حرب الاعلام والوقاية** ،موقع على شبكة الانترنت*http :www.elyahyaoui.org*

4-وسائل الاعلام: (Media) تلقى هذه الوسائل اقبالا كبيرا من قبل الجمهور المتلقي، نظرا لسرعة انتشارها وكثرة متابعيها، وتأثيرها على النفس البشرية. دخلت هذه الوسائل عالم الحروب السيبرانية عبر فضائيات التلفزة، ومحطات البث المحلي الملتقطة عبر الراديو ومواقع الفيديو الاجتماعي كاليوتيوب (Youtub)، والدبلاج الكاريكاتيري(Dubbing cartoon)، وغيرها من وسائل الاعلام الاخرى. وتستخدم العديد من الدول هذه الوسائل بشكل كبير خاصة في الخطابات السياسية، وهي سلاح متعدد الاطراف يتم توجيهه الى دولة أو نظام أو مجموعة بغية تهديدها والتأثير عليها نفسيا ومعنويا[1].

5-الاقمار الصناعية : (Satellites) هي أسلحة ذات دلالات استحواذية هدفها السيطرة على أكبر قدر ممكن من المعلومات ، وذلك عبر التقاط ملايين الصور للهدف وارسالها 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 تم استخدامها في الحرب الباردة[2]. في حين تستخدم الاقمار الصناعية في التشويش على المحطات الفضائية ومنعها من البث بأجندة وأهداف سياسية، هي تعبير جديد عن الحروب السيبرانية الدائرة في العالم الافتراضي كبعض التشويش التي تعرضت له قناة الجزيرة العربية خلال الثورات العربية.

6-**شبكات التواصل الاجتماعي : (Social Networks)** وهي تركيبات اجتماعية تقنية ذات محتوى رقمي، تقوم بربط الحلقات الاجتماعية ببعضها البعض كالعمل والدين وغيرها ، والتي تضم في طياتها مختلف الفئات العمرية وجميع المستويات الاجتماعية والاقتصادية، وكافة الدرجات الثقافية والتعليمية، وتتمثل هذه الشبكة باقة من المواقع ذات النفوذ القوي في العالم ومن أشهرها:

الفيس بوك face book،التويتر Twiter،اليوتوب Youtub،البريد الالكتروني E-mail،الماسنجر Messenger،غوغل بليس Google plus، المدونات الالكترونية وغيرها تعد بيئة أكثر تناسبا وتناغما مع الحروب السيبرانية ، واكثرها صراعا باعتبارها سهلة الوصول والاستخدام والتفاعلية، ولها شعبية كبيرة ومتطورة وذات طابع اصطيادي أي يمكن الايقاع بالضحايا الالكترونيين ،كما أنها منبرا حاشدا للتغيير السياسي.[3]

---

[1]- **حرب الفضاء والأقمار الصناعية: صراع استراتيجي جديد**، موقع شبكة النبأ المعلوماتية على شبكة الأنترنت،25شباط/فيبراير2008.*http://www.annabaa.org/nhaare.ws/69/a22.htm*

[2]- مرجع سابق ، ص89.

[3]- مراد فيصل ، **التحديات الإقليمية الراهنة للأمن القومي الجزائري**، رسالة ماجستير منشورة (المدرسة العليا للعلوم السياسية : قسم الدراسات العسكرية والاستراتيجية ،2014/2013 ، ص 2 .

الشكل رقم 02 :أشكال الحروب السيبرانية .

المصدر: القناة الاخبارية CNBC عربية : على الموقع : https://wwwcnbcarabic.com

المبحث الثالث : الأمن السيبراني و أبعاده

يشهد البعد الأمني على وجه الشمول والشؤون الاستراتيجية والعسكرية خصوصا، بروز تحديات أمنية لا تماثلية منذ نهاية الحرب الباردة، وبروز الفضاء السيبراني كوسيط ومصدر لأدوات جديدة للصراع الدولي، وباتت هذه التحديات الأمنية محورا مهما في مجال الحفاظ على الأمن 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 لـ غياب العناية ،ف"Sine" معناها "بلا "و cura" تعني "عناية"[1]

إلا أن الأمن كمصطلح يحمل معنيين متعارضين، فيقصد به إما حالة الأمن كمعنى مقصود ،أو حالة الأم ن من جهة أخرى، فقد عبر عنه في الأصول اليونانية بمصطلح :"Asphaleia " بمعناها الأمن والسلامة؛ والمشتقة من كلمة "Sphallo" والدالة على التعثر والسقوط[2].

كما أن كلمة "آمن" (Secure) تعني "Careless" (se+cura) أي الحرية من القلق و الاضطراب. فقد أشار "Larouse Moderne Dictionay" أن الاستخدام الفرنسي لا يدمج الأمن كإحساس بعدم الخوف ،وأشار "فافر دي دوخلاس Vavere de daugelas "إلى الانفصال أن الأمن يختلف عن اليقين والثقة.

ولكنه يقترب إلى الثقة. أما"Oxford English Dictionary" يمنح للكلمة معنيين ؛الأول يتجلى في الشروط التي تجعلنا في أمان ، والثاني يتمثل في الوسائل[3].

[1]- يوسف بوغرارة ، **الأمن السيبراني : الاستراتيجية الجزائرية للأمن والدفاع في الفضاء السيبيري**، مجلة الدراسات الافريقية وحوض النيل ، المركز الديمقراطي العربي، المجلد الأول ، العدد الثالث،2018، ص 105.

[2]- مرجع سابق، ص 105.

أما الجانب اللغوي للأمن " فهو نقيض الخوف أي السلامة ، وكلمة " الأمن " لغة مصدر الفعل أمن أمنا وأمانا وأمنة: أي اطمئنان النفس وسكون القلب وزوال الخوف، ويقال : أمن من الشر أي سلم منه ،وكذلك يقال أمّن فلان على كذا أي وثق به وجعله أمينا عليه...تعني الاطمئنان بأن الشيء في حرز وحماية من الخطر"[1] .

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

وتتجلى العلاقة التفاعلية بين "الأمن "و"الفضاء السيبراني"، بظهور مصطلح "الأمن السيبراني" ومنع يعتبر الأمن السيبراني:" هو مجموعة الوسائل التقنية والادارية ،التي يتم استخدامها لمنع الاستخدام غير المصرح به على شبكات الكمبيوتر، وسوء الاستغلال واستعادة المعلومات الالكترونية التي تحتويها بهدف ضمان استمرارية عمل نظم المعلومات ، وتأمين وحماية وسرية خصوصية البيانات الخاصة بفواعل الفضاء السيبراني"[2].

وترجع المقاربة الايتيمولوجية لمصطلح "**سيبار**" **Syber** ،هو لفظ يوناني الأصل مشتق من كلمة"Kybernetes"

بمعناها الشخص الذي يدير دفة السفينة، حيث تستخدم مجازا للمتحكم "governor".وتم استخدامها من طرف افلاطون للتعبير عن الحكم ، وتجدر الاشارة أن 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 وازدهار الثورة التقنية استبدل مصطلح الآلة بالحاسوب.

وقد قدمت وزارة الدفاع الأمريكية تعريفا دقيقا لمصطلح الأمن السيبراني بأنه "جميع الاجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكالها المادية والالكترونية، من مختلف الجرائم ،الهجمات، التخريب، التجسس، والحوادث.

واعتبر الإعلان الأوروبي أن معنى الأمن السيبراني: هو قدرة النظام المعلوماتي على مقاومة محاولات اختراق التي تستهدف البيانات، وهذا ما عبر عنه أستاذ الاتصالات بجامعة كاليفورنيا **ريتشارد كمرر**، حيث عرفه :"عبارة عن وسائل دفاعية من شأنها تكشف وتحبط المحاولات التي يقوم بها

[1]- ابراهيم مدكور، **المعجم الوجيز**: مجمع اللغة العربية ، ددن ، القاهرة ، 1989 ، ص 25 .

[2]- عكاظ ، **ما هو الأمن السيبراني** ،09:42، يوم:2020/06/22 على الموقع:*https ://www.okaz.com.sa/article/1585529/*

القراصنة"[1].وبالتالي الأمن السيبراني مفهوم أوسع من أمن المعلومات، أي يهتم بكل ما هو موجود على السايبر، على عكس أمن المعلومات الذي يهتم بأمن المعلومات الفزيائية (الورقية)[2].

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 ، وانما يرتبط بمجموعة من الأبعاد السياسية منها والعسكرية والاقتصادية والاجتماعية والثقافية والنفسية ...
- ✓ ***الديناميكية*** : يعني أن الأمن ليس حقيقة ثابتة ، ولا يوصف بالجمود بل هم مفهوم مرن ، ومتطور يعنى بأشياء مختلفة في أوقات وأماكن مختلفة، بمعن مسألة الأمن المتغيرة تتأثر بتطور الوضع الداخلي والدولي .

المطلب الثاني : أبعاد الأمن السيبراني .

يعتبر متغير الأمن السيبراني مفهوم ذات أبعاد نسبية أهمها :

1- **البعد العسكري** : كانت البدايات الأولى للأنترنت في البيئة العسكرية ، وبعد انتقلت إلى الأوساط العلمية والأكاديمية وأبحاث تخدم القدرات العسكرية، وتشتمل الميزة النسبية للأمن السيبراني في بعد العسكري، عن طريق قدرة القوة السيبرانية على ربط الوحدات العسكرية ببعضها البعض عبر العالم الافتراضي، وهذا ما يسهل عملية تبادل المعلومات ، والذي ينعكس ايجابا على تحقيق الأهداف العليا للمؤسسة العسكرية . كما توجد في هذا المجال عدة أمثلة توضح البعد العسكري للأمن السيبراني ومدى خطرة الهجمات السيبرانية ، وهو ما حصل في جورجيا، واستونيا، وكوريا الجنوبية، وايران على بعض الهجمات والاختراقات ، والتي أشارت إلى اندلاع صراع مسلح لاحق .كذلك الذي وقع بين جورجيا وروسيا ،أو بانقطاع الاتصال بالأنترنت في استونيا بين الدولة والمواطنين والتشويش على الادارات الحكومية[3].

كذلك اختراقات أنظمة المنشآت النووية الايرانية ، والتلاعب بها أدى إلى تهديد الأمن القومي للدولة المعنية .فسيناريوهات الهجمات السيبرانية نتائجها كارثية ، الأمر الذي العمل بجدية في تحقيق الأمن السيبراني دون التقاعس أو انتظار وقوع كارثة تكون نتائجها أكثر دراماتيكية[4] .

---

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

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

[3]- منى الأشقر جبور، **السيبرانية هاجس العصر**، المركز العربي للبحوث القانونية والقضائية، بيروت، 2017، ص 28.

[4]- نفس المرجع ، ص28.

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 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] بالمقابل 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 "ويكيليكس" أثرا سلبيا على العلاقات بين الدول ومصداقيتها[2].

3- **البعد الاجتماعي** : تعتبر الشبكة الدولية للمعلومات مجالا مفتوحا لجميع الأفراد، حيث يمكن لجميع المتعلمين السيبرانيين أن يستفيدوا من البنى التحتية والخدمات المتاحة لهم دون تحمل مخاطر أمنية ، وهنا يجب التنويه إلى ضرورة التحسيس بأخلاقيات الأمن السيبراني. بالمقابل ساهمت جميع فئات المجتمع في تطور الفضاء السيبراني، وذلك بتبادل الأفكار والمعلومات المختلفة ،وانفتاح المجتمع على الآخر، يؤسس لتبادل الخبرات والأفكار وتكوّن حاجات جديدة وآفاق 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 : الإباحية والترويج للإتجار بالممنوعات ، والارهاب، والتجنيد لقضايا تمس الأمن والسلام الدوليين، وعليه لا بدى من بناء مجتمع مسؤول ومدرك لمخاطر الفضاء السيبراني، والتعامل معه بحد أدنى من قواعد السلامة مع إدراك العواقب القانونية[4].

4- **البعد القانوني** : يترتب على النشاطات الفردية والمؤسساتية والحكومية في الفضاء السيبراني، نتائج قانونية تتمثل في ايجاد 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 ، والابلاغ عن المخالفات والجرائم السيبرانية ،وهذا ما أدى إلى ضرورة وجود ترسانة قانونية مع المتغيرات الحاصلة [3] . كذلك بروز تحولات جديدة على مستوى جميع المجالات ، وتصاعد ازدياد القضايا التي

[1]- منى الأشقر جبور، **السيبرانية هاجس العصر**، المركز العربي للبحوث القانونية والقضائية، بيروت، 2017، ص 28.

[2]- نفس المرجع ، ص29

[3]منى الأشقر ، مرجع سابق ، ص 29.

[4]- نفس المرجع ، ص 29

رفعت أمام المحاكم ، مما يستدعي اعداد بيئة تنظيمية تشريعية ، وبناء ميثاق لمكافحة الجرائم السيبرانية والحكم[1].

1 **البعد الاقتصادي** : يرتبط الأمن السيبراني ارتباطا وثيقا بالاقتصاد، فقد توسع استخدام تقنيات المعلومات والاتصالات ما أتاح وعزز التنمية الاقتصادية للعديد من البلدان فرص الاستخدام التي تقدمها الشركات الدولية الكبرى، ولا ننسى حلول عصر المال الالكتروني ضمن بيئة تقنية متحركة كوجود المحفظة الالكترونية ، واصدار البطاقات التي تسمح بالدفع الالكتروني[2].

2 المطلب الثالث : 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 الادارة 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) مثلا، وثمة ارتباط شديد بين التوافر ويسر النفاذية (Accessibility)[3]

2- السلامة : Integrity

إن المحافظة على استقامة البيانات، أو معالجة الخدمات يعني وقايتها من التعديل العارض أو المقصود من التلاعب أو التدمير، وهذا لضمان الدقة وبقاء ها 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 المعلومات المعترضة، ويمكن توفير هذه الحماية بواسطة آليات أمن مثل[4]:

•مراقبة صارمة على النفاذ .

---

[1]- 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، ص –ص ،229-231.

[2]- منى الأشقر جبور، **السيبرانية هاجس العصر**، المركز العربي للبحوث القانونية والقضائية، بيروت، 2017، ص 28.

[3]- Electronic money régulation 2011(EMR2011)& the payement service Régulation 2009.

[4]- الاتحاد الدولي للاتصالات، دليل الأمن السيبراني للبلدان النامية، مكتب تنمية الاتصالات، جنيف ، سويسرا ، 2006، ص 22.

•تشفير البيانات .

•الحماية من الفيروسات والديدان أو أحصنة طروادة.

3- **السرية : Confidentaility** ويقصد بذلك الحفاظ على سرية المعلومات، والمعاملات ،والخدمات ، أو الاجراءات التي تجري في الفضاء السيبراني ،وهي تتضمن حماية الموارد والافشاء غير المرخص به. كما يمكن تنفيذ السرية عن طريق مراقبة النفاذ والتشفير .كما يساعد التشفير على حماية سرية المعلومات أثناء الارسال أو التخزين وتحويلها بشكل غير مفهوم لأي شخص لا يمتلك وسائل فك هذا التشفير[1].

الشكل 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 •الاعتمادية •المتانة •الاستمرارية •الصواب	•التصميم •الأداء •علم تصميم الآلات بما يناسب الجسم البشري •نوعية الخدمة •صيانة التشغيل
توفير النفاذ للكيانات المرخص لها (بينما يمنع للكيانات غير مرخص لها)	•السرية •السلامة (لا تغيرات)	•التحكم في النفاذ •الاستيقان •مراقبة الأخطاء •التأكد من التماسك •التشفير
التحقق من الاجراءات	•عدم الرفض •اليقين (بعيد عن الشك) •عدم المماراة	•شهادة التصديق •التسجيل ، امكانية الاقتفاء •التوقيع الالكتروني •آليات البرهان

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

[1]- نفس المرجع ، ص 22.

خلاصة الفصل الأول :

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 تسمى 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 يشكل جزءا أساسيا في السياسة الأمنية للدول بحيث أصبح لدى صناع القرار له أولوية في سياساتهم الدفاعية . وسيطر الأمن السيبراني على عقائد جيوش العالم

الفصل الثاني

الحروب السيبرانية وتحديات الأمن العالمي .

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 تحيا أمنيا عالميا، ومن أبرز التهديدات السيبرانية هي كالآتي:

المطلب الأول : الجريمة السيبرانية.

أصبح الفضاء السيبراني بيئة جديدة للمجرمين السيبرانيين، وصنع عدة جرائم تسمى " الجريمة السيبرانية " والتي تشمل القرصنة، 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 فهي "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 الكترونية أو شبكة الأنترنت، أو بث عبر محتوياتها، وهي ذلك النوع الذي من الجرائم التي تتطلب الإلمام الخاص بتقنيات الحاسب الآلي، ونظم المعلومات لارتكابها أو التحقيق فيها ومقاضاة فاعليها[2].

وكذلك "هي 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 الانترنت بشكات تكنولوجية لتسهيل ارتكاب الجريمة[1]. وبالتالي الجريمة السيبرانية هي إساءة استخدام تكنولوجيا المعلومات والاتصالات من طرف المجرمين ، وذلك على أنها جرائم أنترنت .

[1]- منى الأشقر جبور، **السيبرانية هاجس العصر**، المركز العربي للبحوث القانونية والقضائية، بيروت، 2017، ص 50.

2- عبد الفتاح مراد ،شرح جرائم الكمبيوتر و الأنترنت، دار الكتب والوثائق المصرية، د ط ، وت ، ص 38 .

[3]- يوسف بوغرارة ، **الأمن السيبراني : الاستراتيجية الجزائرية للأمن والدفاع في الفضاء السيبيري**، مجلة الدراسات الافريقية وحوض النيل ، المركز الديمقراطي العربي، المجلد الأول ، العدد الثالث،2018، ص 105.

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 نظرا لعوبة تتبع مصدر الجريمة والتخفي وتزوير الهوية .
- ذكاء المجرمين والتطور التكنولوجي .
- مرتبط 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 تقدما 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 بعوامل سياسية واجتماعية وتقنية ومالية،أو بالحكومة...وتكون مرتبطة بعصابة أو جماعة "**الهاكرز**" Hockers[2] .

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 والحاق الضرر بالغير، والاعتداء على الأنظمة السياسية والأمنية والاجتماعية[3] .

---

[1]- صالح بن علي بن عبد الرحمان الربيعة، **الأمن الرقمي وحماية المستخدم من مخاطر الانترنت**، هيئة الاتصالات وتقنية المعلومات، ص09.

[2]- الاتحاد الدولي للاتصالات ، **دليل الأمن السيبراني للبلدان النامية** ، ص 35.

[3]- منى الأشقر ، مرجع سابق، ص 52 .

رابعا : أهم الجرائم السيبرانية

هناك عدة طرق مختلفة لاستغلال الامكانيات التي تتيحها تكنولوجيات الأنترنت، فهي تقوم في أغلب الأحيان على الخداع والاحتيال. ويمكن اعتبار العمل الجرمي قانونا جريمة سيبرانية عندما يستهدف الهجوم[1]:

- باتت الجرائم السيبرانية في تطور واستهداف العديد من المواقع على الأنترنت في المستقبل، ولعلى أشهر الجرائم السيبرانية هي اطلاق الفيروسات لما تسببه من خسائر اقتصادية، فقد تسبب فيروس "**تميدا**" على سبيل المثال في خسائر قدرت ب530 مليون دولار للاقتصاد الامريكي وكشف تقرير لمكتب التحقيقات الفيدرالي الامريكي **FBI** أن الخسائر المالية تجاوزت 3.5 مليار دولار في عام 2019 بسبب الجرائم السيبرانية[2].

- كما أن هناك عدة جرائم مصحوبة بالإرهاب مثل: التجسس السيبراني، والقرصنة، والجرائم المنظمة والمواقع التحريضية ضد المعتقدات الدينية، ومواقع متخصصة في القذف وتشويه صمعة الأشخاص والمواقع الإباحية، وتزوير البيانات، وغسيل الأموال، واتحال شخصية المواقع، والاغراق بالرسائل والحواسب الآلية، والاقحام والتسلل[3].

- **أمن المعلومات**: أي مصداقيتها وتوافرها وصحتها، وتندرج في هذا الاطار عمليات اختراق الأنظمة، عبر سرقة كلمة السر، أو التصيّد، 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 : الارهاب السيبراني

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

أولا: إن ارهاب الأنترنت مرتبط بطريقتين هما :

- ممارسة الأعمال التخريبية عبر شبكات الحاسوب والانترنت .

[1]- منى الأشقر، مرجع سابق ، ص50.

[2]- يمكن الاطلاع على موقع الانترنت : *http://www.computer world .com /Security topics/Security/vuris.*

[3] - Todd Amegilt .the Dark fruit of globalization :hostile use of the internet . carlisle barracks, PA.US. Army war .college, 2005,P.16

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

عرف **جيمس لويس** (James Lewiss) الارهاب السيبراني بأنه " استخدام أدوات شبكات الحاسوب في تدمير أو تعطيل البنى التحتية الوطنية المهمة مثل: الطاقة، والنقل، أو بهدف ترهيب الحكومة والمدنيين"[1].

وعرف الارهاب السيبراني على أنه "الارهاب الذي يعرف في الفضاء السيبراني ... ويفهم بدوره على أنه الاستخدام المنظم للعنف من أجل تحقيق أهداف سياسية[2].

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

ثانيا: وسائل الارهاب السيبراني .

1 –البريد الالكتروني: يعد من أبرز وسائل الارهاب السيبراني، حيث يستخدم البريد الالكتروني في التواصل بين الارهابيين، وتبادل المعلومات معهم .

2 –انشاء مواقع الأنترنت: لقد سهلت على المنظمات والجماعات الارهابية توسيع أنشطتهم من خلال تبادل الآراء والافكار 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[3].

المطلب الثالث : أنماط التهديدات السيبرانية .

تقسم التهديدات السيبرانية التي تواجهها الدول والأفراد إلى أربعة أنماط رئيسة وهي[4]:

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

حيث يتم اطلاق 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 ابطاء عمله، وهذا ما يسبب ضرر للمستخدم النهائي، وهو هجوم يهدف إلى إيقاف قدرة الهدف على تقديم الخدمات المعتادة ، وذلك عن طريق

[1]- Alix Desforges, **cyber terrorisme :quel périmètre** ?,fiche de L'Irsem n°11,2011,P 03

[2]- **دليل الأمن السيبراني للبلدان النامية** ، الاتحاد الدولي للاتصالات، ص 34 .

[3]- عبد الرحمان بن عبد الله السند، **وسائل الارهاب الالكتروني وحكمها في الاسلام وطرق مكافحتها** على الموقع :*http://shemela.ws/browse 20 page 1244-book.php/* تاريخ الاطلاع : *2020/05/01* .

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

اعتراف جهاز الحاسب الآلي المقدم للخدمة(server[1])،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 الشبكة 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 حربية، سياسية، اقتصادية ، مالية، مما يؤثر سلبا على مهام الخصم.

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[2]:

• التعرض لسرية الاتصالات التي تطال البريد الالكتروني، والدخول إلى الأنظمة والملفات دون إذن، وهذا يعتبر اعتداء على الحريات والحقوق الشخصية.

• التلاعب بالمعلومات الموجودة في نظام معين، وتشويهها أو اتلافها، سواء عبر الاختراق أو نشر الفيروسات .

• الجرائم العادية التي تستخدم الأنترنت كالسرقة، والغش وسرقة الهويات، والاعتداء على الملكية الفكرية وغيرها.

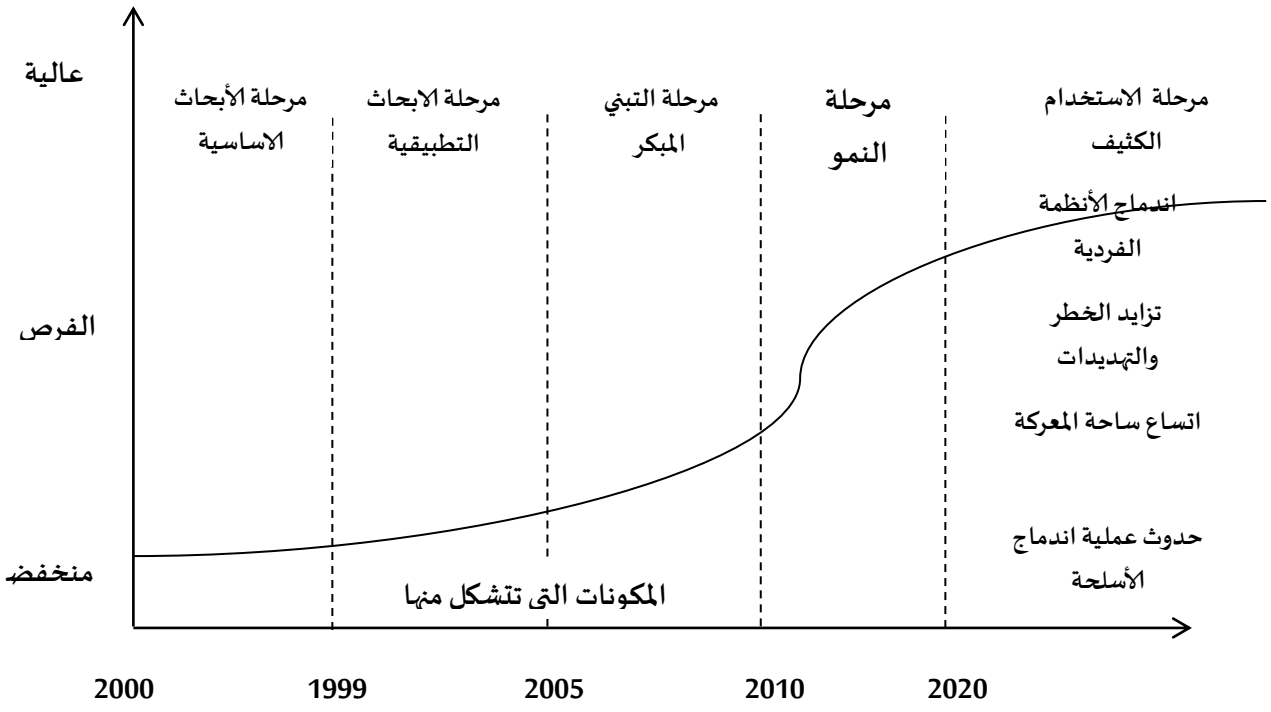
[1]- انوران شفيق، **أشكال التهديدات الالكترونية**، المركز الاوروبي لدراسات مكافحة الارهاب والاستخباراتECC، 29 يناير 2020.

https://www.europarabct.com/?p=34807

[2]- منى الأشقر ، مرجع سابق ، ص353

الجرائم التي تندرج في اطار الجريمة المنظمة، والتي تهدد أمن الأفراد والدول، كتبييض الأموال والارهاب....إلخ.•

شكل04: 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.

المبحث الثاني : تداعيات الحروب السيبرانية على الأمن العالمي

تمهيد : لقد اصبح التعامل الحالي في الفضاء السيبراني عبر شبكة الأنترنت، والتي بنيتها الأساسية هي التقنيات الحديثة، والحاسوب هو القاعدة الأساسية لهذا الفضاء، مما تسبب في بروز تهديدات سيبرانية فشكلت تحديا أمني عالمي، وسيبراني خاص .

المطلب الأول : تصاعد تأثيرات الحروب السيبرانية

تختلف الحروب التقليدية على الحروب السيبرانية، فالأولى مادية ومفهوم يستخدم لوصف مجموعة متنوعة وهائلة من الظروف والسلوكيات، وبداية من خالة النزاع المسلح بين الدول مثل (الحرب العالمية الثانية)، وصولا إلى الحروب الرمزية. أما الثانية مصطلح يستخدم لوصف كل شيء متعلق بحملات

التخريب وتعطيل الأنترنت، وصولا إلى حالة الحرب الفعلية باستخدام الرسائل الالكترونية ، ولها ثلاث معالم رئيسية[1]:

1-الحروب السيبرانية تهدف إلى مآرب سياسية محددة.

2-الحروب السيبرانية دائما " **وحدة عنف** " أساسية .

3-الحروب السيبرانية تمتلك فضاء مستضيفا لها ، وهو الفضاء السيبراني . كما أن الحروب التقليدية فضاؤها البر ، والبحر ، والجو .

وحاليا تحول الولايات المتحدة الأمريكية الوصول بالحروب السيبرانية إلى مستوى الحروب المادية من حيث طبيعة التأثير والنتائج، وأصبح هدفها أن تحقق الهجمات السيبرانية قدرا كبيرا 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 الالكترونية، أو السيطرة عليها[2].

ولقد استطاعت وكالة الاستخبارات الأمريكية والاسرائيلية تصميم فيروس "**ستكسنت** Stuxnet"،يعمل على اختراق وتعطيل المنشآت النووية الايرانية، وقد كان هذا الهجوم دقيقا إلى درجة تحديد عدد أجهزة الطرد المركزي، وبالتالي تم تعطيل هاته الأجهزة بمهارة فائقة، وجعل سرعة الدوران متفاوتة وهذا ما 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 تلحق بالبلدان إلى نشوب حرب باردة، وانقسام ايديولوجي بين الغرب والصين[3].

ومع انتشار "**فيروس كورونا** " **Covid19** في 200 دولة في العالم، زاد عمل القراصنة باستغلال الأزمة الوبائية و تحقيق أهداف شخصية ، وهذا مع توجه الكثير من الشركات والمؤسسات للدول لتبني نمط العمل

---

[1]- نجوى السودة ، **بحث الفضاء السيبراني** ، مؤتمر حروب الفضاء السيبراني ،أطلع عليه يوم :2020/7/05، على الموقع : *نشر يوم: https://scomf.wordpress.com/15/05/2015*

[2]- نفس المرجع على الموقع: *https //scomf.wordprees.com*

[3]- نجوى السودة ، مرجع سابق. 1

عن بعد والتعليم عن بعد، وزيادة الاستهلاك و الاعتماد على الأنترنت والأدوات الرقمية ، وأصبحت هاته البيئة جاذبة لكثير من قراصنة المعلومات وممارسة هوياتهم المفضلة في الاختراق أكثر من ذي قبل[2] .

المطلب الثاني : مظاهر تهديد الارهاب السيبراني لأمن الدول

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

1- تهديد أمني سياسي: تعمل المنظمات الارهابية على الحاق الضرر وشل أنظمة القيادة والسيطرة على الاتصالات ،أو تعطيل أنظمة الدفاع الجوي ،بالإضافة إلى اختراق البريد الالكتروني لرؤساء وكبار المسؤولين للدول والشخصيات السياسية، ونشر رسائل مضللة. ففي عام 2010 قامت مجموعة "**ويكيليكس**" بتسريب وثائق تحتوي معلومات سرية متداولة بين الادارة الأمريكية وقنصلياتها الخارجية بدول العالم[1]. وفي مارس هاجمت مجموعة "**سايبر بيركوث**" الأوكرانية المواقع الالكترونية لحلف الناتو مما أدى إلى تعطيل مواقع الحلف لعدة ساعات .

وأقرت وحدة الجرائم السيبرانية الأمريكية في أوت 2014بأن 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 الامريكي باراك أوباما وتعامله مع موظفيه داخل البيت الأبيض[2]، وهذا يعد تهديدا خطيرا للأمن القومي الأمريكي[1] .

أما أمنيا تعمل الجماعات الارهابية على التسلل الالكتروني 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 الارهابية باختراق النظام المصرفي ، والحاق الضرر بأعمال البنوك أو أسواق المال ،وتعطيل عملية التحويل المالي، ومن أمثلة ذلك قيام مجموعة "هاكرز" المحترفين بسرقة بيانات

[1]- ايهاب خليفة ، **الأمن المعلوماتي :لماذا تصاعدت التهديدات الالكترونية مع انتشار "كورونا"؟**، الموسوعة الجزائرية للدراسات السياسية والاستراتيجية ، العدد4868،يوم:2020/04/10

[2]- هاجر حسونة، **الإرهاب الالكتروني...هل يتحول إلى مصدر التهديد الأول في العالم**، نشر يوم: 5015/05/04 ، على الموقع :اطلع عليه يوم 2020/05/05. *https://alkhalijeonline.net/articles/*1430728333185670700/

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

بطاقات الائتمان من بعض أكبر مراكز التسويق الالكتروني الدولية، وخصم ملايين الدولار من أصحاب تلك البطاقات لتوفير تمويل أعمالها الارهابية 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 مصاريف عالمية، وسرقة نحو مليار دولار[2].

3 -**تهديد اجتماعي** : توجه المنظمات الارهابية رسائلها للإعلام والجمهور الخاص بالمجتمعات، والتي تقوم بترويعها وارهابها وذلك بهدف شن حملات وحرب نفسية ضد الدول، فهي تعرض أفلام مرعبة للرهائن والأسرى أثناء إعدامهم مما يؤثر على المدنيين، بشكل أساسي على كرامة الانسان والسلامة الشخصية ، والتحرش والملاحقة ،أو الترصد، ومع زيادة الاستعمال والادمان أدى تدريجيا إلى انفصال البشر عن محيطهم الاجتماعي البشري ، وهو ما يفقد العلاقات الانسانية مرونتها التقليدية .

المطلب الثالث : مخاطر الحروب السيبرانية على الأمن العالمي

تسببت الحروب السيبرانية من بروز 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 سيطرة استراتيجية .

2-**تعزيز القوة وانتشارها** : عمل الفضاء السيبراني على إعادة تشكيل قدرة الأطراف المؤثرة ، وأدى إلى عملية انتشار القوة بين فاعلين متعددين .

3-**عسكرة الفضاء السيبراني** : حيث برز في الاطار 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 الاجهزة 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 ، **الحروب السيبرانية :تصاعد القدرات والتحديات للأمن العالمي**، المركز العربي لأبحاث الفضاء الالكتروني، على الموقع : اطلع عليه يوم : 2020/04/16 . *http://accornline.com/article-detail.aspx?Id=28395*

4-**ادماج الفضاء السيبراني ضمن الأمن القومي :** بدأت الدول بتحديث جيوشها وتشكيل وحدات متخصصة في الحروب السيبرانية واقامة هيئات وطنية للأمن والدفاع السيبراني ، بالإضافة إلى القيام بالتدريب واجراء مناورات لتعزيز الدفاعات السيبرانية .

5-**الاستعداد لحروب المستقبل :** وهو ما نلاحظه اليوم من تبني العديد من الدول استراتيجية حرب المعلومات باعتبارها حرب المستقبل ، 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 الأنترنت ،والتي يمكن ممارستها وتوجيهها عبر جميع أنحاء العالم بشكل غير مضبوط، دون وجود اطار 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 سينجر والآن 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 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 مطور البرمجيات الخبيثة ،أو الهجوم السيبراني المباشر والكشف عن هويته[2].

المبحث الثالث : أبرز الحروب السيبرانية ودرجة تأثيرها

[1]- سليم دحماني ، مذكرة لنيل شهادة ماستر، مرجع سابق ، ص 51

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

لقد خلق الفضاء السيبراني 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 الاسرائيلي، أو الصراع الهندي الباكستاني، أو الصراع بين الكوريتين الشمالية والجنوبية .كذلك هناك حروب تشنها جماعات دولية للقرصنة للتعبير عن مواقف سياسية أو حقوقية مثل : جماعة "**ويكيليكس**" و "**أنونيموس**" وكذلك في الأزمات الدولية كالتوتر بين استونيا وروسيا في عام 2007، و وكذلك الاختراقات المتبادلة بين الصين والولايات المتحدة الأمريكية ، والصراع بين ايران واسرائيل مثل شن هجمات فيروس "ستكسنت" ضد المنشآت النووية الايرانية بالتعاون مع الولايات المتحدة الأمريكية في نوفمبر 2010[2].

وقد تعرضت روسيا للاتهام بالقرصنة في الانتخابات الرئاسية الأمريكية الأخيرة ، ودم المترشح الجمهوري "**دونالد ترامب**" في مواجهة منافسته الديمقراطية هيلاري كلينتون والتسلل إلى خوادم البريد الالكتروني للجنة الوطنية الديمقراطية، كما تم اختراق البريد الالكتروني الخاص بجون بوديستا رئيس الحملة الانتخابية الرئاسية لهيلاري كلنتون، وعلى اثرها تم طرد 35 دبلوماسيا روسيا[3].

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

[2]- عادل عبد الصادق ، نفس المرجع .

[3]- رغدة البهي ، الردع السيبراني : **المفهوم والاشكالات والمتطلبات**، الموسوعة الجزائرية لدراسات السياسية والاستراتيجية، العدد4741، نشر يوم:2019/11/27، على الموقع : *https://www.politics-dz.com*

كما شنت روسيا بشن هجمات سيبرانية على النرويج والتشيك، وبريطانيا، مما دفع الدول الأخيرة إلى اعلان 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 منطقة الخليج، وتدمير 35 ألف جهز كمبيوتر في شركة النفط " أراكوم " لتخريب صادرات النفط. وهجوم فيروس "ويناكراي" في عام 2017، والذي أتهمت به كوريا الشمالية[1].

المطلب الثاني : الحرب السيبرانية متوسطة الشدة .

يتجلى هذا الصراع في الفضاء السيبراني إلى الساحة الدولية موازيا لحرب تقليدية دائرة على الأرض ، ويكون ذلك تعبيرا على 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 التقديرات التي إلى أن تكلفة هذه الحروب قد تشكل أربعة أضعاف من انفاق نظيراتها التقليدية ، كما تقدر تكلفة تمويل حرب كاملة سيبرانية بتكلفة دبابة.

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

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

المبحث الثالث : الحروب السيبرانية مرتفعة الشدة .

ينشأ هذا النمط في الفضاء السيبراني منفردة، ومتوازية مع الأعمال العسكرية التقليدية، ولم يشهد العالم هذا النوع من الحروب، وان كانت احتمالات وردودها واردة في المستقبل مع تطور القدرات التكنولوجية، واتساع الاعتماد بين الدول والفواعل من غير الدول على الفضاء السيبراني

[1]- عادل عبد الصادق ، مرجع سابق .

[2] - Robert MC Million , **was stuxnet Built to A hack i ram's Nuclear – program** ,PC world, *http://www.pcworld.com/business center/ article/205827/was-stuxnet built- to-ahack-irans-nuclear-program-ht*

وينطوي هذا النوع من الحروب على سيطرة البعد التكنولوجي على ادارة العمليات الحربية، حيث يتم استخدام الأسلحة السيبرانية (الالكترونية) ضد منشآت العدو، وكذلك اللجوء إلى الروبوتات الآلية Robots Automation في الحروب بدون طيار Dorn ، 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 وادارتها عن بعد بخلاف تطوير القدرات في مجال الدفاع والهجوم السيبراني في الاستحواذ على القوة السيبرانية.

وفي هذا السياق يتم أيضا 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 من حالة نشوب صراع[1] .

ولقد شهدت الأسلحة في هذا المجال تطورا أكبر في قدرتها على التأثير في الخصوم، مثل أسلحة الميكروويف عالية القدرة ، وهو قامت به اسرائيل 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) :124-128, online e-article*, http://search .proquest.com/docuriew /200751259accountid=7180*

شكل رقم (05): أبرز الهجمات السيبرانية وخصائص تحديد مصادرها **

الحادث	السنة التي بدأ فيها	التأثير	تحديد المصدر في النطاق العام
مختبر لورنس بيركلي الوطني (الولايات المتحدة)	**1986**	اختراق بيانات حساسة واستخراجها	محاكمة جنائية في ألمانيا الغربية ، 1990
تايتن راين (Titan Rain) (الولايات المتحدة)	**2003**	استخراج بيانات حساسة من منظمات تشمل وكالة ناسا (NASA) ولوكهيد مارتن ومختبرات ساندیا الوطنية (Sandia Laboratoiers National) ومكتب التحقيقات الفيدرالي فضلا عن وزارتي الدفاع الأمريكية والبريطانيةLockheed MARTIN	عزته الحكومة والمصادر الخاصة في وسائل الاعلام بدرجة كبيرة إلى الصين في عام 2005 وهو ما عارضته الدولة الصينية
هجمات القطع الموزّع للخدمة الإستونية (استونيا)	**2007**	هجمات قطع موزّع للخدمة واسع النطاق على المواقع الالكترونية الإستونية في اطار التوترات مع روسيا	اتهمت الحكومة الاستونية جهات فاعلة حكومية روسية ألقت روسيا باللائمة على حركة شبابية مؤيدة للكرملين وليس على جهات فاعلة ترعاها الدولة
دودة ستوكسنت (ايران)	**2010**	أضرار مادية بأجهزة الطرد المركزي الايرانية أصيبت بها أجهزة الكمبيوتر عالميا	عزي بدرجة كبيرة إلى الولايات المتحدة واسرائيل؛ تسريبات من قبل مسؤولين أمريكيين

هجمات القطع الموزع للخدمة على المصارف الأمريكية (الولايات المتحدة)	**2012**	هجمات القطع المزع للخدمة على أكثر من 46 من أبرز المؤسسات المالية في الولايات المتحدة	تصور واسع لرعاية الدولة الايرانية ؛تسريبات أولية من الحكومة الأمريكية وفي نهاية المطاف اتهام الجهات الفاعلة الحكومية الإيرانية في آذار (مارس) 2016
أرامكو السعودية (السعودية	**2012 و2016**	مسح 35000جهاز كمبيوتر تابع لأرامكو السعودية أو تدميرها: هجوم مماثل في أواخر عام 2016	في عام 2012 ربط مسؤولون أمريكيون الهجوك بإيران في وسائل الإعلام
حساب وكالة أسوشيد برس (Associated Press) على تويتر (Twitter) (الولايات المتحدة)	**2013**	قرصنة وكالة أسوشيد برس على تويتر ونشر تغريدة كاذبة عن هجوم على البيت الأبيض ما أدى إلى هبوط حاد في أسعار الأسهم	تبنى الجيش السوري الالكتروني 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 الأول (ديسمبر)2014 وعزتها عملية أوبريشن بلوكباستر (Operation Blockbusrer) إلى مجموعة لازاروس(Lazarus) في عام 2016
غيت هاب(GitHub)	**2015**	هجوم قطع موزع للخدمة كبير ومتواصل على موقع	عزته الشركات الخاصة والباحثون بدرجة

(الولاياتالمتحدة)		التعاون لتطوير البرمجيات	كبيرة إلى جهات فاعلة حكومية صينية
قناة تي في 5 موند (TV5Monde) (فرنسا)	**2015**	تعطيل القناة التلفزيونية لمدة 18 ساعة؛ أدى الحادث المموه إلى الإلقاء باللائمة على داعش	عزته شركة فاير أي للمجموعة القرصنة الروسية أي بي تي 28(APT28) في حزيران (يونيو) 2015
المكتب الأمريكي لإدارة شؤون الموظفين (الولايات المتحدة)	**2015**	استخراج 21.5 مليون سجل خاص بموظفي حكومة الولايات المتحدة	عزي بدرجة كبيرة إلى الصين علما أن الحكومة الأمريكية لم تحدد رسميا المصدر
البرلمان الألماني(ألمانيا)	**2015**	استخراج ونشر 2.420ملفا حساسا ينتمي للاتحاد الديمقراطي المسيحي الألماني (Democratic Union Christian)	عزاه المكتب الفيدرالي لحماية الدستور(BFV) لمجموعة أي بي تي 28 في وسائل الإعلام في أيار (مايو) 2016
شبكة الكهرباء الأوكرانية (أوكرانيا)	**2016**	انقطاع الطاقة لساعات متعددة في محطات توزيع الطاقة الإقليمية وقطع الكهرباء عن 225.000مستهلك	اتّهم مسؤولون أوكرانيون روسيا؛ أشارت شركات خاصة إلى جهات فاعلة حكومية محتملة أو مجرمين 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 سترايك (CrowdStrike) (حزيران) (يونيو) 2016 وتقرير مكتب الاستخبارات القومية الأمريكي (كانون الثاني

			(يناير 2017) إلى جهات فاعلة حكومية روسية
البنك المركزي في بنغلادش (بنغلادش)	**2016**	سرقة مبلغ 81مليون دولار من حساب البنك المركزي في بنغلادش لدى البنك الاحتياطي الفيدرالي في نيويورك باستخدام نظام جمعية الاتصالات السلكية واللاسلكية بين المصارف على مستوى العالم في الميدان المالي المصرفي(SWIFT)	ربطه تقرير شركة سيمانتك بمجموعة لأزاروس في أيار(مايو) 2016 ؛ربطه تقرير وكالات الاستخبارات الأمريكية بدولة كوريا الشمالية وفقا لوسائل الإعلام في آذار (مارس) 2017
موساك فونسيكا (Mossack Fonseca) (بنما)	**2016**	تسريب 11.5 مليون وثيقة تمثل أكثر من 214.488 كيانا خارجيا أدت إلى تهم عديدة بالتهرب الضريبي والفساد	لم يحدد مصدر حتى تاريخه؛ نشطاء محتملون من القراصنة الالكترونيين أو عملية داخلية
دين (Dyn) (الولايات المتحدة)	**2016**	هجوم قطع موزع للخدمة باستخدام شبكة مصابة من أجهزة أنترنت الأشياء استهدف مزود نظام أسماء النطاقات دين وعطل عددا كبيرا من المواقع الالكترونية	لم يحدد المصدر رسميا ؛عزي بدرجة كبيرة إلى منظمة قرصنة ناشطة مثل أنونيموس(Anonymoous) أو نيو و ورلد هاكرز(New World Hackers) أو سباين سكواد (Spain Squad)
واناكري (عالميا)	**2017**	هجوم برنامج فدية طال قطاعي الرعاية الصحية والنقل والبنية التحتية للاتصالات في جميع أنحاء العالم	لم يحدد المصدر رسميا؛ ربطته بعض الشركات الخاصة بمجموعة لازاروس.

			ألقت روسيا باللائمة على الويات المتحدة لابتكارها برمجية إكسبلويت(Exploit) القادرة على تدمير برنامج واناكري

المصدر :مؤسسة ميكروسفت ،نشرته مؤسسة راندRAND،على موقعها الالكتروني :

www.rand.org/t/RR20181

خلاصة الفصل الثاني :

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 الأنترنت ، وفضاؤها قائمة على التكنولوجيا ، اقتحمت الأنظمة الالكترونية ، وانتهكت البيانات الشخصية ، وسبقت العمل العسكري ، واستهدفت السياسة والاقتصاد والمجتمع ، فخرقت الحدود الجغرافية واعتدت على سيادة الدول ،وبالتالي هي حروب لا يرى فيها المهاجم المدافع عدو مجهول ، وأنن 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

المبحث الأول : جهود الدول لمواجهة الحروب السيبرانية .

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

المطلب الأول : الجهود الوطنية لتأمين الفضاء السيبراني .

أولا : وضع التشريعات الوطنية للأمن السيبراني.

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

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

بالإضافة إلى أن معظم الدول الأوروبية، والآسيوية، والعربية، وغيرها من دول العالم التي أضافة إلى قانونها الجزائي ملحقا خاصا لمكافحة الجريمة السيبرانية (مثل الجزائر)، وهناك ثلاث دول عربية فقط سنت قوانين مستقلة لمكافحة الجرائم السيبرانية، وهي (السعودية، عمان، الامارات العربية المتحدة)، هذه الأخيرة تعتبر رائدة في اصدار 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 التقنية اللازمة لحماية النظم الحساسة والبنية التحتية والبيانات، فضلا عن حماية المستخدمين[2].

ثانيا : تشكيل هيئات وطنية للأمن السيبراني .

---

[1]- حسين بن أحمد الشهري ، **الارهاب الالكتروني – حرب الشبكات** - ، المجلة العربية الدولية للمعلوماتية ،2015، ص 19

[2]- فاروق حاتم ، **الامارات تتقدم المنطقة في اصدار 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.

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

- ✓ إعداد استراتيجية وطنية للأمن السيبراني، والسهر على تنفيذها.
- ✓ وضع السياسات وآليات الحوكمة والارشادات المتعلقة بالأمن السيبراني وتعميمه.
- ✓ وضع أطر إدارة المخاطر المتعلقة بالأمن السيبراني.
- ✓ وضع أطر الاستجابة للحوادث والاختراقات.
- ✓ وضع السياسات والمعايير الوطنية للتشفير.
- ✓ رفع مستوى الوعي بالأمن السيبراني.

ثالثا : بناء الجيوش السيبرانية

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

وحسب الوكالة الروسية للاستشارات الأمنية" **زيكوريون**" فإن الولايات المتحدة الأمريكية تنفق أكثر من أي بلد على مجال الفضاء السيبراني، فوزارة الدفاع لديها ميزانية ضخمة سنوية تقدر بـ 07 مليارات دولار للأمن السيبراني، وعدد الموظفين القراصنة يبلغ أكثر من 9000 موظف، وتنفق كل من الصين والمملكة المتحدة سنويا 1.5 مليار دولار و450 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 ، وتنفق وزارة الدفاع الروسية حوالي 300مليون دولار سنويا على مثل هذه الأنشطة[1] .

وحسب القناة الاخبارية CNBCعربية فأن أقوى جيوش العالم في الفضاء السيبراني:

الوحدة العسكرية الالكترونية

Cyber command

مجموعة شنغهاي

تلبيوت

[1] - أفضل خمسة جيوش الكترونية في العالم ، مركز الدراسات كاتيخون ، على الموقع :http://Katehon.com/ar/article/mhy-fdl-khms-jywsh-lktrwny-fy-llm-wm-trtyb-liysh-lsybrny-lrwsy تاريخ النشر: 2017/01/13،تاريخ الاطلاع : 2020/07/08 ، تاريخ المشاهدة : 2020/07/27

المطلب الثاني : الجهود الدولية السلمية لتأمين الفضاء السيبراني

أولا : الحد من سباق التسلح السيبراني

يلعب التسلح أهمية استراتيجية في توازن القوى على المستوى العالمي، في ظل بيئة مبنية على المصالح ويسودها الشك والغموض ،وتدمير تلك المصالح بسرعة الضوء، وهو ما يحمل خطورة عسكرة الفضاء السيبراني ،الأمر الذي جعل كثير من الدول تتبنى استراتيجية الحروب السيبرانية كحرب للمستقبل، وأن النصر في المعركة حليف من يقدر على شل القوة والتشويش على المعلومة[1].

لقد بدأ سباق تسلح خطير لتطوير الأسلحة السيبرانية، وكانت بداية ظهورها بحسب المختصين في الصراع الروسي – الأستوني ، والروسي – الجورجي، والتطور البارز مع فيروس" ستاكسنت " الموجه ضد المنشآت النووية الإيرانية، والذي أتهمت بتطويره إسرائيل والولايات المتحدة الامريكية .

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 العمل على تحقيق التفوق التقني.

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

وحسب **جوزيف ناي** أنه يمكننا أن نتعلم من تاريخ العصر النووي. في حين أن التكنولوجيات السيبرانية والنووية تختلف اختلافا كبيرا، فإن العملية التي يتعلم المجتمع من خلالها التعامل مع تكنولوجيا شديدة التعطيل تظهر تشابه مفيدة، ولقد استغرق عقدين من الزمن للوصول إلى اتفاقيات تعاونية في العصر النووي وفي المجال السيبراني اقترحت روسيا عام 1999 معاهدة للأمم المتحدة لحظر الأسلحة الالكترونية والمعلوماتية (بما في ذلك الدعاية)، ثم واصلت مع الصين وغيرها من أعضاء منظمة شانغهاي للتعاون، من أجل اتفاقية عامة منبثقة عن الأمم المتحدة [2].

اعتبرت الولايات المتحدة الأمريكية هذه الاتفاقية محاولة الحد من القدرات الأمريكية، ولا تزال تعتبر هذه الاتفاقية مظللة 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.

[1]- موقع CNBCعربية : https://wwwcnbcarabic.com ،تاريخ النشر : 2016/08/18.

[2]- عادل عبد الصادق ،**أسلحة الفضاء الالكتروني في ضوء القانون الدولي** ، سلسلة أوراق ، العدد23، مكتبة الاسكندرية، 2016، ص 64.

ولقد اسفرت أعمال تلك المجموعة في البداية عن نتائج هزيلة، ولكن بحلول جوان 2015، أصدرت تقريرا أقرته مجموعة العشرين يقضي بوضع معايير للحد من الصراع وأخرى لبناء الثقة[1].

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.

ثانيا : 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 ابرام صك قانوني عام 2013 يدعى " **دليل تالين** " Tallin manual، الذي أعدته مجموعة من الخبراء في القانون الدولي بدعوى من حلف شمال الأطلسي NATO، قصد دراسة مدى امكانية تطبيق قواعد النظام الدولي الانساني على الحروب السيبرانية، وذلك إثر الهجوم السيبراني الشامل على إستونيا عام 207 من طرف روسيا[2].

ويحتوي دليل " **تالين** " على 95 قاعدة قانونية ارشادية، لعمل أو سلوك الدول في سياق الحرب السيبرانية (الالكترونية). وصدر الإصدار الثاني في العام 2017 ، ويحتوي على 154قاعدة، ليشكل مستوى أكثر اتساعا لمعالجة العمليات الالكترونية، ومراجعة وحسم لنقاط عدم الاتفاق في الإصدار الأول[3].

وتتمثل تحدياته الرئيسية في ضمان توجيه الهجمات ضد الأهداف العسكرية فقط، وتوخي الحذر لحقن دماء المدنيين وحماية البنية التحتية المعلوماتية لحياتهم، وهذا لوجود فضاء سيبراني واحد تتقاسمه الجيوش المسلحة والجيوش السيبرانية مع باقي المستخدمين المدنيين [1]. كما يجيب على أهم النقاط الحساسة المرتبطة بالحروب السيبرانية والهجمات السيبرانية، سواء تنفذها دول أو من غير الدول، وكيفية ادارة الحروب السيبرانية والصراع في الفضاء السيبراني، بالإضافة إلى مراعاة القانون الدولي الانساني كمبدأ التمييز، والشرعية في استهداف المقاتل السيبراني بالوسائل العسكرية المادية كالطائرات العسكرية بدون طيار Drones .

---

[1]- جوزيف س ناي ، **التحكم في الصراع السيبراني**، مدونات الجزيرة ، على الرابط: *http://blogs.aljazeera.net/blogs/2017/* تاريخ النشر 2017/09/8، تاريخ الاطلاع : 2020/07/10.

[2]-جوزاف .س ناي، **التحكم في الصراع السيبراني** ، مدونات الجزيرة ، على الرابط:*http://blogs.aljazeera.net/blogs/2017/8* تاريخ النشر 2017-09-08، تاريخ الاطلاع:2020/07/20.

[3]- سعيد درويش ،**ماهية الحرب الالكترونية في ضوء قواعد القانون الدولي**، حوليات جامعة الجزائر 1، العدد29،ص 119.

ويعتبر دليل "**تالين**" الهجوم السيبراني على أنه "عملية الكترونية سواء هجومية أو دفاعية يتوقع أن تتسبب في اصابة أو قتل أشخاص أو الاضرار بأعيان أو تدميرها"، ولكن لم يتفق الخبراء حول" الضرر "، بحسب اقرار كل بلد بحجم الأضرار التي تبرر خوض الحرب، وهو ما يعرف بمبدأ الحق في اللجوء إلى الحرب"Jus in bellum " ،بشرط تكون مبررة وعادلة، لكي تضفي عليها صفة الشرعية[1].

ثالثا : الاتفاقيات الإقليمية والدولية لأمن الفضاء السيبراني .

نظرا لخطورة وسرعة التهديدات السيبرانية ومواكبة مع تطورها، تتطابق الاتفاقيات الاقليمية والدولية معها، ونذكر عدد من المبررات منها[2]:

- في عام 2002: وضعت مجموعة بلدان الكومنولث قانونا نموذجيا لمكافحة الجريمة السيبرانية، بالإضافة إلى قانون الإثبات الرقمي .
- في عام 2009: بادرت المجموعة الاقتصادية لغرب إفريقيا، إلى اقرار 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** تكتلا لمجموعة من الخبراء الأوروبيين وغير الأوروبيين كالولايات المتحدة، وافريقيا 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[3].

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

---

[1]- حير شهرزاد، **الادارة الدولية للتهديدات اللاتماثلية –الأمن السيبراني انموذجا-** ، محاضرة مقدمة لطلبة السياسة الدولية ، ماستر2، الموسوعة الجزائرية للدراسات السياسية والاستراتيجية، العدد10831،تاريخ النشر:27-11-2019،اطلع عليه يوم:2020/07/20.https://www.politics-dz.com

[2]- اللجنة الدولية للصليب الأحمر، **ماهي القيود التي يفرضها قانون الحرب على الهجمات السيبرانية**؟، على الرابط:https://www.icrc.org/ara/resources/document/faq/130628-cyber-warfare-q-and-a-eng-htm تاريخ النشر:28-03-2013، اطلع عليه يوم:2020/07/21.

[3]- سعيد درويش ، مرجع سابق ، ص 133.

ومن أهم قرارات الهيئة [1]:

- قرار صادر سنة 1990: حول قانون جرائم المعلوماتية.
- قرار صادر سنة 1991: حول مكافحة الاستخدام الجرمي لتقنيات المعلومات والاتصالات .
- عام 2001: انشاء "مجموعة الخبراء الحكومية GGE "، بدأت عملها في 2004، لمناقشة الأخطار القائمة والمحتملة في مجال أمن المعلومات، والاجراءات 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[2] .
- في العام 2010: صدر قرار حول الأمن السيبراني، وملحق حول ضرورة أن تلجأ الدول لمعرفة تناسب أطرها التشريعية وقدرتها على مكافحة الجريمة السيبرانية.

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

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

المطلب الثالث : التعاون الدولي لمجابهة الهجمات السيبرانية .

بذل المجتمع الدولي العديد من الجهود لحظر استخدام أسلحة الدمار الشامل، والتقدم في شأن المناطق الخالية من السلاح النووي، وكانت كذلك حتمية العلاقة بين الأسلحة والتقدم التكنولوجي ، والتي أفرزت ثورة في الشؤون العسكرية، وضهور أسلحة للفضاء 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 الايجابي على السيادة الدولية، كإسهام تلك الاتفاقيات التي تحد من أنتشار الأسلحة النووية، والكيماوية ، والبيولوجية، حيث تسهم تلك الاتفاقيات في حال

[1]- منى الأشقر جبور ، **السيبرانية هاجس العصر**، مرجع سابق، ص103-

2- عادل عبدالصادق ، **الإرهاب الالكتروني في العلاقات الدولية : نمط جديد وتحديات مختلفة** ، مركز الأهرام الدراسات السياسية والاستراتيجية ، القاهرة ، 2009، ص 334

تطبيقها على الفضاء السيبراني والأسلحة التي يمنكن أن تستخدم فيه، من خلال وضع قيود على استخدامها وتوزيعها وانتشارها وتطويرها [1].

ويجب على الدول أن توافق على خضوع الانتهاكات أو 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 لمثل 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 حياديا وموضوعيا، 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 بدى من تغيير تنظيمي قانوني وسياسي وأمني وُقافي شامل. واطلاق حوار دائم يفرق بين الجريمة السيبرانية والارهاب السيبراني، وما يمكن أن يدخل ضمن الاستخدام السلمي وأن يتم التمييز بينهما .

ولكي 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 أساسين هما: مبدأ الضرورة العسكرية ، ومبدأ احتمالية الوقوع .
- التمييز بين الأهداف العسكرية والمدنية .
- التصديق على هذه المعاهدة من المحكمة الجنائية الدولية، حتى يتم تفعيل القانون الدولي لكي يتلاءم مع تلك الظاهرة .

[1]- منى الأشقر ، مرجع سابق ، ص 104.

[2]- عادل عبد الصادق، **أسلحة الفضاء الالكتروني في ضوء القانون الدولي الانساني**، سلسلة أوراق، العدد23، مكتبة الاسكندرية، ص،152.

[3]- نفس المرجع ، ص 153.

[4]- نفس المرجع ، ص ،153.

كما يمكن احكام حركة تفاعلها بالاستناد إلى[1] :

- وسائل المنع أو الوقاية التي تستخدم في تطبيق أحكام القانون الدولي لصالح الضحايا أو يتم تطبيق ها تطبيقا سلميا .
- وسائل للرقابة ؛وهي وسائل الاشراف المتواصل بما يتضمن الالتزام 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 التقنية	التدابير التنظيمية	
التعاون الدولي	تشمل الاهداف : وضع استراتيجيات لاستحداث تشريع نموذجي لمكافحة الجريمة السيبرانية قابل للتطبيق والاستخدام المتبادل عالميا.	يشمل الأهداف: تقديم مقترحات لوضع اطار للحوار والتعاون والتنسيق على الصعيد الدولي.	تشمل الأهداف : وضع استراتيجيات لإيجاد هياكل تنظيمية وسياسات عامة بشأن الجريمة السيبرانية والرصد والانذار والاستجابة للحوادث ونظام هوية رقمي تنوعي عالمي .	**4**
بناء القدرات	تشمل الأهداف : وضع استراتيجيات عالمية لتسيير بناء القدرات البشرية والمؤسسية في المجالات .	وتشمل 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.

[1]- عادل عبد الصادق ، مرجع سابق، ص، 154.

المبحث الثاني : المسؤولية الدولية للحروب السيبرانية .

تعد المسؤولية الدولية من أهم موضوعات القانون الدولي في الوقت الحاضر، وهذا نظرا لتأثيرات البالغة للتطورات 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 ضرر يصيب دولة أخرى أو عدة دول ،فتتحمل الدولة التي أحدث ذلك الضرر، أو تسببت في إحداثه، تبعا ت المسؤولية 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، لكنه نقص القواعد القانونية ،وصعوبة الأدلة والاثبات 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، أنه 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 دوليا :** 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 نجدها لمخافة لقواعد القانون الدولي، لأنها تسبب أضرار مادية وبشرية كبيرة، وهذا مخالف لمقاصد الأمم المتحدة .

3-**الضرر :** يعد 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 المفاعل

[1]- طلال ياسين العيسي، عدي محمد عناب، **المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر**، مجلة الزرقاء للبحوث والدراسات الانسانية ،العدد 01، المجلد 19 ، 2019، ص، 88.https://doi.org/10.12816/0054788

النووية الايرانية، والهجمات على البنوك، وسرقة المعلومات، كلفت تريليون دولار سنويا، لكن رغم توافر الركن للمسؤولية الدولية إلا انه يصعب الكشف عن هوية الفاعلين.

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، وممكن 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 ، لما يتسبب في اصابة أو قتل الأشخاص أو تدمير وشل المنشآت[2] . هذا الوضع هو مناسب ويوفي بالغرض، لكن يصعب على القانون التمييز في الهجمات السيبرانية ومصدرها، وبالتالي السؤال الذي يطرح هو أي أنموذج قانوني يجب أن يضم إطار للهجمات السيبرانية؟، فهذا الطرح يثير نقاش كبير ومحل اختلافات في مجال الحقوق القانونية والمسؤوليات التي تنتج عن الهجمات السيبرانية[3].

وأن مشروعية الأسلحة الجديدة يصب 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 يقوم بنشرها، أو تدرس نشرها لقواعد القانون الدولي الانساني.

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 "الاستعراض الدقيق والمتعدد التخصصات"، وذلك لضمان أن يتخطى تطور التكنولوجيا الحماية القانونية

[1] - طلال ياسين العيسى، عدي محمد عتاب ، **المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر** ، مجلة الزرقاء للبحوث والدراسات الانسانية، العدد الأول ، المجلد التاسع عشر، 20019، جامعة علجون الوطنية ، الأردن، ص 87.

[2] - Philip Levitz , **the law of cyber – Attack** , 2012, Vol. 100 ,Issue 4, P 833.

[3] - طلال ياسين العيسى، عدي محمد عتاب، نفس المرجع ، ص 87.

المكفولة، ويعد استخدام العمليات السيبرانية أثناء النزاعات المسلحة، مثالا جيدا على هذا التطور التكنولوجي[1].

المطلب الثالث : التكييف القانوني للحروب السيبرانية .

لا يزال مفهوم الحروب السيبرانية اختلافا بينا، وهذا ما أدى إلى أكبر تحدي يواجه القانون الدولي ويتجسد ذلك في ضرورة تكييف القوانين والبحث في مصدر التكييف وأساسه ، والمعضلة الأمنية ستكون كبيرة فيما لو تم الإقرار بوجود فراغ قانوني، أي عدم وجود قواعد قانونية محددة تنظم الحروب السيبرانية أو الهجمات، والسؤال الذي يطرح هو : هل توجد قواعد واجبة التطبيق في ظل تزايد مخاطر الحروب السيبرانية مهددة للأمن والسلم الدوليين ؟[2].

ويرى المختصون ذات الصلة بهذا الموضوع، أن المبادئ والقواعد التي أرساها القانون الدولي الانساني تنطبق على تلك الهجمات، وهناك من يراها العكس لأنها ذات صلة باستخدام وسائل وطرائق القتال، ولم تكن الوسائل الالكترونية تستخدم لأغراض عسكرية، ما يعني أنها غير مقننة أصلا[3] .

وأن تكييف استخدام الحروب السيبرانية يدور في فرضيتين اثنين، الأولى في عدم القدرة على اثبات الدليل المادي الناجم عن استخدام الهجمات أو الحروب السيبرانية، وهو العائق الأكبر الذي يواجه المختصون، 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[4] .

أما الفرضية الثانية فعلى العكس، إذ تثبت أن الحروب السيبرانية قد تؤدي إلى أثار مادية ملموسة على المستويات، الاقتصادية والأمنية والعسكرية كافة [5].

---

[1] أحمد العيسى الفتلاوي، **الهجمات السيبرانية : مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدلي المعاصر**، مجلة المحقق الحلي للعلوم القانونية والسياسية، العدد الرابع ، السنة الثامنة ،2016،ص،627.

[2] - نفس المرجع ، ص 628.

[3] - Emily Haslam **",Information Warfare**" : **Technological changes and international Law** ,Journal of conflict and Security law, Vol,5 ,200 0, p,157.

[4] - Micheal Schmit , **Bellum Amricanum :" the law of armed conflict into the next millenium**" , Newport: Naval War ,college, 1998,p,408.

[5] - أحمد العيسى الفتلاوي، مرجع سابق ، ص 629

فخطورة الحروب السيبرانية لم تحدد أثارها في ضوء الاتفاقيات الدولية إما بالحظر أو التقييد، وبالتالي يمكن أن تطال أثار الحروب السيبرانية وتؤدي إلى الدمار الشامل لنواحي الحياة ، وأن تكتم الدول العظمى وتفردها باستخدام الحروب السيبرانية، لأنها لا تحبذ أن يطرح هذا الموضوع 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 حصل في موضوع تأخر بتنظيم حظرا في انتشار الأسلحة النووية لعام 1968م، واتفاقية الحظر الشامل للتجارب النووية عام 1996م[1].

ومن خلال ما تقدم يبدو أن العائق في تكييف الهجمات السيبرانية بإحدى وسائل وطرق القتال ، انما يعود لصالح بعض الرائدة في مجال استخدامها، بالإضافة إلى قدرة الأنظمة الالكترونية في تحويل تلك الاستخدامات إلى برامج عدائية، وتحقيق أهداف سياسية .

المبحث الثالث : الاستراتيجية السيبرانية .

نظرا 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 .

عموما 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 قيام بأي نشاط ضار بالفضاء

السيبراني ، وإعطاء الادارة الأولوية لتأمين معلومات وزارة الدفاع ، كما يجب على الدولة حماية شبكاتها من خلال هيئاتها التشريعية، لسد أي ثغرات قائمة في قانون الأنترنت، وفهم طبيعة التهديدات فلا يمكن المقاومة بشكل فعال دون فهم الخطر .

- **لدفاع السيبراني التفاعلي :** يعمل على استعادة الفعالية، أو الكفاءة بعد الهجوم السيبراني الناجح، وهذه الفئات تشكل سلسلة متصلة من أنشطة الامن 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 الاخرى للقيام بحملة أسلحة مشتركة .

وهذا النوع من الدفاعات تبنته الولايات المتحدة الامريكية بعد 11 سبتمبر ، وأجازت فيه أعمال دفاعية ضد أي خطر يهدد أمنها. كما قامت ايران وكوريا الشمالية أيضا بالاعتراف بهذا النوع من الدفاعات.

ولكن على الصعيد الدولي فقد امتنعت محكمة لعدل الدولية عن ابداء رأي في هذا النوع من الدفاع بالرغم من أنها في قضائها سابقا كانت تجعل التحقق من الهجوم ووقوعه شرطا أساسيا لثبات الحق في الدفاع[1].

المطلب الثاني : مشروعية الرد على الهجوم السيبراني

نص المبدأ الثامن عشر (18)المتعلق بمجلس الأمن الدولي أن لمجلس الأمن الدولي أن يقرر وفقا للفصل السابع إن كان أي نشاط سيبراني يمكنه أن يهدد الأمن الدولي، أو يشكل عملا 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 أيضا، لا سيما إذا خرقت دولة من دول السلم والأمن الدوليين، أو لم تلتزم بواجب الحياد في أية حرب سيبرانية[2] .

وفي هذا الصدد، فإن دليل "**تالين**" يمنح الحق بشن الهجوم المسلح بعد الاعتداء ، وهذا بعد أن أصبحت الحروب السيبرانية تندلع ضمن ساحات رقمية في عالم افتراضي ، مما قد تسبب هذه الحروب في احتدام الصراع ويتحول سريعا إلى حرب حقيقية بالقنابل والصواريخ، لأن القادة العسكريون يمكن أن يفسروه بدعوة اطلاق أول ضربة استباقية في الحرب السيبرانية .

[1]- زينب شنوف ، **الحرب السيبرانية في العصر الرقمي : مابعد كلاوزفيتش** ، المجلة الجزائرية للأمن والتنمية ، العدد02، المجلد 09 جويلية 2020، ص 101.
[2]- يحي الزهراني ، مرجع سابق ، ص ، 241 .

وحتى يكون هذا الرد قانونيا ينطبق عليه صفة الدفاع الشرعي، وبالتالي على الدولة المعتدى عليها التي تنوي الرد أن تحسب المنفعة التي تكمن في هذا الهجوم العسكري مقابل الهجوم السيبراني الذي تعرضت إليه أنظمتها والمنشآت التابعة لها[1]. فالمادة (48) من الملحق الاضافي لاتفاقية **"جنيف "**حدد الأهداف التي تستطيع الدولة استهدافها، وهي الأهداف العسكرية حصرا، ومنعت اتفاقية **"لاهاي"** الرابعة تدمير أو مصادرة ممتلكات المدنيين ، وبالتالي انتهاك هذه القوانين يعتبر جريمة دولية ، يعاقب عليها في اتفاقية **"روما"** المنشئة للمحكمة الجنائية الدولية[2].

ويرى فقهاء القانون الدولي أن حالة التناسب تعرض مصالح وأرواح المدنيين للخطر، ويتسبب الهجوم السيبراني بتعطيل الأنظمة للبنية التحتية كالمستشفيات والمطارات، وهذا يتنافى مع مبادئ القانون الدولي الإنساني [3].

ولذا يجب على الدولة استخدام القوة في الرد على الهجوم السيبراني أن تميز بين الأهداف العسكرية والأهداف الحكومية الأخرى (المدني ين والمقاتلين)، دون تدمير المنشآت الحيوية لدولة المعتدية ، ولا تهاجم مصالح المدنيين تطبيقا لهذه المبادئ الانسانية.

المطلب الثالث : مصير سيادة الدول في ظل الحروب السيبرانية .

تعد فكرة السيادة والاعتراف بها للدول من المبادئ المتفق عليها في ميثاق الأمم المتحدة والاتفاقيات الدولية، ومنه السيادة هي من حق الدولة أن تسيطر على اقليمها والتمتع بمباشرة سلطتها عليه، ومع التطور التكنولوجي والتقني وتطور شبكات الاتصال في الفضاء السيبراني، وأصبح فضاء ومسرحا لبروز تحديات 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[4].

وفي ظل هذه المتغيرات تغير مفهوم التقليدي للسيادة، وأصبح ما يعرف اليوم بالسيادة الرقمية ،و التي تبسط الدولة سيطرتها وولايتها القضائية على الفضاء الرقمي المتمثل بالأنترنت الذي يجتاز حدود الدولة

[1] - Oren Gross, **Cyber Responsibility to Protect Legal Obligation of States Directly Affected by Cyber incident**, Cornell International Law Journal, Vol .48,p 504-510

[2] - Mecheal Gervais ,**Cyber Attack an Law of wars** , Berkeley Journal of International Law ,Volume 30,2012, p 560

[3] - ليث ناجح محمد ،**موقف القانون الدولي من الهجمات الالكترونية** ،مجلة كلية القانون للعلوم القانونية والسياسية، جامعة كركوك ، العدد24، المجلد7،جامعة كركوك ،2018، ص 20.

[4] - أحمد عيسى الفتلاوي، زهراء عماد محمد، **تكييف الهجمات السيبرانية في ضوء القانون الدولي**، مجلة الكوفة، العدد44، الجزء الأول ،2018،ص58

. بالتالي وضع الدولة أمام تحدي حقيقي إذ لا تستطيع الدولة فرض سيطرتها على مواطنيها في الفضاء السيبراني.

وتعتبر الأنترنت أداة جديدة وهامة وقادرة على تخطي الحدود الجغرافية ، وتخطي كل حاجز أمني بكل سهولة ، وايصال 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 تضاءل الانتماءات الوطنية مما يثير التساؤل بشأن نطاق سيادة الدولة، لتشرع الدول بمعالجة 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 الشمال الأطلسي إلى تأكيد منع استخدام البنى التحتية السيبرانية الواقعة في اقليم الدول التي تخضع لسيطرتها الكاملة ، في نشاطات تمس الحقوق السيادية للدول الأخرى[1].

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

[1]- أحمد عيسى الفتلاوي، زهراء عماد محمد، مرجع سابق ، ص 58

خلاصة الفصل الثالث:

نستخلص في هذا الفصل أنّ الدّول بذلت ما في وسعها من الجهود (الوطنية والاقليمية والدولية)، لمواجهة ومجابهة الحروب السيبرانية ومخاطرها، وأسهمت تلك الاتفاقيات والتعاون الدولي في وضع قيود في استخدام التكنولوجيا في رحم الفضاء السيبراني، دون احداث أضرار سواء مادية أو معنوية على المدنيين، لكن رغم كل هذه الجهود المبذولة، إلاّ أنّها لاتزال التّهديدات السّيبرانية هاجس بالنسبة للمجتمعات والدّول. لذا لا بدى من إرادة قوية من طرف الدول وخاصة الدول الرائدة في هذا المجال واستراتيجية سيبرانية شاملة تقف أمامها، بغية الوصول إلى تحقيق فضاء سيبراني سلمي وآمن .

خاتمة

خاتمة:

كان للتّطور التّكنولوجي وثورة المعلومات والاتّصال دور كبير في تطوير المجتمعات والدّول، وفي تشكيل فضاء سيبراني ازداد الاعتماد عليه من طرف الدّول والمجموعات والأفراد، وأصبح هذا الفضاء يعتمد عليها في جميع المجالات السيّاسّية والاجتماعية والاقتصادية والعسكرية.

وأحدث هذا الفضاء تغيّرات جذرية في مفاهيم العلاقات الدّولية كمفهوم الأمن والقوة والصّراع حيث برز الأمن السيبراني وتغيرت القوة بين الفاعلين ، وتحول الصراع إلى صراع سيبراني ، وأصبحت الحروب السيبرانية تطفو على السّطح كتهديد للأمن العالمي، وعليه دعت الضرورة إلى تطوير مفهوم الأمن لمواجهة الحروب السيبرانية، حيث جاء الأمن السيبراني كرد فعل على هذه التهديدات، والتي مست جميع مجالات الحياة المختلفة العسكرية والمدنية . فالاعتماد المتزايد على التكنولوجيا والاتصالات يوما بعد يوم ، زاد في التعرض إلى تهديدات سيبرانية بالغة الخطورة، وبالتالي يتعرض الأمن القومي لمخاطر كبيرة تهدد استقرار الدولة وتماسكها.

هذه الحروب السيبرانية تنوعت أشكالها، فبدأت بجرائم سيبرانية يقوم بها أفراد ومنظمات اجرامية كالاختراق والتّجسس وسرقة الأموال، وتطورت لتصل إلى التّخويف والابتزاز عن طريق الشبكة العنكبوتية ، لتصل إلى صراع بين الدّول وتهديد أمنها القومي، حيث ظهر جليا عسكرة الفضاء السيبراني، وإعداد جيوش سيبرانية تتمتع بمهارات وامكانيات عالية التأثير في شن حروب سيبرانية مدمّرة.

وفي ظل تحديات الحروب السّيبرانية على الأمن العالمي، سعت الدول والحكومات إلى بذل جهود في تطوير قدراتها، واتخاذ اجراءات وقائية لحماية بنيتها التحتية من أي هجوم سيبراني، كما شكلت جيوش سيبرانية تقوم بمهمة الدفاع والهجوم والحماية، أما في الجانب القانوني فطورت الدول منظومتها القانونية لتتلائم وتتكيف مع الحروب السيبرانية والهجمات الجديدة، وبما أن الفضاء السيبراني لا يعترف بالزمان والجغرافية بذلت الدول مساعي إقليمية ودولية، لوضع أطر قانونية واتفاقيات دولية لهذا الفضاء، كاتفاقية بودابست، وجامعة الدول العربية، ولعلى من أبرزها **دليل تالين** عدة مفاهيم غامضة في الفضاء السيبراني .

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

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

فالتّحدي اليوم هو الاستعداد للغد، فالواجب تطوير استراتيجيات 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 :

أولا : النتائج :

- الفضاء السيبراني بعد جديد يتميز بالغموض والتعقيد، وشدت تنوع تهديداته ، مما يجعل الأمن السيبراني كرافد جديد للأمن القومي، و أولوية مهمة في الاستراتيجية الأمنية للدول .
- التطور التكنولوجي والتقني سوف يؤثر تأثيرا كبيرا على السلوك الدولي، وهذا نتيجة الاعتماد على شبكات الأنترنت والاتصالات لدى الدول في خدماتها وتطبيقاتها، مما يزيد من التهديدات.
- في عصرنا الرقمي ، أصبح للفضاء السيبراني مجالا جديدا وهاما للتفاعلات الدولية، وقد أحدث تغيرات في مفاهيم القوة والأمن والصراع (الحرب)، وظهر فاعلون جدد، وانتشرت القوة السيبرانية بينهم، وازداد الصراع في الشبكات، قد يتطور أحيانا لتصبح حروبا جديدة أسلحة سيبرانية .
- الفضاء السيبراني أصبح مجالا جديدا هاما في التفاعلات الدولية ، وأحدث تغيرات في مفاهيم الامن والقوة والصراع ، وظهر فاعلون جدد ، وانتشرت القوة واشتد الصراع احيانا يصبح حروبا جديدة تقاد في الظل عبر شاشة الحاسوب سلاحها المعلومة ، وفضاؤها التكنولوجيا .
- الحروب السيبرانية لها طابع تقني خاص ، بحيث أنها تهديدات عابرة للحدود وانتهاك سيادة الدول ، وعليه تكون المواجهة تقنية بتحديث الجيوش وهيئات الأمن السيبراني ، ومواجهة قانونية بوضع التشريعات الوطنية والاقليمية والدولية ، والتعاون الدولي من اجل فضاء سيبراني سلمي .
- أن الحروب السيبرانية من المفاهيم الحديثة التي لا يوجد اتفاق دولي بشأن تعريفها ، مما يؤدي إلى صعوبة تكييفها ، وتحديد المسؤولية الدولية عنها .
- أن هناك سباق للتسلح السيبراني بين الدول ، وذلك لرغبة الدول المتزايدة في تعزيز دفاعاتها ضد أي هجوم سيبراني .
- أن الحروب السيبرانية ظاهرة عالمية ، يصعب مواجهتها إلا بالتظافر والتعاون، بين جميع الدول على المستوى الاجرائي والجنائي .

- أن هناك علاقة تبادلية بين التكنولوجيا والقانون ،فالتطورات التكنولوجية تفرض تشريعات قانونية تواكب جميع الأصعدة الداخلية والاقليمية 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 عاتها المسؤولية اللازمة، وتبني استراتيجيات شاملة بعيدة الأمد للتقليل من تداعيات الحروب السيبرانية .
- أن هناك جهود وطنية واقليمية ودولية، في مواجهة الحروب السيبرانية، وذلك من خلال عقد المؤتمرات والاتفاقيات لمنع الحروب والهجمات والجرائم السيبرانية، وكل ما يهدد الامن العالمي .

ثانيا : التوصيات :

- ضرورة إدماج الامن السيبراني في العقيدة الأمنية للدول، لما له من علاقة وطيدة مع قضايا التنمية السياسية والاقتصادية والاجتماعية .
- العمل على تحديث جيوش سيبرانية بتقنيات عالية للتعامل مع التهديدات السيبرانية، وأن يكون للمجتمع الدولي دور في العمل على الحفاظ على الطابع السلمي للفضاء السيبراني.
- أهمية نشاء لجنة دولية لا دارة الازمات السيبرانية من خلال دراسة الهجمات السيبرانية والعمل على التحقيق الدولي المستقبل حول المسؤولية السيبرانية حول تلك الهجمات.
- انشاء مركز تدريب لمكافحة الطوارئ المعلوماتية ، والعمل على بناء القدرات في مجال الامن السيبراني
- أهمية تعزيز التعاون الدولي في مكافحة مخاطر الحروب السيبرانية، والعمل على تبادل الخبرات. والعمل على عزيز النظم القضائية.
- أهمية العمل على المستوى الدولي في حل الصراعات الدولية، التي تحدث في الفضاء السيبراني وانعكاس التوتر على الأرض، ومواجهتها بالطرق السلمية.
- يجب تعديل ميثاق الامم المتحدة في بعض تصرفات، التي تهدد السلم والأمن الدوليين، ومنها الحروب والهجمات السيبرانية.

فهرس المصادر والمراجع

أولا : قائمة المراجع باللغة العربية

أ/ الكتب :

1. الاتحاد الدولي للاتصالات، دليل الأمن السيبراني للبلدان النامية، مكتب تنمية الاتصالات، طبع في جنيف سويسرا ، 2006 .
2. ايهاب خليفة ، القوة الالكترونية وأبعاد النحول في خصائص القوة ، مكتبة الاسكندرية ، 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 الاولى ، دار الشروق للنشر والتوزيع ، عمان ، 2006،
5. جوزيف ناي ، المنازعات الدولية، مقدمة للنظرية والتاريخ، ترجمة أحمد أمين الحجمل، وبجدي كامل ،الجمعية المصرية لنشر المعرفة والثقافة العالمية، القاهرة ،1997،.
6. حسين فاروق، فيروسات الحاسوب الآلي ، ، عربية للطباعة والنشر، الطبعة الثانية، القاهرة ،1999.
7. د.الكيالي عبد الوهاب ، الموسوعة السياسية ، الجزء الثاني ، المؤسسة العربية للدراسات والنشر ، الطبعة الاولى ، بيروت ، 1998
8. صالح بن علي بن عبد الرحمان الربيعة، الأمن الرقمي وحماية المستخدم من مخاطر الانترنت، هيئة الاتصالات وتقنية المعلومات.
9. عادل عبد الصادق ، أسلحة الفضاء الالكتروني في ضوء القانون الدولي ، سلسلة أوراق ، العدد23، مكتبة الاسكندرية،مصر،2016.
10. عباس بدران ، الحروب الالكترونية : الاشتباك في عالم متغير ، مركز دراسات الحكومة الالكترونية ، بيروت،2010.
11. عبد الفتاح مراد ،شرح جرائم الكمبيوتر و الأنترنت، دار الكتب والوثائق المصرية، الطبعة الأولى، الاسكندرية.
12. علوة رأفت، قرصنة الأنترنت، مكتبة التجميع العربي للنشر والتوزيع، الطبعة الاولى، عمان ، 2006.
13. عياد سامي ، استخدام تكنولوجيا المعلومات في مكافحة الارهاب ، الطبعة الاولى ، الاسكندرية، دار الفكر الجامعي ، 2007.
14. محمد خالد، الحرب الالكترونية، المكتبة العالمية للطبع والنشر، بغداد، 1986.
15. محمد شلبي، المنهجية في التحليل السياسي، مطبعة دار هومة، الجزائر،2007.
16. مركز نورس للدراسات ، الحرب السيبرانية " الالكترونية " ،نقلة نوعية في الاستراتيجيات العسكرية واثر ملحوظ على العلاقات الدولية .
17. منى الأشقر جبور، السيبرانية هاجس العصر، المركز العربي للبحوث القانونية والقضائية، بيروت، 2017 .
18. نهلا المومني، الجرائم الالكترونية، الطبعة الأولى، عمان .

ب/المجلات والمقالات:

1. زينب شنوف، الحرب السيبرانية في العصر الرقمي: حروب ما بعد كلاوزفيتش، المجلة الجزائري للأمن والتنمية، العدد02، المجلد 09، جويلية2020،
2. سعيد درويش، ماهية الحرب الالكترونية في ضوء قواعد القانون الدولي ، حوليات جامعة الجزائر ،العدد29.
3. لطفي أمين بلغراد، الفضاء السيبراني: 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 الزرقاء للبحوث والدراسات الانسانية، العدد01، المجلد19، 2019.
5. يوسف بوغرارة ، الأمن السيبراني : الاستراتيجية الجزائرية للأمن والدفاع في الفضاء السيبيري، مجلة الدراسات الافريقية وحوض النيل ، المركز الديمقراطي العربي، المجلد الأول ، العدد الثالث،2018.

ج/ المذكرات والبحوث :

1. ايهاب خليفة ، الأمن المعلوماتي :لماذا تصاعدت التهديدات الالكترونية مع انتشار "كورونا"؟، الموسوعة الجزائرية للدراسات السياسية والاستراتيجية ، العدد4868،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 ، 2008م،ص 11.
3. رغدة البهي ، الردع السيبراني : المفهوم والاشكالات والمتطلبات، الموسوعة الجزائرية لدراسات السياسية والاستراتيجية، العدد4741، نشر يوم:2019/11/27، على الموقع:
4. سليم دحمان ، أثر التهديدات السيبرانية على الأمن القومي: الولايات المتحدة انموذجا، مذكرة مقدمة لنيل شهادة ماستر اكاديمي، كلية الحقوق والعلوم السياسية ،قسم العلوم السياسية، جامعة المسيلة، 2018/2017، ص 27
5. عادل عبد الصادق، الهجمات السيبرانية :أنماط وتحديات جديدة للأمن العالمي، الموسوعة السياسية الجزائرية ، العدد 18601، يوم : 2019/11/27، على الموقع :
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 ، 2017/01/13.
7. فيصل مراد ، التحديات الإقليمية الراهنة للأمن القومي الجزائري، رسالة ماجستير منشورة (المدرسة العليا للعلوم السياسية : قسم الدراسات العسكرية والاستراتيجية ،2014/2013 .

د/القواميس :

1. ابراهيم 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.

ه/المواقع الالكترونية:

1. بورحلي ريمون ،التكنولوجيا الحديثة في المجالات العسكرية ، مجلة : الجيش اللبناني على شبكة الانترنت ل ع :236 (فبراير /شباط 2005م). http://www.lebarmy.gov.lb/article.asp?ln=ar&id=70066
2. تاريخ الاطلاع : 2020/05/01 .http://shemela.ws/browse .php/book-1244/page 20
3. حرب الفضاء والأقمار الصناعية: صراع استراتيجي جديد، موقع شبكة النبأ المعلوماتية على شبكة الأنترنت،25شباط/فيبراير2008
4. عادل عبد الصادق، الهجمات السيبرانية :أنماط وتحديات جديدة للأمن العالمي، الموسوعة السياسية الجزائرية ، العدد 18601، يوم : 2019/11/27، على الموقع : https://www.politics-dz.com
5. عبد الرحمان بن عبد الله السند، وسائل الارهاب الالكتروني وحكمها في الاسلام وطرق مكافحتها على الموقع :
6. عكاظ ، ما هو الأمن السيبراني ،09:42، يوم:2020/06/22 على الموقع :
7. فاروق حاتم، الامارات تتقدم في اصدار تشريعات الأمن السيبراني، جريدة الاتحاد ، على الرابط:
8. كمال مساعد، الحرب الافتراضية وسيناريوهات محاكات الواقع : مجلة الجيش اللبناني على شبكة الانترنت:
9. المجال الخامس .. الحروب الالكترونية في القرن الـ21 (الجزيرة) ، نشر يوم : 2011/01/12 على الموقع :اطلع عليه يوم :2020/04/16
10. مصطفى الطيب ،الفرق بين أمن المعلومات والأمن السيبراني ،10:30، 2020/06/23 على الموقع: https://www.oolom.com/6124
11. نجوى السودة ، بحث الفضاء السيبراني ، مؤتمر حرب الفضاء السيبراني ، تاريخ النشر : 05 /2014/05 ، على الموقع:https://seconf.wordpress.co
12. نوال الشهري، حرب المعلومات : في مركز التميز لأمن المعلومات (جامعة ملك سعود) ، على الموقع : http://coeia,edu.sa/index;php/ar/assurance-awarmess/articles/47-data-privacy-1263-informationwarfare.html
13. هاجر حسونة، الإرهاب الالكتروني...هل يتحول إلى مصدر التهديد الأول في العالم، نشر يوم: 5015/05/04 ، على الموقع :اطلع عليه يوم 2020/05/05.https://alkhalijeonline.net/articles/1430728333185670700
14. يحي اليحياوي ،حرب الاعلام والوقاية ،موقع على شبكة الانترنت: http:www.alyahyaoui.org

ثانيا: قائمة المراجع باللغة الأجنبية:

A/ Books:

1. Andrew Mclean, Electronic money régulation 2011(EMR2011)& the payement service Régulation 2009.

2. Joseph S.Ney JR, Cyber power , Harvard Kennedy School,2010,
3. Asenio .T.Gumahad , Cyber troopes 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 Informatiun Revolution and Changing International Operating Environment.
5. ITU, cyber Security Geneva: International Télécommunication Union (ITU)2008.
6. Martin C.libicki ,conquestion cyberspace :National Security and information warfare (New York :Combridge 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 Cybercrimelégislation,Geneva,2010

B/Articles:

1. -Fred Schreier, On Cyberwarefare, DCAF horzon 2015 Working paper No, 07.

2-Martin C.libicki , Conquestion Cyberspace :National Security and information warfare (New York) :Combridge University Press, 2007.

C/Dictionaries:

1. -Grand Larousse Encyclopédique ,tome cinquième ,libraire Larousse ,paris,1979.
2. -Le Robert , dictionnaire , alphabétique et analogique de la langue française , tom troisieme , société la nou – veau 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/docuriew /200751259accountid=7180
3. -https://www.europarabct.com/?p=34807
4. -Mbuthia Rex , Cyber warfare versus Information Warfare : Two Very Different Concepts , in the site: http://bit.ly/20H4UKG3 Ibid.

قائمة المصادر والمراجع

ملخص الدراسة:

"الحروب السيبرانية والأمن العالمي" **"Cyberian wars and Global Security"**

-التحديات والمواجهة - **-Challenges and Confrontation-**

ملخص الدراسة:

تعتبر الحروب السيبرانية من بين التحديات الأمنية المعاصرة في الفضاء السيبراني، وأصبحت واحدة من أهم الصراعات بين الدول الكبرى ، بحيث تستهدف القطاعات العسكرية والمدنية، كالتجسس والقرصنة والاختراق وزرع الفيروسات، لتعطيل وتدمير البنية التحتية المعلوماتية للدولة. كذلك أدت الحروب السيبرانية لإحداث تحول في مفاهيم الأمن والقوة والصراع في الفضاء السيبراني ، الذي يتميز بالتطور السريع ، والغموض الشديد، لتشكل تهديدا فعليا على أمن الدول وهو ما دفع بالأمن السيبراني يشغل صدارة أولويات الأمن القومي للدول، ما طرح الاشكالية :**"هل يمكن للحروب السيبرانية أن تشكل تهديدا على الأمن العالمي"**؟. وعلى إثر هذا سارعت الدول إلى بذل الجهود والتعاون على المستوى الاقليمي والدولي ، ووضع آليات قانونية وتقنية، وتبني استراتيجية سيبرانية لمواجهة الحروب السيبرانية والدفاع عن أمنها، وخلق فضاء آمن وسلمي.

أهم المفاهيم: الفضاء السيبراني، الهجمات السيبرانية، الجريمة السيبرانية، الأمن السيبراني، الاستراتيجية السيبرانية .

Summary

The cyberian wars were considered as one of the main modern security challenges. It becom one of the major conflict butween powerful nation. The started targeting both the mitary and civil field , such as , spy , piracy and lack. They took this conflect to another lelevel, (viruses) to break down and destroy the informational background. The world intrressed a radical change in some consepts such as : security , power, and conflict, in cuberian field which is characterized by fast progress and obscurity. As a result, this was consedered as a real threat against national security. It led to the cyberian security to be the alpha lion in national secutity. 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 confort the cyberian wars and keep peace .

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