جامعة 20 أوت 1955 –سكيكدة–

كلية الحقوق والعلوم السياسية

قسم العلوم السياسية والعلاقات الدولية

الحروب السيبرانية في العلاقات الدولية: المفهوم والظاهرة

مذكرة مكملة لنيل شهادة الماستر في العلوم السياسية تخصّص: علاقات دولية

إعداد الطالبة:

أمينة بوطاطة

إشراف الأستاذ:

د. رضا كشان

لجنة المناقشة:

الاسم واللّقب	الرتبة العلمية	الصفة
بشير شايب	أستاذ مساعد –أ–	رئيسا
رضا كشان	أستاذ محاضر –أ–	مشرفا ومقررا
وسام ميهوب	أستاذ مساعد –أ–	مناقشا

السنة الجامعية

1442/ 1443هـ

2022/2021م


بسم الله الرحمن الرحيم

الشكر وعرفان

قال تعالى: {رَبِّ أَوْزِعْنِي أَنْ أَشْكُرَ نِعْمَتَكَ الَّتِي أَنْعَمْتَ عَلَيَّ وَعَلَىٰ وَالِدَيَّ وَأَنْ أَعْمَلَ صَالِحًا تَرْضَاهُ وَأَدْخِلْنِي بِرَحْمَتِكَ فِي عِبَادِكَ الصَّالِحِينَ} سورة النمل 19.

وانطلاقًا من قول النبي ﷺ «لا يَشْكُرُ اللَّهَ مَنْ لا يَشْكُرُ النَّاسَ»

الحمد لله الذي أعانني على إتمام هذه الدراسة جعل الله فيها النفع والفائدة، فأشكر الله تعالى على ما منه علي، ويسر لي أمري في إعداد هذه الدراسة والشكر الجزيل إلى الأساتذة الكرام في قسم العلوم السياسية لتزويدي بالعلم النافع خلال فترة الدراسة، كما يسرني أن أتوجه بخالص الشكر لجنة المناقشة والتقييم، وعظيم الامتنان وعميق التقدير إلي أستاذي الفاضل الدكتور "رضا كشان " المشرف على هذا العمل الذي كان لي الشرف أن أضع اسمه على رسالتي العلمية، الذي أرشدني ووجهني ولم أجد منه إلا الصدر الرحب والخلق الطيب جزاه الله تعالى خيرا وأدام عليه العلم والفضل والنعم.

إهـداء

إلى روح والدي الطاهرة اسكنه الله فسيح جناته، إلى رمز الحب وبلسم الشفاء أمي،

إلى القلب الناصع البياض جدتي الغالية أطال الله عمرها، إلى روح جدتي الطاهرة

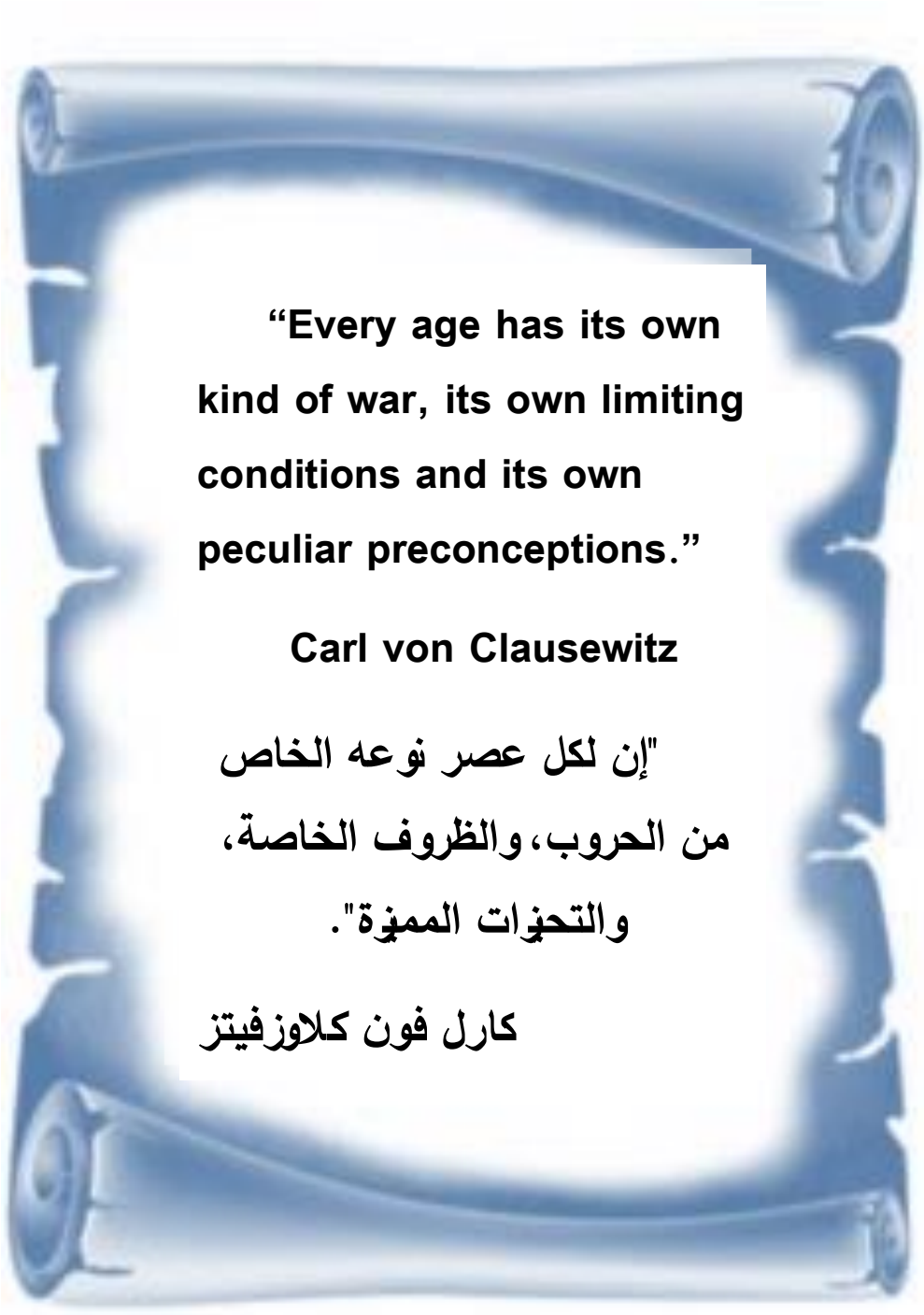
اسكنها الله فسيح جناته.

الى القلوب النقية الى أخي واخواتِ حفظهم الله،

إلى النفوس البريئة أبناء اخوات: أدم، إدريس، جواد، زين، غيث حفظهم الله،

إلى كل من اعرفهم من اساتذتي وأصدقائي وزملائي وكل من ساعدني في إنجاز

هذا العمل اليكم جميعا اهدي ثمرة جهدي وفقكم الله وسدد خطاكم.



“Every age has its own kind of war, its own limiting conditions and its own peculiar preconceptions.”

Carl von Clausewitz

"إن لكل عصر نوعه الخاص من الحروب، والظروف الخاصة، والتحيزات المميزة".

كارل فون كلاوزفيتز

خطة البحث:

مقدمة

الفصل الأول: الإطار المفاهيمي للحروب السيبرانية.

المبحث الأول: التّطور التاريخي للحروب الالكترونية.

المطلب الأول : نشأة وتطور الحُروب الإلكترونية.

المطلب الثاني : نشأة وتطور الحُروب السيبرانية.

المبحث الثاني: مفهوم الحرب السيبرانية.

المطلب الأول : تعريف الحُروب السيبرانية.

المطلب الثاني : أنماط الحروب السيبرانية.

المبحث الثالث: الفضاء السيبراني والتحول في المفاهيم.

المطلب الأول : مفهوم الفضاء السيبراني.

المطلب الثاني: مفهوم القّوة السيبرانية.

المطلب الثالث : مفهوم الأمن والصراع في الفضاء السيبراني.

الفصل الثاني: آليات وفواعل الحروب السيبرانية.

المبحث الأول: الأسلحة والعمليات العسكرية السيبرانية.

المطلب الأول: الأسلحة السيبرانية.

المطلب الثاني: العمليات العسكرية السيبرانية.

المبحث الثاني: فواعل الحروب السيبرانية.

المطلب الأول : الفواعل الدولاتية.

ملخص الدراسة :

تختلف أشكال الحروب من جيل إلى آخر، ومع التطور التكنولوجي والتقني الذي نعيشه، واستخدامه في الأغراض العسكرية طرأت تغييرات في مفهوم الحرب، كمواكبة للنظام الدولي وللتطور الحادث في مجال العلاقات الدَولية، حيث أصبح الفضاء السيبراني مجالاً هامًا للتفاعلات الدَولية، هذا المجال الغامض المليء بالتهديدات والمخاطر.

وفي هذا البحث المعنون بمفهوم وظاهرة الحروب السيبرانية في العلاقات الدولية، والاشكالية التي انطلقت منها الدراسة حول مدى تأثير ظاهرة الحروب السيبرانية على واقع العلاقات الدولية، سنحاول فك الغموض على مفهوم الحروب السيبرانية وبيان تأثيرها على العلاقات الدولية، من خلال عرض أهم نماذج للحروب التي تدار في الفضاء السيبراني، الذي أصبح مرتبط بالأمن القومي بشكل مباشر.

وفي ظل شيوع هذه الظاهرة خلصت الدراسة إلى عدة نتائج أهمها أن الحروب السيبرانية هي حروب ذات طبيعة تكنولوجية، والعديد من الدول تتسابق لتطوير قدراتها السيبرانية لاستخدامها كهجوم ضد دول أخرى أو كحماية لفضائها السيبراني، بالإضافة إلى إضعاف المفهوم التقليدي للقوة العسكرية.

الكلمات المفتاحية: الفضاء السيبراني، الحروب السيبرانية، الهجمات السيبرانية، الأمن السيبراني، العلاقات الدولية.

Abstract:

The forms of war differ from one generation to another, and with the technological and technical development that we live in, and its use for military purposes, changes have occurred in the concept of war, as keeping pace with the modern system and the development in the field of international relations, where cyberspace has become an important area for international interactions, this mysterious field full of threats and risks.

In this research, entitled The concept and phenomenon of Cyber wars in international relations, and the problem from which the study was launched about the impact of the phenomenon of electronic wars on the reality of international relations. Cyberspace, which has become directly linked to national security.

In light of the prevalence of this phenomenon, the study concluded several results, the most important of which is that cyber wars are wars of a technological nature, and many countries are racing to develop their cyber capabilities to be used as an attack against other countries or as protection for their cyberspace, in addition to weakening the traditional concept of the military state.

Keywords: cyber space, cyber war, cyber attack, cyber security, international relations.

مُقدِّمة

مقدمة:

تعد الحروب في حقل العلاقات الدولية ظاهرة اجتماعية وإنسانية معقدة، رافقت البشرية عبر مختلف الحقب والأزمنة، فكانت على مدار العصور حروب ميزت كل جيل، بسمات خاصة من استراتجيات وأساليب وتقنيات، وبحلول القرن الحادي والعشرين ومع نهاية الحرب الباردة، ومواكبةً للثورة المعرفية لتكنولوجيا المعلومات والاتصالات الذي يعيشه عالمنا اليوم، أعاد الفضاء الرقمي تشكيل مفهوم الحرب، وبروز شكل جديد من أشكال الحروب هي "الحرب السيبرانية"، التي تعتمد على تفوق التكنولوجي والقدرة على اختراق أنظمة الحواسيب في الفضاء السيبراني كمجال جديد للفعل والتأثير في النظام الدولي، هذا المجال الذي يضاف للنطاق الدولي التقليدي كمجال خامس بعد (البر، البحر، الجو والفضاء).

وقد تحول الفضاء الرقمي إلى ساحة للتفاعلات الدولية نتيجة ارتباط العالم المتزايد به، في ظل التصاعد المستمر في أعداد مستخدمي الشبكة العنكبوتية في مختلف أنحاء العالم، والتقدم السريع في عالم الحواسيب، مع تزايد اعتماد الدول على هذه البيئة الجديدة في شتى المجالات، وربطها بالبنية التحية الحرجة، لاسيما المؤسسات العسكرية والمرافق الهامة كمنشآت الطاقة النووية، أصبح الفضاء السيبراني يواجه مخاطر متصاعدة، وبدأ الحديث عن تطوير القدرات السيبرانية، مع دخول فواعل من غير الدول في النظام الدولي مثل الأفراد والمنظمات، التي قد تفوق قدراتها الفواعل الدولية، وهو ما كان له انعكاس على العلاقات الدولية، إذ يعد منعرج جديد وخطير في العلاقات الدولية.

فرض الفضاء السيبراني نوعية الحروب التي تتشابك فيه، حيث باتت الدول تتسارع على تطوير آلياتها لكي تتوافق مع هذا المجال لاستخدامها للأغراض العسكرية، من خلال ابتكار أنواع جديدة من الأسلحة فوق التقليدية، متمثلة في الأسلحة السيبرانية التي تصيب الحواسب المرتبطة بالبنى التحتية الحيوية لدولة ما، عن طريق عمليات الاختراق وتسلل داخل النظم

المعلوماتية، بواسطة برمجيات ضارة معقدة على غرار الفيروسات وديدان، لها أثار تدميرية هائلة قد تفوق الأسلحة التقليدية في خسائرها، يقودها جيوش من الخبراء في عالم الحواسيب والإنترنت.

ودخل الفضاء الافتراضي ضمن المحددات الجديدة للعلاقات الدولية، لما يملكه من مميزات جعلته مسرح جذاب للصراعات الدولية، كميزة إخفاء الهوية (العدو متخفي غير واضح)، وبطبيعته الدولية التي لا تعترف بالحدود الجغرافية (انعدام الجغرافية)، هذه المزايا لهذا الشكل الجديد من الحرب بأنماطها المتعددة قد تكون هي البديل للحروب المستقبلية، ويمكن رؤية هذا في تأسيس قيادات عسكرية سيبرانية في كل من الولايات المتحدة الأمريكية، روسيا، الصين، وعدة دول أخرى، بالوسائل والعمليات والأدوات الخاصة بالساحة السيبرانية، معتمدة على استراتيجيات سيبرانية للحماية المصالح القومية ولتعزيز التفوق أو التأثير في العالم الافتراضي.

كما دخلت الحروب السيبرانية حيزها بين الدول، وظهر ذلك جليا عام 2007، بين استونيا وروسيا، وعام 2008 في الحرب بين روسيا وجورجيا، وفي الاتهامات المتبادلة بين إيران والتحالف الإسرائيلي الأمريكي، الذي نتج عنه ظهور فيروس "ستاكسنت"، ليكون الحدث الأبرز في تطور استعمال الأسلحة السيبرانية، فضلا عن الهجمات السيبرانية المتبادلة بين الصين والولايات المتحدة الأمريكية، وغيرها من الدول.

ومع ارتفاع معدل الهجمات السيبرانية التي يشهدها العالم على مدار العقد الماضي، أصبح الأمن السيبراني يشكّل جزءًا أساسياً في العقيدة الأمنية للدول، حيث أعلنت ما لا يقل عن 130 دولة عن تخصيص أقسام خاصة بالحروب السيبرانية، لمواجهة التهديدات والمخاطر السيبرانية.[1]

أهمية الموضوع:

1- الأهمية العلمية: تكمن أهمية هذا الموضوع في حقل العلاقات الدولية، ضمن مجال الدراسات الأمنة والاستراتيجية، وما عرفه هذا المجال من تطورات ودخول مفاهيم خاصة من

[1] علي زياد العلي، *المرتكزات النظرية في السياسة الدولية* (مصر: دار الفجر للنشر والتوزيع، 2017)، ص. 225.

مستحدثات التطور التكنولوجي والرقمي الذي نعايشه، حيث فرض الفضاء السيبراني إعادة التفكير في مفهوم الحرب على اثر ذلك برزت حروب جديدة لا يمكننا أن نغفلها على الساحة الدولية في هذا الفضاء الجذاب للحروب، بأنماطها المتعددة ضمن سياق استراتيجية الحرب الباردة، ومن هنا تظهر الحاجة إلى ضرورة فهم ماهية الحروب السيبرانية ودراستها دراسة علمية مستفيضة كمتغير جديد في حقل العلاقات الدولية.

2- الأهمية العملية: تتمثل أهمية الموضوع في زيادة اعتماد مختلف دول العالم على التكنولوجيا في حروبها، ممّا أدى إلى تطور وتزايد الهجمات السيبرانية التي يشهدها العالم، والبحث في هذا الموضوع تمكّننا من تحديد وفهم الحروب في الفضاء السيبراني وما تحمله الهجمات السيبرانية من تداعيات على العلاقات الدولية، من أجل تطوير القدرات السيبرانية لحماية البيانات والأنظمة من الهجمات، والتصدي للتهديدات في العالم السيبراني المغاير تماما للتقليدي، ولعل هذا من أسباب أهمية دراسة الحروب السيبرانية.

أهداف الدراسة:

تهدف الدراسة لتوضيح دور الحروب السيبرانية في العلاقات الدولية ومن خلال هذه الدراسة سيتم التعرف على الأهداف التالية:

- إلقاء الضوء على العديد من المفاهيم في الفضاء السيبراني لإزالة الغموض حولها والوقوف على مقاصدها الحقيقية، وأثره في تحول شكل القوة في المشهد الدولي.

- تحديد مفهوم الحروب السيبرانية وتحديد معالمها، وإيجاد الفرق بينها وبين النمط التقليدي للحروب من حيث طبيعة وخصائص الأمن والصراع.

- الوقوف على أهم الدوافع التي يقوم عليها هذا الشكل من الحروب.

- التعرف على مدى أهمية الحروب السيبرانية في تحقيق توازن القوى.

- معرفة أهم التدابير الوقائية المتاحة للتعامل مع هذا النوع من الحروب.

– التعرف على بعض الحالات التطبيقية للحروب السيبرانية ومدى أهميتها في العلاقات الدولية.

أسباب إختيار الموضوع: اسند اختياري لهذا الموضوع دون غيره مجموعة من الدوافع الموضوعة وأخرى ذاتية.

1. الأسباب الذاتية: من الأسباب التي دفعتني لاختيار هذا الموضوع هو ميلي للبحث في المواضيع المرتبطة بالتطورات التكنولوجية لاسيما المتعلقة بعالم الحواسيب والانترنت، ورغبة مني أن أفهم ظاهرة الحروب السيبرانية، وتسليط الضوء عما يحدث من صراعات بين الدول داخل الفضاء السيبراني، فضلاً عن المساهمة في إثراء الرصيد المعرفي لمكتبتنا وللطالب.

2. الأسباب الموضوعية: أدت الثورة التكنولوجية إلى حدوث تغيرات عالمية، حيث أصبح المجتمع الدولي في حاجة ملحة إلى البحث العلمي يواكب هذه التطورات في شتى المجالات. فنحن نعيش اليوم، في عصر يتطور بسرعة مبهرة ومخيفة في نفس الوقت.

حدود الدراسة :

1- الإطار الزماني: تضمنت عدة مراحل تزامنت مع ظهور الهجمات السيبرانية التي شهدها العالم، وبداية الحروب السيبرانية إلى غاية 2022، مع الرجوع إلى القرن 19 من اجل إبراز تطور التاريخي للحروب الالكترونية.

2- **الإطار المكاني** : العالم الافتراضي لا يعترف بحدود الجغرافية، مع تركيز على الولايات المتحدة الأمريكية، روسيا و ايران.

إشكالية الدراسة:

نعيش الآن في العصر الرقمي كمرحلة من تاريخ البشرية، غزت فيه الحواسيب والإنترنت عالمنا والتي أصبحت هي الأساس الذي يعتمد عليه في جميع المجالات، وما رافقته من تغيرات كبرى في المسرح العالمي، أثرت بشكل كبير في العلاقات الدولية وما نشاهده من خطورة

مواجهات تهديد الحرب السيبرانية، ومن هذا المنطلق تتبلور إشكالية الرئيسية في هذه الدراسة التي مفادها:

ما مدى تأثير ظاهرة الحروب السيبرانية على واقع (مسار) العلاقات الدولية؟

ويتفرع من هذه الإشكالية الرئيسية الأسئلة الفرعية التالية:

- كيف أثر الفضاء السيبراني على مفهوم الحرب؟
- ما المقصود بالحروب السيبرانية؟
- فيما تختلف الحروب السيبرانية عن التقليدية؟
- كيف انعكست من العالم الافتراضي إلى العالم الواقعي؟

فرضيات الدراسة :

استنادا من الإشكالية الرئيسية والأسئلة الفرعية تستهدف الدراسة اختيار الفرضيات التالية:

1- كلما زادت الهجمات بين الدول في العالم الافتراضي، زادت مخاطر التهديدات في العالم الواقعي.

2- تعكس الحروب السيبرانية انتقال التنافس الدولي بين القوى الكبرى في العالم إلى الوسط الرقمي.

3- تزايد التهديدات في الفضاء السيبراني نتاج عن نقص مستوى الوعي بالأمن السيبراني.

الاطارالمنهجي للدراسة :

المنهج التاريخي: يسمح لنا المنهج التاريخي في العودة إلى التسلسل الزمني لمراحل تطور مفهوم الحروب السيبرانية، والخروج بمدلولات وقرائن تساعد على فهم وتحليل أحداث الموضوع في الحاضر.

- **المنهج الوصفي** : وهو المنهج الذي يسمح لنا بوصف الظاهرة، من خلاله يمكننا تحديد المفاهيم وتحليل ظاهرة الحروب السيبرانية، وتفسيرها وتحديد خصائصها وأسبابها وصولا إلى نتائجها.

- **المنهج القانوني:** بحيث نورد من خلاله إلى أهم التدابير والإجراءات القانونية، من المعاهدات والاتفاقيات الدولية التي لها علاقة بالحروب السيبرانية.

- **المنهج الاحصائي** : تم توظيف هذا المنهج في الدراسة من خلال عرض إحصاءات عن تطور استعمال الهجمات السيبرلنية، إلى إحصاءات عن مستعملي شبكة الانترنت وإحصاءات عن الأمن السيبراني للدول.

- **منهج دراسة الحالة** : تمكن أهميته في الجانب التطبيقي للحروب السيبرانية، والمتمثل في الفصل الثالث لنوضح على أهم نماذج الحروب السيبرانية التي تدار لكل من روسيا، الولايات المتحدة الأمريكية وإيران.

أدبيات الدراسة:

أهم الدراسات السابقة التي تناولت الجوانب المختلفة لعنوان الدراسة: الحروب السيبرانية في العلاقات الدولية(المفهوم و الظاهرة) ما يلي :

1. كتاب: الحرب الالكترونية، فيصل محمد عبد الغفار، الجنادرية للنشر وتوزيع، 2016.

انطلقت هذه الدراسة في التعرف على التسلسل الزمني لمراحل تطور مفهوم الحروب الالكترونية، وتحديد ملامح وأهداف التي جاءت بها الحروب الإلكترونية، كما تناولت الدراسة نظم السيطرة الإلكترونية في الحروب، ثم يعرض لنا التطبيقات المستخدمة في هذا النوع من الحرب، لا سيما منظومات التمويه والخداع الالكتروني، وأخيرا كنموذج يضع لنا الباحث النزاع العربي الإسرائيلي في الفضاء الالكتروني.

2. كتاب: السيبرانية: هاجس العصر، منى الأشقر جبور، المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية، 2016.

سعت هذه الدراسة إلى تسليط الضوء على عدد من المفاهيم والمسائل المتعلقة، بالأمن السيبراني وحوكمة الانترنت وما فرضه من تحولات، وتطرقت لأنواع المخاطر في الفضاء السيبراني، من الاعتداءات والجريمة السيبرانية وكذلك الإرهاب السيبراني، وأبرزت الحروب السيبرانية وأدواتها كإحدى المخاطر في الفضاء السيبراني، كما تناولت مشكلة السيادة على العالم الافتراضي وعلى العلاقات التي تحاك عبر شبكة الانترنت.

3. كتاب: حرب الفضاء الالكتروني(الخطر القادم على الأمن القومي وسبل مواجهته)، ريتشارد ايه كلارك وروبرت كيه كنيك، مركز الإمارات للدراسات والبحوث الإستراتجية، 2012.

هدفت الدراسة إلى توضيح مفهوم الحرب الفضاء الإلكتروني، كما تطرق الكتاب لخصائص وسمات الحروب السيبرانية، وأسبابها وطرقها، ومخاطرها، وسبل التحكم فيها، وتتعرج في الدراسة إلى عدد من النتائج أهمها، أن امتلاك قدرات سيبرانية يمكن أن تغير ميزان القوى العسكرية العالمية، وأن الحروب في الفضاء السيبراني قد تكون قائمة بذاتها أو بداية للحروب التقليدية أو متزامنة معها. كما يعرض الكتاب أهم نماذج الهجمات في الفضاء السيبراني، وفي الأخير يشير الكتاب إلى قدرات الولايات المتحدة الأمريكية ودول أخرى التي تمتلك وحدات متطورة للحروب السيبرانية، لاسيما روسيا، كوريا الشمالية، والصين.

4. كتاب: المنطقة المعتمدة " التاريخ السري للحرب السيبرانية"، فرد كابلان، سلسلة عالم المعرفة للنشر، 2019.

قدمت هذه الدراسة قراءة واسعة للفضاء السيبراني وللحروب التي تدار فيه، ويوضح الكاتب بأن الحروب السيبرانية واقعية، كما توقع بأنها حروب ستكون حروب المستقبل في العصر الرقمي السيبراني، كما عرض الكاتب تجربة الولايات المتحدة في الصراعات السيبرانية، ويزيح الستار عن الفواعل في هذا الفضاء سواء حكومية أو غير حكومية، ويؤكد

على اضـعاف المفهوم التقليدي للحرب فلم يعد النصـر من نصـيب من لديه القوة العسـكرية التقليدية، بل من يمتلك القوة السيبرانية حتى يسيطر بها على الفضاء السيبراني.

5. كتاب: مجتمع ما بعد المعلومات " تأثير الثورة الصناعية الرابعة على الأمن القومي"، إيهاب خليفة، العربي للنشر والتوزيع، 2019.

تناول الباحث عملية تأثير الفضاء الافتراضي والانترنت في تغير أشكال وأنماط الحياة، حيث أصبح الفضـاء الالكتروني هو الجهاز العصـبي لهذا المجتمع، كما يوضـح هذا الكتاب عددا من الظواهر في مجال الفضاء السيبراني مثل: الهجمات السيبرانية، الحروب السيبرانية، الإرهاب السيبراني، الصراع السيبراني، القوة السيبرانية، الدفاع السيبراني، كما ناقش مؤشرات الحروب السيبرانية وأبرز أشكال الأسلحة السيبرانية.

6. كتـــاب: الإرهـــاب الإلكتروني:القـــوة فـــي العلاقـــات الدوليـــة" نمـــط جديـــد وتحـديات مختلفـة"، عـادل عبـد الصـادق ، مركـز الدراسـات السياسـية والإسـتراتجية، 2009.

هدفت الدراسة إلى توضيح الأهمية الإستراتجية للفضاء السيبراني في النظام الدولي، وطبيعة وأنماط استخدام الفضاء السيبراني في الصراعات الدولية، كما قام بفك الغموض عن عدة مفاهيم أمنية في العالم السيبراني، وتناول الباحث إشكالية الهجمات في العالم الافتراضي إن كانت إرهاب أو حرب سيبرانية، كما تطرق في الفصل الأخير من الكتاب إلى الجهود الدولية في تأمين الفضاء السيبراني.

7. رســـالة ماجســـتير: صـــلاح حيـــدر عبـــد الواحـــد، حـــروب الفضـــاء الإلكترونـــي، دراســـة فـــي مفهومهـــا وخصائصـــها وســـبل مواجهتهـــا، جامعـــة الشـــرق الأوسط، عمان، 2021.

هدفت الدراسة إلى معالجة إشكالية الحروب في الفضاء الإلكتروني، حيث تناول البحث في الفصل الأول أهمية الدراسة وخلفيتها، واختص الفصل الثاني بدراسة مفهوم الحروب وخصائصها، والمسؤولية الدولية اتجاهها في الفصل الثالث، وخلصت الدراسة إلى سبل

وإمكانيات المتاحة لواجهة هذا النمط الحروب في ضوء الواقع السيبراني، مع وضع أهم الاستنتاجات والتوصيات.

مصطلحات الدراسة:

الخادم (Server): وهو عبارة عن جهاز كمبيوتر له إمكانيات متفوقة ومواصفات خاصة، يعمل على تقديم المساعدة إلى أجهزة كمبيوتر أخري داخل الشبكة، يتحمل العمل لفترات طويلة، لأن توقفه يعنى توقف جميع المواقع والتطبيقات والخدمات والأنظمة المُستضافة عليه[1].

البرمجيات الخبيثة (Malware): هي برامج ضارة تستخدم للوصول إلى أنظمة الحاسوب، بطريقة سرية بهدف إلحاق الضرر به كعرقلته أو تخريبه، وانتهاك سرية وسلامة المعلومات والبيانات لهذه الأنظمة[2].

نظام التشغيل (Operating System): هو مجموعة من البرامج التي تدير جهاز كمبيوتر، فهو يدير كل ما يتعلق بذاكرة وعمليات الكمبيوتر، فهو الوسيط بين الإنسان والحاسوب، كما يعتبر نظام تشغيل ويندوز أهم نظام التشغيل، إذ يستحوذ على ثلاث أرباع من المستخدمين في العالم.

البنية التحتية الحرجة (Critical infrastructure): هي أي أنظمة يؤدي تعطيلها أو الدخول الغير مصرح به لها أو للبيانات والمعلومات التي تحفظها أو تعالجها، إلى أثار اقتصادية أو مالية أو اجتماعية كبيرة على المستوى الوطني.

[1] "ما هو السيرفر (خادم)؟ شرح 10 أنواع سيرفر Server "، نشر بتاريخ: 21 مارس2019 ، اطلع عليه بتاريخ: 05/15 /2022، الساعة: 22:05، على الرابط: https://hostingwdomain.com/what-is-server/

[2] "مصطلحات الأمن السيبراني Cyper Security "، نشر بتاريخ: 22 مارس 2022، اطلع عليه بتاريخ: 2022/05/15، الساعة: 23:55على الرابط: https://2u.pw/S0ntb.

خطة الدراسة:

قسمنا الدراسة إلى مقدمة وثلاثة فصول رئيسية ثم خاتمة، **الفصل الأول** عبارة عن إطار مفاهيمي للدراسة خصصنا المبحث الأول منه لنشأة وتطور الحروب الالكترونية والحروب في الفضاء السيبراني، أما المبحث الثاني تطرقنا فيه إلى مفهوم الحروب السيبرانية وأنماطها، كما عالجنا في المبحث الثالث مفهوم الفضاء السيبراني والتحول في مفهوم القوة وعدة مفاهيم أمنية.

وفي **الفصل الثاني** حاولنا من خلاله معرفة طبيعة خاصة للحروب السيبرانية، والتعرف على الأسلحة والعمليات العسكرية السيبرانية في المبحث الأول، وكذلك معرفة فواعل هذا الشكل الجديد من الحروب في المبحث الثاني، أما المبحث الثالث عرضت فيه أهم القوانين الدولية المعالجة لظاهرة الحروب السيبرانية وسبل مواجهتها.

أما **الفصل الثالث** والأخير أختص بالجانب التطبيقي لظاهرة الحروب السيبرانية، ركزنا فيه على أهم نماذج التي جسدت من سياسة الدفاع والهجوم السيبراني، لكل من الولايات المتحدة الأمريكية في المبحث الأول، وروسيا في المبحث الثاني، وإيران في المبحث الثالث والأخير.

الفصل الأول: الإطار المفاهيمي للحروب السيبرانية

الفصل الأول: الإطار المفاهيمي للحروب السيبرانية.

في ظل التطور التكنولوجي والتقني ظهر مجال خامس في ساحة التفاعلات الدولية، وهو الفضاء السيراني حيث أصبح ميدان جديد للفعل والتأثير في العلاقات الدولية، أعاد تشكيل عدة مفاهيم ودخول مفهوم الحرب السيبرانية، وهذا ما سنعالجه في هذا الفصل، وذلك بتناول التطور التاريخي للحروب الالكترونية، وعرض تحول مفاهيم منها مفهوم القوة في الفضاء السيبراني بصفة عامة هذه العلاقة الإرتباطية أدت إلى ظهور الحروب السيبرانية بإعتبارها وسيلة من وسائل استخدام القوة، مما أدى إلى تطور في مفهوم الحرب، كنتيجة حتمية للتحولات في الفضاء السيبراني التي ظهرت على الساحة العالمية.

المبحث الأول: التّطور التاريخي للحروب الالكترونية.

لقد أدّى التّطور السريع في المجال التكنولوجي إلى إحداث ثورة معلوماتية ورقمية، كما شكّل أبعادًا جديدة في جميع مجالات الحياة خصوصًا الأمنية كتغيير طريقة الحُروب، بداية من الحُروب الالكترونية إلى الحُروب السيبرانية والمرتبطان بمسائل الاتصالات والمعلومات.

المطلب الأول : نشأة وتطور الحُروب الإلكترونية.

من الناحية التاريخية تعود جذور الحرب الإلكترونية (Electronic war) لما قبل اندلاع الحرب العالمية الأولى، فقد بدأت الاتصالات بين أرجاء العالم المختلفة بإستخدام المواصلات السلكية عن طريق المورسّ* وكان ذلك عام 1837، ولم يتحقق أي اتصال آخر في ذلك الوقت إلا من خلال تبادل المراسلات، بإستخدام السفن في نقل الرسائل في الموانئ البحرية[1].

وعند اندلاع الحرب الأهلية في الولايات المتحدة الأمريكية أفريل عام 1861، استخدمت لأول مرة البرقية في الحرب، حينها أصبحت برقية التلغراف جزء مهم في المنظومة الحربية ، بعدها في عام 1888، كانت بداية الإتصال اللاسلكي مع العالم الألماني هارتز(HERTZ)، حيث أثبت أن الطاقة الكهربائية تخلق ترددات في الفضاء تكون بمثابة إشارات يمكن اعتمادها ورصدها، وقد قاد هذا الاكتشاف إلى الإهتمام بما عرف فيما بعد بـ(الذبذبات الهرتزية) التي استخدمت في تطوير نظام الراديو في إنكلترا، وفي سنة 1904 قصفت السفينتان اليابانيتان الحربيتان (كاسوجا ونيشين) القاعدة البحرية الروسية لميناء (آرثر)، وكان ذلك أول تطبيق عملي لهذه التقنية أثناء الحرب الروسية–اليابانية، وكانت معهما سفينة صغيرة تصحح النيران بإستخدام الراديو (اللاسلكي). وبالمصادفة سمع أحد عمال الروس الإشارة، وتضمنت تعليمات تصحيح النيران فاستخدم جهاز الإرسال اللاسلكي لإعاقة الاتصال الياباني بالضغط على مفتاح

---

* وهي شـفرة حرفية تعتمد على مبدأ بسـيط وهو تحويل الإشـارات الكهربائية المنقولة عبر خطوط البرق من اجل إرسـال المعلومات، باستخدام تتابعات قياسية من عناصر طويلة وقصيرة تعبر عن الحروف والأرقام والعلامات الخاصة الموجودة في الرسالة.

[1] فيصل محمد عبد الغفار، *الحرب الالكترونية*(الأردن: الجنادرية للنشر وتوزيع، 2016)، ص. 18.

الإرسال على تردد الشبكة اليابانية نفسها، ممّا أدّى إلى تعّطل بلاغات تصحيح النيران من أن تُبّلغ لمدفعية السفينتين، ولم ينتج عن هذا القصف البحري سوى إصابات طفيفة لعدم دقة نيران في إصابة الهدف المراد، وذلك بفضل هذا الاكتشاف[1].

وحتّى عام 1906 تمكّن مكتب معدات البحرية الأمريكية من إستحداث جهاز تحديد إتجاه لاسلكي لخدمة الملاحة البحرية في البحر، بهدف إرشاد وتحديد مواقع السفن وأيضًا خطوط سيرها، وهو ما عرف باسم المنارة اللاسلكية الذي كان له أثر كبير في مجالات الحرب الإلكترونية لاحقا[2].

وفي بداية الحرب العالمية الأولى استعملت أجهزة الاتصال وأجهزة نقل معلومات الاستطلاع بكثرة، ففي عام 1914، استطاعت إحدى السفن الانجليزية التنصت وإرسال بالراديو معلومات عن تحرك بعض السفن الألمانية في البحر الأبيض المتوسط ولكن بعد أن تمكن الألمان من رصد تلك الإرساليات تمكنوا من التشويش بالكامل عليها، وفي عام 1916 وضع الانجليز بعض موجات إتجاه الإرسال قرب الأسطول الألماني، وخلال معركة جوتلاند حددت تلك الأجهزة موقع الأسطول الألماني وتم إشعار القيادة الانجليزية، أما في الحرب العالمية الثانية كانت البداية الحقيقية في الحرب لاستخدام أجهزة الحرب الالكترونية ففي عام1939، قام الألمان باستخدام طريقة " تقاطع موجات الإرسال فوق الهدف " (BEAM-INTERSECTION) لكي يقصفوا المدن الانجليزية خاصة أثناء الليل، فوضع الانجليز جهاز الإرسال (BROMIDE)الذي قام بالتشويش مضلل مما جعل هذا التقاطع فوق مكان غير حيوي وتم اختيار لذلك بحر المانش، وفعلا وقع قصف الطائرات الألمانية على بحر المانش ولم

[1] علي عبد الرحيم العبودي، "هاجس الحروب السيبرانية وتداعياتها على الأمن والسلم الدوليين"، قناة الحوار المتمدن، نشر بتاريخ: 21مارس2019، اطلع عليه بتاريخ: 15 /01 /2022، الساعة: 22:05على الرابط: https://2u.pw/NlKWe

[2] فيصل محمد عبد الغفار، مرجع سابق، ص 20.

تتضرر المدن الانجليزية التي أراد الألمان أن يقصفها، كما استخدم الحلفاء* أجهزة تشويش على الرادارات الألمانية عند الساحل الغربي لفرنسا[1].

وفي أواخر 1941، وقبل دخولها حرب مباشرة أنتجت الولايات المتحدة الأمريكية رادارات متقدمة ركبت فيما بعد بالسفن الحربية، وحاملات الطائرات، والطرادات، مما دفع إلى التغلب على أعمال الاستطلاع أعمال الاستطلاع والإعاقة الرادارية[2].

واستمر الصراع الدائر للحصول على أحدث التكنولوجيا لإنشاء أحدث النظم الإلكترونية اللازمة للتمكن من السيطرة وإدارة الحُروب والقتال. حيث كان يتبعها دائمًا العمل الدائم في مراكز الأبحاث للوصول إلى أكثر المعدات الخاصة بالحرب الإلكترونية تعقيدًا تصعب على وسائل الاستطلاع والإعاقة، ثم يأتي دور إختبار هذه المعدات في الحرب الإلكترونية ويتم إنزالها إلى ساحة المعارك لمعرفة قوتها ونتائجها، وبعدها تجري عليها أعمال التطوير على ضوء ما يدرس من مزاياها وعيوبها. ظهر ذلك واضحاً في حروب ما بعد الحرب العالمية الثانية: "حرب كوريا، حرب فيتنام، حرب 1967، حرب 1971، حرب 1973، حرب لبنان، خليج سرت، حرب تحرير الكويت ثم حرب البلقان[3].

المطلب الثاني : نشأة وتطور الحُروب السيبرانية.

تقترن بداية الحُروب السيبرانية (Cyber War) بحدثين مهمينّ: الحدث الأول كان في منتصف الخمسينيات من القرن المنصرم حيث تمّ استحداث أجهزة الكمبيوتر كأداة لمعالجة وحفظ المعلومات رقميا(DIGITAL)، رافقه تضافر جهود عدد من الشركات، حيث تُوّج بتطوير وحدة المعالجة المركزية (CPU)، وذلك لتسهيل المهام الموكلة له، وقد تطور ذلك بصورة جذرية

* تضم مجموعة كبيرة من الدول التي وقفت معاً لمواجهة دول المحور خلال الحرب العالمية الثانية (1939-1945)، روجت دول الحلفاء أن الحلف جاء لإيقاف عدوان كل من ألمانيا، إيطاليا واليابان.

[1] جاسم محمد البصيلي، *الحرب الالكترونية أسسها وأثرها في الحروب*، ط.2 (لبنان: المؤسسة العربية للدراسات والنشر، 1989)، ص،ص. 41-42.

[2] فيصل محمد عبد الغفار، مرجع سابق، ص، ص. 24-25.

[3] نفس المرجع، ص. 25-26.

في العقود اللاحقة، حتّى أصبح جهاز الكمبيوتر، أساسا في عمل الكثير من مؤسسات الخاصة والعامة، فضلاً عن الحياة اليومية للأفراد[1].

أما الحدث الثاني فقد إرتبط بأواخر الستينيات في الولايات المتحدة الأمريكية حيث ظهر ما يسمى الانترنت (Internet)، عندما شكلت وزارة الدفاع لجنة من الخبراء أوكلت إليهم مهمة إنشاء شبكة تربط بين الحواسيب، وبذلك أنشئت أول شبكة للانترنت في العالم تحت مسمى شبكة وكالة مشاريع الأبحاث المتطورة(Advanced Research Projects Agency Network) اختصاراً الأربانت (ARPANET) [2].

وتعتبر الثورة المعلوماتية الحالية بمثابة الجيل الثالث للثورات التقنية التي عرفتها البشرية، وغيرت في أسلوب الحياة وإمكانيات البشرية، وبعبارة أخرى الثورتان الزراعية والصناعية وأخيرا الثورة المعلوماتية[3].

وعند الاستقصاء التاريخي لبداية الحُروب السيبرانية نجد أنّ أول موقعة سيبرانية تعود إلى فترة الحرب الباردة كان ذلك عام 1982، بين الولايات المتحدة الأمريكية والاتحاد السوفييتي، حيث كانت هناك عملية ضخمة لجهاز المخابرات السوفييتي "KGB" تسمى "LineX"، صُممت لمساعد الإتحاد السوفييتي الذي كان متأخراً في مجال تصميم التكنولوجي والإلكترونيات الدقيقة، على تجاوز هذه الفجوة وذلك عن طريق سرقة تكنولوجيا المعلومات من الغرب[4].

وفي التّسعينيات من القرن المنصرم سارعت الدول في استخدام أجهزة الكمبيوتر لتحقيق قفزات نوعية (leapfrogging) لتسخر التكنولوجيا خدمة للمجال الأمني والعسكري، حتّى أطلق

---

[1] احمد عبيس نعمة الفتلاوي، "الهجمات السيبرانية : مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر،" *مجلة المحقق الحلي للعلوم القانونية والسياسية*8، رقم. 4 (2016)، ص. 622.

[2] شوقي يعيش تمام، *الجريمة المعلوماتية: دراسة تاصيلية مقارنة*(الجزائر: مطبعة الرمال، 2019)، ص. 16.

[3] احمد عبيس نعمة الفتلاوي، مرجع سابق، ص. 622.

[4] محمود محمد علي، "الحروب السيبرانية وتطور الإستراتجية العسكرية للدول"، نشر بتاريخ: 03 فيفري 2022، اطلع عليه بتاريخ 06 /03 /2022، الساعة: 20:00، على الرابط:https://2u.pw/V0FSu .

عليها البعض مصطلح الحرب السيبرانية الباردة(CYBER COLD WAR) أو سباق التسلح السيبراني (CYBER ARMS RACE) [1].

ومع نهاية 2006 في شهر ديسمبر أُجبرت "الناسا" على حجب رسائل البريد الإلكتروني، التي تأتي مع مرفقات قبل إطلاق المركبات الفضائية خشية اختراقها، وذكرت مجلة بيزنس ويك "BusinessWeek" الأميركية أن خطط إطلاق مركبات الفضاء الأميركية الأخيرة حصل عليها مخترقون أجانب مجهولين، وفي عام 2007، تعرّضت شبكات حاسوب الحكومة الإستونية لهجوم من نوع الحرمان من الخدمة من طرف مجهولين، بعد خلاف مع روسيا حول إزالة نصب تذكاري، وتعطلت بعض الخدمات الحكومية الإلكترونية والخدمة المصرفية عبر الإنترنت،وأصابت الهجمات شبكات الكمبيوتر في برلمان استونيا والوزارات الحكومية والبنوك ووسائل الإعلام والعديد من الأحزاب السياسية بالشلل، وهو ما أدّى إلى قطع اتصال حوالي 58 موقعاً استونيا، وفي صيف سنة 2008، وفي الشهر الثامن اخترقت شبكة حواسيب في جورجيا من طرف مخترقين مجهولين خلال فترة صراعها مع روسيا[2].

وفي أواخر 2009، أوردت الحكومة الكورية الجنوبية تقريرا عن تعرّضها لهجوم من قبل جارتها كوريا الشمالية يهدف لسرقة خطط دفاعية سرية تتضمن معلومات عن شكل التّحرك الكوري الجنوبي والأمريكي في حالة حصول حرب في شبه الجزيرة الكورية، وفي بداية نفس السنة في شهر جانفي وخلال العدوان الإسرائيلي على قطاع غزة تعرضت بنية الإنترنت التحتية في إسرائيل لعدة هجمات إلكترونية تركزت على مواقع إلكترونية حكومية، ونفذت الهجمات باستخدام نحو خمسة ملايين حاسوب على الأقل وفقا لمجلة "ناتو ريفيو" (NATO Review) الإلكترونية، وتبنت مجموعة أنونيموس* (Anonymous) الكثير من تلك الهجمات، وصولا إلى

---

[1] احمد عبيس نعمة الفتلاوي، مرجع سابق، ص. 622.

[2] "الاختراقات الإلكترونية.. البداية إشارات مورس"، قناة الجزيرة، نشر بتاريخ: 05 جانفي 2015، اطلع عليه بتاريخ: 06 /03 /2022، الساعة: 23:00، على الرابط: https://2u.pw/mtKKj .

*مجموعة دولية من نشطاء القراصنة المجهولين من مختلف الدول يرفضون الكشف عن أسمائهم، كما لا يوجد لهم قيادة معلنة أي تحكم فيها اللامركزية.

شهر جويلية 2010، حيث أكدت ألمانيا أنها واجهت عمليات تجسس شديدة التعقيد من قبل الصين وروسيا كانت تستهدف قطاعات صناعية والبنى التحتية الحساسية في البلاد و من بينها شبكة الكهرباء التي تغذي الدولة[1].

أمّا في 25 سبتمبر من عام 2010، أعلنت إيران أن العديد من وحداتها الصناعية تعرضت لهجوم إلكتروني بعد إصابتها بفيروس ستكسنت(Stuxnet) *، الذي استخدم لمهاجمة برنامج إيران النووي. حيث كان الخبراء يعتقدون في بداية أن مهمة الفيروس هي التجسس ونقل المعلومات لمحاولة كسب المال أو لسرقة الملكية الفكرية، لكن اتضح فيما بعد أنّ الأمر مختلف كليا، ويعتقد على نطاق واسع انه من تطوير الولايات المتحدة وإسرائيل، فبعد قرابة أربعة أشهر من العمل، ظهر أن الأمر أكثر تعقيدا مما كان متصورا، وأننا نقف اليوم أمام نوع جديد متطور ومعقّد يُؤدي إلى دمار واقعي في البلد المستهدف حتّى دون الانترنت[2].

كما ذكرت صحيفة صحيفة أمريكية (The Daily Beast)، أن إسرائيل تمكّنت من تطوير التقنيات اللازمة لأي هجوم على إيران حيث سيكون مدعومًا بغارات الكترونية وفيروسات، و عمليات التشويش فقد تمكنت، من إيقاف شبكة الهاتف الإيرانية، مع إمكانية تعطيل نظام الإندار ومنعه من بث الرسائل اللازمة، بعد هجمة إستباقية، تشنها الطائرات على سبيل المثال، فقد تمكنت إسرائيل من تعطيل الرادارات السورية لدى إغارتها وقصفها موقع الكبر النووي السوري بالقرب من دير الزور ويلاحظ دخول العديد من الدول، وان بصورة خفية مجال الأعمال الإستخبارتية السيبرانية والاختراقات المتبادلة لأنظمة المعلومات[3].

---

[1] فيصل محمد عبد الغفار، مرجع سابق، ص. 13.

* أول سلاح رقمي في العالم، ويعد هذا الفيروس من أعقد الفيروسات التي تم استخدامها عند ظهوره.

[2] حكيم غريب وصبرينة شرقي، "تداعيات الحرب الإلكترونية على العلاقات الدولية: دراسة في الهجوم الالكتروني على إيران –فيروس ستكنست–،" *دفاتر السياسة والقانون 12*، رقم 02 (2020)، ص، ص. 101–102 .

[3] منى الأشـقر جبور، *السـيبرانية: هاجس العصـر*، (جامعة الدول العربية :المركز العربي للبحوث القانونية والقضـائية، 2016)، ص. 69.

وتعتبر خدمات تليفزيون الانترنت هي خدمات متعددة الوسائط تشمل خدمات التليفزيون والفيديو والخدمات الإذاعية والنصوص والبيانات التي يتم إرسالها عبر الشبكات التي تستخدم شبكة العنكبوتية وكذلك تبث مباشرة منها دون الحاجة لتلفاز وضبطه بالأقمار.

ونلاحظ اليوم أنّ أكبر الشبكات في هذا المجال تستثمر في أكبر الشبكات الإعلامية العالمية ، مثل: ما قامت به شبكة (CNN)* الأمريكية، خلال الحرب على العراق2003، حتّى عُرفت أنداك بأنها حربّ (CNN) على العراق، وكذلك عرفت الحرب في أفغانستان ضد القاعدة وطالبان بأنّها حرب قناة الجزيرة القطرية[1].

وقد أحدث استخدام معدات الحرب الإلكترونية في الحُروب الحديثة تطورًا هائلاً في مجالات هذه الحُروب ومراحلها، وأصبح الحسم في المعارك الحديثة لصالح الجيوش والقوات التي تستخدم الحديث منها، وبقدر ما يمتلكه كل طرف من الأطراف المتصارعة، بعد أن كانت تحسم لمصلحة الطرف الذي يمتلك التفّوق العددي أو النّوعي، أو يمتلك الأسلحة البعيدة المدى، والدليل على ذلك أنّ معدّات الحرب الإلكترونية المستخدمة في الطائرات المقاتلة يقترب ثمنها من نصف قيمة الطائرة[2].

وخلاصة القول أن هناك خلط في الأدبيات العربية بين المصطلحين الحرب الالكترونية (Electronic war)، والحرب السيبرانية (Cyber war)، حيث نجد الاستعمال الشاسع لمصطلح الحرب الالكترونية بدل السيبرانية رغم الاختلاف في المفهومين، فالأخيرة (أي الحروب السيبرانية)، تعتبر شكلا من أشكال الحُروب الالكترونية، أي مرحلة من مراحل الحروب الإلكترونية.

* إحدى أشهر القنوات الأميركية والعالمية المتخصصة في البث المتواصل للأخبار والأحداث الدولية.

[1] اسماعيل قادير، إدارة الحروب النفسية في الفضاء الالكتروني: الإستراتيجية الأمريكية الجديدة في الشرق الأوسط، (ندوة بعنوان : عولمة الإعلام السياسي وتحديات الأمن القومي للدول النامية، كلية الحقوق والعلوم السياسية، جامعة ورقلة، 2017) ص. 12.

[2] فيصل محمد عبد الغفار، مرجع سابق، ص. 30.

المبحث الثاني: مفهوم الحرب السيبرانية.

أصبح القرن الواحد والعشرين قرن الحُروب الذّكية (الالكترونية)، التي تعتمد بدرجة أولى على العامل التكنولوجي، وبسبب هذه التطورات المعلوماتية الهائلة التي شاهدتها البشرية، أفرزت عن شكل جديد من أشكال الحُروب وهي الحرب السيبرانية المرتبطة بالفضاء السيبراني.

المطلب الأول : تعريف الحُروب السيبرانية.

إن تعريف الحرب السيبرانية (Cyber War) ليس بالأمر السهل كما يبدو لكثير الباحثين في واقع تعريفا، لا يوجد تعريف متفق عليه عالميا، فغالبا ما تفتقر هذه المصطلحات إلى تعريفات دقيقة ومجمع عليها.

وما أتفق عليه أغلب العلماء ضمن اختصاص العلاقات الدولية أن الهدف الأساسي من وراء دراسة العلاقات الدولية هو تجنب الحرب وتحقيق السلم "Peacemaking" حتّى وإن اختلفت سبل تحقيق ذلك[1].

عرفت الحرب "The War" بمفهومها التقليدي أنها مفهوم يشير إلى صراع باستخدام القوات المسلحة بين دولتين أو أكثر متنازعين لفرض إرادة وشروط المنتصر، بعد فشل الدبلوماسية، فالحرب هي الانتقال من حالة السلم إلى العنف.

بينما اختلفت تشريعات الدول الفاعلة في الحقل الدولي لوضع تعريف محدد للحرب السيبرانية(Cyber War)، عرفها جيفري كار "Jeffrey Carr" بأنها:" فن وعلم القتال بدون قتال، من هزيمة الخصم دون إراقة دمائه"[2].

---

[1] أحمد محمد أبو زيد، "نظريات العلاقات الدولية والحرب:مراجعة للأدبيات:1-2،" *الناقد للدراسات السياسية*، رقم. 01 (2017)، ص. 12.

متوفر على الرابط: https://www.asjp.cerist.dz/en/downArticle/501/1/1/70080

[2] Michael Robinson, Kevin Jones, and Helge Janicke, "Cyber warfare: Issues and challenges", Computers & Security 94, (2015), p. 8. DOI:10.1016/j.cose.2014.11.007

إذن فالحرب السيبرانية فعل تقوم بها دولة ما لاختراق دولة أخرى، عن طريق شبكات أو الحواسيب لأغراض التسبب في الضرر أو اضطراب [1].

وقدمت وزارة الدفاع الأمريكية "البنتاغون" تعريفاً للحرب السيبرانية فأعتبرتها على أنها: "توظيف القدرات السيبرانية حيث يكون الغرض الأساسي هو تحقيق أهداف أو تأثيرات عسكرية في الفضاء السيبراني أو من خلاله"[2].

وفي السّياق ذاته عرفها مجلس الأمن الدولي بأنها: "هي استخدام أجهزة الحاسوب،أو الوسائل الرقمية، من قبل حكومة، أو بمعرفة صريحة، أو موافقة من تلك الحكومة ضد دولة اخرى، أو ملكية خاصة داخل دولة أخرى، بما في ذلك الوصول المتعمد أو اعتراض البيانات، أو تدمير البنية التحتية الرقمية وإنتاج وتوزيع الأجهزة التي يمكن استخدامها لتخريب" [3].

أما ريتشارد كلارك (Richard Clarke) فعرف الحرب السيبرانية بأنها : "اختراق شبكة أو حاسوب دولة أخرى اختراقا غير مصرح به بواسطة حكومة ما، أو نيابة عنها، أو دعما لها، أو أي نشاط آخر يؤثر على نظام حاسوبي بغرض إضافة أو تغيير أو تزييف البيانات، أو التسبب في تعطيل جهاز حاسوب أو إتلافه، أو تعطيل أو إتلاف جهاز متصل بشبكة أو الأشياء التي يتحكم فيها نظام الحاسوب"[4].

---

[1] Petr hruza, Jiri cerny,"cyberwarfare", International conference KNOWLEDGE-BASED ORGANIZATION 23, No.1, (2017), p. 155.
DOI:10.1515/kbo-2017-0024

[2] Department of Defense Dictionary of Military and Associated Terms, Joint Publication 1-02, 12 April 2001 (As Amended Through 17 October 2008), P. 141.
متاح على الرابط: https://www.bits.de/NRANEU/others/jp-doctrine/jp1_02(10-08).pdf

[3] Fred Schreier, *On Cyberwarfare*, (Geneva Centre for Security Sector Governance, 2015), p. 17.
متاح على الرابط: https://2u.pw/bZpcd

[4] علاء الدين فرحات، "الفضاء السيبراني: تشكيل ساحة المعركة في القرن الحادي والعشرين،" *مجلة العلوم القانونية والسياسية 10*، رقم. 03 (2019)، ص. 94.
متاح على الرابط التالي:https://2u.pw/aShlz

ومن خلال هذه التّعاريف نستنتج أن الحروب السيبرانية لها أدوات جديدة، ومجال خامس جديد هو الفضاء السيبراني الذي يضاف إلى المجالات الأربعة التقليدية : البحر، اليابسة، الجو، الفضاء.

وتتميز كذلك الحرب السيبرانية (CyberWar) عن الحرب التقليدية، أنّ مفهوم الحرب التقليدية يعتمد على استخدام الجيوش النظامية يتقّدمها إعلان واضح لحالة حرب وميدان محدد، عكس الحرب السيبرانية التي تجري في السر ولا تحتاج إلى إعلان وساحة محددة لأنها تتخطّى الحدود، كذلك من حيث طبيعة السلاح إذ تعتمد الهجمات السيبرانية على أسلحة سيبرانية متطورة يتم توجيهها ضد المنشآت الحيوية أو دسها عن طريق العملاء[1].

وعلى خلاف الحرب التقليدية تتميز الحُروب السيبرانية كذلك بعدم الاعتراف بها على مستوى الحكومات، حيث سميت "الحرب الخبيثة"، خشية من الانتقام والخوف ويمكن أن تتصاعد إلى حرب حركية[2].

إذن فالحرب السيبرانية مصطلح واسع يصف استخدام القدرات السيبرانية في الفضاء السيبراني، من قبل دولة ضد أخرى لتحقيق أهداف محددة إلى جانب الخصائص المذكورة يمكن أن نلخص أهم خصائص الحرب السيبرانية بما يلي[3]:

1- حـروب غيـر تناظريـة "Asymmetric" : (غيـر مكلفـة) مقارنـة مـع الحُـروب التقليديـة، حيـث تعـد تكلفـة إطـلاق الهجمـات أقـل مـن أي سـلاح تقليـدي آخـر مـع إلحـاق أكبر ضرر بالعدو، وبالإمكان أن يكون هناك أطراف فاعلة من غير الدول.

---

[1] عادل عبد الصـادق ،"الحروب السـيبرانية : تصـاعد القدرات والتحديات للألمن العالمي"، المركز العربي لأبحاث الفضـاء الالكتروني، نشر بتاريخ: 12-03-2017، تم الاطلاع على الموقع بتاريخ 16-03-2022، الساعة:14:00،على الرابط: https://2u.pw/cShuM .

[2] تغريد معين حسن المشـهدي، "الأثر العسكري للأمن السيبراني في الجغرافيا السياسية للدولة،" *مجلة البحوث الجغرافية1*، رقم. 30(2019)، ص. 247.

[3] عبد الغفار، مرجع سابق، ص، ص. 11-12.

2- تمتع المهاجم بأفضلية واضحة: يتمتع المهاجم بأفضلية على المدافع، فهذه الحُروب تتميز بالسرعة والمرونة والمراوغة، جدا على عقلية التحصن لوحدها أن تنجح، فالتحصين سيجعل من هذا الطرف عُرضة لمزيد من محاولات الاختراق والضغط.

3- توسع الأهداف : حيث لا ينحصر إطار حروب السيبرانية بأهداف عسكرية فقط، مع زيادة الاعتماد الكتروني إذ باتت الكثير من الدول بربط بنيتها التحتية بالفضاء الإلكتروني، فاصبح بإمكانها استهداف البنى التحتية المدنية والحساسة في البلدان المستهدفة خصوصا مع رقمنة اغلب القطاعات.

4- صعوبة الردع: إذ أنّ هناك معضلة في تحديد الدولة والجهة التي قامت بالهجوم.

5- اضمحلال حدود الداخل والخارج : حيث لا توجد حدود جغرافية واضحة في العالم الافتراضي[1].

المطلب الثاني : أنماط الحروب السيبرانية.

تنوعت أنماط الحروب السيبرانية من حيث مدى درجة شدة الصراع من عدمهما، بين الحروب الباردة والساخنة ومن أبرزها:

أولاً ← الحرب السيبرانية الباردة منخفضة الشدة (Low intensity) : عادة ما يتم اللجوء إلى القوة الناعمة في الفضاء الإلكتروني للحرب منخفضة الشدة، وتعبر عن صراع مستمر بين الفاعلين المتنازعين، وأحيانا تكون ذات طبيعة ممتدة ودائمة النشاط الغير السلمي[2].

---

[1] صالح حيدر عبد الواحد، "حروب الفضاء الإلكتروني: دراسة في مفهومها وخصائصها وسبل مواجهتها،"(رسالة ماجستير العلوم السياسية، جامعة الشرق الأوسط، كلية الآداب والعلوم، قسم العلوم السياسية،2021)، ص. 44.
متاح على الرابط: https://2u.pw/0l4Ok .

[2] عادل عبد الصادق،" أنماط الحرب السيبرانية وتداعياتها على الأمن العالمي"، من مؤلف جماعي بعنوان: "الصراع السيبراني: التنازع العالمي على قوة الفضاء السيبراني،" *مجلة السياسة الدولية* 52، رقم. 208 (2017)، ص. 34.

وذات بعد تاريخي وديني وفكري ممتد، مثل أن تكون امتدادا أو جزءا من الصراعات التقليدية كالصراع العربي–الإسرائيلي (بعد اجتماعي – ديني ممتد)، أو الصراع بين كوريا الشمالية وجارتها الجنوبية كذلك الصراع الهندي الباكستاني. وتشمل هده الحرب السيبرانية على عدة وسائل، مثل الحروب النفسية، الجوسسة وسرقة المعلومات، حرب الأفكار، وله نواح متعددة سواء سياسية، ثقافية، أو اقتصادية، أو اجتماعية، ويستخدم هذا النمط أساليب خلق الأزمات السياسية لإثارة الاضطرابات والرأي العام ضد الدولة المستهدفة، وبث الإشاعات للإضرار بالاقتصاد الدول، وقد شهدنا نماذج منها مع بدء تنفيذ إستراتيجية الفوضى الخلاقة (Constructive Chaos)* [1].

وفي مثل هذا النمط من الحروب السيبرانية، تنشط جماعات دولية للقرصنة للتعبير عن مواقفها سواء سياسية او غيرها مثل جماعة موقع ويكيليكس (Wikileaks)*، وكذلك أيضا في حالات الأزمات الدولية، مثلما حدث في 2007 بين استونيا وروسيا، وكذا الاختراقات المتبادلة بين عدة دول أهمها الصين ، الولايات المتحدة، روسيا وإيران[2].

ثانياً ← الحرب السيبرانية متوسطة الشدة(Medium intensity): حيث يعبر هذا النمط عن تحول الصراع عبر الفضاء الإلكتروني إلى ساحة موازية لحرب تقليدية دائرة على

متاح على الرابط: https://2u.pw/CL94T

*هي حالة سياسية أو إنسانية يتوقع أن تكون مريحة بعد مرحلة فوضى متعمدة الإحداث، ويعتقد أصحاب وأنصار الفوضى الخلاقة بأن خلق حالة من الفوضى وعدم الاستقرار، سوف يؤدي حتماً إلى بناء نظام سياسي جديد، يوفر الأمن والازدهار والحرية، غير أنه عادة ما يكون لها أهداف أخرى تصب في مصلحة من يقوم على إحداثها.

[1] عبدالغفار عفيفي الدويك، "الأزمات والحروب السيبرانية... تهديدات تتجاوز الفضاء الإليكتروني"، مركز الأهرام للدراسات السياسية والاستراتجية، نشر بتاريخ 03 فيفري 2019، اطلع عليه بتاريخ 12 /03 /2022، الساعة: 15:00،على الرابط: https://acpss.ahram.org.eg/News/16843.aspx

*موقع ويكيليكس، ومعناها "تسريبات الويكي" يعتبر موقع ويكيليكس –كما يقول القائمون عليه– موقعا للخدمة العامة مخصصا لحماية الأشخاص الذي يكشفون الفضائح والأسرار التي تنال من المؤسسات أو الحكومات الفاسدة، وتكشف كل الانتهاكات التي تمس حقوق الإنسان أينما وكيفما كانت.

[2] حكيم غريب وصبرينة شرقي، مرجع سابق، ص. 97.

ارض الواقع، وهذا النمط لا يحتاج إلى سيناريوهات أو بدائل كما في الأزمات السياسية، الأمر يتوقف على قوة الأطراف وقدراتها السيبرانية في الدفاع أو الهجوم[1].

كما قد يمهد هدا النمط لعمل عسكري، وتدور حروب الفضاء السيبراني في هذا النمط عن طريق اختراق وتخريب المواقع الإلكترونية، اضافة إلى شن حرب نفسية ضد الخصم وغيرها، وشهدنا بعض نماذج هذا النمط في هجمات حلف الناتو في عام 1999 على يوغوسلافيا، حيث استهدفت الهجمات الإلكترونية تعطيل شبكات الاتصالات اليوغوسلافية، وفي عام 2006 شاهدنا هدا النمط من خلال الحرب بين حزب الله وإسرائيل، وبين حماس وإسرائيل في عامي 2008 و 2012، وكذلك بين روسيا وجورجيا في عام 2008[2].

ثالثا ← الحرب السيبرانية الساخنة مرتفعة الشدة(High intensity): لم سبق وأن شهد العالم هذا النمط حيث يعبر هدا النمط عن نشوء حروب في الفضاء السيبراني منفردة وغير متوازية مع الأعمال العسكرية التقليدية، وإن كانت احتمال حدوثها في المستقبل وارد مع التطور التكنولوجي الهائل، وزيادة الاعتماد على الفضاء الإلكتروني[3].

وينطوي هذا النمط من الحروب السيبرانية على تحقيق "الهيمنة السيبرانية الواسعة" حيث يتم استخدام الأسلحة الإلكترونية فقط ضد منشآت العدو ومنه سيطرة التكنولوجيا على إدارة العمليات العسكرية، ويرى بعض الخبراء ان هجوم فيروس "ستاكسنت" ضد المنشآت النووية الإيرانية، من طرف إسرائيل بالتعاون مع الولايات المتحدة الامريكية عام 2010، نموذجاً تقريبيا لهذا النمط من الحروب السيبرانية، ومن أكثر الهجمات السيبرانية شيوعاً "هجمات الحرمان من الخدمات" أو "هجوم حجب الخدمة" Distributed Denial of Service"، وهجوم "شخص في المنتصف "Man In The Middle " ، كذلك التصيد الاحتيالي " Attacks Phishing"، وهجوم

[1] عبدالغفار عفيفي الدويك، موقع سابق.

[2] عادل عبد الصادق،" أنماط الحرب السيبرانية وتداعياتها على الأمن العالمي"، مرجع سابق، ص. 34.

[3] نفس المرجع، ص، ص. 34-35.

كلمة المرور "Passwords Attacks"، وتتوقف قوة آثار هذه الهجمات على ثلاث عوامل، هي: أهمية الخدمة المقدمة، والاحتياطات المسبقة، وقوة الهجمة[1].

تنوعت تعريفات الحروب السيبرانية بين تقنية وعسكرية، كما تدرجت أنماطها الحروب من منخفضة الشدة المتمثل في أساليب القوة الناعمة إلى متوسطة الشدة الذي يكون عن طريق إختراق المواقع الإلكترونية للعدو، وصولا إلى نمط الأعلى مرتفع الشدة الذي يتم فيه استخدام الأسلحة السيبرانية بهدف إلحاق أضرار مادية في منشآت العدو، هذا الشكل من الحروب يدار في ميدان جديد مغاير تماما للتقليدي وهو الفضاء السيبراني الذي تحولت وتشابكت فيه المفاهيم.

[1] عبد الغفار عفيفي الدويك، موقع سابق.

المبحث الثالث: الفضاء السيبراني والتحول في المفاهيم.

حتّى يتضح لنا مفهوم الحرب السيبرانية ونستطيع إزالة اللّبس حوله لابّد أولاً من تحديد بعض المصطلحات المرتبطة الحُروب السيبرانية، لذلك سوف نتطرّق في هذا المبحث إلى مفهوم الفضاء السيبراني ومفهوم القوّة السيبرانية والأمن السيبراني والصراع السيبراني، وأهم التّعريفات التي يقدمها لنا مجتمع البحث.

المطلب الأول : مفهوم الفضاء السيبراني.

كلمة السيبراني "Cybernetic" مشتقة من المصطلح الإغريقي "kybernetes" والتي تعني الطيار أو القائد أو الحاكم، ويفيد الاشتقاق بأنّ كلمة سيبرانية تتضمن آليات تعقيب تتيح القيادة والتّحكم في الأنظمة[1]، بمعنى القيادة والتحكم عن بعد.

واصطلاحا: السيبرانية هي صفة لأي شيء مرتبط بالحواسيب وشبكة الانترنت من برمجيات وخدمات مختلفة.

وقد استخدم مصطلح السيبرانية لأول مرة عام 1948 من قبل عالم الرياضيات الأمريكي نوربرت وينر "Norbert Wiener" حيث وضع كتاب بعنوان "السيبرانية أو التحكم والاتصال في الحيوان والآلة"، من أجل وصف نظام التغذية الراجعة "Feedback" الذي وضعه[2].

---

[1] بيتر بي سيل، *الكون الرقمي: الثورة العالمية في الاتصالات* ترجمة. ضياء وراد(المملكة المتحدة : مؤسسة هنداوي سي آي سي، 2017)، ص. 22.
متاح على الرابط: https://downloads.hindawi.org/books/83063951.pdf

[2] سعد علي الحاج بكري، "الأمن «السيبراني».....ومعضلة حمايته"، جريدة العرب الاقتصادية الدولية ، نشر بتاريخ: 24 أوت 2017، اطلع عليه بتاريخ 11 /03 /2022، الساعة: 18:00، على الرابط: https://2u.pw/0kTwu.

أما مصطلح الفضاء السيبراني فقد ظهر في ثمانينات القرن الماضي، من طرف الكاتب الروائي الأمريكي الكندي ويليام جيبسون (William Gibson) مصطلح في إحدى قصصه ذات الخيال العلمي[1].

وعلى العموم هناك عدّة تعريفات للفضاء السيبراني فالوكالة الفرنسية لأمن أنظمة الإعلام"ANSSI" عرفته على أنه: "فضاء التواصل المشكّل من خلال الربط البيني العالمي لمعدات المعالجة الآلية للمعطيات الرقمية"[2]، وبالنظر إلى هذا التعريف نجد أنه يركز على الجانب التقني للفضاء السيبراني ويهمل جوانب أخرى.

وعرفته الإستراتيجية العسكرية الأمريكية لعمليات الفضاء الإلكتروني (NMS-CO) بأنه: "المجال الذي يتميز باستخدام الإلكترونيات والطيف الكهرومغناطيسي لتخزين البيانات وتعديلها وتبادلها عبر الأنظمة المتصلة بشبكة الانترنت وما يرتبط بها من أنظمة البنى التحتية"[3].

أما فراد شراير "Schreier Fred" عرف الفضاء السيبراني بأنه : "وسيلة يمكن إنشاء المعلومات والتصرف في أي وقت وفي أي مكان ومن قبل أي شخص"[4].

وعرفت الأمم المتحدة الفضاء السيبراني بأنه : "النظام العالمي لأنظمة أجهزة الكمبيوتر الدولية ، والبنى التحتية للاتصالات، وكيانات عقد المؤتمرات عبر الإنترنت، قواعد البيانات ومرافق المعلومات المعروفة عمومًا بالشبكة"[5].

---

[1] نورة شلوش، "القرصنة الالكترونية في الفضاء السيبراني "التهديد المتصاعد لأمن الدول"،" *مجلة مركز بابل للدراسات الإنسانية 8*، رقم. 02 (2018)، ص. 190.
متوفر على على الرابط: https://iasj.net/iasj/download/bce8f50577f3c83f

[2] منى عبد الله السمحان، "متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود: المملكة العربية السعودية،" *مجلة كلية التربية 1*، رقم.111 (2020)، ص. 11.
متاح على الرابط:https://2u.pw/EFxAt

[3] Jason Andress, Steve Winterfeld, "*Techniques Tactics and Tools for security practitioners*", (USA: Elsevier, 2011), p. 2.

[4] Fred Schreier, Op.Cit, p. 13.

[5] Jason Andress, Steve Winterfeld, Op.cit, p. 2.

فالفضاء سيبراني هو عبارة عن بيئة افتراضية تفاعلية، تضم عدة عناصر مادية وغير مادية، ومكون من مجموعة من الأجهزة الرقمية، والشبكات والبرمجيات، والمستخدمين[1]، يتشابك مع عالمنا المادي ويتأثر به ويؤثر فيه، أي تقوم العلاقة بين العالمين على نظرة تكاملية تحمل في طياتها مزايا ومليء بالمخاطر يبدي لنا أن طبيعة الفضاء كساحة عالمية عابرة لحدود الدول"[2].

وحسب تعريف وزارة الدفاع الأمريكية"USDoD فالفضاء السيبراني هو: "مجال شامل داخل بيئة المعلومات يتكون من شبكة مترابطة من البنى التحتية لتكنولوجيا المعلومات، بما في ذلك الإنترنت وشبكات الاتصالات وأنظمة الكمبيوتر والمعالجات المدمجة وأجهزة التحكم"[3].

وبمفهوم شامل الفضاء السيبراني عبارة عن مجال افتراضي، يعتمد على الحواسيب وشبكة الانترنت، مع كم هائل من المعلومات والبرمجيات والمستخدمين[4].

ويتكون الفضاء الالكتروني من ثلاثة مكونات أساسية متمثلة في ثلاث طبقات وهي[5]:

1- الطبقة المادية "Hardware" : وتعد بنيتها التّحتية تشمل المعدّات المادية والأجهزة مثل الحواسيب، البرمجيات، الكابلات والأسلاك.

2- الطبقة المنطقية "software": وتشمل المكونات المنطقية والتقنية الخاصة بمجال البرمجة، فهي تعتمد على الخوارزمية، من خلال لغات برمجة

---

[1] منى عبد الله السمحان، مرجع سابق، ص. 11.

[2] تغريد معين حسن المشهدي، مرجع سابق، ص. 241.

[3] Department of Defense, Dictionary of Military and Associated Terms, 12 April 2001(As Amended Through 17 October 2008),p 141.
متوفر على الرابط: https://www.bits.de/NRANEU/others/jp-doctrine/jp1_02(10-08).pdf

[4] "ما هو الفضاء السيبراني؟"، سايبر وان، نشر بتاريخ: 5 نوفمبر2021، اطلع عليه بتاريخ:2022/03/15،الساعة:15:00،على الرابط: https://2u.pw/xYK4Z

[5] "تعريف الفضاء السيبراني"، ترينـد، اطلع عليه بتاريخ:2022/03/15،الساعة: 19:00، على الرابط: https://2u.pw/jCH42

مختلفة حتّىيستطيع الإنسان التعامل معها بمعنى الانتقال من لغة الإنسان إلى لغة الكمبيوتر.

3- طبقة الوسائط"Media ": وتسمى أيضا الطبقة الاجتماعية أو الإعلامية، تضم كل ما يخص المستخدم من هويته الرقمية وبياناته شخصية مثل : صورة شخصية على مواقع التواصل الاجتماعي، بريد الإلكتروني، رقم الهاتف وغيره من الأمور الشخصية.

أهم خصائص الفضاء السيبراني [1]:

1 – هو فضاء إلكتروني افتراضي عملياتي يعتبر الميدان الخامس للحروب .

2 – تُعد البنى التحتية لأنظمة الاتصالات وتقنية المعلومات جزءا جوهري من الفضاء السيبراني .

3 – الفضاء السيبراني لا يقتصر على شبكة الإنترنت فقط وإنما شبكات أخرى مثل:

شبكة الهاتف العامةPSTN، نظام التموضع العالمي، GPSنظام جمع وإرسال تقارير الاتصالات في الطائرات ACARS .

4 – يحتوي على كمية هائلة من المعلومات والبيانات.

وللفضاء الالكتروني مجموعة من مزايا وعيوب أهمها[2]:

أ-**المزايا:**

[1] تغريد صفاء مهدي التميمي، "توظيف القوة السيبرانية في الأداء الاستراتيجي الأمريكي،" (أطروحة دكتوراه في علوم السياسية، جامعة النهرين، كلية العلوم السياسية،2021)، ص. 4.

[2] أسماء شاكر، "الفضاء الإلكتروني والواقع الافتراضي في علم الاجتماع الرقمي"، إي عربي، نشر بتاريخ: 28سبتمبر2021، تم الاطلاع على الموقع بتاريخ: 2022/03/11، على الرابط:https://2u.pw/WpZLD

1- **مصدر المعلومات:** يعتبر مكتبة افتراضية للمعلومات، خصوصا للدراسة مع مواقع التعلم.

2- **يسهل عملية التواصل:** حيث أصبح إرسال واستقبال الرسائل بشكل أسهل وأسرع.

3- **يسهل على الإنسان المجهود:** من خلال عمليات التسوق والحجز لمختلف الخدمات.

4- **مصدر فعال للبحث:** مثل البحث عن وظيفة وفرص عمل وما إلى ذلك .

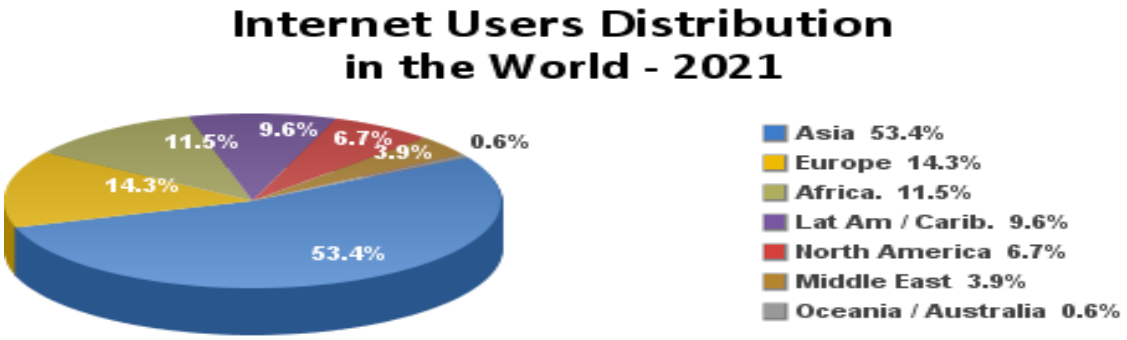
ب-العيـوب:

1- وجود كم هائل من البيانات المخزنة، يجعله سلاحاً قوياً في أيدى المجرمين، قد تؤدي سرقة البيانات إلى تدمير مؤسسات صناعة المحتوى في العالم .

2- تهديدات والاحتيال مجهولة المصدر يصعب تتبعها، حيث اصبح مكان جيد للسارقين والهاكرز.

3- بفضل فضاء السيبراني أصبح من سهل تدمير بنى تحتية للدول وتجسس، ودخول في صراعات سيبرانية.

الشكل 01: مستخدمي الانترنيت حول العالم لسنة 2021.



المصدر: www.internetworldstats.com

وفقاً لهذه الإحصائيات يفوق مستخدمي الانترنيت 5 مليارات شخص حول العالم، وهذا الرقم يفوق 60% من إجمالي سكان العالم، البالغ عددهم حوالي 8 مليار إنسان، كما تحتوي قارة أسيا على أكثر من نصف مستخدمي الانترنت، تاليها أوروبا بثاني أكبر عدد من مستخدمي الإنترنت، ثم إفريقيا بأكثر من 600 مليون مستخدم، وعليه فيجب توعية المستخدمين بمخاطر الانترنت.

المطلب الثاني: مفهوم القّوة السيبرانية .

تعددت مفاهيم القوة في العلاقات الدولية كما تعددت مصادرها وأشكالها، فالقوة من أكثر المفردات استخداما في العلاقات الدولية، ومع التطور السريع لتكنولوجيا الكمبيوتر، وخاصة مع ظهور شبكة الانترنت أحدثت تحولا كبيرا في مفهوم القوة فلم تعد القوة العسكرية هي المعيار الأساسي لقياس القوة في العلاقات الدولية، فبعد الثورة المعلوماتية ظهر شكل جديد من أشكال القوة وهي القوة السيبرانية (cyber power) لتتواكب مع متغيرات النظام الحديث، والتي كان لها دورًا كبيرًا في تغيير موازين القوى.

وتعرف القوة في العلاقات الدولية بصفة عامة بأنها "القدرة على التأثير في الآخرين"، وهناك من عرفها بأنها المشاركة في صنع القرار، وهناك من جمع بينها[1].

أما القّوة السيبرانية (cyber-power)، فقد عرفها دانيال كويل "Daniel Kuehl" على أنها: "القدرة على استخدام الفضاء الإلكتروني لخلق مزايا والتأثير على الأحداث في بيئات تشغيلية وذلك عبر أدوات القوة "[2].

بينما عرّفها جوزيف ناي*: "القوة الإلكترونية هي القوة التي تعتمد على مصادر المعلومات والسيطرة على الأنشطة الإلكترونية والحواسيب والبنية التحتية المعلوماتية ذات الصلة بالفضاء الإلكتروني"، وعرفها كذلك بأنها "القدرة على الحصول على النتائج المفّضلة من خلال استخدام موارد المعلومات المترابطة إلكترونيًا"[3].

ومنه فالقوة السيبرانية عبارة مجموعة من التأثيرات الإستراتجية في الفضاء السيبراني[4].

ويرى فراد شراير "FRED SCHREIER" أن للقوة السيبرانية ثلاث خصائص رئيسية: موجودة في كل مكان ومتكاملة ، ويمكن أن تكون ظاهرة[5].

---

[1] عادل علي سليمان موسى العقيبي، "مفهوم القوة في العالقات الدولية 1991-2017(المنظور الأمريكي: دراسة حالة)،" (رسالة ماجستير في علوم السياسية، جامعة الشرق الأوسط ، كلية الاداب والعلوم،2018)، ص، ص. 24-25.
متاح على الرابط: https://meu.edu.jo/libraryTheses/5ca84ef6e8983_1.pdf

[2] Daniel T. Kuehl, *"From Cyberspace to Cyberpower: Defining the Problem"*, in *Cyberpower and National Security*, Edited by. Franklin D Kramer, Stuart H Starr, and Larry K Wentz(USA: National Defense University Press and Potomac Books, 2009), p. 38.

* جوزيف صموئيل ناي استاذ في جامعة هارفارد ومساعد وزير الدفاع سابقا الولايات المتحدة الأمريكية.

[3] Joseph S.Nye JR, *"Cyber Power,"*(USA: Belfer Center for Science and International Affairs, 2010), p. 4.
متاح على الرابط : https://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf

[4] زينب شنوف،"الحرب السيبرانية في العصر الرقمي : حروب ما بعد كلاوزفيتش،" *المجلة الجزائرية للأمن والتنمية9* ، رقم. 02(2020)، ص. 92.
متاح على الرابط: https://2u.pw/AkysF

[5] Fred Schreier, Op.cit , p. 16

والجدير بأن القوة السيبرانية يجب أن تتوفر على ستة عناصر رئيسية[1]:

1- **بنية تحتية:** وجود بنية تحتية تكنولوجية سيبرانية.

2- **أسلحة إلكترونية:** البرامج الضارة مثل الفيروسات.

3-**العمليات التكنولوجية:** تشمل المهاجمة والدفاع، والتجسس على الخصم.

4- **بنية مؤسسية وتشريعية:** تتولى مهمة ممارسة القوة السيبرانية وتحقيق الأمن السيبراني للدولة وتشريعية تكون ضامنة ومحددة استعمال القوة السيبرانية.

5- **خطة إستراتجية:** خطة العمل بمثابة خطة الطريق التي تسهل تحقيق الأهداف الموضوعة وآليات التنفيذ وتحدد الوظائف لكل جهة.

6- **العنصر البشري:** الفرد الكفء والمدرب والمعد إعداداً جيد على استخدامها.

وفي نفس السياق طور جوزيف ناي مفهوم القوة وجعلها أكثر ارتباطا بامتلاك التكنولوجية، والقدرة على استخدامها. من خلال استغلال الفضاء الإلكتروني لتأثير في الأحداث التي تجري عبر البيئات التشغيلية، مستعينًا بأدوات القوة المختلفة سواء كان عسكرية أو اقتصادية أو دبلوماسية أو معلوماتية، وقد حدد ناي ثلاثة أنواع من الفاعلين الذين يمتلكون القوة الالكترونية وهم الدول والفاعلين من غير الدول والأفراد[2].

وحسب جوزيف ناي في مقال منشور في ماي 2010، بمركز بلفور للعلوم والشؤون الدولية لكلية كينيدي بجامعة هارفرد، تحت عنوان "القوة السيبرانية Cyber Power" حدد ثلاثة أنماط ولها استخدامات صلبة وناعمة [3]:

---

[1] إيهاب خليفة، *القوة الالكترونية :كيف يمكن أن تدير الدول شؤونها في عصر الانترنت* (مصر: العربي للنشر والتوزيع،2017)، ص. 80.

[2] نفس المرجع، ص. 56.

[3] Joseph S.Nye JR, Op.Cit, p. 7.

1 – يؤثر الفاعل "أ" على الفاعل "ب" :

القوة الصلبة: هجمات رفض الخدمة، إدخال البرامج الضارة، اعتقال المدونين.

القوة الناعمة: حملة إعلامية لتغيير التفضيلات الأولية للقراصنة، تجنيد أعضاء المنظمات الإرهابية.

2 –التحكم في أجندة الآخرين: أي قدرة الفاعل "أ" على استبعاد استراتيجيات الفاعل "ب".

القوة الصلبة: جدران الحماية والضغط على الشركات لاستبعاد بعض الأفكار.

القوة الناعمة: المراقبة الذاتية لمزودي خدمة الإنترنت ومحركات البحث .

3 –قدرة الفاعل "أ" على ترتيب أولويات الفاعل "ب" :

القوة الصلبة: تهديدات بمعاقبة المدونين الذين ينشرون مواد خاضعة للرقابة.

القوة الناعمة: معلومات لخلق التفضيلات (على سبيل المثال تحفيز القومية).

المطلب الثالث : مفهوم الأمن والصراع في الفضاء السيبراني.

هناك مجموعة من المفاهيم والألفاظ لها صلة بظاهرة "الحُروب السيبرانية"، والتي تتشابك وتتفاعل في محيط الفضاء الرقمي. ويمكن تفصيل ذلك على النحو الآتي:

1– الأمن السيبراني (Cyber security) : وهو الإجراءات المتخذة للدفاع عن الأنظمة المتصلة بالإنترنت ضد الهجمات الضارة، ويتم استخدام مصطلح الأمن السيبراني في مجموعة متنوعة من السياقات، ويمكن تقسيمه إلى عدة فئات فيما يلي[1]:

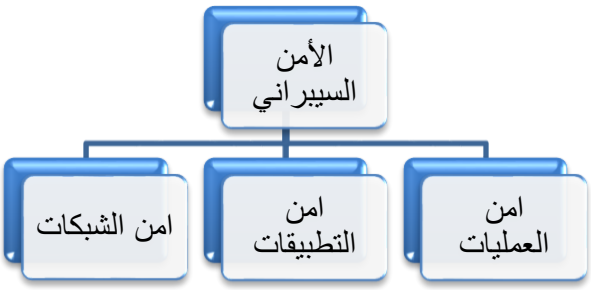
[1] "Was ist Cybersicherheit?", kaspersky, Date of Entry:01/03/2022, at 22:00, on the site: https://2u.pw/PJSsz .

أ- **أمن الشبكات(Network-security):** هو طريقة للحماية من الوصول غير المصرح بهم سواء من الأفراد أو البرامج الضارة إلى شبكة الكمبيوتر.

ب- **أمن التطبيقات(Application-security):** يشمل الحفاظ على البرامج والأجهزة آمنة من الهجمات.

جـ- **أمن العمليات(Operational-security):** هي العمليات والقرارات لمعالجة أصول البيانات وحمايتها.

الشكل رقم02: مكونات الأمن السيبراني



المصدر: من إعداد الطالبة

ويوضح هذا الجدول أكثر الدول أمانا في الفضاء السيبراني الاتحاد الدولي للاتصالات:

الجدول 01: ترتيب أفضل 10 دول في مؤشر الأمن السيبراني العالمي لسنة 2021

Country Name	Score	Rank
United States of America**	100	1
United Kingdom	99.54	2
Saudi Arabia	99.54	2
Estonia	99.48	3
Korea (Rep. of)	98.52	4
Singapore	98.52	4
Spain	98.52	4
Russian Federation	98.06	5
United Arab Emirates	98.06	5
Malaysia	98.06	5
Lithuania	97.93	6
Japan	97.82	7
Canada**	97.67	8
France	97.6	9
India	97.5	10

المصدر: الاتحاد الدولي للاتصالات التابع للأمم المتحدة على الموقع:
https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

كما موضح في جدول المؤشر العالمي للأمن السيبراني "جي سي آي" (GCI) لعام 2021، والأخير الصادر عن الاتحاد الدولي للاتصالات، احتلت الولايات الامريكية المتحدة المرتبة الاولى بـ 100 نقطة (نقاط كاملة) من بين 194 دولة خاضعة لاستطلاع تصنيف GCI الرابع. أما عربيا كان لسعودية المرتبة الثانية عالميا بـ 99.54 نقطة والامارات العربية المتحدة المركز الثاني عربياً والخامس عالميا بـ98.06 نقطة من أصل 100 نقطة، بينما أحتلت الجزائر المرتبة الـ104 عالميا برصيد 33.95 نقطة.

2- الصّراع السيبراني(cyber conflict): ونقصد به استخدام الوسائل والأدوات السيبرانية داخل الفضاء الافتراضي، تسعى من خلاله أطراف الصراع لفرض هيمنتها،

لأغراض التدمير، أو تعديل ، أو تغيير المعلومات في الفضاء الالكتروني[1].

وقد يأخذ الصراع السيبراني مستويين أساسيين في تفاعلته، الأولّ هو صراع سيبراني على المعلومات الالكترونية ، ويتعلّق بسعي الأطراف المتنازعة الاستحواذ على المعلومات المخزنة في الفضاء الافتراضي والتحكم بها، أما الثاني يتمثل بأنه نزاع إلكتروني تحركه دوافع مرتبط بتفاعلات الواقع، ومنه يستخدم الفضاء السيبراني لتحقق أهداف على ارض الواقع[2]. ويمكن تقسيم مستوى الصراع السيبراني من حيث تأثيراته وأضراره إلى أربعة مراحل على شكل هرمي.

الشكل 03: مستويات الصّراع السيبراني

المصدر: من إعداد الطالبة

أ-**القرصنة السيبرانية(cyber-hacking)**: هي عملية اختراق لأجهزة الحاسوب عن طريق استغلال ثغرات أمنية في نظامه، قصد القيام بتعديل أو تخريب أو إلغاء محتوياته، ومن أمثلة القرصنة، القيام بعمليات قرصنة المواقع الإلكترونية[3]، وحجب الخدمة (DDoS).

ب -**الجريمة السيبرانية(Cybercrime)** : تشير إلى أي نشاط غير مشروع لتقنية المعلومات، ضد أفراد أو جماعات سواء بطريقة مباشرة أو غير مباشرة، بدافع إجرامي مادي

[1] سماح عبد الصبور،"الصراع السيبراني "طبيعة المفهوم وملامح الفاعلين،" من مؤلف جماعي بعنوان: الصراع السيبراني: التنازع العالمي على قوة الفضاء السيبراني، مرجع سابق، ص. 6.

[2] احمد عبيس نعمة الفتلاوي، مرجع سابق، ص، ص. 105-106.

[3] محمد عبد الغفار، مرجع سابق، ص. 10.

أو معنوي[1]، وتتمثل في عدد محدود من الأعمال التي تمس بسرية البيانات أو إحداث أضرار بالنظم الحاسوبية[2].

جـ –التجسس السيبراني (Cyber Espionage): هو شكل حديث من أنواع التجسس، يتيح اختراق وسرقة المعلومات بصفة مجهولة وغير مكلفة من أي مكان في العالم من مكانك حيث يتم عن طريق الحواسب أو شبكات الانترنت، يتم حصول على معلومات بطرق غير مشروعة دون إذن ومعرفة صاحب المعلومات، من أجل منفعة سياسية أو عسكرية أو اقتصادية، فالتجسس السيبراني هو ذلك التجسس الذي يعتمد على إستخدام التقنيات التكنولوجية في الفضاء السيبراني للحصول على معلومات[3].

د– الإرهاب السيبراني(Cyberterrorism): وهو استخدام الفضاء الالكتروني من قبل الدول، أو الجماعات أو الأفراد كأداة للتهديد أو عدوان أو التخويف سواء المادي أو المعنوي لتحقيق أهداف معينة[4]. ولكي يعتبر الشخص إرهابيا وليس مخترقا في الفضاء الالكتروني، يجب أن تؤدي الهجمات التي يشنها إلى عنف ضد الأشخاص أو الممتلكات، أو إلحاق الضرر الكافي لنشر الخوف والرعب[5].

---

[1] نبيل دريس، "الجريمة السيبرانية بين المفاهيم والنصوص التشريعية:الجزائر نموذجا،" *مجلة القانون والمجتمع 10*، رقم. 02 (2017)، ص. 30.

[2] تقرير عن اجتماع فريق الخبراء المعني بإجراء دراسة شاملة عن مشكلة الجريمة السيبرانية، مكتب الأمم المتحدة المعني بالمخدرات والجريمة، 2019. متاح على الرابط التالي: https://2u.pw/B183x

[3] إدريس عطية، "مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري،" *مجلة مصداقية 1*، رقم. 01 (2019)، ص. 110.
متاح على الرابط : https://2u.pw/vSoGg

[4] عادل عبد الصادق، *الإرهاب الإلكتروني: القوة في العلاقات الدولية" نمط جديد وتحديات مختلفة"*، ط.2 (مصر: مركز الدراسات السياسية والإستراتجية، 2009)، ص. 116.

[5] هشام بشير،"الإرهاب الالكتروني في ظل ثورة المعلومات"، مجلة اراء حول الخليج، نشر بتاريخ: 01 ماي 2012، تم الاطلاع عليه بتاريخ:10 /2022/03، على الرابط:https://2u.pw/kMXqq .

فالفضاء السيبراني مجال افتراضي يضم كم هائل من المعلومات والبرمجيات والمستخدمين، ومن المعلوم أنه أعاد تشكيل عدة مفاهيم، فالقوة بأبعادها الجديدة من حيث الفاعلين كونها ليست حكرا على دول فقط، وكذلك من حيث طبيعتها وأنماط استخدامها فالقوة السيبرانية، أصبحت حقيقة أساسية في العالم، وتؤثر في سلوك الوحدات السياسية، والفضاء السيبراني لا يعترف بالمكان والزمان، وأصبح من الضروري أن تحقق الدولة الأمن السيبراني حتّى تستطيع التصدي للمخاطر والصرعات المحتملة في العالم الافتراضي.

منذ نهاية القرن العشرين شاهد العالم ثورة معلوماتية في تكنولوجيا المعلومات والاتصالات، ونتيجة لهذه التطورات أحدثت تغييرا للكثير من المفاهيم الامنية، وأصبح الفضاء السيبراني مجال خامس للحرب مختلفة تماما على النطاق التقليدي (بر، بحر، جو وفضاء)، فلا شك إن القوة السيبرانية أصبحت هي القوة المستقبلية القادمة، ومن يمتلكها سيكون هو المهيمن على الساحة الدولية، ومع تحول في هذا المفهوم ظهر نمط جديد للحروب ساحتها الفضاء الافتراضي تتمثل في الحُروب السيبرانية التي تتداخل فيها الأهداف، بتعدد أنماطها المتعددة وفواعلها، فمن يستحوذ على القدرات السيبرانية يصبح أكثر قدرة على تحقيق أهدافه العسكرية أو المدنية، هو ما سنتعرض إليه في الفصل الثاني من هذا البحث.

الفصل الثاني: آليات وفواعل الحروب السيبرانية

الفصل الثاني: آليات وفواعل الحروب السيبرانية.

أعاد الفضاء السيبراني تشكيل مفهوم الحرب، وبزور حروب سيبرانية حديثة من حيث طبيعتها المميزة، التي سوف نتناولها في هذا الفصل بتوضيح آليات وفواعل الحروب السيبرانية، من حيث طبيعة الأسلحة المعتمدة في هذا النمط من الحروب، كما نتطرق إلى العلميات العسكرية في الفضاء الافتراضي، هو ما كان له انعكاس على قدرات الدول وتحولات عميقة على مستوى علاقاتها الدولية، ونعرج أيضًا لتشخيص طبيعة اللاعبين السيبرانيين التي ليست حكرا على الدول كسابقتها من الحروب التقليدية، وظهور فواعل جديدة مثل: الافراد و المنظمات، مع عرض مستويات الحروب السيبرانية، ونطرح في المبحث الأخير مسألة التأمين السيبراني وماهي السبل الوقائية التي تحول للحد من الاختراقات السيبرانية، وننتقل إلى التشريعات القانونية والاتفاقيات الدولية لمواجهة الحروب في الفضاء السيبراني.

المبحث الأول: الأسلحة والعمليات العسكرية السيبرانية.

تزامنا مع التقدم الحاصل في الوسائل والمعدات المستخدمة في العمليات العسكرية، ومع ظهور الحروب السيبرانية في سياق دولي يغلب عليه الطابع التكنولوجي والتقني، تم ابتكار أنواع جديدة من الأسلحة تتوافق مع المجال السيبراني، مهمتها تسلل داخل النظم المعلوماتية لتحقيق الأهداف المرجوة، تستخدم العمليات السيبرانية العسكرية المختلفة.

المطلب الأول: الأسلحة السيبرانية.

وهي عبارة عن برامج إلكترونية مصممة خصيصا لاختراق نظم الكمبيوتر، بهدف تعطيلها أو إتلافها، بصفة أساسية على برمجيات خبيثة (malware)، التي يتم تصميمها للقيام بعدة وظائف وتوجد بعدة نماذج أهمها:

1- فيروسات الحاسوب (Computer Virus): عبارة عن برامج خارجية يتمّ إنشاءها بهدف إلحاق الضرر بأجهزة الحاسب أو السيطرة عليه، وقد يتم استخدامها لتعطيل شبكات الخدمات أو البنية التحتية للطرف المستهدف[1]، اكتسبت اسمها بسبب كيفية انتشارها حيث أنها سريعة العدوى داخل أجزاء الجهاز، كما ساهمت الانترنت في انتشارها نظرا للحجم الكبير التبادل بين مستخدمي الشبكة العكنبوتية وقد تصل أضرارها إلى تدمير نظام التشغيل الخاص بالحاسوب[2] ، ويوجد العديد من أنواع الفيروسات أهمها[3]:

⟸ **فيروس قطاع التمهيد (Boot sector virus):** هو فيروس تم تحميله في الذاكرة يتم تنفيذه كلما قمت بتشغيل جهاز الكمبيوتر.

---

[1] إيهاب خليفة، *القوة الالكترونية :كيف يمكن أن تدير الدول شؤونها في عصر الانترنت*، مرجع سابق، ص. 83.

[2] عادل عبد الصادق، *الإرهاب الإلكتروني:القوة في العلاقات الدولية" نمط جديد وتحديات مختلفة"*، مرجع سابق، ص. 126.

[3] "What is a Computer Virus?", Date of Entry:15/01/2022, at 22:05, on the site: https://2u.pw/oHNGA .

⇦ **فيروس عدوى الملفات (File infectors virus):** هو فيروس يصيب الملفات الموجودة على جهاز الكمبيوتر.

⇦ **فيروس ماكرو (Macro virus):** هو فيروس يُصيب الأومر المكتوبة بلغة الماكرو، ويمكن لهذا الفيروس تنفيذ عمليات النظام مثل إنشاء الملفات أو حذفها أو الكتابة في ملفات موجودة، وبالتالي لديه القدرة على إحداث قدر كبير من الضرر.

⇦ **فيروس متعددة الأشكال(Polymorphic virus):** هو فيروس يغير شكله كلّما يكتَشف برامج مكافحة الفيروسات.

⇦ **فيروس العدوى السريعة والبطيئة:** يحاول تجنب اكتشافه إما بإصابة جميع الملفات على النظام بسرعة أو عن طريق إصابتها ببطء.

2. دودة الحاسوب (Computer worm) : هي برنامج تنتشرعبر الإنترنت عن طريق نسخ نفسها على أجهزة الكمبيوتر، على عكس الفيروسات لا تتطلب الديدان مساعدة بشرية من أجل العدوى أو التكاثر*، فقد تم تصميمهم للسيطرة على أجهزة الكمبيوتر التي ينزلون عليها أو لسرقة معلومات المستخدم السرية أو لتحويلها إلى "زومبي" أو "روبوتات" يتم التحكم فيها عن بعد[1].

3. أحصنة طروادة (Trojan Horses): برامج تختبئ على مرأى من الجميع من خلال التنكر في ملفات أو برامج و بمجرد التنزيل والتثبيت، تقوم أحصنة طروادة بإجراء تغييرات على جهاز الكمبيوتر وتنفيذ أنشطة ضارة، دون علم الضحية أو موافقته[2].

*الفرق بين الفيروس والدودة هو أن الفيروس يحتاج إلى برنامج آخر ليعمل، مثل متصفح الويب. أما الدودة قائمة بذاتها ويمكنها تشغيل ونسخ وإرسال نسخ من نفسها بمفردها.

[1] Mike Barwise,"What is an internet worm?", BBC, 9 September 2010, Date of Entry:15/03/2022,at 20:15. on the site : https://2u.pw/ptH0j

[2] "Malware & Computer Virus Facts & FAQs", kaspersky, Date of Entry:15/03/2022, at 22:25, on the site : https://2u.pw/KxZbZ

4. برامج التجسس (Spyware): تقوم برامج التجسس بتجسس على ما تفعله على جهاز الكمبيوتر، وتعتبر برامج التجسس برامج ضارة لأن المستخدمين ليسوا على دراية بها، القصد الوحيد من برامج التجسس هو تجميع البيانات دون أي اعتبار لكيفية استخدام البيانات وقد تقوم برامج التجسس أيضًا بتعديل إعدادات أمان معينة على جهاز الكمبيوتر أو تتداخل مع اتصالات الشبكة[1].

ويوضح هذا الجدول أكثر فيروسات الكمبيوتر تدميراً حسب الخسائر المالية عبر التاريخ:

الجدول 02: أكثر 5 فيروسات الكمبيوتر تدميراً حسب الخسائر المالية.

اسم البرنامج الضار	سنة الظهور	الخسائر المالية التي تسبب بها
1) Mydoom	2004	38 مليار دولار أمريكي
2) Sobig	2003	30 مليار دولار أمريكي
3) Klez	2001	19.8 مليار دولار أمريكي
4) ILOVEYOU	2000	15 مليار دولار أمريكي
5) Swen	2003	10.4 مليار دولار أمريكي

المصدر : من إعداد الطالبة إعتمادًا على الموقع:

https://www.hp.com/us-en/shop/tech-takes/top-ten-worst-computer-viruses-in-history

و هناك برامج أخرى بارزة مثل[2]:

[1] نفس المرجع. اطلع عليه بتاريخ 16 /03 /2022، الساعة: 15:00.

[2] Tom Gerencer, "The Top 10 Worst Computer Viruses in History", Hp, 4 november 2020, Date of Entry:01/03/2022, at 21:00. on the site: https://2u.pw/xuHah

- **Yaha:** وهي دودة ذات متغيرات متعددة، يعتقد أنها نتيجة حرب إلكترونية بين باكستان والهند.

- **Storm Worm** : ظهر عام 2007 وهاجمت ملايين أجهزة الكمبيوتر برسالة بريد إلكتروني.

- **Tanatos / Bugbear** : فيروس مسجل لوحة مفاتيح 2002 استهدف المؤسسات المالية وانتشر إلى 150 دولة.

- **Melissa** : ظهر في عام 1999 ، وكان أخطر فيروسات الكمبيوتر لهذه السنة، قدر مكتب التحقيقات الفدرالي الأمريكي تكاليف التنظيف والإصلاحه بـ 80 مليون دولار.

- **Stuxnet** : يقال إن هذه الدودة دمرت أجهزة الطرد المركزي النووية الإيرانية عن طريق إرسال تعليمات ضارة.

- **Flame** : برنامج معقد جدا يبلغ تعقيده أضعاف ستوكسنت، استعمل للتجسس على بلدان في الشرق الأوسط، وحسب الخبراء مدى تعقيده يوحي بأنه تم تطويره بدعم من إحدى الحكومات.[1]

كما يتم اكتشاف يوماً أكثر من 350 ألف من البرامج الضارة، بتكلفة سنوية تزيد عن 55 مليار دولار، وهذه البرامج الخبيثة ليست سوى غيض من فيض، مع وجود 127 مليون تطبيق برمجيات خبيثة[2]. فالاسلحة السيبرانية هي أسلحة صامتة تستخدم من أجل تحقيق عدة

[1] "اكتشاف فيروس خارق يهاجم أنظمة الكمبيوتر في دول بالشرق الأوسط من بينها مصر"، جريدة الأهرام، نشر بتاريخ: 30 ماي 2012، اطلع عليه بتاريخ: 17 /03 /2022، الساعة: 23:30، على الرابط:
http://www.ahram.org.eg/The-First/News/152146.aspx

[2] Tom Gerencer, Op.cit.
Date of Entry:18/03/2022, at 21:00.

أهداف، ولا تتطلب ميزانية ضخمة من الدول، كل ما تحتاجه مجموعة الحواسيب تستعمل من قبل خبراء في مجال الحوسبة.[1]

المطلب الثاني: العمليات العسكرية السيبرانية.

ويمكن تقسيمها إلى أربعة أنواع رئيسية ذات أربعة أهداف متداخلة :

1. عملية جمع المعلومات الاستخباراتية:

هي عملية تستخدم فيها الأجهزة الاستخبارات السيبرانية (CYBINT) طرق تهدف إلى الحصول على معلومات وبيانات، عن طريق الشبكة الإلكترونية أو الرقمية من الفضاء الإلكتروني[2]، حول أنشطة وقوة وخطط وقدرات الدول أو المؤسسات والأفراد، لإعطاء خلفية عن الذين يشكلون تهديداً للأمن القومي للدول.[3] حيث توفر المعلومات للدول والشركات ميزاتٍ استراتيجية لحماية أمنها القومي من التهديدات الخارجية وكذلك الداخلية، بما يجنبها سباق التسلح السيبراني الهجومي، الذي يستنزف موارد ضخمة. وفي هذا الإطار، توصي السلطات المالية في المملكة المتحدة –على سبيل المثال– بعدد من الخطوات لحماية المؤسسات المالية من التهديدات السيبرانية، بما في ذلك تلقّي المشورة من مزودي المعلومات الاستخباراتية داخل الحكومة البريطانية[4].

---

[1] فرد كابلان، *المنطقة المعتمة: التاريخ السري للحرب السيبرانية* ترجمة. لؤي عبد المجيد(الكويت: سلسلة عالم المعرفة، المجلس الوطني للثقافة والآداب، 2019)، ص. 16.

[2] محمد العميرة، "الاستخبارات والطرق الاستخباراتية لجمع المعلومات"،The Intel Den، نشر بتاريخ : 25 نوفمبر2020، اطلع عليه بتاريخ: 19 /03 /2022، الساعة: 16:00على الرابط:https://2u.pw/DnGzs

[3] "آليات جمع المعلومات الاستخبارية وتوظيفها إلى صناع القرار"، المركز الأوروبي لدراسات مكافحة الإرهاب والاستخبارات ، نشر بتاريخ: 22مارس2021 ، اطلع عليه بتاريخ 17 /03 /2022، الساعة: 22:30.

على الرابط: https://2u.pw/7DV9J

[4] وليد خضر، "الإستخبارات السيبرانية"، بوابة السفير العربي الدولية، نشر بتاريخ: 13 جوان 2021، اطلع عليه بتاريخ 17 /03 /2022، الساعة: 22:30، على الرابط:https://2u.pw/9hFjS

ومن ثمّ فإنها تُعد أحد التدابير الاستباقية التي تحول دون الاختراقات السيبرانية، وتتجنب التكاليف اللازمة لإصلاح.

2. عمليات هجومية "الهجوم السيبراني (Cyber Attack)": هو استهداف مواقع الكترونية التي تهدف إلى تعطيل أو تدمير البيانات المتوفرة فيها أو الاستحواذ عليها[1].

وفي سياق مشابه، تشمل العمليات الهجومية كذلك إلحاق مزيد من الضرر المادي بأفراد الخصم وعتاده، فمن المستطاع استخدام عمليات الهجوم لإضعاف دفاعات الخصم الإلكترونيّة التي يملكها(مثل أنظمة الدفاع الجوي)، وإضعاف قيادته وقطع أنظمة الاتصال بين الوحدات العسكرية، وكذلك تدمير بناه التحتيّة بهدف التأثير فيه عسكرياً أو سياسياً[2].

وتهدف الهجمات التشويش على مصادر المعلومات وتدميرها وحرمان العدو من استخدامها لمصلحتهم، واستعمال التجسس الرقمي لنقل المعلومات والبيانات سرية أو حساسة أو ملكية فكرية نقل معلومات سرية تتعلق بك إلى المهاجم، لاكتساب ميزة[3].

---

[1] احمد عبيس نعمة الفتلاوي، مرجع سابق، ص. 616.

[2] اوستن لونج وآخرون، *الحروب المستقبلية في القرن الحادي والعشرين*(الامارات العربية المتحدة: مركز الإمارات للدراسات والبحوث الإستراتيجية،2014)، ص. 57.

[3]"What is Cyber Espionage?", VMware, Date of Entry:18/03/2022,at 22:00, on the site: https://2u.pw/9nmSR

الشكل 4: الهجمات السيبرانية من 2005 إلى 2020.

المصدر: موقع صندوق النقد الدولي على الرابط التالي:

https://www.imf.org/ar/News/Articles/2020/12/07/blog-cyber-risk-is-the-new-threat-to-financial-stability

فالإحصائيات في هذا الشكل توضح لنا تزايد وتيرة الهجمات السيبرانية ، ولقد تضاعف عدد الهجمات السيبرانية على مدار العقد الماضي، وخاصة في ظل تأثير هذه الهجمات على المؤسسات حيوية للدول، فمن الواضح أن الأمن السيبراني أصبح مصدر تهديد على الأمن القومي للدول.

3.العمليات الدفاعية" الدفاع السيبراني(Cyber Defense)":

وهو عبارة عن آلية دفاع من أجل حماية أنظمة وأجهزة ومعلومات الدولة والجيش والمجتمع والبنية التحتية[1].

[1] علي عبد الرحيم العبودي، "هاجس الحروب السيبرانية وتداعياتها على الأمن والسلم الدوليين،" *مجلة قضايا سياسية*، رقم. 57 ،(2019)، ص. 109.

تتضمن مجموعة من الإجراءات هدفها حماية الشبكات وأجهزة الكمبيوتر من أي عملية اختراق خارجية بالأسلحة الالكترونية، ومنع وصول الخصم إلى معلومات وأنظمتها، عن طريق تامين مستوى البرمجيات والمكون المادي للشبكات[1].

4.العمليات النفسية (Psychological Operation PSYOPS) :

تنفذ العمليات النفسية ضد الخصم بهدف إلحاق الضرر بالروح المعنوية، وترمي كذلك هذه العمليات إلى زعزعة إرادة القتال لدى شعب العدو، وبث التفرقة بين صفوفهم عبر الدعاية والتضليل المعلوماتي[2]، وقد تنفد العمليات النفسية لحلفاء الخصم حتى يتم إضعافهم[3].

السلاح السيبرانى مغاير تماما للتقليدي هو عبارة عن برمجيات إلكترونية غير مكلفة، تستهدف نظم كمبيوتر العدو ، وتتفاوت في أضرارها وشدة تدميرها، كما تطورت بشكل سريع ومعقد لتصبح أكثر شراسة، تستعمل ضد أهداف عسكرية أو مدنية أو في عمليات استخباراتية، من خلال تنفيذ عمليات عسكرية سيبرانية متعددة. كما أن الأسلحة السيبرانية ليست حكرا في يد الدولة حيث يمكن استخدمها من قبل أطراف من غير الدول .

متاح على الرابط:https://2u.pw/LBcYp

[1] إيهاب خليفة، *القوة الالكترونية: كيف يمكن أن تدير الدول شؤونها في عصر الانترنت*، مرجع سابق، ص. 88.

[2] نفس المرجع، ص. 57.

[3] نفس المرجع، ص. 88.

المبحث الثاني: فواعل الحروب السيبرانية.

فتح الفضاء السيبراني المجال لدخول فواعل غير دولاتية، فالحروب السيبرانية ليست حكرا على الدول فقط كما هو مألوف في الحروب التقليدية، بل هناك عدة فواعل حكوميين وغير حكوميين، وهو ما كان له انعكاس على العلاقات الدولية.

المطلب الأول : الفواعل الدولاتية.

الفواعل الدولاتية في هدا السياق يقصد بها الدول والحكومات، انطلاقا من إمكاناتها المادية والبنيوية والبشرية والقانونية تعتبر الدولة فاعل محوري في تسيير الفضاء السيبراني، حيث لابد للدولة ان تتحكم تحكم في مجال الفضاء السيبراني لبسط نفودها وتحقيق اهدافها، في هذا الميدان السيبراني الذي يزاحمها فيه العديد من الفواعل الأخرى، التي قد تصل الى حد تهديد مصالحها[1].

وحسب تقسيم جوزيف ناي لأنماط القوة (القوة ناعمة والقوة الصلبة)، حيث اعتبرت القدرات السيبرانية جزء من القوة الناعمة لدلك سعت الدول على تطوير قدراتها سيبرانية فلم تعد الدول الكبرى كالولايات المتحدة الأمريكية،الصين، بريطانيا وروسيا وحدها من تملك قدرات سيبرانية متطورة بل ظهرت دول جديدة مثل : الهند، استراليا، اندونسيا، كوريا الجنوبية، ايران وتركيا[2].

كما أوضح تقرير لمؤسسة *Risks Control أن نسبة الزيادة في أعداد الهجمات السيبرانية لدوافع السياسية خلال عام 2015 بلغت 56 % [3]. وتضع الدول استراتيجيات سيبرانية لتأمين

[1] حكيم غريب وصبرينة شرقي، مرجع سابق، ص. 98.

[2] علي عبد الرحيم العبودي، مرجع سابق، ص. 102.

*إحدى المؤسسات العالمية المستقلة في مجال استشارات المخاطر السياسية والأمنية.

[3] حكيم غريب وصبرينة شرقي، مرجع سابق، ص. 98.

الفضاء السيبراني وتضم القدرات الدفاعية والهجومية للدول في أغلب الأحيان من الجيش والمحاربين السيبرانيين.

1- **الإستراتيجية السيبرانية:** تعني تطوير وتوظيف القدرات مع المجالات التشغيلية للعمل في الفضاء السيبراني، لتحقيق أو دعم الأهداف بواسطة عناصر القوة الوطنية، وتبنى الإستراتجية السيبرانية على مجموعة ممنهجة من الغايات والوسائل، والطرق (كيف الوسائل تُستخدم لإنجاز الغايات)، لتحقيق الأهداف المختلفة سواء العسكرية والسياسية أو غيرها، وتعمد على الصراحة والوضوح لإظهار كيفية تحقيق جميع الاستراتيجيات الأخرى خصوصا إستراتيجية الأمن القومي، فالإستراتجية السيبرانية تعتبر الجسر الذي يربط بين السياسة واستغلال الأداة السيبرانية [1].

2- **الجيوش السيبرانية (Cyber Armies):** وهم مجموعة من الأفراد مختصون في مجال تكنولوجي المعلومات، ويعملون لصالح حكومات لحفظ أمنها السيبراني الوطني، يعملون في الخفاء دون الظهور للعلن وتستخدمهم الدول لشن الهجمات السيبرانية على أهدافٍ معاديةٍ و تشكيل حائط للدفاع عنها[2].

ومن أبرز الجيوش السيبرانية في العالم نجد:

أ- **القيادة السيبرانية الأمريكية (US Cyber Command):** تأسست في جوان 2009، وهي جزء من القيادات العسكرية التابعة لوزارة الدفاع الأمريكية، مهمتها بمراقبة وإدارة عمليات الفضاء السيبراني، سواء من ناحية تأمين أو القيام بعمليات سيبرانية عسكرية ضد أهداف خارجية ، وقد تولى الجنرال ألكسندر بي كيث (Keith B. Alexander) قيادة القيادة السيبرانية

[1] Fred Schreier, Op.Cit, p. 18.

[2] وائل سليمان، "ما هي الجيوش السيبرانية"، موسوعة اراجيك، نشر بتاريخ: 3 جانفي 2020، أطلع عليه بتاريخ 03/15 /2022، الساعة: 23:25، على الرابط التالي:https://2u.pw/MYPDX

للولايات المتحدة، كأول جنرال عسكري لإدارة الحروب السيبرانية، وبحلول عام 2016 ضمت هذه القيادة حوالي 6000 جندي سيبراني[1].

كما تعتمد هذه القيادة السيبرانية على وكالة المخابرات المركزية (CIA)، تتمثل مهمتها في جمع المعلومات وإعداد الدراسات والأبحاث عن النظم والجهات والشخصيات المستهدفة، إضافة إلى وكالة الأمن القومي الأمريكي (NSA)، تتمثل مهمتها في جمع المعلومات والبيانات الالكترونية، عن طريق التجسس على الاتصالات التي تجري عبر شبكة الانترنت للدول و لقادة دول، و شخصيات عالمية من سياسيين و مسؤولين كبار، عن طريق شركات أمريكية رائدة في الخدمات الإلكترونية المرتبطة بالإنترنت، حيث أن هذه الشركات تابعة تنظيمياً لوكالة الأمن القومي و البنتاغون، كشركة Google وشركات المواقع التواصل الاجتماعي على غرار تويتر وشركة ميتا التي تضم فيسبوك وانستغرام وواتساب، هذا التطبيق الأخير للمراسلات الفورية يستخدم من قبل الوكالات الأمنية الأمريكية لتنصت على مجمل الهواتف الذكية، وهو ما دفع عدة دول لحظره مثل ايران [2]، الصين ، سوريا، كوبا وكوريا الشمالية.

ب – الوحدة 61398 في الصين: مقرها في شنغهاي عاصمة الصين الاقتصادية، وهي وحدة سرية تابعة للجيش التحرير الشعبي الصيني، مهمتها القيام بعمليات التجسس الإلكتروني وسرقة المعلومات والبيانات، حيث تقوم الشركة الصينية للاتصالات بإمدادها بنوع خاص من الألياف الضوئية لنقل بيانات الإنترنت، ويعتقد أنها تقف وراء الاختراقات السيبرانية للمعلومات الاقتصادية، خاصة من الولايات المتحدة الأمريكية[3].

جـ – هيئة السايبر في إسرائيل: في الوحدة 8200 التابعة لجهاز لفيلق المخابرات العسكرية الإسرائيلية، مسئولة عن توجيه وتنسيق عمليات الجيش الإسرائيلي في الفضاء

---

[1] ايهاب خليفة، مجتمع *ما بعد المعلومات: تأثير الثورة الصناعية الرابعة على الأمن القومي* (مصر: العربي للنشر والتوزيع 2019)، ص. 151.

[2] علي محمد الحاج حسن، *الحرب الناعمة: الأسس النظرية والتطبيقية*(العراق: المركز الإسلامي للدراسات الإستراتيجية، 2018)، ص، ص. 61-63.

[3] ايهاب خليفة، مجتمع *ما بعد المعلومات: تأثير الثورة الصناعية الرابعة على الأمن القومي*، مرجع سابق، ص. 152.

السيبراني، لتعزيز قدراتها السيبرانية وتحقيق أهداف أمنية دفاعية، وحماية النظم الرقمية لجميع القطاعات العاملة في إسرائيل، وكذلك القيام بهجمات سيبرانية على أهداف خارجية[1].

د – وحدة 74455 الروسية: تعرف كذلك بإسم دودة الرمل (Sandworm Team) و لفايكينج الحديدي (Iron Viking) والدب فودو (Voodoo Bear) وتيلي بوتس (Telebots)، **و**هي وحدة عسكرية روسية تابعة لـ GRU المسؤولة عن الاستخبارات العسكرية الروسية[2].

ويمكن اعتبار روسيا بلد "المليون قرصان" لما تمتلكه من الموارد البشرية ذات الكفاءات والقدرات العالية المؤهلة للقيام بالعمليات السيبرانية، حيث تعتمد على القراصنة سواء متطوعون، أو يتم توظيفهم لخدمة أغراض عسكرية[3]. وهكذا انتقلت اللعبة من التعويل على اللاعبين الحكوميين، إلى اللاعبين غير حكوميين من أفراد أو شركات خاصة مثل الولايات المتحدة الامريكية.

2– المحاربون السيبرانيون (Cyber Warriors): هم خبراء سرّيون يعملون على تطوير قدراتها في مجال الهجمات لإلكترونية عادةً لأغراض إستراتيجية أو عسكرية، وقد يتمتعون بالاستقلالية في اختيار الهدف والزمان وطرق تنفيذ الهجوم[4].

المطلب الثاني : الفواعل اللادولاتية.

وهنا نجد الأفراد والمنظمات غير الحكومية والشركات متعددة الجنسيات، والجماعات الارهابية، فنجد فواعل فردية وأخرى جماعية وأهم هذه الفواعل كالتالي:

1– الأفراد (Individuels) :

[1] فيصل محمد عبد الغفار، مرجع سابق، ص، ص. 172–173.

[2] "About: Sandworm (hacker group)" , Dbpedia, Date of Entry:16/05/2022,at 22:00,on the site: https://2u.pw/btrni

[3] ايهاب خليفة، مجتمع *ما بعد المعلومات: تأثير الثورة الصناعية الرابعة على الأمن القومي*، مرجع سابق، ص. 154.

[4] حكيم غريب وصبرينة شرقي، مرجع سابق، ص. 99.

يعتبر الفرد فاعلاً أساسيا في الفضاء السيبراني، حيث أنّه له القدرة على إحداث الثورة الرقمية، وقد تلجأ بعض الدول أو المؤسسات غير الحكومية إلى الاستعانة بهم، ومثال ذلك ما قام به "مارك زوكربارغ" (Mark Zoukerberg) حين أسّس شبكة (فايس بوك) عام 2004، استطاع أن يستقطب ما يفوق عن مليار مستعمل عبر العالم[1]، ففي العالم الافتراضي الفرد يمكنه الانضمام إلى عدّة مجموعات بمختلف الأهداف .

2- المنّظمات غير الحكومية (Non-governmental Organizations):

تعتمد هذه المنظمات بشكل كبير على شبكة الانترنت ووسائل التكنولوجيا الحديثة في تعبئة الرأي العام، والضغط على الحكومات من خلال ترتيب الحملات الاجتماعية وتعبئة المجتمع المدني من أجل الضّغط على الحكومات للتّغيير في سياسات معينة، مثل ما تقوم به اليوم معظم منظمات البيئة العالمية على اثر قرار الرئيس الأمريكي (دونالد ترامب) التخلي عن اتفاقيات التغير المناخي.

3- الشّركات المتعددة الجنسيات (Multinational Corporation):

تتمتع الشركات متعددة الجنسيات بقوة هائلة في الفضاء السيبراني تملكه من إمكانيات مادية وبشرية قد تفوق قدرات بعض الدول، تسمح لها بامتلاك بيانات ضخمة في مختلف أنحاء العالم، مثل: مايكروسوفت(Microsoft)*، غوغل(Google)**، أبل(Apple)***،

---

[1] علي عبد الرحيم العبودي، مرجع سابق ، ص. 104.

* شركة أمريكية متعددة الجنسيات متخصصة في تصنيع وتطوير برمجيات الحاسوب وأنظمة التشغيل وألعاب الفيديو، كما تعمل في مجال إنتاج وتصنيع مكونات الحواسيب والخوادم والهواتف، وفي العام 2016م بلغ عائدها السنوي أكثر من 85 مليار دولار.

** شركة متعددة الجنسيات أميركية متخصصة في الخدمات والمنتجات ذات الصلة بالإنترنت، والتي تشمل تقنيات الإعلان عبر الإنترنت ومحرك البحث والحوسبة السحابية والبرمجيات والأجهزة، يعتبر الموقع الأكثر زيارة في جميع أنحاء العالم وتوجد العديد من مواقع المملوكة لشركة جوجل مثل: يوتيوب و بلوغر.

*** شركة أميركية متعددة الجنسيات متخصصة في تصميم وتطوير وبيع الأجهزة الإلكترونية وبرامج الحاسوب والحواسيب الشخصية.

أمازون (Amazon)**** ، ومن ابرز الأمثلة على قيام الشـــركات المتعددة الجنســـيات في مجال الفضـاء الالكتروني بالتأثير على العلاقات الدولية الصـراع بين شـركة غوغل والحكومة الصـينية، حيث قامت السـلطات الصـينية باختراق البريد الإلكتروني لنشـطاء صـينيين، وتم حضـر موقع جوجل في الصـين منذ عام 2010، ممّا جعل بعض الخبراء يصـفون هدا بأنه جزء من الخلاف الصـيني الامريكي، حيث سـارعت الأخيرة بالدفاع عن شـركة جوجل ودعم حرية الانترنت، مطالبة السلطات الصينية بتقديم تفسير فيما يتعلق بالاختراقات[1].

وتمثل الحرب على التكنولوجيا الصينية أحد أهم سمات المواجهة الأمريكية مع الصين، و حفاظا على مصالح واشنطن حول العالم، صنفت شركات التكنولوجيا الصينية بأنها تهديد للأمن القومى الأمريكى، حيث اتخذت واشنطن إجراءات عقابية وحمائية متعددة أمام عدة شركات صينية منها شركة هواوى(HUAWEI)، تيك توك (TikTok) ووي شات (WeChat)، كمحاولات لواشنطن تحجيم الشركات الصينية، وابعادها عن منافسة الشركات الأمريكية[2]. وكذلك الصّدام المتكرّر بين شركة أبل والسلطات الأمريكية بسبب رفضها إعطاء معلومات عن مستخدميها، وكذلك بين شركات مواقع التواصل الاجتماعي وبعض الدول مثل إيران وتركيا، بسبب امتلاك هده الشركات المعلومة يعصب الحصول عليها، ومع استمرار هده الشركات في تطوير التكنولوجيات وأدوات التخزين مثل اللاي فاي (li-fi)*، فإن احتمال الصدام مع الدول مستقبلا يزداد، خاصة مع الدول النامية التي تعجز عن الاستثمار في التكنولوجيا، ومنه مشاركة الشركات المتعددة الجنسيات للدول في سيادتها المعلوماتية على مواطنيها[3].

**** شـركة أميركية للتجارة الإلكترونية يعد موقع أمازون أكبر سـوق إلكتروني في العالم تتجاوز قيمة سـلعها مئة مليار دولار سنويا.

[1] إيهاب خليفة، *القوة الالكترونية : كيف يمكن أن تدير الدول شؤونها في عصر الانترنت*، مرجع سابق، ص. 69-68.

[2] محمد المشناوي، "تكنوـــ بوليتيكس.. الصراع من الدول إلى الشركات"، جريدة الشروق، نشر بتاريخ: 11 فيفري 2021، اطلع عليه بتاريخ: 16 /03 /2022، الساعة: 23:00، على الرابط:https://2u.pw/oicby

*اختصارًا لـLight Fidelity أي الاعتماد على الضوء، وهو مُصطلح خاص بنقل البيانات عبر موجات الضوء.

[3] ايهاب خليفة، مجتمع *ما بعد المعلومات: تأثير الثورة الصناعية الرابعة على الأمن القومي*، مرجع سابق، ص. 29.

4- المجموعات الافتراضية (Default groups):

وهنا يأتي دور القراصنة (Hackers)، وغالبا ما يسعون لتحقيق أهداف مختلفة (ربحية، سياسية، إيديولوجية...)، وابرز مثال على ذلك المجموعة الافتراضية المشهورة الانونيمس (Anonymous)، من ابرز وظائها كشف المعلومات السرية وتسويق قضايا سياسية في العالم، كما قاموا بشن العديد من الهجمات الافتراضية على عدد من المواقع الحكومية والشركات العالمية وتشويهها، وكذلك قاموا ببعض الهجمات الإلكترونية لدعم الثورات العربية، كما يعتمدون على عدم التَّصريح بهوَّيتهم "مجهولون"[1].

الفواعل في الحروب السيبرانية ليست حكرا على الدول فقط، بل هناك عدة فواعل غير الدول منها الجماعات الإرهابية الأفراد والمنظمات غير الحكومية، حيث أسهمت بشكل فعال في مجمل العمليات السيبرانية، وعقدت عملية تطبيق القوانين والتأمين.

[1] حكيم غريب وصبرينة شرقي، مرجع سابق، ص. 99.

المبحث الثالث : الطبيعة القانونية للحروب السيبرانية وتأمينها.

تزامنا مع تطور الحروب تطورت منظومة القانون الدولي المعنية بتنظيم الحروب قانونيا، و يفترض أن يكون هدا التطور مستمرا باستمرار تطور أشكال الحروب وأدواتها، ومع تزايد معدل الهجمات السيبرانية في النواحي العسكرية، وهنا يثار التساؤل عن مدى إمكانية مواجهتها تقنيا وقانونيا، ومدى تطبيق مبادئ وقواعد القانون الدولي الإنساني على هذا الشكل الجديد من الحروب.

المطلب الأول: الطبيعة القانونية للحروب السيبرانية

بالنظر إلى تواريخ أهم معاهدات القانون الدولي الإنساني والقانون الدولي العرفي، لم يكن للهجمات السيبرانية خلال إبرامها أي وجود. حيث لم يكن هناك استخدام الأنظمة الالكترونية للأغراض العسكرية وجود، حيث نجدها في منتصف القرن الثامن عشر وما بعده ، تحديدا عام1864، تاريخ اعتماد اتفاقية جنيف الأولى وبالخصوص اتفاقيات لاهاي الاولى عام 1899 وثانية عام 1907. وكذلك اتفاقيات جنيف لعام 1949[1]، والتي أُلحقت إلى اتفاقيات جنيف بروتوكولان إضافيان عام 1977 ، ينص البروتوكول الأول على حماية ضحايا النزاعات الدولية المسلحة، ويحكم البروتوكول الثاني حماية ضحايا النزاعات المسلحة غير الدولية[2].

إضافة إلى أنّه من خصائص الحروب السيبرانية أنّ أغلب هجماتها مجهولة المصدر، أي يصعب أو يستحيل تحديد مصدرها، كما لا تعلن الدول رسميا عن تباني هذه الهجمات[3].

---

[1] احمد عبيس نعمة الفتلاوي، مرجع سابق، ص. 628.

[2] "القانون الدولي الإنساني والقانون الدولي العرفي"، اللجنة الدولية للصليب الأحمر، اطلع عليه بتاريخ 25 /03 /2022، الساعة:23:30، على الرابط التالي:

https://www.icrc.org/ar/document/treaties-and-customary-law

[3] صالح حيدر عبد الواحد، مرجع سابق، ص. 49.

كما أن إمكانية تطبيق قواعد القانون الدولي الإنساني على الحرب السيبرانية يدور حول تفسير مفهوم القوة في العلاقات الدولية[1].

وهناك نصوص مُدونة في ميثاق الأمم المتحدة تتلائم مع طبيعة الحرب السيبرانية ويمكن أن تُطبق عليها، جيث تنّص المادة الثانية الفقرة الرابعة من ميثاق الأمم المتحدة على أنه : "يمتنع أعضاء الهيئة جميعاً في علاقاتهم الدولية عن التهديد باستعمال القوة أو استخدامها ضد سلامة الأراضي أو الاستقلال السياسي لأية دولة أو على أي وجه آخر لا يتفق ومقاصد الأمم المتحدة"[2]، وهنا يمكن اعتبار استخدام القوة بمفهومها السيبراني اختراق لهذه الفقرة من ميثاق الأمم المتحدة.

وهنا أيضا ظهر الجدل حيث ترى الدول المتفّوقة في مجال الحروب السيبرانية مثل الولايات المتحدة والصين و روسيا..الخ، أن هذه الفقرة من ميثاق الأمم المتحدة تقتصر على التهديد أو الاستخدام الفعلي للقوات المسلحة على ارض الواقع فقط، أما الدول الغير متفوقة في مجال الفضاء الافتراضي ترى أن هذه الفقرة توسعة لمفهوم القوة، لتضم ايضا القوة السيبرانية.

بينما ذهب العديد من الباحثين على رأسهم "كال شين"، و" ماركو روسيني" إلى جدلية تكييف تلك الهجمات السيبرانية أنه من الممكن أن تعتبر خرق واضح لحكم هذه الفقرة، شرط أن تخلف هذه الهجمات آثار مادية ملموسة سواء مدنية عسكرية، وهنا فالدولة المعتدى عليها، لها الحق في اللجوء إلى استخدام القوة بحكم المادة51 من ميثاق الأمم المتحدة [3] ، والتي جاء فيها: "ليس في هذا الميثاق ما يضعف أو ينتقص الحق الطبيعي للدول، فرادى أو جماعات،

---

[1] يحيى ياسين سعود، "الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني،" *المجلة القانونية* 4، رقم. 4 (2019)، ص. 86.

[2] ميثاق الأمم المتحدة (النص الكامل)،على الرابط التالي:

https://www.un.org/ar/about-us/un-charter/full-text

اطلع عليه بتاريخ 01 /04 /2022، الساعة:18:00 .

[3] احمد عبيس نعمة الفتلاوي، مرجع سابق، ص. 630.

في الدفاع عن أنفسهم إذا اعتدت قوة مسلحة على أحد أعضاء الأمم المتحدة"[1]، اذا حسب هذه المادة فالقانون الدولي يعطي للدولة الحق في اللجوء إلى استخدام القوة للدفاع عن نفسها إذا تعرضت لأي هجوم دون تحديد شكله أو وسيلته.

ونجد كذلك القرار الصادر عن الجمعية العامة للأمم المتحدة جانفي لسنة 2001، الخاص بمكافحة إساءة استعمال تكنولوجيا المعلومات، والذي جاء فيه: "الحاجة إلى تعزيز التنسيق والتعاون بين الدول في مكافحة إساءة استعمال تكنولوجيا لأغراض اجرامية "[2]، إلا أنه لم يرتق إلى مستوى تنظيم الحروب التي تكون اطرافها الدول، بل اقتصر على حالات فردية.

وفي عام 1977 في الملحق (البروتوكول) الأول الإضافي إلى اتفاقيات جنيف في مادته36 المتعلقة بالأسلحة الجديدة إذ نصت على ما يلي : "يلتزم أي طرف سام متعاقد, عند دراسة أو تطوير أو اقتناء سلاح جديد أو أداة للحرب أو إتباع أسلوب للحرب, بأن يتحقق مما إذا كان ذلك محظوراً في جميع الأحوال أو في بعضها بمقتضى هذا الملحق " البروتوكول " أو أية قاعدة أخرى من قواعد القانون الدولي التي يلتزم بها الطرف السامي المتعاقد"[3].

وبالتالي، فإن هذه المادة تنص على ضرورة التحقق في مدى مشروعية استخدام لوسائل وأساليب الحرب الجديدة وفقاً لقواعد القانون الدولي.

ومن خلال ما سبق نلاحظ أن التكييف القانوني للحروب السيبرانية، لم يصل بعد إلى مرحلة إبرام اتفاقيات دولية واضحة حيث لا يزال ضمن مستوى القياس والاجتهاد، بسبب عدة عراقيل تضعها الدول المهيمنة في مجال حروب الفضاء الإلكتروني مثل: الولايات المتحدة الأمريكية، وروسيا، والصين لتجنب طرحه على المنابر الدولية [4]. حتى تتصرف بكل حرية في

[1] ميثاق الأمم المتحدة (النص الكامل)، مرجع سابق.

[2] "مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية"، قرار الجمعية العامة للأمم المتحدة، بتاريخ 22 جانفي 2001، على الرابط التالي:https://2u.pw/ihbVt

[3] "الملحق (البروتوكول) الأول الإضافي إلى اتفاقيات جنيف 1977"، اللجنة الدولية للصليب الأحمر، اطلع عليه بتاريخ 05 /04 /2022، الساعة: 22:00، على الرابط التالي:https://2u.pw/Qk0Ag

[4] صالح حيدر عبد الواحد، مرجع سابق، ص. 53.

حروبها ولتحقيق أهدافها داخل الفضاء السيبراني دون أي قيود تعرقلها في مهمتها وتبقى خارج نطاق المسائلة القانونية، وأيضا طبيعة استخدام الفضاء السيبراني المتاح لفواعل من غير الدول يزيد من صعوبة التكييف القانوني لهده الحروب.

وكخلاصة لم يتمكن القانون الدولي الإنساني حتى الآن من تنظيم استخدام الفضاء السيبراني، والاتفاق على وضع قانون صريح يخص استخدام القوة السيبرانية، فالحروب السيبرانية بحاجة لقوانين جديدة ملزمة، على عكس "دليل تالين"*، الذي تضمن قواعد غير إلزامية تنطبق على الحرب السيبرانية، كما حدد الدور الذي ستلعبه قواعد القانون الدولي الإنساني في السياق السيبراني[1]، حيث نأمل أن يسهم بشكل فعال في خلق الارادة الدولية للدفع للمزيد من النقاش بين الدول خصوصا من قبل الدول المتفوقة، حول تنظيم الحروب السيبرانية، وأن تضمن الدول وغيرها من الفواعل من غير الدول، أن اللجوء للعمليات السيبرانية سيجري وفقًا لالتزاماتها الدولية[2].

المطلب الثاني : التأمين السيبراني.

وهنا نجد الردع والدفاع السيبراني، ويعرف الردع السيبراني بصفة عامة على أنه: " قدرة الدولة على تطوير قدرات عسكرية موثوقة ومتبادلة ومتماثلة في الفضاء الالكتروني، وتكون قادرة على التأثير في قرارات الخصم ومنعه من شن هجمات عسكرية عبر الفضاء الالكتروني"[3].

*تالين دليل على القانون الدولي المطبق في الحروب السيبرانية، تم نشره في افريل 2013 تم كتابته بدعوة من مركز التميز للدفاع الإلكتروني التعاوني التابع لحلف الناتو ومقره تالين عاصمة إستونيا ، من قبل مجموعة دولية من حوالي عشرين خبيرا.

[1] دليل تالين، على الرابط: https://2u.pw/h17nq

[2] " ما هي القيود التي يفرضها قانون الحرب على الهجمات السيبرانية؟"، اللجنة الدولية للصليب الأحمر، اطلع عليه بتاريخ 06 /04 /2022، الساعة: 20:00، على الرابط التالي:
https://www.icrc.org/ar/doc/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm

[3] ايهاب خليفة، مجتمع *ما بعد المعلومات: تأثير الثورة الصناعية الرابعة على الأمن القومي*، مرجع سابق، ص. 161.

ويرتكز الردع السيبراني على المستوى النظري على ثلاثة ركائز هي عماد إستراتيجية الدفاع السيبراني، تتمثل فيما يلي[1]:

1- مصداقية الدفاع (Credible Defense):

ويشمل حماية أنظمة المعلومات، والوقوف في وجه أي محاولة لتسلل لها، وتوافر أنظمة نسخ احتياطية، مما يعني أن أي هجوم ناجح عليها، لن يسفر عن التدمير الكلي للمعلومات أو فقدان كل ما تحويه من معلومات، ورغم التكلفة الباهضة لهذا الحل إلا إنه الأكثر فعالية.

2- القدرة على الانتقام (An Ability to Retaliate):

وهو إلحاق الضرر بالمهاجم بعد التعرف عليه- إذا أمكن- أكثر مما ما وقع عليه من اضرار بسبب الهجوم، وهذا يتطلب القدرة على الانتقام وشن هجمة سيبرانية أو عدة هجمات ضد الخصم.

3- الرغبة في الانتقام(A Will to Retaliate):

على من تعرض للهجوم أن يعلن عن رغبته في الانتقام من الخصم،لأن امتلاك القدرة على الانتقام وحدها لا تكفي لردعه.

كما تتعددت السبل المقترحة للردع، نذكر منها ما يلي[2]:

1- الردع السلبي: وهو عدم الرد على المهاجم، مع العمل على تطوير أنظمة الأمن السيبراني.

2- التحركات الدبلوماسية: يمكن أن يصل التوتر الدبلوماسي مع الدولة التي يشتبه في تورطها الهجوم السيبراني الى طرد احدى مسؤوليها الدبلوماسيين، وقد يرد المعاملة بالمثل.

---

[1] رغدة البهي، "الردعي السيبراني: المفهوم والإشكاليات والمتطلبات،"مجلة الدراسات الإعلامية، رقم.01 (2017)، ص، ص. 207-208.

[2] نفس المرجع، ص، ص. 216 - 208

3- التدابير القانونية: أي اتخاذ إجراءات قانونية ضد الدولة التي يشتبه في وقوفها وراء الهجوم.

4- العقوبات الاقتصادية: فرض العقوبات الاقتصادية على الدولة التي يشتبه في شنها الهجوم.

5- الانتقام في الفضاء السيبراني: عن طريق قرصنة معلومات المهاجم أو استهداف بنيته التحتية.

6- الانتقام العسكري: قد يصل التصعيد إلى استعمال القوة العسكرية ضد الدولة التي شنت الهجوم.

أما إستراتيجية الردع السيبراني تتمثل في:

أ- **الأنظمة البديلة:** الاعتماد على عدة أنظمة كأنظمة احتياطية، يمكن اللجوء إليها حالة حدوث هجوم سيبراني.

ب- إعادة التأسيس: وهو التخفي عن الجميع، ورغم كونه أفضل سبيل للردع السيبراني، إلا أنه يعرضه لعدة مسائل قانونية[1].

ويعرف الدفاع السيبراني أنه آلية للدفاع عن الحواسيب ويتضمن الاستجابة للإجراءات وتأمين البنية التحتية، وضمان حماية المعلومات للمنظمات والهيئات الحكومية وغيرها من الشبكات، ويركز الدفاع السيبراني على الوقاية والكشف وتوفير الاستجابة في الوقت المناسب من المخاطر السيبرانية، بحيث لا يتم العبث بالبنية تحتية أو المعلومات[2]، بمعنى عام الدفاع

[1] نفس المرجع، ص. 219.

[2] Darko Galinec, Darko Možnik & Boris Guberina, "Cybersecurity and cyber defence: national level strategic approach", Journal for Control, Measurement, Electronics, Computing and Communications 58, NO. 3 (2017), P. 274.
doi.org/10.1080/00051144.2017.1407022

السيبراني هو القدرة المنظمة والمستعدة للقتال في الفضاء السيبراني، والتي تشمل الأنشطة الاستغلالية والدفاعية والهجومية [1].

وتتمثل أهداف الدفاع السيبراني فيما يلي [2]:

1- حماية الأهداف و البيانات العسكرية.

2 - حماية البنية التحتية الحرجة.

3 - دعم وحدات الحرب السيبرانية.

4 - تحقيق الردع السيبراني.

5 - تحقيق الأمن السيبراني.

بُذلت عدة مساعي دولية لوضع تشريعات قانونية واتفاقيات دولية لمواجهة تحديات الفضاء السيبراني، ولكن مع غياب إرادة دولية بسبب عرقلة الدول المهيمنة في هذا المجال للوصول إلى حل في تنظيم القانوني لهذه الحروب، لأن مثل هذه الحروب تمثل مصالح إستراتيجية لها، كما اتخذت الدول عدة استراتجيات لحماية فضائها السيبراني من الهجمات السيبرانية من خلال الدفاع السيبراني والردع.

أحدث التطور التكنولوجي والمعلوماتي ثورة رقمية، ساهمت في إعطاء بعد عسكري على مستوى الفضاء السيبراني، من خلال علميات عسكرية رقمية وابتكار أسلحة سيبرانية مغايرة تماما للتقليدية ذات طبيعة معلوماتية، التي تتعدد وتتزايد وتتطور بصورة يصعب حصرها، ومن حيث طبيعة الفواعل تحتوي العالم الافتراضي على فواعل الدولاتية بجانب فواعل جديدة غير دولاتية مثل: الافراد، الشركات المتعددة الجنسيات، المجموعات الافتراضية، بحيث أصبح شبه مستحيل حصرها أو تطوير إستراتيجيات مُحكمة لصدها بشكل كلي، على الرغم وضع عدة

[1] Ibid, P. 12.

[2] ايهاب خليفة، مجتمع *ما بعد المعلومات: تأثير الثورة الصناعية الرابعة على الامن القومي*، مرجع سابق، ص 172-173.

سبل تقنية لصد الحروب السيبرانية من دفاع ودرع سيبراني، في مجال الفضاء السيبراني الذي يفتقر فيه القانون إلى قوة التنفيذ، هذه المزايا دخل المجال السيبراني ضمن المحددات الجديدة للعلاقات الدولية التي تأثرت بالتحولات الموجودة فيه ودخول الدول حيز الحروب السيبرانية، وهذا ما سوف نوضحه في الفصل الثالث.

الفصل الثالث: نماذج من الحروب السيبرانية

الفصل الثالث: نماذج من الحروب السيبرانية.

تسارعت الدول من اجل تطوير وإستحواذ القدرات السيبرانية في العالم السيبراني، تزامنا مع ربط المصالح القومية للدول والبنى التحتية الحرجة بالفضاء السيبراني في عصر المعلومات، حيث يستطيع المهاجم أن يوقع خسائر مادية فادحة ويتسبب في تعطيل البنية التحتية للطرف المستهدف، أدخلت ظاهرة حروب الفضاء السيبراني في استراتيجيات الأمن القومي للدول، ودخلت العديد من الدول للفضاء الافتراضي كملعب للصراعات الدولية بدون حدود مثل الولايات المتحدة الأمريكية والصين وروسيا وإيران وغيرها، وبالتالي أضحى الصراع الجديد في المجال السيبراني له تأثير كبير في العلاقات الدولية.

المبحث الأول: الحروب السيبرانية للولايات المتحدة الأمريكية.

تعتبر العلاقات الأمريكية مع كل من الصين وروسيا وكوريا الشمالية من أكثر العلاقات تعقيدا في العالم، بما تتضمنه من صراعات معلنة وغير معلنة، ومنذ ما يقرب من عقد من الزمان بدأت الولايات المتحدة في اتهام هذه الدول بشن هجمات سيبرانية ضدها، من خلال عمليات في التجسس السيبراني وسرقة المعلومات.

المطلب الأول : الصين.

وكبداية في عام 2001، وخلال الفترة الممدة من 30 أفريل إلى 7 ماي، نفد قراصنة صينيين هجمات على ما يقرب من 1200 موقع أمريكي، استهدفت العديد من المواقع الرسمية على غرار موقع البيت الأبيض، القوات الجوية الأمريكية وموقع وزارة الطاقة، وذلك على خلفية حادثة تصادم في الجو في الأول من أفريل من نفس السنة، فوق سماء جزيرة هاينان الصينية، بين المقاتلة الصينية من طراز "J-8 LAND" مع طائرة تجسس أمريكية طراز " E-P-3" وقد دفعت هذه الهجمات لاستحداث وزارة الأمن الداخلي في الولايات المتحدة الأمريكية (DHS) التي أنشئت في الـ27 من نوفمبر عام 2002.[1]

على صعيد آخر في سنه 2002 ، قامت الصين بإنشاء وحدة جيش التحرير الشعبي رقم 61398 ، حيث بدأت في أولى عملياتها السيبرانية عام 2006 على الأقل، وحسب موقع ماندياند (Mandiant**) للمعلومات قامت بسرقة مئات البيانات الخاصة لـ141 منظمة حول العالم، تشمل المخططات التكنولوجية، وخطط التسعير والتسويق و كذلك نسخ عن البريد

[1] إيهاب خليفة، *القوة الالكترونية : كيف يمكن أن تدير الدول شؤونها في عصر الانترنت*، مرجع سابق، ص، ص. 10-11.

** شركة أمن سيبراني عامة أمريكية.

الالكتروني وقوائم الاتصال، ومالا يقل عن 80% من الشركات التي تعرضت للقرصنة موجودة في الولايات المتحدة الأمريكية[1].

ومن أبرز الهجمات السيبرانية المنسوبة للصين ضد الولايات المتحدة، هي سلسلة الاختراقات منذ عام 2003، المعروفة باسم تيتان رين (Titan Rain)، والتي استمرت إلى غاية 2005 مستهدفة معامل الطاقة، و المؤسسات الدفاعية على غرار كلية الحرب البحرية وكلية الدفاع الوطني التي تسببت في إيقافها لفترة طويلة، كما قام قراصنة صينيون بشن هجمات استهدفت وزارة الدفاع الأمريكية، بما في ذلك أحد أجهزة الكمبيوتر الخاصة بوزير الدفاع الأمريكي، وازدادت الهجمات السيبرانية الصينية ضد الولايات المتحدة أثناء الحملة الانتخابية الامريكية، حيث تم اختراق أنظمة الكمبيوتر لكل من المترشح الجمهوري للبيت الأبيض جون ماكين وخصمه مرشح الحزب الديمقراطي باراك اوباما[2].

تصاعدت مشكلة الولايات المتحدة مع أنشطة الصين في الفضاء السيبراني في 2013، حيث أفاد المسؤولون صينيون أن موقع وزارة الدفاع الصيني، قد تعرضا لعدة هجمات مصدرها الولايات المتحدة الأمريكية، كما تم إحصاء 144 ألف هجوم كل شهر، ثلثها من الولايات المتحدة [3].

وكسابقة تاريخية في الشهر الخامس من سنة 2014، حسب جريدة نيويورك تايمز "The New York Times"، كشفت وزارة العدل الأمريكية عن لائحة اتهام لخمسة أعضاء في جيش التحرير الشعبي الصيني رقم 61398، مع صور للعديد منهم تحمل علامة Wanted

---

[1] ايهاب خليفة، *مجتمع ما بعد المعلومات : تأثير الثورة الصناعية الرابعة على الأمن القومي*(مصر: العربي للنشر والتوزيع، 2019)، ص. 152.

[2] Scott W Harold, Martin C Libicki, & Astrid Stuth Cevallos, *Getting to Yes with China in Cyberspace(USA:* RAND Corporation, 2016) p. 38-39.
متاح على الرابط: https://www.rand.org/pubs/research_reports/RR1335.html

[3] "قراصنة أمريكيون يحاولون اختراق موقع وزارة الدفاع الصينية"، بي بي سي، نشر بتاريخ: 28 فيفري 2013، اطلع عليه بتاريخ 15 /04 /2022، الساعة: 21:00، على الرابط التالي: https://2u.pw/VNSYw ،

"by the F.B.I" أي مطلوب من قبل مكتب التحقيقات الفيدرالي، بتهمة سرقة معلومات تجارية وكذلك زراعة برمجيات خبيثة على حواسيب هذه الشركات الامريكية. وسرق المتسللون ما يقرب من 700 ألف صفحة من رسائل البريد الإلكتروني، بما في ذلك بعض من رئيسها التنفيذي، وقال المدعي العام باسم مكتب التحقيقات الفيدرالي إريك إتش هولدر جونيور: "عندما تستخدم دولة أجنبية موارد وأدوات عسكرية أو استخباراتية ضد مسؤول تنفيذي أمريكي أو شركة أمريكية للحصول على أسرار تجارية أو معلومات تجارية حساسة لصالح الشركات المملوكة للدولة ، يجب أن نقول: هذا يكفي ". ومن جهة نفت الصين ما نسب إليها، متهمة الولايات المتحدة بالنفاق وتقول إنها أيضا وقعت ضحية لهجمات سيبرانية أمريكية، أبرزها على شركة الاتصالات الصينية العملاقة "Huawei "، من أجل مراقبة شبكات الدول التي تشتري المعدات الصينية الصنع، كما تخلت عن مباحثاتها الثنائية الرسمية مع الولايات الأمريكية المتحدة بشأن القواعد والقوانين الخاصة بالفضاء السيبراني والتي بدأت في عام 2013 [1].

وكشفت صحيفة واشنطن بوسط عن تقرير مسرب للكونجرس، عن تعرض الولايات المتحدة الأمريكية، لاختراقات نسبت إلى متسللين صينيين تابعين للحكومة الصينية، في عملية القرصنة وسرقة بيانات عسكرية أمريكية، استهدفت منظومات مضادة للصواريخ نوع باتريوت "بي إي سي 3" (PEC3)، ونظام ثاد (THAAD)، واستهدف كذلك سرقة معلومات مرتبط بالطائرات والسفن العسكرية، وهذا الاختراق مكن الحكومة الصينية من توفير الوقت والجهد والأموال التي كانت ستصرفها لتطوير هذه الأسلحة[2].

[1] Michael S. Schmidt and David E. Sanger,"5 in China Army Face U.S. Charges of Cyberattacks", the New York Times, 19 May 2014, Date of Entry: 16/04/2022, at 19:00.

on the site: https://2u.pw/NXgOY.

[2] إيهاب خليفة، *القوة الالكترونية : كيف يمكن أن تدير الدول شؤونها في عصر الانترنت*، مرجع سابق، ص. 198.

كما اتهمت أمريكا قراصنة صينيون بشن هجمات سيبرانية على شركة لوكهيد مارتن (Lockheed Martin)*، حيث تم سرقت معلومات عن تصنيع مقاتلة "أف – 35"، والتي استخدمتها الصين لتصميم وتصنيع مقاتلة "تي 20 " الصينية الواعدة[1].

وفي عام 2015، هددت إدارة أوباما بفرض عقوبات على الصين، بعد أن استهدفت إحدى الهجمات الجريئة، مكتب إدارة شؤون الموظفين بالولايات المتحدة الامريكية من قبل قراصنة صينيين، تم من خلاله سرقة معلومات شخصية حساسة، وأكثر من 20 مليون بصمة أصابع لأميركيين حصلوا على تصريح أمني. وبعد مرور بضعة أسابيع، توصل "باراك أوباما" رئيس الولايات المتحدة إلى جانب نظيره الرئيس الصيني "شي جينبينغ"، إلى اتفاق يهدف لكبح الاختراقات في الفضاء السيبراني لمدة سنة ونصف خلال فترة إدارة أوباما، وحقق الاتفاق نجاحا ملحوظ حيث انخفضت عمليات الاختراقات الصينية[2].

ولم تدم الهدنة طويلا بين الولايات المتحدة والصين، حيث زاد التوتر بينهما بحلول عام 2018 في عهد الرئيس دونالد ترمب، حول سلوك كل منهما في الفضاء السيبراني، وازدادت الهجمات السيبرانية الصينية ضد الولايات المتحدة، إذ طالما ما كانت الصين واحدة من أكبر مصادر القلق والتهديدات الرقمية للولايات المتحدة، ومن جانب الصين تنفي اتهامات الولايات المتحدة لها بالقرصنة. ومن وجهة نظر الولايات المتحدة، ترى أن هناك ثلاثة دوافع رئيسية تقود الصين للهجمات السيبرانية[3]:

1- تجسس ذي الدوافع الاقتصادية بغرض سرقة الملكية الفكرية أو المعلومات التجارية.

* شركة أمريكية، وهي أكبر شركة للصناعات العسكرية في العالم من حيث الدخل.

[1] "أمريكا تتهم الصين بسرقة تكنولوجيا صنع مقاتلة أف – 35"، قناة روسيا اليوم، نشر بتاريخ: 14 مارس 2014، اطلع عليه بتاريخ: 2022/04/20، الساعة: 20:00، على الرابط: https://2u.pw/2w17x

[2] "تحولت إلى التهديد الإلكتروني الأول.. كيف تستخدم الصين هجمات الشبح المعقدة ضد الولايات المتحدة؟"، قناة الجزيرة، نشر في 27 جويلية 2021، اطلع عليه بتاريخ:2022/04/21،الساعة: 18:00.
على الرابط:https://2u.pw/q6Ta8

[3] Scott W Harold, Martin C Libicki, & Astrid Stuth Cevallos , Op.cit, p. 6-7.

2- لأغراض تجسس تقليدية متعلقة بالأمن القومي.

3- احتمالية أن تكون الصين على الاستعداد لاستخدام هجوم لتدمير البنية التحتية الأمريكية في حال حدوث أزمة ما.

المطلب الثاني : روسيا وكوريا الشمالية.

1- روسيا:

في بداية سنه 2017 ذكر تقرير الاستخبارات الأمريكية، أن الرئيس الروسي "فلاديمير بوتين" أمر بشن حملة الكترونية للتأثير على مسار الانتخابات الرئاسية الأمريكية، تستهدف التشويه بسمعة المرشحة للرئاسة الديمقراطية هيلاري كلينتون، على حساب المرشح الجمهوري "دونالد ترامب"[1].

وذكرت صحيفة "واشنطن بوست" في 2016/12/31، انه تم اكتشاف الرمز المرتبط بـ Grizzly Steppe الخاص بالنشاط السيبراني الروسي الضار، في نظام الشبكة الكهربائية لولاية فيرمونت (Vermont) الأمريكية، وحسب مسؤول أمريكي لم يخلف هذا الحادث أضرار في التيار الكهربائي للولاية[2].

وبعد نحو عامين في 2019، أعلنت روسيا أن قراصنة من الولايات المتحدة الأمريكية، اخترقوا نظام شبكتها الكهربائية، وكما نشر في صحيفة نيويورك تايمز (New York Times) أن المخترقين قاموا بغرس برامج ضارة لها القدرة على شل الشبكة الكهربائية الروسية[3].

---

[1] "الاستخبارات الأميركية: بوتين أمر بشن حملة إلكترونية لمساعدة ترامب"، جريدة الغد، نشر بتاريخ:7 جانفي 2017، اطلع عليه بتاريخ:2022/04/21، الساعة: 23:00، على الرابط: https://2u.pw/3iJb1

[2] Juliet Eilperin and Adam Entous, "Russian operation hacked a Vermont utility, showing risk to U.S. electrical grid security", officials say, 31 December 2016, Date of Entry:23/04/2022, at 17:00,on the site: https://2u.pw/QOIpn

[3] عماد الشدياق، "الحرب السيبرانية بين موسكو وواشنطن.. هل تتحول إلى حرب عسكرية؟"،قناةالجزيرة، نشر بتاريخ: 27 مارس 2022،، اطلع عليه بتاريخ: 2022/04/24،الساعة: 19:00، على الرابط : https://2u.pw/WvTDT

وفي العام الذي يليه 2020، تعرضت أمريكا لأخطر اختراق سيبراني في تاريخها، نتج عنه طرد واشنطن 10 دبلوماسيين روس مع فرض عقوبات مالية على روسيا، حيث تم قرصنة شركة سولارويندز (SolarWinds) * الأمريكية، و استهدف عدة إدارات وزارات أمريكية من بينها وزارة الداخلية، وزارة الدفاع ، ووزارات التجارة والطاقة والصحة، من جهتها روسيا نفت مسؤوليتها عن هذا الهجوم[1] ، ونتج عن هذا الاختراق تضرر 18 ألف عميل وأكثر من 100 شركة أمريكية [2].

في عام 2017، حظرت الولايات المتحدة الأمريكية استخدام برنامج مكافحة الفيروسات الروسي الشهير كاسبرسكاي(Kaspersky) في الإدارات الحكومية الامريكية، مشيرة انه يشكل خطر على الأمن القومي الاميريكي[3].

2- كوريا شمالية:

تعتبر من أكثر الدول التي تعمل على تطوير قدراتها السيبرانية، لاسيما في الشق الهجومي ففي عام 2009، أكدت الحكومة الكورية الجنوبية في تقرير لها أنها تعرضت لهجوم شنه قراصنة من كوريا الشمالية، يهدف لسرقة معلومات عن كيفية تحرك كوريا الجنوبية

*شركة أمريكية تقوم بتطوير برامج للشركات ، تستخدم من قبل الوكالات الفدرالية والحكومية الأمريكية والشركات الأميركية الكبرى.

[1] نايلة الصليبي، "الحرب الإلكترونية حاضرة في جنيف بين الرئيسين الأمريكي والروسي"، إذاعة مونت كارلو الدولية، نشر في 15 جوان 2021، اطلع عليه بتاريخ:2022/04/24،الساعة: 19:00،على الرابط التالي:https://2u.pw/tgpww

[2] "خبير أمريكي يربط بين اختراق سولار ويندز والهجوم على مواقع أمريكية"، الخليج الجديد، نشر في 15 جوان 2021، ، اطلع عليه بتاريخ:25 /2022/05، الساعة: 20:00،على الرابط التالي:https://2u.pw/cGqGC

[3] محمد منصور، "لماذا تمنع أمريكا استخدام برنامج روسي شهير لمكافحة الفيروسات؟"، صحيفة المصري اليوم، نشر بتاريخ: 14 سبتمبر2017، اطلع عليه بتاريخ:25 /2022/05، الساعة: 23:30، على الرابط التالي: https://2u.pw/yOzdd

والولايات المتحدة الأمريكية في حالة نشوب حرب بين الكوريتين[1]. كما تم تعطيل موقع البيت الأبيض في خوادم قارة آسيا[2].

وعدة مواقع الكترونية لمؤسسات أمريكية كموقع المباحث الفدرالية ووكالة المخابرات العامة ومؤسسة الفضاء ناسا، ووسائل اتصالات وتجارة، ومواقع مدنية وبنكية [3].

واتهمت إدارة الرئيس جو بايدن كوريا الشمالية بممارسة أنشطة سيبرانية خبيثة، وفي هذا السياق صرح في مؤتمر صحفي المتحدث باسم الخارجية الأمريكية نيد برايس أن: "كوريا الشمالية تمثل تهديدا سيبرانيا ملموسا على المؤسسات المالية، ولا يزال يهددنا تجسسها السيبراني، وهي تحتفظ بالقدرات على شن هجمات سيبرانية تخريبية"[4].

وتملك كوريا الشمالية أربع وحدات بمهام مختلفة تستخدمها لحروبها السيبرانية، وحدة 121، وحدة 110، وحدة 204، وأصغرهم وحدة 35، التي تحتوي على ما يصل إلى ألف عميل تابع للجيش الكوري الشمالي متمركزون حول العالم اغلبهم في الصين[5].

تم تسليط الأضواء أكثر على القدرات السيبرانية لكوريا الشمالية في ماي 2017، عقب هجوم فيروس واناكراي (WannaCrypt) الذي سبب خسائر قدرت بالمليارات ، وهو فيروس استهدف نظام مايكروسوفت ويندوز (Microsoft Windows)، له دوافع مالية حيث طلب دفع فدية تقدر ب 300 دولار أمريكي "تدفع بعملة البتكوين الالكترونية" مقابل حل التشفير[6]، و

---

[1] فيصل محمد عبد الغفار، مرجع سابق، ص. 13.

[2] ريتشـــارد ايه كلارك وروبرت كيه كنيك، حرب *الفضـــاء الالكتروني:الخطر القادم على الأمن القومي وســـبل مواجهته* (الامارات العربية المتحدة: مركز الإمارات للدراسات والبحوث الإستراتجية، 2012)، ص. 41.

[3] *ملفات ساخنة 1 :حرب التحكم الآلي سلاح الحرب الخامس*(الأردن: دار الجليل للنشر والتوزيع، 2013)، ص. 51. متاح على الرابط:https://2u.pw/idRBO .

[4] "واشنطن: أنشطة كوريا الشمالية السيبرانية تمثل تهديدا لنا"، روسيا اليوم، نشر في 17 فيفري 2021، اطلع عليه بتاريخ 27 /04 /2022، الساعة: 15:00، على الرابط التالي:https://2u.pw/0vrPP

[5] ريتشارد ايه كلارك وروبرت كيه كنيك، مرجع سابق، ص، ص. 44-45.

[6]"ما هو فيروس اي وانا كراي"، موســـوعة اراجيك، نشـــر بتاريخ 19 أوت 2019، اطلع عليه بتاريخ 27 /04 /2022، الساعة: 17:00.

باتت تستخدم لتزويد كوريا الشمالية بالعملة الصعبة ، في حين نفت بيونغ يانغ الاتهامات الأميركية المتعلقة فيروس واناكراي الذي واخترق نحو 300 ألف جهاز كمبيوتر في 150 دولة[1]، وما يميز الهجمات سيبرانية لكورية الشمالية أنها غالبا ما تستهدف الشبكات المالية في مختلف أنحاء العالم خصوصا في الولايات المتحدة .

أصبحت الولايات المتحدة تتجه للفضاء السيبراني كملعب للتأثير في العلاقات الدولية، وكأداة جديدة للهيمنة وللملاقاة، حيث شنت عدة هجمات سيبرانية على كل من الصين وروسيا، وعلى رغم من ريادة الولايات الامريكية على الفضاء السيبراني إلا أنها وقعت ضحية لعدة هجمات استهدف البنى التحتية الحرجة من طرف كوريا الشمالية والصين وروسيا.

على الموقع التالي:https://2u.pw/gf0nR

[1] "جيش كوريا الشمالية الإلكتروني متهم بسرقة هذه البنوك"، قناة العربية ، نشر في: 26 ماي 2021، اطلع عليه بتاريخ 27 /04 /2022، الساعة: 22:00. على الموقع التالي: https://2u.pw/q8byl

المبحث الثاني: الحروب السيبرانية لروسيا.

دخلت روسيا في صراعات سيبرانية عديدة، حيث تعرضت وشنت عدة هجمات في الملعب السيبراني، خاصة مع دول اتحاد السوفياتي السابقة مثل: أوكرانيا واستونيا وجورجيا، بغرض تحقيق أهداف سياسية وعسكرية .

المطلب الأول : أوكرانيا.

بدأت أولى الهجمات السيبرانية بين روسيا وأوكرانيا في أواخر عام 2013، على خلفية احتجاجات جماهيرية ضد الرئيس الأوكراني عقب رفض الرئيس الأوكراني التوقيع على اتفاقية شراكة سياسية مع الاتحاد الأوروبي،[1] حيث قامت روسيا بحملة تجسس إلكتروني بشكل منهجي أو ما تعرف بعملية هرمجدون (Operation Armageddon) التي استهدف الحكومة الأوكرانية ، والمسؤولين العسكريين وعدة وكالات أوكرانيا، على أن تساعد هذه المعلومات السرية في إعطاء ميزة عسكرية لروسيا في هذه المظاهرات[2].

بحلول نهاية سنة 2014، خلال أزمة القرم تزايدت الهجمات الإلكترونية بين أوكرانيا وروسيا، حيث تم الابلاغ عن العديد من الهجمات بين البلدين، هاجم قراصنة موالون لأوكرانيا مواقع حكومية لشبه جزيرة القرم بعد أن ضمتها روسيا إلى أراضيها، مثل موقع البرلمان ، كما كشفت عن بيانات سرية لها صلة بالنزاع قرصنت من الحكومة الروسية، في حين أعلنت روسيا أنها ستنشئ وحدة عسكرية خاصة بالحرب الإلكترونية في في شبه الجزيرة [3].

---

[1] Glib Pakharenko,"*Cyber War in Perspective: Russian Aggression against Ukraine",in* Cyber Operations at Maidan: A First-Hand Account , Edited by. Kenneth Geers (Estonia : NATO CCD COE Publications, 2015), p. 60.

متاح على الرابط: https://2u.pw/Mh3vo

[2] Ibid, Jen Weedon, P. 73.

[3] Ibid, Glib Pakharenko, P. 62.

وأفرجوا عن رسائل البريد الإلكتروني يعود لأحد مستشارين الرئيس الروسي بوتين يكشفون فيه العلاقة بين روسيا والجماعات الانفصالية في شرق أوكرانيا[1].

وفي تقرير لشركة (FireEye) الخاصة بالأمن السيبراني، مند بداية الازمة بين البلدين تزايد معدل الهجمات الإلكترونية باستخدام البرامج الضارة المختلفة بين كييف وموسكو، ومن ابرز هذه البرامج: BlackEnergy، Snake7[2]،KillDi، Industroyer، Uroboru و Turla.

وفي نفس السنة يوم 25 ماي، تم قرصنة الانتخابات الرئاسية الاوكرانية، من قبل مجموعة قراصنة مؤيدون لروسيا تدعى (CyberBerkut)*، تم من خلاله تعطيل نظام الخاص بالانتخابات لما يقرب 20 ساعة[3].

وفي نهاية شهر ديسمبر من عام 2015، كسابقة عالمية شنت هجومات سيبرانية استهدفت شبكة الكهرباء الأوكرانية ما تسبب في انقطاعات بالكهرباء، أدى هذا الانقطاع إلى الحاق الضرر حوالي 190 ألف مستهلك، حصلت هذه الهجمات باستخدام البرنامج الخبيث (KillDisk)، الذي لديه القدرة على إتلاف الأنظمة، تم الاشتباه في وقوف مجموعة الدودة الرملية الروسية (the Sandworm) وراء هذا الهجوم الالكتروني، وفي ديسمبر 2016، تعرضت أوكرانيا لاختراق الثاني لشبكة الكهرباء نجم عنه انقطاع التيار الكهربائي في كييف، وتسببه برنامج الضار(Industroyer/CrashOverride) المرتبط بمجموعة الدودة الرملية الروسية[4].

---

[1] Marie Baezner, Patrice Robin, *Hotspot Analysis:Cyber and Information warfare in the Ukrainian conflict*, ed. 2(Switzerland :Center for Security Studies (CSS), 2017), P. 10.
متاح على الرابط: https://2u.pw/ZaUqR

[2] **Ibid,** P. 9.

* مجموعة قراصنة تدعم الانفصاليين في شرق أوكرانيا ، لكنها لا تزال غير مؤكدة سواء كانت تتألف من الأوكرانيين الموالين لروسيا أو الروس، ام الاثنين معا.

[3] Kenneth Geers, Op.cit, pp. 90-56.

[4] Klaus Saalbach, *Cyber war Methods and Practice* (Germany :Osnabrueck University, 2020),PP. 48-49.

على صعيد أخر في عام 2017 تعرضت أوكرانيا لعدة هجمات استهدفت مواقع الإلكترونية وأنظمة المعلومات، في قطاعات المال والطاقة والحكومة الأوكرانية، حيث وقع أكبر هجوم للبرامج الضارة في التاريخ، من حيث قدرت التكلفة الخسائر على الشركات في جميع أنحاء العالم مقدرة بحوالي 10 مليار دولار، استخدم المهاجمون فيه برمجيات خبيثة من نوع "NotPetya" و تمثلت 80٪ من هذه الهجمات في أوكرانيا، ووفقا للإدارة الرئاسية الأمريكية بعد تحقيقها أكدت أن الجيش الروسي كان وراء هذا الهجوم[1].

أما في 2020 شهدت أوكرانيا سلسلة من الهجمات إلكترونية، نسبت اغلبها لروسيا ففي فترة من جانفي إلى أكتوبر تعرضت لـ 280 ألف هجوم الكتروني، ونحو 397 ألف هجمة كإجمالي هجمات لعام 2020[2].

وصولا إلى 2022، وقبل الحرب بساعات اتهمت أوكرانيا روسيا بالوقوف خلف الهجوم السيبراني الذي تعرضت له، الذي ادى إلى شل المواقع الحكومية الاوكرانية وعدة مؤسسات الدولة في هجوم حجب الخدمة (DDoS)* والماسح **(Wiper)، حيث تم إيقاف حوالي 70 موقعا حكومي في أكبر هجوم من نوعه على أوكرانيا منذ 2017، كما أعلن الحلف الأطلسي والاتحاد الأوروبي والولايات المتحدة الأمريكية دعمهم لأوكرانيا للتعامل مع الهجومات

https://repositorium.ub.uni-osnabrueck.de/handle/urn:nbn:de:gbv:700-202009303605

[1] Alexander Salt & Maya Sobchuk, "Russian Cyber-Operations in Ukraine and the Implications for NATO", Canadian Global Affairs Institute, August 2021, Date of Entry: 15/04/2022, at 20,on the site:

https://www.cgai.ca/russian_cyber_operations_in_ukraine_and_the_implications_for_nato

[2] Ukraine Russia Crisis: Terrorism Briefing, Institute for Economics & Peace, The Institute for Economics & Peace Briefing Series 4, Sydney, 2022, P 5.

* وهي اختصـــــار ل "Distributed Denial-of-Service Attack", وتعني أن مجموعة من أجهزة الكمبيوتر تقوم بمهاجمة خادم واحد بهدف حجب الخدمة عليه.

** برامج ضارة يمكنه حذف البيانات من دون ملاحظة ذلك.

السيبرانية[1]. وتلقت الدعم كذلك من مجموعة قراصنة "Anonymous" والتي أعلنت بدورها الحرب على روسيا، حيث تعرضت عدة المواقع الحكومية في روسيا للغلق، على غرار موقع روسيا اليوم (rt.com) المدعوم من الكرملين[2].

المطلب الثاني : أستونيا وجورجيا.

في أفريل 2007، تعرضت إستونيا إحدى جمهوريات الاتحاد السوفيتي السابق، لعدة هجمات سيبرانية، بعد أن قررت الحكومة الإستونية نقل التمثال البرونزي الذي يخلد ذكرى أبطال السوفييت، من وسط المدينة إلى مقبرة تابعة للجيش[3]، تعطلت المواقع الإلكترونية الرسمية للهيئات الحكومية الإستونية والخدمات عبر الإنترنت للتجارة والبنوك وكذلك وسائل الإعلام، كانت النتيجة خسائر بملايين الدولارات، وإن لم يكن هناك دليل ملموسا على تورط حكومة الكرملين، الا أنه وجهت الاتهامات لروسيا بسبب هذه الحادثة [4].

تعد هجمات الحرمان من الخدمة (DDoS)، أول بداية للهجمات الذي أدى إلى شل حوالي 58 موقعا أستونيا[5]، رفعت فيهم صور تمجد الجنود السفيات وأقوال لمارتن لوثر كينغ [6].

وتم تعطيل النبية التحية الاقتصادية الرقمية، حيث لم يتمكن المواطنيين الإستونيين من إجراء أي معاملة بنكية عن طريق الانترنت حيث أن ماكينات الصرف الآلي والخدمات

---

[1] Joe Tidy,"Ukraine cyber-attack: Russia to blame for hack, says Kyiv", BBC, 14 January 2022, Date of Entry: 30/04/2022, at 20:00, on the site: https://2u.pw/YtJ2v

[2] "أنونيموس تنشر مقاطع فيديو لاختراقها قنوات روسية وتعرض صورا من المعركة"، قناة الجزيرة، نشر بتاريخ :28 فيفري 2022، اطلع عليه بتاريخ 30 /04 /2022، الساعة: 22:00، على الموقع:https://2u.pw/loFnL

[3] ريتشارد ايه كلارك وروبرت كيه كنيك، مرجع سابق، ص، ص. 27 –28.

[4] فيصل محمد عبد الغفار، مرجع سابق، ص. 13.

[5] إسراء تريسي، "هجمة إلكترونية تشلّ مؤسسات الدولة بأكملها.. قصة "تمثال الأحرار" الذي أشعل الحرب السيبرانية بين أستونيا وروسيا"، عربي بوسط، تم النشر بتاريخ : 26 نوفمبر 2021، اطلع عليه بتاريخ 01 /05 /2022، الساعة: 13:00، على الرابط:https://2u.pw/S6man

[6] رغدة البهي، مرجع سابق، ص. 210.

المصرفية كانت معطلة، ولم يعد بإمكان موظفو الحكومة التواصل مع بعضهم عبر خدمة البريد الإلكتروني ولا الصحف والمذيعون يستطيعون توصيل الأخبار[1].

ونظرا لتواصل الهجمات السيبرنية لعدة أسابيع و تعقيدها، طالبت أستونيا من حلف الشمال الاطلسي الذي تنتمي إليه المساعدة لمواجهة هذه الهجمات، وتفعيل المادة الخامسة من اتفاقية الحلف التي تنص أن يدافعون عن بعضهم البعض من آي هجوم أو عدوان ضد طرف منهم[2]، الا يتم تفعيلها في حال أدى الهجوم الالكتروني إلى خسارة في الأرواح، ومن جهة رفضت روسيا النداءات الأستونية للحصول على المساعدة وتعقب المهاجمين[3].

وتتضمن المادة الخامسة من تحالف الدول الأوروبية أن أعضاء الناتو يدافعون عن بعضهم البعض، حتى لو كان هذا الهجوم إلكترونيا. لكن المادة الخامسة لا يتم تفعيلها إلا إذا أدى الهجوم إلى خسارة كبيرة في الأرواح تعادل الهجوم العسكري التقليدي.

وفي سنة 2008 ردا هده الهجمات فقد أنشأ حلف الشمال الاطلسي، مركز الدفاع الإلكتروني التعاوني (CCDCOE) مقره تالين عاصمة إستونيا[4]، الذي اصدر ما يعرف بدليل تالين بشأن القانون الدولي المطبق على الحروب السيبرانية.

دفعت هذه الهجمات استونيا إلى زيادة استثمارها في الأمن السيبراني لتصبح رائدة في هذا المجال، بعد إنشاء وحدة طوعية للدفاع السيبراني ورابطة الدفاع الإستونية ووحدة الدفاع السيبراني من قبل وزارة الدفاع.

---

[1] Damien McGuinness, "How a cyber attack transformed Estonia",BBC, 27 April 2017 ,Date of Entry:01/05/2022,at 15:00,on the site: https://www.bbc.com/news/39655415

[2] احمد عبيس نعمة الفتلاوي، مرجع سابق، ص. 624.

[3] ريتشارد ايه كلارك وروبرت كيه كنيك، مرجع سابق، ص. 31.

[4] نفس المرجع، ص. 32.

في عام 2008، قبل قيام روسيا على اجتياح جورجيا في عالم الواقع تعطلت شبكة الانترنت الجورجية، وتوقفت عدة مواقع جورجية عن العمل من بينها موقع الرئيس الجورجي، ومواقع خاصة بالوزارات والمؤسسات المالية مثل البنوك الجورجية[1].

في الشهر الثامن من سنة 2008، بعد الحملة العسكرية الروسية داخل الأراضي الجورجية نشأ نزاع مسلح بين روسيا ودولة جورجيا على الجنوب أوسيتيا، ورافقت هذا النزاع عنصر هجمات سيبرانية منسقة[2]، حيث استخدمت عدة أساليب في الهجوم السيبراني الجورجي، على غرار هجمات الحرمان من الخدمات (DDoS)، ونشر البرامج النصية الخبيثة (MS) على الرغم منه انه تقريبا لا يوجد أدلة تورط الحكومة الروسية أو المنظمات الحكومية في هذه الهجمات ، إلا انه جوهريا كان يعتقد أن المتسللين روس[3].

كما نجح قراصنة الانترنت في السيطرة على كابلات ألياف ضوئية التي تعتمد عليها جورجيا في ربطها بالانترنت، والتي تعبر على كل من روسيا وتركيا، وشلت معظم الاتصالات الجورجية عبر الانترنت، بمعنى أخر تعطل الخادم الخاص لدولة جورجيا المعروف بالرمز "eg." ، وتم تحويلهم إلى خوادم أخرى خارج دولة جورجيا(بشكل أساسي إلى الولايات المتحدة)[4]، رغم هذا تمكن القراصنة من تنفيد هجومات ناجحة على الخوادم الخارجية التي كانت تستعملها جورجيا باستخدام الخوادم غير الروسية أو عناوين IP مظللة، كما أشار محللون أن الهدف من

[1] عادل عبد الصـــادق، *الإرهاب الإلكتروني:القوة في العلاقات الدولية" نمط جديد وتحديات مختلفة"*، مرجع ســـابق، ص. 226.

[2] Paulo Shakarian,"The 2008 Russian Cyber-Campaign Against Georgia", Military Review, decembre 2011, P. 63.

[3] Donald L. Buresh,"Russian Cyber-Attacks on Estonia, Georgia, and Ukraine, Including Tactics, Techniques, Procedures, and Effects", Journal of Advanced Forensic Sciences 1. N°.2 (2021), P. 17.
DOI : 10.14302/issn.2692-5915.jafs-21-3930

[4] ريتشارد ايه كلارك وروبرت كيه كنيك، مرجع سابق، ص، ص. 34 – 35.

الهجمات السيبرانية على جورجيا كانت من أجل عزل الجورجيين عن العالم الخارجي، وإسكات وسائل الإعلام الجورجية[1].

وعلى عكس استونيا، رغم أن الهجوم على جورجيا كان أكثر تطورا واحترافا على الهجوم في استونيا[2]، لم يحقق الهجمات خسائر اقتصادية قاسية أو معاناة للسكان، بحكم أن الجورجيين لا يعتمدون على خدمات الإنترنت في حياتهم كثيرا[3].

وحسب العديد من خبراء المختصون الأمن، قد تكون هذه الهجمات الإلكترونية بمثابة طوارئ العملية قبل عام 2008، أي أن القراصنة الروس استعدوا للهجمات السيبرانية قبل 2008 ، قد تعود لوقت مبكر من عام 2006، نظرا لدقتها وسرعتها في استهداف الأهداف، وكانت هناك مؤشرات أخرى كتحليل صور الغرافيتي التي استعملت تستخدم لتشويه المواقع الجورجية، كما تم تحديد استخدام الروبوتات المعروفة باسم شبكة (Machbot)، والتي من المعروف أنها تستخدم من قبل القراصنة الروس[4].

وتعتبر الحرب على جورجيا سابقة تاريخية كأول مرة استعملت فيها روسيا الحرب السيبرانية دعما للعمليات التقليدية للحرب.

يمثل الفضاء السيبراني أهمية كبيرة لروسيا لممارسة النفوذ، حيث تم استخدامه في إدارة التفاعلات الدولية، لتحقيق بعض الأهداف السياسة والعسكرية، كما تتمتع روسيا بقدرات سيبرانية لا يمكن الاستهانة بها.

---

[1] Paulo Shakarian, Op.cit , p. 65.

[2] عادل عبد الصادق، *الإرهاب الإلكتروني:القوة في العلاقات الدولية" نمط جديد وتحديات مختلفة"*، مرجع سابق، ص. 227.

[3] Donald L. Buresh, Op.cit , p. 17.

[4] Paulo Shakarian, Op.cit , p. 66.

المبحث الثالث: الحروب السيبرانية لإيران.

منذ سنوات تبادلت إيران مع إسرائيل والولايات المتحدة الأمريكية العديد من الهجمات الإلكترونية والتي مازالت إلى يومنا، حيث تعرضت إيران لعدة هجمات تهدف إضعاف قوتها النووية، لتبادر إيران في ردها على بالمثل على هذه الهجمات مستهدفة عدة منشات إسرائيلية وأمريكية.

المطلب الأول : إسرائيل.

في عام 2010، اتهمت إيران لأول مرة كل من إسرائيل بتعاون مع الولايات المتحدة الأمريكية، في هجوم سيبراني ضرب شبكة الحواسيب والمعلومات في منشآتها النووية، حيث تم رصد استخدام دودة حاسوبية خبيثة ستوكسنت(Stuxnet) ، وكان أول هجوم سيبراني معروف في العالم يتسبب في أضرار مادية تجاوزت جهاز الكمبيوتر المخزن للبيانات[1]. ونجح في تعطيل حوالي ألف وحدة لتخصيب اليورانيوم [2]، واستهدف ما لا يقل عن 30 ألف حاسب في إيران بينما الضرر كان ضئيلا[3]، حسب تصريح الرئيس الإيراني احمدي نجاد لوسائل الإعلام، وكذلك أشار على انه يمكن تصنيف الهجوم السيبراني على منشآتها النووية بأنه استعمال للقوة ضمن المعنى الذي نصت عليه المادة (2) في الفقرة (4) من الميثاق الأمم المتحدة، أو بموجب

---

[1] Gil Baram, Yael Ram, & Isaac Ben Israel, "Cyberwar Between Iran and Israel Out in the Open", ResearchGate, November 2020, P. 1.

متاح على الرابط: https://2u.pw/CFvKN

[2] احمد بن علي الميموني،"الجبهة النشطة: تداعيات المواجهة السيبرانية بين إيران و إسرائيل،" *مجلة الدراسات الإيرانية4*، رقم. 12 (2020)، ص. 76.

متاح على الرابط: https://2u.pw/hag6R

[3] *ملفات ساخنة 1 :* حرب *التحكم الآلي سلاح الحرب الخامس*، مرجع سابق، ص. 189.

المادة 51، أو ما إذا كان يشكل فعل حرب، إذ يعتبر من اعقد البرامج الضارة التي تم إنشاؤها على الإطلاق[1].

وعلى الرغم من عدم وجود دليل ملموس يورط إسرائيل في الهجوم، فإن الإجماع الحالي هو أن إسرائيل ستستمر في العمل في الفضاء السيبراني لمنع إيران من تحقيق أهداف برنامجها النووي، في الوقت نفسه كانت دودة الكمبيوتر Stuxnet بمثابة جرس إنذار لإيران، حيث أدركت أنها موضع استهداف من طرف إسرائيل، و لذلك هي ثابتة في رغبتها في تعزيز قوتها القدرات السيبرانية لكي تصبح لاعب محوري في الفضاء السيبراني[2]، خاصة بعد تزايد الهجمات الإلكترونية ضدها.

وفي سياق الحرب السيبرانية السرية التي تشنها إسرائيل على إيران، في ماي 2012، تعرضت منشأت النووية الايرانية لهجماتٍ إلكترونية أخرى، استخدم فيها فيروس مغاير يدعى لهب (Flame)، وحسب شركة كاسبريسي الفيروس له قدرات تفوق ستاكسنت بعشرين مرة، وحسب الخبراء فقد هاجم الفريوس 189 كمبيوتر في إيران تاليها فلسطين 98 حاسوب، وكذلك ضرب في عدة دول عربية وإسلامية، مما أثار شك حول وقوف إسرائيل وراء هده الهجمات، كما صرح الفريق الإيراني للاستجابة لطوارئ الكمبيوتر ، الفريوس قد يكون له علاقة بهجمات مسؤولة عن فقدان كم هائل من البيانات في بعض أنظمة الحواسيب الإيرانية[3].

على صعيد آخر، مع بداية سنة 2020 أدت سلسلة الهجوم السيبراني الذي تعرضت له إيران على شبكة الانترنت إلى تعطيل ما يقارب 25% من نشاطها، على الجانب الآخر حامت الشكوك الإيرانية حول إسرائيل في ضلوع خلف هذا الهجوم[4].

---

[1] y James P. Farwell & Darby Arakelian, “What Does Iran’s Cyber Capability Mean For Future Conflict?”, The Whitehead Journal of Diplomacy and International Relations 14, N°. 1, (2013) P. 51.

[2] Yael Ram and others, Op.Cit, p. 01.

[3] *ملفات ساخنة 1 :حرب التحكم الآلي سلاح الحرب الخامس*، مرجع سابق، ص، ص. 195 – 196– 197.

[4] يوني بن مناحيم، "الحرب السـايبيرية بين إيران وإسـرائيل"، الخنادق، نشـر بتاريخ: 31 مارس 2021، تم الاطلاع على الموقع بتاريخ 05-05-2022، الساعة:17:00، على الموقع:https://2u.pw/dNduy

أما في 24 من افريل لسنة 2020، كانت أول محاولة هجوم سيبراني علني لإيران، حيث تمكنت إيران من اختراق البنية التحتية للمياه والصرف الصحي لإسرائيل[1]، وحسب مسؤول في إسرائيل الهجمات لم تحقق أي أضرار كبيرة ، باستثناء توقف مضخة في شبكة مياه في منطقة شارون بوسط إسرائيل عن العمل، وردا على ذلك أطلقت إسرائيل صاروخا هجوم إلكتروني على ميناء الشهيد رجائي جنوبي إيران كانت إسرائيل، مما أدى إلى تعطيل حركة الملاحة في الميناء الرئيسي لإيران[2].

وشهد العام 2020 كذلك سلسلة من الهجمات الغامضة على منشأة نطنز النووية، والمجتمع العسكري في بارشين بإيران[3]، وحسب صحيفة "جيروزاليم بوست" و"هآرتس" الإسرائيليتان إن الهجوم على الأرجح نفذته إسرائيل، وجاءت هده الهجمات السيبرانية بعد أيام قليلة من الهجوم على سفينة إيرانية في البحر الأحمر[4].

ولم تبقى إيران مكتوفة الأيادي، حيث جاء الرد الإيراني عن طريق استهداف منشأتين للبنية التحتية للمياه الإسرائيلية بعد ثلاثة أشهر فقط من الهجوم الأول، حيث استهدفت مضخات المياه الزراعية في منطقة الجليل الأعلى واستهدفت البنية التحتية في وسط إسرائيل، ووفقا لتصريحات مسؤولين في اسرائيل إن الهجمات لم تلحق أضرار كبيرة[5].

---

[1] Gil Baram, Yael Ram, & Isaac Ben Israel, Op.Cit, p. 02.

[2] Bergman, Ronen and Halbfinger, David, "Israel Hack of Iran Port Is Latest Salvo in Exchange of Cyberattacks", New York Times, May 19, 2020,Date of Entry:06/05/2022,at 22:00, on the site : https://2u.pw/UjBag

[3] احمد بن علي الميموني، مرجع سابق، ص. 79.

[4]"حادث منشأة نطنز النووية الإيرانية.. تقارير إسرائيلية ترجح هجوما إلكترونيا وطهران لا تستطيع تأكيد فرضية العمل التخريبي"، قناة الجزيرة، نشر بتاريخ:11 افريل 2021، تم الاطلاع على الموقع بتاريخ: 07-05-2022، الساعة:22:00، على الموقع:https://2u.pw/7N7u6

[5] "هجوم إلكتروني جديد يستهدف المياه في إسرائيل"، قناة الحرة، نشر بتاريخ : 17 جويلية 2020، تم الاطلاع على الموقع بتاريخ: 07-05-2022، الساعة:23:30، على الموقع:https://2u.pw/eQL60

وخلال سنة 2022 صرح مسؤول إيراني لوسائل إعلام إيرانية، عن إحباط هجوم سيبراني واسع استهدف البنية التحتية للبلاد، حيث تمكن المتسللون من اختراق أكثر من 100 موقع إلكتروني لمؤسسات إيرانية رسمية وخاصة، إلا أن القراصنة لم يستطيعوا الوصول إلى البايانات الأساسية، وغالبا ما توجه طهران الاتهام في الهجمات السيبرانية إلى كل من تل أبيب و واشنطن[1].

في عام 2012 يوم 27 جويلية، ووفقا لمختبر كسبسكي سكيليرت الإسرائيلي المتخصص بحماية المعلومات الالكترونية، الذي أعلن عن اكتشافه فيروس إيراني "حصان طروادة" يحمل اسم "مهادي"، تمكن من التسلل إلى أجهزة كمبيوتر تعود لشخصيات رفيعة في إسرائيل، وحسب هذا المختبر فإن "مهادي" يعمل منذ عدة أشهر على جمع بيانات لها صلة بالبنية التحتية، إضافة لحواسيب رجال الأعمال والمؤسسات الاقتصادية الإسرائيلية وكذلك لأجهزة طلبة الهندسة وأخرى تابعة لجهات حكومية. كما أفاد المختبر أن الفيروس تحتوي على مكونات خاصة باللغة والتاريخ الفارسي، ما يشير إلى وقوف إيران وراء هذا الفيروس، كما ادعى خبراء هذه الشركة أن الفيروس في فترة ثمانية أشهر تمكن من التسلل إلى 800 جهاز كومبيوتر إيراني و54 حاسوب إسرائيلي وعدة أجهزة كومبيوتر في عدة دول حول العالم[2].

المطلب الثاني : الولايات المتحدة الأمريكية.

تخوض إيران حربا سيبرانية متبادلة مع الولايات المتحدة الأمريكية منذ عام 2010، كما أوضح جوزيف ليبرمان رئيس لجنة الأمن الداخلي والشؤون الحكومية، انتقمت إيران في سبتمبر 2012، على العقوبات الغربية التي فرضت على طهران بغية عرقلة التقدم في برنامجها النووي، حيث استهدفت البنية التحتية المصرفية الأمريكية بسلسلة من هجمات تشمل مواقع

[1] "مسؤول إيراني يؤكد: 100 موقع تعرض لهجمات سيبرانية"، العربية الحدث، نشر بتاريخ: 25 افريل 2022، تم الاطلاع على الموقع بتاريخ: 08-05-2022، الساعة:21:30، على الموقع:https://2u.pw/5OtvE

[2] *ملفات ساخنة 1 :حرب التحكم الآلي سلاح الحرب الخامس*، مرجع سابق، ص، ص. 192 -193.

الإلكترونية لأكبر بنك في الولايات المتحدة، "جي بي مورغان تشيز" (JPM) وثاني بعده "بنك أوف أمريكا"(Bank of Americ) [1].

في ديسمبر عام 2011، استطاع محققون من الولايات المتحدة الأمريكية بعد اختراق مجموعة قراصنة حاسوب مكسيكية، من كشف تورط جهات إيرانية رسمية مع هذه المجموعة، من أجل اختراق المباحث الفدرالية ومنشآت الدفاع والمخابرات والمنشآت النووية الأميركية، وتم إظهار صور للسفير الإيراني في المكسيك في تشاور مع قراصنة، حيث بدت المجموعة رغبتها في الحصول على دعم وتمويل من الحكومة الإيرانية، لتنفيذ عمليات اختراق ضد الولايات المتحدة الأمريكية، ومن جهته أشار السفير أن السلطات الإيرانية تسعى للحصول على معلومات استخبارتية، حول قيام الولايات المتحدة الأمريكية بشن هجوم محتمل على منشآت إيران النووية، وفي الأخير تعهد بنقل طلباتهم إلى الجهات الرسمية في طهران، مطالبا ببقاء على اتصال معه[2].

يأتي التصعيد الأخر في عام 2013، حيث تسلل قراصنة إيرانيون إلى نظام تحتكم سد نيويورك، تمكنوا من الوصول إلى معلومات عن كيفية تحكم في عمل أنظمة الفيضانات[3].

وفي 27 سبتمبر من نفس السنة، قام القراصنة الإيرانيين الذين من المحتمل أن يكونوا تابعين للحكومة الإيرانية بخرق حواسيب تابعة للبحرية الأمريكية أثناء المحادثات حول البرنامج النووي الإيراني[4].

ملفات ساخنة 1 :حرب التحكم الآلي سلاح الحرب الخامس، مرجع سابق، ص. 202.

[2] نفس المرجع، ص، ص. 178 – 179.

[3] "قراصنة إيرانيون يستهدفون سدا في نيويورك"، قناة بي بي سي، تم الاطلاع على الموقع بتاريخ 10-05-2022، الساعة:07:00 ، نشر بتاريخ : 21 ديسمبر 2015، على الرابط:https://2u.pw/2Ee2g

[4] "مسؤولون أمريكيون: قراصنة ايرانيون اخترقوا أجهزة حاسوب تابعة للقوات البحرية الأميركية"، قناة الميادين، نشر بتاريخ: 28 سبتمبر 2013، تم الاطلاع على الموقع بتاريخ 10-05-2022، الساعة:09:00، على الموقع: https://2u.pw/0N8iM

وفي مواجهة أخرى، في صيف 2019 بعد إسقاط إيران طائرة استطلاع أميركية بدون طيار من طراز "غلوبال هوك"، أثناء تحليقها بالقرب مضيق هرمز، شنت إدارة ترمب حسب وسائل إعلام أميركية هجوم الكتروني، استهدف أجهزة الحواسيب التي تستخدم في إدارة عمليات إطلاق الصواريخ، استهدفت كذلك شبكة تجسس إيرانية مكلفة بمراقبة عبور السفن في مضيق هرمز[1].

على صعيد آخر في شهر أكتوبر، كشفت شركة مايكروسوفت أنه تم رصد محاولات اختراق حسابات البريد الالكتروني الحملة الرئاسية الأمريكية، إضافة إلى حسابات صحافيين ومسؤولين في أمريكيين،من طرف مجموعة "الفوسفور"*(Phosphorous)، وأضافت أن مركز تهديدات مايكروسوفت، وفي فترة شهر لاحظ أن مجموعة الفوسفور قامت بأكثر من 2700 محاولة لتحديد هوية المستهلكين من خلال البريد الإلكتروني المرتبطة بمستخدمين معينين لمايكروسوفت، ثم قامت بمهاجمة 241 من هذه الحسابات[2].

نشرت وسائل إعلام إيرانية في جوان 2019، أن طهران فككت شبكة تجسس الكترونية تعمل لصالح وكالة المخابرات المركزية الأمريكية (CIA) في إيران، تتكون من 17 جاسوسا، تم إصدار أحكام بالإعدام على البعض منهم[3].

---

[1] "بعد إسقاط الطائرة المسيرة . ترامب ينتقم من إيران بطريقته الخاصة"، قناة دي دابل فاو، نشر بتاريخ: 23 جوان 2019، تم الاطلاع على الموقع بتاريخ 10-05-2022، الساعة:10:00، على الرابط:
https://p.dw.com/p/3KvjI

*معروفة أيضاً باسمي "القطط الجميلة و"أي بي تي 35". وهي مجموعة قرصنة إلكترونية إيرانية.، يعتقد أنهم يعملون لصالح الحرس الثوري الإيراني.

[2] "مايكروسوفت تكشف عن قراصنة إيرانيين يستهدفون حملة رئاسية ومسؤولين أمريكيين"، ارابيك سي ان ان، نشر بتاريخ: 04 أكتوبر 2019، تم الاطلاع على الموقع بتاريخ 11-05-2022، الساعة:17:00 ،على الموقع:
https://2u.pw/XgJs4

[3]"إيران تحكم بالإعدام على أشخاص تقول إنهم تجسسوا لصالح واشنطن"، قناة دي دابل فاو، نشر بتاريخ : 22 جويلية 2019، تم الاطلاع على الموقع بتاريخ 11-05-2022، الساعة:22:00، على الرابط:
https://p.dw.com/p/3MW0G

من الواضح أن الصراع بين المثلث الإسرائيلي– الإيراني – الأمريكي، لم يعد قاصر على مواجهات في الواقع فقط، بل تعدت إلى مواجهات في الفضاء الافتراضي، حيث تميزت الهجومات السيبرانية التي تنسب إلى الولايات المتحدة الأمريكية واسرائيل، ضد إيران أنها غالبا تستهدف منشآت النووية الإيرانية، أما الهجمات التي نفدتها إيران تميزت باستهداف المواقع الإلكترونية التجارية في أمريكا، والبنى التحتية في إسرائيل.

أثرت الحروب السيبرانية بشكل واضح على واقع العلاقات الدولية باعتبارها وسيلة لفرض إرادات عسكرية وسياسية وغيرها، حيث بات جليا أن هذا النمط الجديد من الحروب في العالم الافتراضي، بات يتصدر أجندة الدول على المستوى التطبيقي لشن هجومات مدمرة ماديا ومعنويا ضد المنشآت الحيوية للبنية التحتية، خاصة من طرف الدول الكبرى و النووية في مقدمتها الولايات المتحدة الأمريكية، روسيا، الصين، إيران، كوريا الشمالية، وأيضا مع دخول فواعل من غير الدول في النظام الدولي، ما كان له انعكاس على قدرات الدول ومنعطف جديد وخطير في العلاقات الدولية، وتأثيرهم على سيادة الدول في العصر الرقمي، وبالتالي أصبحت الحروب السيبرانية لها تأثير كبير في العلاقات الدولية، ولا توجد دولة في مأمن من خطر التعرض للهجوم سيبراني.

الخاتمة

الخاتمة:

توسع مفهوم الحرب ليتضمن أشكل أخرى مغايرة لمفهومها التقليدي، حيث بات الفضاء السيبراني بنية خصبة لنوع جديد من الحروب مختلفة تماما عن سابقتها، أصبحت فيه الحروب السيبرانية بأدواتها ووسائلها المختلفة تمثل المعيار الرئيسي لتحقيق التفوق في هذا المجال، ومن يمتلكها بإمكانه تسيير مسار حروب سيبرانية.

إن الحرب السيبرانية في الوقت الحالي أصبحت واقع الذي أرعب حتى الدول الكبرى، فالحرب السيبرانية ليست استخدام افتراضي فقط، بل هي تعبير حقيقي عما يمكن إلحاقه من أضرار عن طريق الهجمات السيبرانية، التي قد تفوق قدرتها التدميرية الأسلحة التقليدية، فالهجمات منخفضة التكلفة أما الأضرار قد تصل إلى المليارات من الدولارات سواء أضرار نفسية أو مادية، قد يعاني منها أفراد أو مؤسسات حكومية أو خاصة، ويمكن أن تحدث أيضا تعطيل وزعزعة استقرار البنى التحتية في عدة قطاعات، مما يؤدي إلى شلل في الأنشطة المختلفة للدول المستهدفة.

الهجوم السيبراني يستخدم التكنولوجيا المتاحة، ونظرا للتطور السريع للتكنولوجيا، فمن الأكيد أن لا تكون الأسلحة السيبرانية المتوفرة حاليا والتي تم عرضها في برمجيات ضارة من أنواع الفيروسات والديدان الحاسوبية والقنابل المنطقية والأحصنة الطروادية، مشابها لما سوف تكون في المستقبل القريب، وسيكون هناك تغيير في نوعية الأسلحة السيبرانية في المستقبل، حيث تكون أكثر تطورا وتدميرا مما هي عليه الآن، لأنها تتطور حسب تاريخ الهجوم والتكنولوجيا المتوفرة المعتمدة على البرمجيات التي تستخدم من طرف المخترقين على سبيل المثال فيروس ستكنست .

إن الفضاء السيبراني الذي بات يشكل تهديد للأمن العالمي، فرض نفسه بقوة على واقع العلاقات الدولية، و قد يصبح هو سلاح المستقبل، لما يوفره للجهات الفاعلة من مزايا وخصائص، على سبيل المثال أتاح إمكانية إخفاء الهوية أو تزويرها (إستخدام خوادم من

دول أخرى)، ونظرا إلى طبيعة الفضاء السيبراني الذي لا تحده الحدود يصعب اكتشاف مصدر المتسللين على الإنترنت، مما سمح للمهاجم من التملص من المسؤولية، إضافة إلى تعدد الفواعل في العالم الافتراضي، وعلى الصعيد أخر انخفاض تكلفة الأسلحة السيبرانية مقارنة بالحروب والعمليات العسكرية التقليدية، كما بإمكان تحقيق الاختلال في التوازن حيث بمقدور الدول الصغيرة التي تملك قدرات عسكرية محدودة أن تقوم بضرب الدول أكثر قوة منها في العالم الواقعي وتسبب لها أضرار بالغة، كذلك في ظل الظروف الحالية وغياب قوانين دولية أو معاهدة صريحة تجرم الهجمات السيبرانية، فتح المجال أمام الحروب في العالم الافتراضي لتصبح هي البديل الأمثل الذي يلجأ إليه الدول في صراعاتها، سواء في الهجوم أو للدفاع عن النفس، رغم صعوبة الوقاية في ظل زيادة فاعلية التهديد السيبراني.

كما ارتبط مصطلح الحرب السيبرانية بعدة هجمات شهدها العالم الافتراضي، التي انتقلت أضرارها إلى العالم الواقعي على غرار الهجمات السيبرانية التي تعرضت لها إستونيا سنة 2007، جورجيا 2008، إيران2010، فإن الفضاء السيبراني أصبح ساحة للمعارك الدولية، وفي ظل نمو وتيرة التهديدات السيبرانية وتزايد التعرض للهجمات ضد البنية التحتية والتلاعب بالبيانات من خلال الفضاء السيبراني، متزامنة مع زيادة اعتماد المجتمع على شبكة الإنترنت لتسهيل خدامتها وتوزيع المعلومات على مواطنيها، فإنها أصبحت هدف جذابا للهجمات، حيث سارعت الدول على توسيع قدراتها العسكرية لتشمل شبكة الإنترنت وأنظمة الكمبيوتر، بإتخاذ إجراءات وقائية لمواجهة ظاهرة الحروب السيبرانية أو التقليل من مخاطرها، عن طريق الردع والدفاع السيبراني، إضافة إلى سعي على اتخاذ إجراءات قانونية دولية للتصدي لهذه الظاهرة، وما خلفته من عواقب خطيرة قبل أن تتفاقم مع تطور الرهيب في أنواع الأسلحة المستخدمة في الفضاء السيبراني.

وخلصت الدراسة لمجموعة من النتائج والتوصيات أهمها:

أ. النتائج:

✓ ساهمت الثورة التكنولوجية والرقمية في تطوير شبكة الانترنت والحواسيب بروز نوع جديد من الحروب فرض نفسه مغاير تماما للحروب التقليدية، عرف بالحروب السيبرانية التي اختلفت فيه التعريفات بين تقنية وعسكرية، في ضوء الواقع السيبراني الذي أحدثت تحولات في المفاهيم الأمنية.

✓ تتأثر العلاقات الدولية بتحولات في الفضاء السيبراني، فنلاحظ إضعاف المفهوم التقليدي للدولة العسكرية ومدلول الدولة الصغيرة، حيث قلب الفضاء السيبراني الموازين وسمح لدول غير متفوقة عسكريا، والفواعل من غير الدول في التأثير في النظام الدولي وشن هجمات ضد دول كبرى عسكريا.

✓ يمكن أن تمثل الحروب السيبرانية المظهر الجديد للحروب في المستقبل بما تمتاز من ديناميكية وخصائص مغايرة لسابقتها، ساهمت في أن تكون البديل المستقبلي للحروب التقليدية أو على أقل يستخدم كبداية لحسم حرب.

✓ تنوعت أنماط الحروب السيبرانية من منخفض الشدة إلى متوسط الشدة، وصولا إلى نمط مرتفع الشدة والذي لم يشهده العالم بعد.

✓ تعددت الفواعل في الحروب السيبرانية فهي ليست حكرا على الدول فقط، بل هناك عدة فواعل غير الدول منها الجماعات الإرهابية، الأفراد والمنظمات غير الحكومية والشركات متعددة الجنسيات.

✓ يتم استغلال الفضاء الافتراضي بما يتمتع به من خصائص للقيام بالحروب السيبرانية من خلال أدوات ووسائل، تتطور بشكل سريع ومعقد على سبيل المثال:البرامج الخبيثة من فيروسات وديدان أو أي برمجية أخرى متعلقة بالهجوم، مما أضعف قدرة الردع.

✓ مع تزايد الاعتماد على الخدمات الرقمية، تزايد أيضا عدد الهجمات بين الفواعل الدولية وغير الدولية في المسرح السيبراني، ومن تستحوذ على أفضل الخبراء في عالم الانترنت والحواسيب، هو من يسيطر على أجواء الحرب السيبرانية.

✓ اتخذت الدول عدة سبل وقائية تحول للحد من الاختراقات، كما بدلت عدة مساعي لوضع تشريعات قانونية واتفاقيات دولية لمواجهة تحديات الفضاء السيبراني، ولكن مع غياب إرادة دولية بسبب عرقلة الدول المهيمنة في هذا المجال للوصول إلى تنظيم القانوني لهذه الحروب.

✓ هذا النوع من الحروب يدار في فضاء لا يعترف بالحدود الجغرافية ولا بالزمان، فمن الصعب في هذا المجال ممارسة السيادة الوطنية.

✓ صعوبة التحقيق وتحديد الدقيق لمصادر الاختراقات أو المواقع التي تنتح منها البرمجيات الخبيثة والتي تنتقل من دولة إلى أُخرى بسرعة هائلة.

✓ ربط القوة العسكرية بالميدان السيبراني قد يستخدم في المستقبل كمعيار لقياس القوة العسكرية للدول.

ب. <u>التوصيات:</u>

» ضرورة إدراج الأمن السيبراني في العقيدة الأمنية للدول، واعتبارها عنصر مهم في الأمن القومي.

» ضرورة وضع استراتيجيات سيبرانية لتأمين الفضاء السيبراني من مخاطر الحروب السيبرانية.

» تعزيز التعاون على المستوى الإقليمي والدولي، في مجال الأمن السيبراني باعتباره جزء لا يتجزأ من العقيدة الأمنية للدول.

» تطوير القدرات السيبرانية الدفاعية والهجومية، بالحرص على امتلاك وتحديث برامج حماية لكشف ولصد الاختراقات السيبرانية، وتطوير الأسلحة السيبرانية وتكوين جنود سايبر.

» ضرورة تحرك المجتمع الدولي لصياغة تشريعات قانونية واتفاقيات دولية، تخص الحروب السيبرانية، مع إشراك مدخلات تقنية وعسكرية لتعزيز الأمن في الفضاء السيبراني.

» على الدول مواكبة التطور التكنولوجي وإدراج دراسات الفضاء السيبراني ضمن مناهج التعليم وتشجيع البحوث والاستثمارات في مجال البرمجيات.

» توعية المجتمع وتزويدهم بالمعلومات عن التحديات الأمنية للعصر الرقمي والمخاطر الناتجة عن هذه الحروب والأهداف المرجوة منها.

المراجع

قائمة المراجع:

أ. قوانين:

1) موقع الأمم المتحدة، ميثاق الأمم المتحدة: النص الكامل، على الرابط:
https://www.un.org/ar/about-us/un-charter/full-text

2) موقع اللَجنة الدولية للصليب الأحمر، الملحق (البروتوكول) الأول الإضافي إلى اتفاقيات جنيف 1977،على الرابط التالي: https://2u.pw/Qk0Ag

3) دليل تالين، على الرابط: https://2u.pw/h17nq

ب. كتب:

1) الأشقر جبور، منى *السيبرانية. هاجس العصر*. جامعة الدول العربية :المركز العربي للبحوث القانونية والقضائية، 2016.

2) ايه كلارك، ريتشارد وكيه كنيك، روبرت. *حرب الفضاء الالكتروني:الخطر القادم على الأمن القومي وسبل مواجهته*.الامارات العربية المتحدة: مركز الإمارات للدراسات والبحوث الإستراتجية، 2012.

3) البصيلي، جاسم محمد *الحرب الالكترونية. أسسها و أثرها في الحروب* ، ط.2 . لبنان: المؤسسة العربية للدراسات والنشر، 1989.

4) بي سيل، بيتر .*الكون الرقمي: الثورة العالمية في الاتصالات* ترجمة. ضياء وراد. المملكة المتحدة : مؤسسة هنداوي سي آي سي، 2017.

5) الحاج حسن، علي محمد. *الحرب الناعمة: الأسس النظرية والتطبيقية*. العراق: المركز الإسلامي للدراسات الإستراتيجية، 2018.

6) خليفة، إيهاب. *القوة الالكترونية :كيف يمكن أن تدير الدول شؤونها في عصر الانترنت*. مصر: العربي للنشر والتوزيع،2017.

7) (-.-). *مجتمع ما بعد المعلومات: تأثير الثورة الصناعية الرابعة على الأمن القومي*. مصر: العربي للنشر والتوزيع، 2019.

8) عبد الصادق ،عادل. *الإرهاب الإلكتروني: القوة في العلاقات الدولية" نمط جديد وتحديات مختلفة"* ، ط.2. مصر: مركز الدراسات السياسية والإستراتجية، 2009.

9) عبد الغفار، فيصل محمد. *الحرب الالكترونية*. الأردن: الجنادرية للنشر وتوزيع، 2016.

10) العلي، علي زياد . *المرتكزات النظرية في السياسة الدولية*. مصر: دار الفجر للنشر والتوزيع، 2017.

11) كابلان، فرد. *المنطقة المعتمة: التاريخ السري للحرب السيبرانية* ترجمة. لؤي عبد المجيد. الكويت: سلسلة عالم المعرفة، المجلس الوطني للثقافة والآداب، 2019.

12) لونج، اوستن، وآخرون. *الحروب المستقبلية في القرن الحادي و العشرين*. الامارات العربية المتحدة: مركز الإمارات للدراسات والبحوث الإستراتيجية،2014.

*13) ملفات ساخنة 1 :*حرب *التحكم الآلي سلاح الحرب الخامس*. الأردن: دار الجليل للنشر والتوزيع، 2013.

14) يعيش تمام، شوقي. *الجريمة المعلوماتية: دراسة تاصيلية مقارنة*.الجزائر : مطبعة الرمال، 2019.

جـ. مقالات:

1) بن علي الميموني، احمد. "الجبهة النشطة: تداعيات المواجهة السيبرانية بين إيران و إسرائيل."*مجلة الدراسات الإيرانية4*، رقم. 12 (2020): 67-85.

2) البهي، رغدة ."الردعي السيبراني: المفهوم والإشكاليات والمتطلبات."، مجلة الدراسات الإعلامية، رقم.01 (2017): 202-234.

3) دريس، نبيل."الجريمة السيبرانية بين المفاهيم والنصوص التشريعية:الجزائر نمودجا."، *القانون والمجتمع 10*، رقم. 02 (2017): 20-40.

4) سعود، يحيى ياسين. "الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني." *المجلة القانونية* 4، رقم. 4 (2019): 80-108.

5) شلوش، نورة. "القرصنة الالكترونية في الفضاء السيبراني "التهديد المتصاعد لأمن الدول." *مجلة مركز بابل للدراسات الإنسانية 8*، رقم. 02 (2018): 185-206.

6) شنوف، زينب. "الحرب السيبرانية في العصر الرقمي : حروب ما بعد كلاوزفيتش." *المجلة الجزائرية للأمن والتنمية9* ، رقم. 02 (2020) :89-103.

7) عبد الصادق، عادل." أنماط الحرب السيبرانية وتداعياتها على الأمن العالمي"، من مؤلف جماعي بعنوان: "الصراع السيبراني": التنازع العالمي على قوة الفضاء السيبراني. *مجلة السياسة الدولية* 52، رقم. 208 (2017): 03-36.

8) عبد الله السمحان، منى. "متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود: المملكة العربية السعودية." *مجلة كلية التربية 1*، رقم.111 (2020): 2-29.

9) العبودي، علي عبد الرحيم. "هاجس الحروب السيبرانية وتداعياتها على الأمن والسلم الدوليين."*مجلة قضايا سياسية*، رقم. 57 (2019): 345-374.

10) عطية، إدريس. "مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري." *مجلة مصداقية 1*، رقم. 01 (2019): 100-123.

11) غريب، حكيم وشـرقي، صـبرينة ."تداعيات الحرب الإلكترونية على العلاقات الدولية: دراسـة في الهجوم الالكتروني على إيران "فيروس ستكنست"." *دفاتر السياسة والقانون 12*، رقم 02 (2020): 92-107.

12) الفتلاوي، احمد عبيس نعمة ."الهجمات السيبرانية : مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر." *المحقق الحلي للعلوم القانونية والسياسية8*، رقم. 4 (2016): 611-687 .

13) فرحات، علاء الدين. "الفضاء السيرباني: تشكيل ساحة المعركة في القرن الحادي والعشرين."*مجلة العلوم القانونية والسياسية 10*، رقم. 03 (2019): 88-107.

14) محمد أبو زيد، أحمد. "نظريات العلاقات الدولية والحرب: مراجعة للأدبيات:1-2." *مجلة الناقد للدراسـات السياسية*، رقم. 01 (2017): 09-34.

15) معين حسن المشهدي، تغريد. "الأثر العسكري للأمن السيبراني في الجغرافيا السياسية للدولة." *مجلة البحوث الجغرافية1*، رقم. 30 (2019): 239-260.

د. تقارير :

1) تقرير عن اجتماع فريق الخبراء المعني بإجراء دراسة شاملة عن مشكلة الجريمة السيبرانية، صادر عن مكتب الأمم المتحدة المعني بالمخدرات والجريمة، 2019، اطلع عليه بتاريخ 05 /04 /2022.على الرابط التالي: https://2u.pw/B183x،

2) تقرير مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية، الصادر عن الجمعية العامة للأمم المتحدة، بتاريخ 22 جانفي 2001، اطلع عليه بتاريخ 05 /05 /2022على الرابط:https://2u.pw/ihbVt

هـ. المداخلات العلمية :

1) قادير، إسماعيل. إدارة الحروب النفسية في الفضاء الالكتروني: الإستراتيجية الأمريكية الجديدة في الشرق الأوسط، ندوة بعنوان : عولمة الإعلام السياسي وتحديات الأمن القومي للدول النامية، كلية الحقوق والعلوم السياسية، جامعة ورقلة، 2017.

و. المذكرات والرسائل الجامعية:

1)سليمان موسى العقيبي، عادل علي. "مفهوم القوة في العالقات الدولية 1991-2017(المنظور الأمريكي: دراسة حالة)."رسالة ماجستير في علوم السياسية، جامعة الشرق الأوسط، كلية الاداب والعلوم،2018.

2)عبد الواحد، صالح حيدر. "حروب الفضاء الإلكتروني: دراسة في مفهومها وخصائصها وسبل مواجهتها." رسالة ماجستير العلوم السياسية، جامعة الشرق الأوسط، كلية الآداب والعلوم، قسم العلوم السياسية،2021.

3) مهدي التميمي، تغريد صفاء. "توظيف القوة السيبرانية في الأداء الاستراتيجي الأمريكي." أطروحة دكتوراه في علوم السياسية، جامعة النهرين، كلية العلوم السياسية،2021.

ز. مواقع الانترنت :

1) "أنونيموس تنشر مقاطع فيديو لاختراقها قنوات روسية وتعرض صورا من المعركة"، قناة الجزيرة، نشر بتاريخ :28 فيفري 2022، اطلع عليه بتاريخ 30 /04 /2022، الساعة: 22:00، على الموقع: https://2u.pw/loFnL

2) "الاختراقات الإلكترونية.. البداية إشارات مورس"، قناة الجزيرة، نشر بتاريخ: 05 جانفي 2015، اطلع عليه بتاريخ: 06 /03 /2022، الساعة: 23:00، على الرابط: https://2u.pw/mtKKj .

3) "الاستخبارات الأميركية: بوتين أمر بشن حملة إلكترونية لمساعدة ترامب"، جريدة الغد، نشر بتاريخ:7 جانفي 2017، اطلع عليه بتاريخ:2022/04/21، الساعة: 23:00، على الرابط: https://2u.pw/3iJb1

4) بن مناحيم، يوني. "الحرب السايبيرية بين إيران وإسرائيل"، الخنادق، نشر بتاريخ: 31 مارس 2021، تم الاطلاع على الموقع بتاريخ 05-05-2022، الساعة:17:00، على الموقع:https://2u.pw/dNduy

5) تريسي، إسراء. "هجمة إلكترونية تشلّ مؤسسات الدولة بأكملها.. قصة "تمثال الأحرار" الذي أشعل الحرب السيبرانية بين أستونيا وروسيا"، عربي بوسط، تم النشر بتاريخ : 26 نوفمبر 2021، اطلع عليه بتاريخ 01 /05 /2022، الساعة: 13:00، على الرابط:https://2u.pw/S6man

6) شاكر، أسماء. "الفضاء الإلكتروني والواقع الافتراضي في علم الاجتماع الرقمي"، إي عربي، نشر بتاريخ: 28سبتمبر2021، تم الاطلاع على الموقع بتاريخ: 2022/03/11، على الرابط:https://2u.pw/WpZLD

7) "اكتشاف فيروس خارق يهاجم أنظمة الكمبيوتر في دول بالشرق الأوسط من بينها مصر"، جريدة الأهرام، نشر بتاريخ: 30 ماي 2012، اطلع عليه بتاريخ: 17 /03 /2022، الساعة: 23:30، على الرابط: http://www.ahram.org.eg/The-First/News/152146.aspx

8) "أمريكا تتهم الصين بسرقة تكنولوجيا صنع مقاتلة أف – 35"، قناة روسيا اليوم، نشر بتاريخ: 14 مارس 2014، اطلع عليه بتاريخ: 2022/04/20، الساعة: 20:00، على الرابط: https://2u.pw/2w17x

9) "إيران تحكم بالإعدام على أشخاص تقول إنهم تجسسوا لصالح واشنطن"، قناة دي دابل فاو، نشر بتاريخ: 22 جويلية 2019، تم الاطلاع على الموقع بتاريخ 11-05-2022، الساعة:22:00، على الرابط: https://p.dw.com/p/3MW0G

10) "بعد إسقاط الطائرة المسيرة . ترامب ينتقم من إيران بطريقته الخاصة"، قناة دي دابل فاو، نشر بتاريخ: 23 جوان 2019، تم الاطلاع على الموقع بتاريخ 10-05-2022، الساعة:10:00، على الرابط: https://p.dw.com/p/3Kvjl

11) "تحولت إلى التهديد الإلكتروني الأول.. كيف تستخدم الصين هجمات الشبح المعقدة ضد الولايات المتحدة؟"، قناة الجزيرة، نشر في 27 جويلية 2021، اطلع عليه بتاريخ:2022/04/21،الساعة: 18:00.على الرابط:https://2u.pw/q6Ta8

12) "تعريف الفضاء السيبراني"، تريند، اطلع عليه بتاريخ:2022/03/15،الساعة: 19:00، على الرابط: https://2u.pw/jCH42

13) "جيش كوريا الشمالية الإلكتروني متهم بسرقة هذه البنوك"، قناة العربية ، نشر في: 26 ماي 2021، اطلع عليه بتاريخ 27 /04 /2022، الساعة: 22:00. على الموقع التالي: https://2u.pw/q8byl

14) "حادث منشأة نطنز النووية الإيرانية.. تقارير إسرائيلية ترجح هجوما إلكترونيا وطهران لا تستطيع تأكيد فرضية العمل التخريبي"، قناة الجزيرة، نشر بتاريخ:11 افريل 2021، تم الاطلاع على الموقع بتاريخ: 07-05-2022، الساعة:22:00، على الموقع:https://2u.pw/7N7u6

15) "خبير أمريكي يربط بين اختراق سولار ويندز والهجوم على مواقع أمريكية"، الخليج الجديد، نشر في 15 جوان 2021، ، اطلع عليه بتاريخ:25 /2022/05، الساعة: 20:00،على الرابط التالي: https://2u.pw/cGqGC

16) الحاج بكري، سعد علي. "الأمن «السيبراني».....ومعضلة حمايته"، جريدة العرب الاقتصادية الدولية ، نشر بتاريخ: 24 أوت 2017، اطلع عليه بتاريخ 11 /03 /2022، الساعة: 18:00، على الرابط: https://2u.pw/0kTwu.

17) عبد الصادق ،عادل."الحروب السيبرانية : تصاعد القدرات والتحديات للألمن العالمي"، المركز العربي لأبحاث الفضاء الالكتروني، نشر بتاريخ: 12-03-2017، تم الاطلاع على الموقع بتاريخ 16-03-2022، الساعة:14:00،على الرابط :https://2u.pw/cShuM .

18) عفيفي الدويك، عبدالغفار. "الأزمات والحروب السيبرانية... تهديدات تتجاوز الفضاء الإليكتروني"، مركز الأهرام للدراسات السياسية والاستراتجية، نشر بتاريخ 03 فيفري 2019، اطلع عليه بتاريخ 12 /03 /2022، الساعة: 15:00،على الرابط: https://acpss.ahram.org.eg/News/16843.aspx

19) العبودي، علي عبد الرحيم."هاجس الحروب السيبرانية وتداعياتها على الأمن والسلم الدوليين"، قناة الحوار المتمدن، نشر بتاريخ: 21مارس2019، اطلع عليه بتاريخ: 15 /01 /2022، الساعة: 22:05على الرابط: https://2u.pw/NIKWe

20) الشدياق، عماد. "الحرب السيبرانية بين موسكو وواشنطن.. هل تتحول إلى حرب عسكرية؟"،قناةالجزيرة، نشر بتاريخ: 27 مارس 2022،، اطلع عليه بتاريخ: 2022/04/24،الساعة: 19:00، على الرابط : https://2u.pw/WvTDT

21) "قراصنة أمريكيون يحاولون اختراق موقع وزارة الدفاع الصينية"، بي بي سي، نشر بتاريخ: 28 فيفري 2013، اطلع عليه بتاريخ 15 /04 /2022، الساعة: 21:00، على الرابط التالي: https://2u.pw/VNSYw

22) "قراصنة إيرانيون يستهدفون سدا في نيويورك"، قناة بي بي سي، تم الاطلاع على الموقع بتاريخ 10-05-2022، الساعة:07:00 ، نشر بتاريخ : 21 ديسمبر 2015، على الرابط:https://2u.pw/2Ee2g

23) "ما هو السيرفر (خادم)؟ شرح 10 أنواع سيرفر Server "، نشر بتاريخ: 21 مارس2019 ، اطلع عليه بتاريخ: 05/15 /2022، الساعة: 22:05، على الرابط: https://hostingwdomain.com/what-is-server/

24) "ما هو الفضاء السيبراني؟"، سايبر وان، نشر بتاريخ: 5 نوفمبر2021، اطلع عليه بتاريخ:2022/03/15،الساعة:15:00،على الرابط: https://2u.pw/xYK4Z

25) "ما هو فيروس اي وانا كراي"، موسوعة اراجيك، نشر بتاريخ 19 أوت 2019، اطلع عليه بتاريخ 27 /04 /2022، الساعة: 17:00.

" ما هي القيود التي يفرضها قانون الحرب على الهجمات السيبرانية؟"، اللجنة الدولية للصليب الأحمر، اطلع عليه بتاريخ 06 /04 /2022، الساعة: 20:00، على الرابط التالي:

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

26) "مايكروسوفت تكشف عن قراصنة إيرانيين يستهدفون حملة رئاسية ومسؤولين أمريكيين"، ارابيك سي ان ان، نشر بتاريخ: 04 أكتوبر 2019، تم الاطلاع على الموقع بتاريخ 11-05-2022، الساعة:17:00 ،على الموقع:https://2u.pw/XgJs4

27) العميرة، محمد. "الاستخبارات والطرق الاستخباراتية لجمع المعلومات"،The Intel Den، نشر بتاريخ : 25 نوفمبر2020، اطلع عليه بتاريخ: 19 /03 /2022، الساعة: 16:00على الرابط: https://2u.pw/DnGzs

28) المشناوي، محمد. "تكنو بوليتيكس.. الصراع من الدول إلى الشركات"، جريدة الشروق، نشر بتاريخ: 11 فيفري 2021، اطلع عليه بتاريخ: 16 /03 /2022، الساعة: 23:00، على الرابط:https://2u.pw/oicby

29) منصور، محمد .”لماذا تمنع أمريكا استخدام برنامج روسي شهير لمكافحة الفيروسات؟"، صحيفة المصري اليوم، نشر بتاريخ: 14 سبتمبر 2017، اطلع عليه بتاريخ:25 /2022/05، الساعة: 23:30، على الرابط التالي:https://2u.pw/yOzdd

30) محمد علي، محمود. "الحروب السيبرانية وتطور الإستراتجية العسكرية للدول"، نشر بتاريخ: 03 فيفري 2022، اطلع عليه بتاريخ 06 /03 /2022، الساعة: 20:00، على الرابط:https://2u.pw/V0FSu .

31) "آليات جمع المعلومات الاستخبارية وتوظيفها إلى صناع القرار"، المركز الأوروبي لدراسات مكافحة الإرهاب والاستخبارات ، نشر بتاريخ: 22مارس2021 ، اطلع عليه بتاريخ 17 /03 /2022، الساعة: 22:30.على الرابط: https://2u.pw/7DV9J

32) "مسؤول إيراني يؤكد: 100 موقع تعرض لهجمات سيبرانية"، العربية الحدث، نشر بتاريخ: 25 افريل 2022، تم الاطلاع على الموقع بتاريخ: 08-05-2022، الساعة:21:30، على الموقع: https://2u.pw/5OtvE

33) "مسؤولون أمريكيون: قراصنة ايرانيون اخترقوا أجهزة حاسوب تابعة للقوات البحرية الأميركية"، قناة الميادين، نشر بتاريخ : 28 سبتمبر 2013، تم الاطلاع على الموقع بتاريخ 10-05-2022، الساعة:09:00، على الموقع:https://2u.pw/0N8iM

34) "مصطلحات الأمن السيبراني Cyper Security "، نشر بتاريخ: 22 مارس 2022، اطلع عليه بتاريخ: 2022/05/15، الساعة: 23:55على الرابط: https://2u.pw/S0ntb.

35) الصليبي، نايلة. "الحرب الإلكترونية حاضرة في جنيف بين الرئيسين الأمريكي والروسي"، إذاعة مونت كارلو الدولية، نشر في 15 جوان 2021، اطلع عليه بتاريخ:2022/04/24،الساعة: 19:00،على الرابط التالي:https://2u.pw/tgpww

36) "هجوم إلكتروني جديد يستهدف المياه في إسرائيل"، قناة الحرة، نشر بتاريخ : 17 جويلية 2020، تم الاطلاع على الموقع بتاريخ: 07-05-2022، الساعة:23:30، على الموقع:https://2u.pw/eQL60

37) بشير،هشام. "الإرهاب الالكتروني في ظل ثورة المعلومات"، مجلة اراء حول الخليج، نشر بتاريخ: 01 ماي 2012، تم الاطلاع عليه بتاريخ:10 /2022/03، على الرابط:https://2u.pw/kMXqq .

38) "واشنطن: أنشطة كوريا الشمالية السيبرانية تمثل تهديدا لنا"، روسيا اليوم، نشر في 17 فيفري 2021، اطلع عليه بتاريخ 27 /04 /2022، الساعة: 15:00، على الرابط التالي:https://2u.pw/0vrPP

39) سليمان، وائل. "ما هي الجيوش السيبرانية"، موسوعة اراجيك، نشر بتاريخ: 3 جانفي 2020، أطلع عليه بتاريخ 03/15 /2022، الساعة: 23:25، على الرابط التالي:https://2u.pw/MYPDX

40) خضـر، وليد. "الإسـتخبارات السـيبرانية"، بوابة السـفير العربي الدولية، نشـر بتاريخ: 13 جوان 2021، اطلع عليه بتاريخ 17 /03 /2022، الساعة: 22:30، على الرابط:https://2u.pw/9hFjS

باللّغة الأجنبية :

In English:

A. Dictionary:

1) Department of Defense Dictionary of Military and Associated Terms, Joint Publication 1-02, 12 April 2001 (As Amended Through 17 October 2008).

B. Books :

1) Andress, Jason & Winterfeld, Steve. *Techniques Tactics and Tools for security practitioners*.USA: Elsevier, 2011.
2) Baezner, Marie & Robin, Patrice. *Hotspot Analysis:Cyber and Information warfare in the Ukrainian conflict*. Ed.2.Switzerland :Center for Security Studies (CSS), 2017.
3) Pakharenko, Glib." *Cyber War in Perspective: Russian Aggression against Ukraine"."* Cyber Operations at Maidan: A First-Hand Account", Edited by. Geers, Kenneth. Estonia : NATO CCD COE Publications, 2015.
4) S.Nye JR, Joseph. *Cyber Powe*.USA: Belfer Center for Science and International Affairs, 2010.
5) Saalbach, Klaus. *Cyber war Methods and Practice*.Germany :Osnabrueck University, 2020.
6) Schreier,Fred. *On Cyberwarfare*. Switzerland: Geneva Centre for Security Sector Governance, 2015.
7) T. Kuehl, Daniel .*"From Cyberspace to Cyberpower: Defining the Problemin. In Cyberpower and National Security*. Edited by. D Kramer, Franklin. H Starr, Stuart .and K Wentz, Larry .USA: National Defense University Press and Potomac Books, 2009.
8) W Harold, Scott. C Libicki, Martin & Stuth Cevallos, Astrid. *Getting to Yes with China in Cyberspace.USA:* RAND Corporation, 2016.

C) journals:

1) Baram, Gil. Ram, Yael & Ben Israel, Isaac “Cyberwar Between Iran and Israel Out in the Open”, ResearchGate, November 2020
2) Galinec, Darko. Možnik, Darko & Guberina, Boris. “Cybersecurity and cyber defence: national level strategic approach.”Journal for Control, Measurement, Electronics, Computing and Communications 58, NO. 3 (2017): 273 286.
3) hruza, Petr & cerny,Jiri. “cyberwarfare.” International conference KNOWLEDGE-BASED ORGANIZATION 23, No.1, (2017): 155-.160
4) L. Buresh, Donald. Russian “Cyber-Attacks on Estonia, Georgia, and Ukraine, Including Tactics, Techniques, Procedures, and Effects.” Journal of Advanced Forensic Sciences 1. N°.2 (2021): 15-26.
5) Robinson, Michael. Jones,Kevin & Janicke,Helge. "Cyber warfare: Issues and challenges.” Computers & Security 94, (2015):70-94.
6) Shakarian,Paulo.” The 2008 Russian Cyber-Campaign Against Georgia.”Military Review, decembre 2011
7) Ukraine Russia Crisis: Terrorism Briefing, Institute for Economics & Peace, The Institute for Economics & Peace Briefing Series 4, Sydney, 2022.
8) y James P. Farwell & Arakelian, Darby. “What Does Iran’s Cyber Capability Mean For Future Conflict?.”The Whitehead Journal of Diplomacy and International Relations 14, N°. 1, (2013): 49-65**:**

C .Web Sites :

1) "About: Sandworm (hacker group)" , Dbpedia, Date of Entry:16/05/2022,at 22:00,on the site: https://2u.pw/btrni
2) "Malware & Computer Virus Facts & FAQs", kaspersky, Date of Entry:15/03/2022, at 22:25, on the site : https://2u.pw/KxZbZ
3) Barwise, Mike. "What is an internet worm?", BBC, 9 September 2010, Date of Entry:15/03/2022,at 20:15. on the site : https://2u.pw/ptH0j
4) Bergman, Ronen and Halbfinger, David, "Israel Hack of Iran Port Is Latest Salvo in Exchange of Cyberattacks", New York Times, May 19, 2020,Date of Entry:06/05/2022,at 22:00, on the site : https://2u.pw/UjBag
5) Euplerid, Juliet & Entous, Adam. "Russian operation hacked a Vermont utility, showing risk to U.S. electrical grid security", officials say, 31 December 2016, Date of Entry:23/04/2022, at 17:00,on the site: https://2u.pw/QOIpn
6) McGuinness, Damien. "How a cyber attack transformed Estonia",BBC, 27April 2017, Date of Entry:01/05/2022,at 15:00,on the site: https://www.bbc.com/news/39655415
7) S. Schmidt, Michael & E. Sanger, David."5 in China Army Face U.S. Charges of Cyberattacks", the New York Times, 19 May 2014, Date of Entry: 16/04/2022, at 19:00. on the site: https://2u.pw/NXgOY

8) Salt, Alexander & Sobchuk, Maya.“Russian Cyber-Operations in Ukraine and the Implications for NATO”, Canadian Global Affairs Institute, August 2021,Date of Entry: 15/04/2022, at 20,on the site: https://www.cgai.ca/russian_cyber_operations_in_ukraine_and_the_implications_for_nato

9) Tidy, Joe."Ukraine cyber-attack: Russia to blame for hack, says Kyiv", BBC, 14 January 2022, Date of Entry: 30/04/2022, at 20:00, on the site: https://2u.pw/YtJ2v
10) Tom Gerencer, "The Top 10 Worst Computer Viruses in History", Hp, 4 november 2020, Date of Entry:01/03/2022, at 21:00. on the site: https://2u.pw/xuHah
11) Was ist Cybersicherheit?", kaspersky, Date of Entry:01/03/2022, at 22:00, on the site: https://2u.pw/PJSsz .
12) "What is Cyber Espionage?", VMware, Date of Entry:18/03/2022,at 22:00, on the site: https://2u.pw/9nmSR

الفهارس

فهرس الأشكال والجداول :

فهرس المحتويات:

الفهرس