وزارة التعليم العالي والبحث العلمي

المدرسة الوطنية العليا للعلوم السياسية

تطور استخدام الهجمات السيبرانية في الحروب الروسية الأوكرانية 2014-2021

مذكرة مقدمة للاستكمال متطلبات نيل شهادة الماستر.

تخصص: علوم سياسية وعلاقات دولية.

إعداد الطالبة:

بدراني أية ريهام

إشراف الأستاذة :

د. تسعديت مسيح الدين

أعضاء لجنة المناقشة

الرتبة العلمية: اسم ولقب الأستاذ	مؤسسة الانتساب	الصفة
د. سيد أحمد كبير	المدرسة الوطنية العليا للعلوم السياسية	رئيسا
د. تسعديت مسيح الدين	المدرسة الوطنية العليا للعلوم السياسية	مشرفا ومقررا
د. فراني حياة	المدرسة الوطنية العليا للعلوم السياسية	عضوا مناقشا

السنة الجامعية: 2024/2023


بسم الله الرحمن الرحيم

شكروعرفان

إنه لمن دواعي الفخر والسرور أن أتقدم بخالص الشكر وعظيم الامتنان لكل من ساهم في إنجاز هذه المذكرة وأخذ بيدي في مسيرتي العلمية.

أتوجه بخالص الشكر والتقدير للأستاذة "تسعديت مسيح الدين" على توجيهاتها ونصائحها القيمة فقد كان لها الفضل في إرشادي خلال إنجاز هذا البحث.

كما أشكر أعضاء لجنة المناقشة الكرام على قبولهم مناقشة مذكرتي.

كما لا يسعني إلا أن أتقدم بالشكر والامتنان لكل الأستاذة والموظفين في المدرسة الوطنية العليا للعلوم السياسية كل باسمه لقاء جهودهم ودعمهم المستمر.

أهدي لكم هذا العمل تعبيرًا عن عميق شكري وامتناني، وأسأل الله أن يجزيكم عني كل خير، وأن يبارك في علمكم وعملكم.

الإهداء

أهدي عملي هذا إلى والدتي التي كانت ولا تزال مصدر إلهامي وقوتي.

إلى أخي سندي وضلعي الذي لا يميل وإن مالت الدنيا.

إلى أختي أوفى مشجعة وخير صديقة.

إلى رفقائي الذين كانو لي خير عون.

إلى كل من ساهم في مسيرتي العلمية.

بأي شكل من الأشكال، أهديكم هذا العمل تعبيرًا عن امتناني وشكري العميق

الملخص:

يتوافق موضوع الدراسة مع تطور الذي يشهده مجال تكنلوجيا المعلومات وتزايد التهديدات اللا تماثلية التي أصبحت تشكل خطرا على الفواعل في البيئة الدولية خاصة الدول ،حيث تهدف هذه الدراسة إلى البحث في مسار تطور الهجمات السيبرانية منذ سنة 2014 إلى غاية حرب 2021 والغزو الروسي الأوكراني، باعتبار موضوع الهجمات السيبرانية متغير جديد في حقل العلاقات الدولية يجب تكثيف الدراسات حوله بالإضافة إلى كونه جزءا من استراتيجية الصراع بين البلدين، حيث قد ساهمت هذه الهجمات بشكل واضح في تغيير الكثير من المفاهيم المرتبطة بحقل العلاقات الدولية وأصبحت تشكل تهديدا حقيقيا يمس سيادة الدول وأمنها السيبراني وجب التعامل معها وإيجاد أليات بإمكانها التصدي لها وكذا ردع مرتكبيها .

الكلمات المفتاحية

الهجمات السيبرانية، التطور العلمي، الأمن القومي، تكنلوجيا المعلومات ،الحرب الروسية الأوكرانية.

Abstract:

The study topic aligns with the evolution in the field of information technology and the increasing asymmetric threats that pose a danger to actors in the international environment, especially states. This study aims to investigate the evolution of cyber-attacks from 2014 to the present, notably the Russian invasion of Ukraine. Cyber-attacks have emerged as a new variable in the field of international relations, necessitating intensified research. They are not only part of the strategic rivalry between countries but have also significantly altered concepts related to international relations. These attacks now constitute a real threat to state sovereignty and cyber security, requiring the development of mechanisms to address and deter perpetrators effectively.

Key words:

cyber-attacks، Scientific Progress، National security، Information Technology، The Russo-Ukrainian War.

مقدمة

مقدمة:

شهد القرن الواحد والعشرين بروز العديد من المتغييرات في ظل التطورات الهائلة في مجال تكنولوجيا الإعلام والإتصال، وانتشارها على مستوى البيئة الدولية، مما أدى إلى تغير في بعض المفاهيم السائدة في حقل العلاقات الدولية. وعلى الرغم من الإيجابيات التي جاءت بها ثورة المعلومات من تحسين للمستوى المعيشي للشعوب، وتيسير حياتهم من خلال سهولة الوصول إلى المعلومة التي كانت سابقا حكرا على فئة معينة، إلا أنها ساهمت بشكل ملحوظ في تحول العديد من المفاهيم و الثوابت التي قامت على أساسها التفاعلات الدولية سيما مفهوم القوة، وحالتي الحرب والسلم، التي أصبحت تحمل دلالات تكاد تختلف عما كانت عليه سابقا.

بذلك أضحى الفضاء السيبراني من أهم المؤثرات على الأمن القومي للدول أو بعبارة أخرى أصبح لا يمكن الحديث عن دولة كاملة السيادة ما لم تكن في منأى عن التهديدات السيبرانية التي يمكن أن تطال المحتوى المعلوماتي العسكري، الأمني، الفكري، السياسي، والاجتماعي وحتى الاقتصادي وتعتبر العلاقات الروسية الأوكرانية من أهم الأمثلة على مسار تطور الهجمات السيبرانية منذ سنة 2014 إلى غاية بروز أليات الحرب الا تماثلية القائمة حاليا منذ نهاية سنة 2021 حيث استعملت فيها العديد من وسائل الحرب التقليدية والجديدة ،رغبة في حسم هذه الحرب وإثبات المكانة الدولية والقوة التي تمتلكها روسيا وإعادة مكانتها الدولية في سلم القوى الدولية.

انطلاقا من هذا كله صار لزاما على الدول والمنظمات الدولية حشد جهودها وإمكانياتها للتفكير في أليات وحلول يمكن بواسطتها الحد من المخاطر ذات المصدر السيبراني، خاصة ما تعلق بالهجمات السيبرانية باعتبارها أكثر ما يهدد الدول حاليا ويمكنه التأثير على البنية التحتية للدول.

أولا : الإطار المنهجي :

المشكلة البحثية:

لقد أصبحت الحرب في عصر المعلوماتية أكثر تعقيدا واتساعا، وذلك بظهور أدوات جديدة وفضاءات إضافية مختلفة تماما عما كانت عليه خلال الحرب التقليدية، ولعل أهم من استغل هذا الفضاء الجديد المعروف بالسيبراني هو روسيا في حروبها الجديدة ضد العديد من الدول أهمها أوكرانيا والتي لم تتوان عن تطوير نفسها للتصدي لمثل هذه الاعتداءات، وانطلاقا من هذا يمكننا طرح الإشكالية التالية:

- ما هي مكانة الهجمات السيبرانية في الحرب المستمرة بين روسيا وأوكرانيا منذ سنة 2014، وما هي آثار ذلك على العلاقات بينهما؟

الدراسات السابقة:

من أهم الدراسات التي تم الاعتماد عليها نذكر:

_ مقال "الحروب الهجينة: الأزمة الأوكرانية أنموذجا، أسماء حداد منشور على **مجلة مدارات سياسية**، المجلد01، العدد 03، لسنة 2017، حيث قامت الباحثة بطرح الإشكالية التالية: فيما تتجلى مظاهر وسمات الاستراتيجية الروسية في التعامل مع الأزمة الأوكرانية؟

وركزت الباحثة في طرحها للموضوع على الاستراتيجية العسكرية لروسيا وظروف وأسباب غزوها لمنطقة أوكرانيا، بأبعاد القوة العسكرية أكثر من تركيزها على أهمية الهجمات السيبرانية التي تعد من أبرز أساليب الصراع الهجين بين الدولتين.وانطلاقا من هذا فإن دراستنا تسلط الضوء على أهمية الهجمات السيبرانية في الحرب الدائرة بين الدولتين.

_ مقال بعنوان "مفهوم الحروب السيبرانية والأمن السيبراني"لكل من شويرب الجيلالي ومراد فائزة، المنشور في **مجلة الحقوق والحريات**، المجلد 11، العدد01، لسنة 2023،حيث سعى الباحثان إلى الإجابة عن الإشكالية التالية: كيف شكل الفضاء السيبراني العلاقات الدولية الحديثة في السلم وفي الحرب ؟

حاول الباحثان دراسة ظاهرة الحروب السيبرانية وتأثيرها على التفاعلات الدولية، ومدى تلاؤم خصوصية النزاع السيبراني مع قواعد القانون الدولي الإنساني القائم في حالة النزاعات الدولية. في حين أهملا آثار الهجمات السيبرانية على البنية التحتية للدول واقتصاداتها خاصة في فترات السلم وهو ما تم الحديث عنه في هذه الدراسة.

_ مذكرة تخرج للاستكمال متطلبات نيل شهادة الماستر في ميدان الحقوق والعلوم السياسية_للطالبة نورة عقون بعنوان ، واقع الفضاء السيبراني وإشكالية الدفاع الوطني في الجزائر بجامعة قاصدي مرباح ورقلة كلية الحقوق والعلوم السياسية، 2018، 2019، حيث قدمت الباحثة تصور شامل عن الفضاء السيبراني وأنواع الهجمات السيبرانية التي تطال سيادة الدول وتؤثر على أمنها القومي وكدراسة حالة قامت بالتركيز على الاستراتيجية الجزائرية لمواجهة هذه التهديدات الجديدة.

التساؤلات الفرعية:

- ما مفهوم الهجمات السيبرانية؟
- ما موقع الهجمات السبيرانية من وسائل الصراع الدائر بين روسيا وأوكرانيا؟
- ما هي الجهود الدولية التي ينبغي تكريسها للحد من استخدام الهجمات السيبرانية في الصراعات الدولية؟

1. **مجالات الدراسة:**

المجال المكاني:

تشمل الدراسة العلاقات الروسية الأوكرانية ومن ثمة يتحدد المجال المكاني في مجالات الصراع بين الدولتين بما في ذلك المجال الافتراضي، والفواعل المدعمة لكل منهما.

المجال الزماني:

تركز هذه الدراسة على الفترة الممتدة من سنة 2014 تاريخ بداية المواجهة العسكرية بين روسيا وأوكرانيا لتمتد إلى غاية حرب 2021 التي مازالت قائمة بين الطرفين.

المجال الموضوعي:

يغطي المجال الموضوعي للدراسة كل مجالات الصراع بين روسيا وأوكرانيا وما يشمله من وسائل سياسية السياسية، التكنلوجية، الثقافية والتاريخية التي تندرج ضمن العلاقات بين الدولتين.

2. **الفروض العلمية:**

تم صياغة أربعة فروض كإجابة مؤقتة للمشكلة البحثية وهي:

- تُعَدّ الهجمات السيبرانية أداة رئيسية في الحرب الهجينة المستمرة بين روسيا وأوكرانيا منذ عام 2014.
- يؤدي استخدام الهجمات السبيرانية إلى زيادة الانكشاف الأمني للدول.

- كلما ازداد استخدام الهجمات السيبرانية دخلت الخلافات القائمة بين الدول مرحلة التصعيد الذي قد يؤدي إلى الحرب.
- زيادة استخدام الهجمات السيبرانية يقوض فرص السلم بين الدول لذا لابد من مضاعفة الجهود الدولية للحد منها.

3. **الأهمية العلمية والعملية للدراسة:**

الأهمية العلمية:

تتجلى الأهمية العلمية لموضوع الهجمات السيبرانية في كونه ظاهرة جديدة في حقل العلاقات الدولية، زاد الاهتمام بها مؤخرا نظرا لمكانتها وتأثيرها على مجريات التفاعلات الدولية. بالإضافة إلى أن هذه الدراسة هي بمثابة محاولة بسيطة للإزالة اللبس المعرفي عن بعض المفاهيم المرتبطة بالتهديدات الجديدة واكتشاف الفرق بين مجمل المصطلحات المتشابهة بغرض ضبطها، وكذلك التعرف على أهم الهجمات السيبرانية ومدى تأثيرها على الأمن والاستقرار الدوليين.

الأهمية العملية:

يعد موضوع الهجمات السيبرانية من المواضيع التي يهتم بها صناع القرار والأنظمة السياسية ككل، خاصة ما تعلق منها بالدول الكبرى كروسيا مثلا نظرا لتأثيرها على الأمن القومي والدولي على حد سواء، وتبرز الأهمية العملية لهذه الدراسة من خلال معرفة أسلوب تعامل كل من روسيا وأوكرانيا تجاه التهديدات التي مصدرها الفضاء الإلكتروني وكيفية مواجهتها بغرض تقييم هذه الجهود والاستفادة من تجارب الدول الأخرى في هذا المجال.

أهداف الدراسة

تهدف هذه الدراسة إلى:

- التعرف على أشكال التهديدات التي تواجه الدول في العصر الحالي، والتعريف بأهم المفاهيم المتعلقة بالفضاء السيبراني والتمييز بينها.
- إدراك مدى أهمية القوة بأبعادها الجديدة ومكانة القوة التقليدية من الصراعات بين الدول وبين روسيا وأوكرانيا. كدراسة حالة.
- الوقوف على أهم الجهود الدولية لمواجهة التهديدات الجديدة المرتبطة بالفضاء السيبراني ومدى فعاليتها.

- الوصول إلى مقترحات قد تكون مفيدة بالنسبة للاستراتيجية الدول في مواجهة الهجمات السيبرانية.

4. مناهج الدراسة والإقترابات:

يعرف عبد الرحمان بدوي المنهج" **بأنه الطريق المؤدي إلى الكشف عن الحقيقة في العلوم بواسطة مجموعة من القواعد العامة تهيمن على سير العقل وتحدد عملياته حتى يصل إلى نتيجة معلومة"**[1].

كما يعرف المنهج العلمي على أنه "**أسلوب للتفكير والتنفيذ يعتمده الباحث لإنجاز البحث العلمي"**[2] أي أنه باختصار بمثابة المسار العلمي أو الأسلوب الذي يعتمد بغرض تنظيم وتنسيق المعطيات للوصول إلى نتائج أو حلول أو نظريات يمكن اعتمادها. ولمعالجة هذا الموضوع تم الاعتماد على عدة مناهج ومقاربات رغبة في رؤية الظاهرة من عدة نواحي أهمها ما يلي:

- المنهج الإسترادادي:

يعرف على أنه أسلوب علمي يمكن بواسطته دراسة الأحداث والوقائع التي حدثت في الماضي بغرض فهم ظواهر الحاضر وتفسير أسباب حدوثها، ويتمكن الباحثون من خلاله من تتبع حركة تطور النظم والظواهر الاجتماعية خاصة وتفسيرها[3].

- منهج دراسة حالة:

والذي يعرف على أنه "**المنهج الذي يتجه إلى جمع البيانات العلمية المتعلقة بأية وحدة كانت سواء فردا أو مؤسسة أو نظاما اجتماعيا أو مجتمعا محليا أو مجتمعا عاما**"[4]ويعتبر من المناهج الشائع استخدامها في العلوم الاجتماعية ويقوم على دراسة حالة فردية أو حالات محدودة لفهم عميق ودقيق للظاهرة المدروسة.

تم توظيف هذا المنهج من خلال الدراسة المعمقة للحرب بين كل روسيا وأوكرانيا منذ سنة 2014.

5. أدوات جمع البيانات:

تعرف على أنها كل الأدوات التي يعتمدها الباحث لجلب المعلومات والوصول إلى نتائج واستنتاجات حول الظاهرة المدروسة، وبحكم أن موضوع الدراسة متعلق بالعلوم السياسية التي تعد من العلوم الاجتماعية

---

[1] عبد الرحمان بدوي، ***مناهج البحث العلمي***، (الكويت: وكالة المطبوعة، ط.1977,03)، ص.05.

[2] نجيم حناشي، "البحث العلمي مناهجه وأساليبه العلمية"، ***مجلة دراسات لجامعة عبد الرحمان ميرة ببجاية***، م.11، ع.01، (ماي 2022)، ص ص665-682

[3] - أية الطبر، **تعريف المنهج التاريخي**،https://n9.cl/ofoxko ،تاريخ الاطلاع(2024/06/06).

[4] محمد شلبي، **المنهجية في التحليل السياسي مفاهيم –مناهج –إقترابات**، (الجزائر :ديوان المطبوعات الجامعية،1997)،ص 87.

فهو يعتمد خاصة على الأدوات الكيفية أكثر من اعتماده على الكمية نظرا لصعوبة قياس الظواهر الإنسانية التي تتميز بالتغير المستمر.

قد تم الاعتماد على الوثائق من (كتب ومذكرات تخرج ومقالات منشورة على مجلات سواء إلكترونية أو مكتوبة بالإضافة إلى الجرائد الإلكترونية، المواقع الإلكترونية، الأفلام الوثائقية) لغرض جمع المعلومات وكسب قدر من المعرفة لتفكيك الظاهرة ومحاولة الوصول إلى نتائج تتسم بالمصداقية والدقة وذات مصدر علمي.

ثانيا: الإطار النظري:

النظرية الو اقعية

لقد تم التركيز في هذه الدراسة على النظرية الواقعية على اعتبارها النظرية المفسرة بدقة وتفصيل لظاهرة القوة في حقل العلاقات الدولية. فالنظرية الواقعية كما وصفها المفكر جوناثان هاسلام أستاذ تاريخ العلاقات الدولية في جامعة كامبردج "**مجموعة من الأفكار التي تدور حول المقترحات المركزية الأربعة: السياسة الجماعية والأنانية والفوضى والقوة**"[1]

وعلى هذا الأساس يمكن القول أن النظرية الواقعية ترى من خلال تحليلها للواقع الدولي أن الطبيعة الفوضوية الموجودة على الساحة الدولية بالضرورة ستشمل الفضاء الإلكتروني الذي سيشهد حالة عدم يقين، فقد "**ركزت الو اقعية على القوة السيبر انية على اعتبارها ضابط للتوازنات الداخلية والخارجية، واعتبر جيرفيس (Robert jervis) التكنولوجيا أحد أهم محددات التوازن الهجومي والدفاعي للدول، وبأقل التكاليف وذات فعالية في التسبب في حالات اللا أمن. أما المفكر ريتشارد(Richard) فقد أكد على أن الدول تعمل على زيادة قوة دفاعها السيبر اني كجزء من دفاعها العسكري كالصين وروسيا**"[2]. وهذا يعني أن الدول تسعى للتحكم في الأنترنت بغرض زيادة قوتها بما يجعلها قادرة على تحقيق أهدافها والدفاع عن مصالحها في البيئة الدولية عبر تنفيذها للعديد من الهجمات السيبرانية في حالة الهجوم وحماية منشأتها الحيوية ضد أي محاولة للمساس بسيادتها.

---

[1] فيصل عبدون، الواقعية السياسية، https://2u.pw/CEXeUSY6 ،تاريخ الاطلاع (2024/06/06).

[2] سمير باي، "التهديدات الأمنية السيبرانية: دراسة في انعكاسات الحرب لإلكترونية على الأمن القومي للدول واستراتيجيات المقاومة، ***مجلة الرسالة للدراسات والبحوث الإنسانية***، م.08،ع.02،(جوان 2023)،ص ص 189-200.

التقسيم المنهجي للدراسة:

لقد تم تقسيم خطة العمل إلى ثلاثة فصول تطرقنا من خلال الفصل الأول إحاطة عامة حول الموضوع بداية من التعريف بالهجمات السيبرانية بالإضافة نشأتها وأنواعها وأهم الفواعل في الفضاء السيبراني ومخاطر هذه الهجمات وكذا تأثيرها علي أهم مفاهيم العلاقات الدولية كمفهوم القوة والصراع.

أما بالحديث عن الفصل الثاني فتم إدراج تاريخ العلاقات الروسية الأوكرانية إضافة إلى أهم الهجمات التي تعرضت لها منذ 1991 سواء بواسطة الغزو العسكري أو حتى عبر الفضاء الإلكتروني كما تضمن هذا الفصل مجموعة من التحليلات بناءا على المعلومات السابقة بهدف معرفة المكاسب التي تمكنت روسيا من تحقيقها عبر هذه الهجمات على الأراضي الأوكرانية والهدف الحقيقي منها.

أما في الفصل الأخير فقد تم الحديث عن التطور الذي شهدته الهجمات السيبرانية والمكانة التي أصبح يحظى بها الفضاء السيبراني، بالإضافة إلى الاستراتيجية الدفاعية لكل من روسيا وأوكرانيا ضد التهديدات اللا تماثلية القائمة في الفضاء السيبراني وكذلك الجهود الدولية لمحاربة هذه التهديدات ذات البعد الدولي وأهم الاتفاقيات المبرمة في هذا الشأن.

وكختام للبحث كان لا بد من إدراج نظرة استشرافية عن مستقبل العالم أو بشكل أدق سيادة الدول في ضل الهجمات السيبرانية المتواصلة والتحول الجذري الذي شهدته ظاهرة الحرب.

الفصل الأول
الإطار المفاهيمي والنظري للدراسة

تمهيد:

لقد ساهمت التطورات الحاصلة في مجال تكنلوجيا المعلومات إلى بروز تهديدات جديدة على الساحة الدولية، أصبحت تأخذ حيزا كبيرا من اهتمام الباحثين والمفكرين في هذا المجال نظرا للأهميتها وكذا تأثيرها المحسوس على مختلف الفواعل في البيئة الدولية، ومن أهم هذه التهديدات نجد التهديدات القادمة من الفضاء السيبراني التي تتميز بسرعة الانتشار والغموض بالإضافة إلى صعوبة التتبع ما جعل الدول تسعى للإدراج أساليب الأمن السيبراني ضمن أولوياتها.

وفي هذا الإطار سيتم تقسيم هذا الفصل إلى ثلاثة مباحث لدراسة هذه الظاهرة بشكل معمق:

- ✓ المبحث الأول: مفهوم الهجمات السيبرانية.
- ✓ المبحث الثاني: تأثير الهجمات السيبرانية على الأمن القومي للدول.
- ✓ المبحث الثالث: تأثير الهجمات السيبرانية على العلاقات الدولية.

المبحث الأول: ضبط مفهوم الهجمات السيبرانية

مس التطور التكنلوجي جميع مناحي الحياة، حتى أنه غير من طبيعة الحروب والصراعات، من تقليدية إلى جديدة بالاعتماد على التقنيات والوسائل التي يمكن استعمالها لتقليل هامش التكاليف وتحقيق الأهداف المرجوة في البيئة الدولية، ومنه استعمال الفضاء السيبراني فيما يسمى بالهجمات السيبرانية التي سنتعرف على جميع تفاصيلها فيما بعد.

المطلب الأول: الفضاء السيبراني والهجمات السيبرانية

قبل الولوج إلى مفهوم الهجمات السيبرانية وجب تعريف الفضاء السيبرانية، حيث ثمة العديد من التعريفات للمجال الافتراضي أو السايبر، إذ يعرفه الاتحاد الدولي للاتصالات على "**أنه المجال المادي وغير المادي الذي يتكون و ينتج عن العناصر التالية: أجهزة الكمبيوتر، الشبكات ،البرمجيات، حوسبة المعلومات ،المحتوى، معطيات النقل والتحكم، ومستخدموكل هذه العناصر**".[1] ويعرف الفضاء السيبراني حسب معجم أكسفورد أنه" **البيئة الافتراضية التي يتم عبرها إتمام عملية الاتصال عبرشبكات الحاسوب**"
[2]

بالإضافة إلى هذا هناك من يعرف المجال السيبراني بأنه ساحة الحرب الخامسة خاصة وأنه مع بروز الفضاء السيبراني واستعماله بشكل كبير أصبح الحديث عن حرب حقيقية ذات بعد سيبراني بالإضافة إلى الأبعاد الأخرى للحرب التقليدية المتمثلة في البر والبحر والجو والفضاء الخارجي[3]

1-تعريف الهجمات السيبرانية

يعتبر هذا المصطلح حديثا نوعا ما حيث ينطوي على التسلل إلى مواقع إلكترونية غير مرخص بالدخول لها بهدف تعطيل أو إتلاف البيانات المتوفرة أو الاستحواذ عليها وهو فعل الدولة[4] كما عرفها المفكر كارل شميت (Carl Schmitt) على أنها مجموعة من الإجراءات التي تتخذها الدولة على نظم المعلومات المعادية بهدف التأثير عليها والإضرار بها وللدفاع عن نظم المعلومات الخاصة بها.[5]

نلاحظ في التعريفات السابقة أنها ركزت على الدولة كفاعل محوري في التخطيط لهذه الهجمات السيبرانية وتنفيذها في حين أغفلت الفواعل الأخرى في البيئة الدولية لذا وجب إعادة إعطاء تعريف جديد للهجمات السيبرانية يتناسب مع المتغيرات الدولية الجديدة. وهنا يقدم تعريف الدكتور هاربرت لين Herbert)

---

[1]إسماهيل زروقة، الفضاء السيبراني والتحول في مفاهيم القوة والصراع، مجلة العلوم القانونية والسياسية،م.10،ع.01،

[2] نورة عقون ***واقع الفضاء السيبراني وإشكالية الدفاع الوطني في الجزائر***، مذكرة تخرج للاستكمال متطلبات نيل شهادة الماستر في ميدان الحقوق والعلوم السياسية، (جامعة قاصدي مرباح ورقلة كلية الحقوق والعلوم السياسية، 2018، 2019ص 14.

[3]عادل عبد الصادق، **الإرهاب الإلكتروني القوة في العلاقات الدولية نمط جديد وتحديات مختلفة** (مصر مركز الأهرام للدراسات السياسية والاستراتيجية 2009)، ص 106.

[4]بوطلاعة وداد بوكورو منال،" الهجمات السيبرانية على البنية التحتية الحرجة "، **مجلة حقوق الإنسان والحريات العامة**، م07،ع02، (2022)، ص ص ،322-355.

[5]- المكان نفسه .

(Linكبير العلماء في مجلس الحاسوب والاتصالات السلكية واللاسلكية التابع لمجلس البحوث الوطني الأمريكي بالقول "**الهجوم السيبراني استخدام أنشطة متعمدة لتغيير، أو إفساد، أو خداع، أو إضعاف، أو تدمير أنظمة الحاسوب، أو شبكات الحاسوب للخصم أو عبر إتلاف بيانات ذات أهمية استراتيجية**[1]. كما جاء في دليل تالين *(Tallinn guide) "**على أنها العمليات الإلكترونية سواء كانت هجومية أو دفاعية من المتوقع بشكل معقول أن تتسبب في إصابة الأشخاص...أو إلحاق الضرر أو تدمير الأشياء**"[2]

نلاحظ من خلال التعريفات السابقة أن مجملها ركزت على التقنيات والوسائل التي بواسطتها تنفذ الهجمات السيبرانية بالإضافة إلى الأضرار الناجمة عنها مثل التجسس وإتلاف البيانات ذات الأهمية بالنسبة للأفراد أو حتى الدول خاصة في مراكز صنع القرار ورسم السياسة الخارجية للدولة. ويشهد النظام الدولي تنوع وتعدد اللاعبين الدوليين الذين بإمكانهم التأثير على مخرجاته خاصة في العصر الحالي عصر تكنولوجيا المعلومات حيث أصبح لديها فواعل لها من الإمكانيات والقدرة على التحكم في التكنولوجيا ما يمكن أن تصل إلى تهديد الأمن القومي لدولة ما.

من هذا كله يمكننا إعطاء تصور شامل لمفهوم الهجمات السيبرانية بالإضافة إلى أهم خصائص هذه الهجمات. تعرف الهجمات السيبرانية على أنها نوع من التهديدات الجديدة التي تدور وقائعها في الفضاء السيبراني، وتصدر عن جملة من الفواعل منها الدول ذات السيادة وفواعل لا دولاتية أخرى على مستوى النظام الدولي كالشركات متعددة الجنسيات والمنظمات الدولية الحكومية وغير الحكومية، ويتم ذلك باستخدام تقنيات ووسائل رقمية متطورة بغرض الوصول إلى معلومات وبيانات سرية عن طريق التجسس وقرصنة المواقع الإلكترونية أو بهدف إتلافها أو حتى تدمير البنى التحتية للدول أو ضرب الوحدة الوطنية وزرع الفتن داخل المجتمع عبر نشر الأخبار والمعلومات المغلوطة.

من أبرز خصائص الهجمات السيبرانية:

- تجري على مستوى الفضاء السيبراني ويكون الغرض منها تحقيق مكاسب سياسية أو قومية في الغالب يشارك في الصراعات ذات الطبيعة الإلكترونية المدنيون وكذلك العسكري وبواسطة أجهزة الاستخبارات[3]
- تكون خاطفة أي سريعة ومدتها قصيرة ما يصعب عملية تتبعها والتعرف على مصدرها
- تكون واسعة النطاق وغير مرتبطة بدولة أو منطقة دون الأخرى.

---

[1] هيربرت لين، "النزاع السيبراني والقانون الدولي الإنساني "، **المجلة الدولية للصليب الأحمر** ،م.94،ع.01،(2012) ص ص 515-531.

*دليل تالين: يتكون هذا الدليل من مجموعة من المبادئ التوجيهية - تشتمل على 154 قاعدة - تحدد رأي المحامين في تطبيق القانون الدولي على الحرب السيبرانية، والتي تتناول جميع ما يتعلق باستعمال المرتزقة السيبرانيين وباستهداف أنظمة حواسب الوحدات الطبية.

[2] بوطلاعة ، بوكورو، مرجع سابق ، ص 326.

[3] محمود علي عبد الرحمن، "الفضاء الكتروني وأثره علي مفاهيم القوة والأمن والصراع في العلاقات الدولية"، **مجلة كلية السياسة والاقتصاد**،م.16،ع15،(جويلية 2022)،ص ص.423-443.

- يصعب التصدي لها بسبب تنوع مصادر الهجمات وكذا تباين عناوين المنفذين أي لا يمكن معرفة هويتهم الحقيقية وانتماءاتهم وبالتالي يصعب ضبطهم ومتابعتهم قضائيا.
- لا تكلف منفذيها كثيرا، فميزانيتها أقل بكثير من الميزانية التي تخصصها الدول للتسلح، ومع ذلك يمكن لها إلحاق ضرر كبير على الدول.

2-المفاهيم المرتبطة بالهجمات السيبرانية:

يعتبر مفهوم الهجمات السيبرانية جد معقدا نظرا لارتباطه بالعديد من المتغيرات والفواعل على مستوى البيئة الدولية، بالإضافة إلى مشكل الخلط بينه وبين العديد من المفاهيم الأخرى ذات الصلة، لهذا وجب رفع اللبس عنه وتقديم تعريف مبسط لهذه المفاهيم وتبيان طبيعة علاقتها بهذا المفهوم

أ-القوة السيبرانية:

تعرف على أساس أنها قدرة الحصول على مكاسب عن طريق استخدام الفضاء السيبراني والمميزات التي يحتوي عليها بغرض التأثير على الفواعل الأخرى عبر أدوات القوة المتاحة.

يمكن استخدام الأدوات السيبرانية لتحقيق مكاسب على مستوى الفضاء السيبراني أو حتى في مجالات أخرى. ويكون بمثابة وسيلة للوصول إلى أهداف أخرى[1] مثل زعزعة أمن واستقرار دولة ما. فالدول التي لها مكانة على مستوى النظام الدولي أي القوى الدولية بالضرورة هي من تمتلك وسائل القوة سواء العسكرية أو الاقتصادية أو حتى السيبرانية التي تمكنها من لعب أدوار رئيسية، والتأثير في بنية النظام الدولي وبهذا فالعلاقة بين القوة السيبرانية والهجمات السيبرانية علاقة تفاعلية فمثلا يمكن لدولة أن تستخدم قدراتها السيبرانية لتوجيه هجمات السيبرانية ضد خصومها وتدميرهم. كما يمكن لأي دولة استخدام هذه الهجمات بغرض تقويض القوة السيبرانية لدولة أخرى أو التأثير على الأحداث القائمة على الفضاء السيبراني.

ب-التهديدات السيبرانية:

"**فعل يقوض من قدرات وظائف شبكة الكمبيوتر لغرض قومي أو سياسي من خلال استغلال نقطة ضعف ما تمكن المهاجم من التلاعب بالنظام**"[2] تعرف أيضا على أنها جملة التهديدات التي يكون مصدرها الأساسي هو الفضاء السيبراني وهدفها الاختراق والتجسس على البيانات أو استخدام برامج حديثة للسيطرة على أنظمة المعلومات وتمس الدول كما يمكنها أن تطال الأفراد العادين.

ومن هنا يظهر أن مصطلحي الهجمات والتهديدات متشابهان إلى حد كبير، ولكن واقعيا يختلفان من حيث مبدأ التنفيذ فالتهديدات السيبرانية تعني استخدام نقاط ضعف العدو إلحاق الهزيمة عبر وسائط الفضاء الإلكتروني أو استغلال مجمل الثغرات الأمنية التي يمكن أن تحقق هدف المهاجمين. في حين يقصد بالهجمات

[1] JOSEPH .NYE ،Cyber Power .(Cambridge :Harvard Kennedy school belfer center for science and international affaires،may 2010):p4.

[2] عبد الغاني شرقي "التهديدات السيبرانية وإشكالية السيادة" ، **مجلة السياسة العالمية**،م7،ع2،ص ص 270-286.

السيبرانية التنفيذ الحقيقي الفعال للتهديدات السيبرانية، إذ يقوم المهاجم بتنفيذ التهديد على مؤسسة ما أو هدف معين بشرط أن يتسبب بضرر أو يحقق الغاية من فعله أي يحقق المكاسب المرجوة.

ج-الحرب السيبرانية:

"عبارة عن حرب في الفضاء الإلكتروني يقوم بتنفيذها مجموعة من المختصين في المعارك الإلكترونية بالتخطيط للنشاطات الهجومية والدفاعية وتنفيذها عبر الفضاء السيبراني "[1]

وهي أيضا مجمل الإجراءات التي تتخذها الأطراف في النزاع المسلح لكسب ميزة على خصومها من خلال إتلاف أو تدمير أو تعطيل أو اختراق أنظمة الحاسوب للعدو أو الحصول على معلومات سرية (التجسس السيبراني) متى كانت في إطار نزاع مسلح يصل إلى مستوى الحرب[2].

أما العلاقة بين الهجمات السيبرانية والحرب السيبرانية فالهجمات تعتبر من الوسائل الرئيسية التي يستعملها الفاعلون في النزاعات أو الحروب لتحقيق هزائم بالعدو في الجانب السيبراني لغرض جمع البيانات والتجسس أو حتى ضرب البنية التحتية للدول عبر شل قطاعاتها الحيوية.

3- عن نشأة الهجمات السيبرانية:

إن تحديد الفترة التي بدأت فيها الهجمات السيبرانية في الظهور على مستوى التفاعلات الدولية لهو بالأمر الصعب نظرا لعدة أسباب من بينها:

- ✓ قدرة المهاجمين على التخفي وصعوبة الكشف عن جرائمهم في بادئ الأمر مما يجعل عملية معرفة تاريخ بداية الهجوم صعبا.
- ✓ هناك بعض الهجمات متعلقة بالجانب الأمني للدولة والاستخباراتي ولا يمكن بأي شكل من الأشكال الكشف عنها أو التصريح بحدوثها لأن ذلك يمس بكفاءتها وبقدرتها على حماية بياناتها والحفاظ على سيادتها الرقمية.
- ✓ هناك العديد من الهجمات السيبرانية التي وقعت سابقا غير أنها كانت ضد شركات غير معروفة على نطاق واسع أو محلية النشاط لم تلفت انتباه الرأي العام أو الإعلام ولم يسلط عليها الضوء.

ورغم هذا إلا أن أغلب الدراسات تشير إلى أن الحديث عن الهجمات السيبرانية تزامن مع بداية الاعتماد على الأنترنت من طرف الأفراد وإضافة معلوماتهم الشخصية مع سبعينات القرن الماضي ،حيث استغل المهاجمون هذه الظروف لقرصنه واختراق بيانات الأفراد والحكومات، ولكن الهجمات في هذه الفترة كانت تقليدية وغير متطورة[3] إلا أنه ومع بداية الثمانينيات والتطورات التقنية الهائلة في الفضاء السيبراني عامة وفي

[1] أية هندي، **التهديدات السيبرانية وأثرها على الأمن القومي الجزائري** ،مذكرة للاستكمال متطلبات نيل شهادة الماستر في العلوم السياسية والعلاقات الدولية (جامعة الجزائر 03كلية العلوم السياسية والعلاقات الدولية ،2022-2023)ص 33.

[2] شويرب الجيلالي ومراد فائزة "مفهوم الحروب السيبرانية والأمن السيبراني " ، **مجلة الحقوق والحريات** ،م 11،ع1،(2023)ص ص 157-178.

[3] كيرو البدري،" مفهوم الأمن السيبراني ونشأته وتطوره "،في https://n9.cl/bikmb ،تاريخ الإطلاع (2024/04/15)

نظم الكمبيوتر وشبكات المعلومات خاصة أصبحت الهجمات السيبرانية تشهد تطورا هائلا في أساليبها وأبعادها على الأمن القومي للدول. **"وقد ظهر مصطلح الفضاء السيبراني لأول مرة في رواية للكاتب الأمريكي** وليام جيبسون **يصف العصر الحالي بالعصر الرقمي"**[1] نظرا لما يشهده من ثورة المعلومات والتطورات في كل مناحي الحياة، مما يشكل قفزة نوعية بالنسبة للمستخدمين لهذه التقنيات، وكذا أمن واستقرار الدول الذي بفضل التطور التقني الحاصل أصبحت تواجه تهديدات لا مرئية ومنها ما يسمى بالهجمات السيبرانية. فمع الاعتماد الكبير على التكنولوجيا الحديثة أصبحت الجماعات الإجرامية وما ترتكبه من جرائم المعلوماتية منتشرة بكثرة وتشكل خطرا على جميع الأفراد والدول باستخدام الفيروسات وبرامج التجسس ...وغيرها، وهي أدوات يمكن وصفها مجازا بالجراثيم المستحدثة [2]

الجدول رقم 1 جدول يمثل أهم الهجمات السيبرانية حول العالم تاريخ تنفيذها.

اسم الهجوم السيبراني	السنة
هجمات حلف الناتو الإلكترونية على صربيا بهدف تعطيل منظومة الدفاع الجوية	1998
الحرب الإلكترونية بين حزب الله والكيان الصهيوني	2006
الهجمات الروسية الإلكترونية على إستونيا	2007
الهجمات الروسية الإلكترونية على جورجيا	2008
الهجمات الأمريكية الصهيونية على المنشأة النووية الإيرانية (فيروس ستاكسنت)	2010
المواجهات الإلكترونية بين حماس والكيان الصهيوني (قطاع غزة)	2023-2008
هجمات فيروس" شمعون " ضد شركة أرامكو وبعض المنشأة الحيوية في السعودية	2017-2012
هجمات فيروس "دوكو" على شبكة فنادق استضافت محادثات تتعلق بالملف النووي الإيراني	2015-2014
اتهام روسيا بالقرصنة الإلكترونية في الانتخابات الأمريكية لدعم المرشح الجمهوري دونالد ترامب	2016
هجوم الكيان الصهيوني على مفعل "نتانز" النووي الإيراني	2021
اتهام روسيا بشن هجمات الفدية على مؤسسات أمريكية	2021

[1] نورة شلوش ،"القرصنة الإلكترونية في الفضاء السبيراني التهديد المتصاعد للأمن الدول"، ***مجلة مركز بابل للدراسات الإنسانية*** ،م.8،ع.2،(2018)،ص ص .185-206.

[2] المكان نفسه.

المصدر: ياسين محمد أحمد بونة،"الهجمات السيبرانية : الحرب الرقمية التي تجاوزت الحدود الجغرافية"، مجلة شمال إفريقيا للنشر العلمي،م1،ع4،(ديسمبر2023)ص ص.154-168.

المطلب الثاني: أسباب تنامي الهجمات السيبرانية:

لقد شهد عصر تكنولوجيا المعلومات تنامي وتوسع ظاهرة الهجمات السيبرانية في البيئة الدولية مما جعل الدول تسعى جاهدة للحفاظ على سيادتها خاصة في ظل الارتباط الكلي بالفضاء السيبراني في جل القطاعات المدنية وحتى العسكرية. ورغم المرونة التي تتمتع بها الدول التي استطاعت دمج المتغير التكنلوجي في معاملاتها، إلا أنها تبقى عرضة للكثير من الأعمال العدائية والتهديدات الأمنية المرتبطة بالفضاء الإلكتروني ولعل من أهم الأسباب التي ساعدت في تنامي الهجمات السيبرانية ما يلي:

1- التطور العلمي والتكنولوجي والاعتماد المتزايد على وسائل التكنلوجيا الحديثة

يعد الأنترنت والأليات التكنولوجية الحديثة من الوسائل التي استطاعت تحقيق التقدم والتواصل بين الشعوب بالإضافة إلى اكتساب المعرفة، بحيث أصبح الفضاء الإلكتروني مساحة جديدة تمارس فيها جميع الأنشطة الإنسانية سواء بالحديث عن الأفراد أو حتى الدول وهذا ما جعل التهديدات الأمنية تتعدي الإطار التقليدي وتصبح ذات أبعاد أخرى أشد تعقيدا وأكثر خطورة من سابقتها [1].بالإضافة إلى أن شبكة الأنترنت تشهد ما يفوق خمسة مليار مستخدم حول العالم مما يجعل منها أكثر مكان يمكن للأفراد التواصل فيما بينهم عبره لتبادل الأفكار والخبرات، في حين لا يجب إغفال أن الأنترنيت تحتوي على كل البيانات والمعلومات الخاصة بمستخدميها خاصةفيما تعلق بوسائل التواصل الاجتماعي كالفيسبوك (Facebook)والأنستغرام (Instagram) ، الأمر الذي يجعل هذه المعلومات غير محمية أي يمكن لأي فرد أو أي جهة كانت اختراقها واستعمالها لأغراض التشهير أو الابتزاز، ويمكن حتى استغلال هذه البيانات من طرف الشركة التي توفر هذه الخدمة التواصلية بين الأفراد والتاريخ يشهد على العديد منها مثل فضيحة كامبريدج أناليتيكا[2] حيث تعرضت منصة فيسبوك للاتهام بشأن تسريب بيانات أكثر من 87مليون مستخدم لشركة كامبردج أناليتيكا (Cambridge analytica) المتخصصة في جمع البيانات وتحليلها للوصول إلى نتائج يمكن العمل على إبقائها أو حتى تغييرها لصالح الطرف المراد فوزه في الانتخابات الرئاسية، مثل ما هو الحال في الانتخابات الأمريكية سنة 2018التي انتهت بفوز المرشح الجمهوري دونالد ترامب (Donald Trump)رئيسا للولايات المتحدة الأمريكية بإيعاز من هذه الشركة الخاصة وتعاونا مع شركة فيسبوك على تقديم هذه البيانات أو بيعها لاستعمالها في التأثير على الرأي العام الأمريكي.

[1] نوران شفيق، ***أثر التهديدات الإلكترونية على العلاقات الدولية "دراسة في أبعاد الأمن الإلكتروني"***(القاهرة مصر، المكتب العربي للمعارف،2016)،ص19.

[2] **شركة كامبريدج أناليتيكا** : شركة خاصة تعمل على جمع البيانات وتحليلها ومن تم الوصول إلى نتائج لحل مشكلة ما أو تقديم نصيحة حول قضية مطروحة لتسويتها تأسست في 2013تعمل خاصة في محاولة الوصول إلى استنتاجات بخصوص العملية الانتخابية عن طريق جمع البيانات حول الناخبين تم الوصول إلى نتائج أو نظريات تستخدم في عمل الحملات الدعائية مركزة استنادا إلى النتائج المتحصل عليها وبالتالي التأثير في العملية الانتخابية.

وللتلخيص، يمكننا القول إنه في عالم اليوم لا شيء بالمجان أي أنك إذا لم تدفع مقابل الشيء فاعلم أنك أنت البضاعة ويمكن إسقاطها على فضيحة كامبردج أناليتيكا (Cambridge analytica) وتواطأها مع فيسبوك، بالقول أن الخدمات التي تقدمها مواقع التواصل الاجتماعي للأفراد ليست مجانية فهي بالمقابل تستولي على بياناتهم الشخصية حتى يتسنى لها بيعها واستعمالها والعمل بها وحتى التأثير فيها عبر الدعايات والإعلانات الممولة أو التلاعب بمخرجاتها لصالح طرف معين أو نصرة قضية ما لغرض حسمها.

بالإضافة إلى أن "**الفضاء السيبراني أصبح مجالا لظهور أنواع جديدة من الإرهاب غير التقليدي هدفه الأساسي القيام بعمليات هجومية لتدمير البنى التحتية للمعلومات وهو ما نتج عنه مخاطر سياسية وأمنية وقانونية فقد استفاد الإرهابيون من التحديثات التكنلوجية والثورة المعلوماتية وأصبح بإمكانهم الاستفادة من البحث والتطوير عبر أجهزة التواصل الكونية**"...وكل هذا يتم بسرعة فائقة وسرية كبيرة ودون تكاليف باهظة.[1]

وبهذا فالهجمات السيبرانية تشهد تطورا كبيرا تزامنا مع المتغيرات الجديدة في هذا المجال كالذكاء الاصطناعي الذي سيكون له دور كبير وفعال في العديد من المسائل المتعلقة بالفضاء السيبراني سواء ما تعلق بالجانب الهجومي أو حتى كأدات تمكن الدول من الحفاظ على سلامة وأمان مواطنيها وبياناتهم من أي اختراق قد يطالها.

2-تعدد الفواعل من دون الدول في الفضاء السيبراني:

يشهد الفضاء السيبراني تنوعا كبيرا في فواعله منذ ظهور العولمة والثورة في مجال تكنولوجيا المعلومات حيث أصبح بإمكانها التحكم في توجهات الدول وفق ما يتناسب مع مصالحها وأهدافها في البيئة الدولية، فقد حدد جوزيف ناي ثلاثة أنواع من الفواعل الذين يمتلكون القوة السيبرانية وهم الدول ذات السيادة والفاعلون من غير الدول (الشركات متعددة الجنسيات، المنظمات الإرهابية والمنظمات غير الحكومية ....) وكذا الأفراد الذين يمتلكون مهارات فائقة يتم توظيفها[2]

بعد أن كانت الدول هي الفاعل الوحيد في العلاقات الدولية أصبحت هناك جملة من الفاعلين الذين لهم تأثير على النظام الدولي، وهذا ما يدل على زيادة التهديدات الأمنية التي تشكل خطرا على الأمن القومي للدول باعتبار أن الفواعل اللادولاتية تتميز بخصائص لا تمتلكها الدول بأجهزته الأمنية، ومنها القدرة على التخفي وحشد أكبر عدد من الأفراد من جنسيات مختلفة للمشاركة في الهجوم الإلكتروني والقدرة التقنية التي تفوق الدول والتحكم في وسائل التكنولوجيا الحديثة، وتتميز الأسلحة السيبرانية بأنها تقوى على الإتلاف والتدمير

[1] محمد زهير عبد الكريم ،" الإرهاب السيبراني وأزمة عالمية جديدة"، ***مجلة القضايا السياسية***،ع 64(يناير 2021)،ص ص.277-294، متاحة على الرابط التالي : https://political-encyclopedia.org/library/1561/download

[2] حسن هاني محمود وأخرون ،"أثر التهديدات السيبرانية على الأمن القومي :دراسة حالة ماليزيا 2015-2022"،في **https://democraticac.de/?p=90955** تاريخ الاطلاع(2024/03/10).

بأقل الخسائر الممكنة بما في ذلك الهجمات التي تشنها الجماعات الإرهابية على أجهزة الدولة الحساسة ومنشآتها الحيوية أنظمة الطاقة ،النقل ،البنو).[1]

وكمثال على ذلك: "**عندما تسبب أحد الأفراد عام 2000بإيقاف شبكة (CNN)عن البث ومواقع أي باي(EBay) وأمازون (Amazon)على شبكة الأنترنت و أيضا عندما تعرضت إستونيا في 2007، لسلسلة هجمات إلكترونية ضد مواقع مرتبطة بالحكومة وأخرى عامة وهذا ما نتج عنها أضرار جسيمة وخلل كبير في الخدمات الأساسية لدى المواطنين كون أن إستونيا تعتمد على الأنترنت بشكل كبير**."[2]

منه نستنتج أن السطو على شبكة المعلومات بغرض الأعمال التدميرية قد يكون تأثيره عميقا على البنية التحتية للدول ويهدد الأمن والاستقرار خاصة ما تعلق بالهجمات المرتبطة بالإرهاب الإلكتروني.

3-صعوبة اكتشاف و إثبات الهجمات السيبرانية

إن الهجمات السيبرانية لا تترك دليلا أو أثرا لفاعليها أو هوية منفذيها نظرا للاحترافية العالية للمهاجمين. وهذا ما يسهل من عملية اختراق الأنظمة المعلوماتية وسهولة الحركة داخل الموقع المستهدف. فلا يمكن للدول إدراك وقوع الجريمة أو الاختراق حتى تتمكن من تحقيق أهدافها المرجوة من الهجوم. وهنا يكون من غير الممكن إيقافها بالإضافة إلى أنه لا يمكن إثبات الجاني علنا فليس هناك معطيات كافية لإدانته بهذه التهمة ما يسهل عملة الإنكار.[3]فمثلا انطلاقا من التهم الموجهة لروسيا بخرقها للانتخابات الأمريكية سنة 2016صرح فلاديمير بوتين في النهاية "**أنه من الممكن أن يكونوا قراصنة روسيين ولكن ليست لهم أي علاقة بالحكومة الروسية هذا ما يفسر جليا مقولة أنت تعلم أننا فعلناها ولكنك لا تستطيع إثبات ذلك وهذا ما يسمى الإنكار**"[4]

4- سهولة الاستخدام والتكلفة المتدنية

من الخصائص الأساسية للهجمات السيبرانية أنها سهلة الاستخدام والتنفيذ خاصة عندما يتعلق الأمر بالأفراد أو الهيئات المتخصصة في ذلك، بالإضافة إلى أنها لا تستغرق وقتا طويلا هذا ما يجعلها خيارا جيدا بالنسبة للدول أو الفاعلين غيرها لإلحاق ضرر هائل على الجهة المستهدفة بتكلفة ضئيلة إذا تمت مقارنتها بتكاليف الحرب المباشرة على ساحة المعركة التي أضحت تثقل كاهن الدولة وتستنزفها داخليا.

"**وفي نفس السياق هناك دراسات تقول أن التهديدات السيبرانية تكلف4%فقط من تكلفة الآلة العسكرية حتى أن هناك من يشير إلى أنه يمكن تمويل الحرب السيبرانية كاملة عبر الأنترنت بتكلفة ذبابة واحدة**."[5]

---

[1] ياسين محمد أحمد بونة،"الهجمات السبيرانية: الحرب الرقمية التي تجاوزت الحدود الجغرافية"، ***مجلة شمال إفريقيا للنشر العلمي***،م01،ع04،(ديسمبر2023)ص ص.154-168.

[2] عبد الكريم، **مرجع سابق** ، ص 286.

[3] بهاء عدنان يحيي، تأثير التهديدات السبيرانية في الصراعات الإقليمية (نماذج مختارة)،***مجلة كلية التربية للبنات للعلوم الإنسانية*** ،ع. 32،ص ص 399-420.

[4] المكان نفسه.

[5] محمود ، المرجع نفسه.

كما أن الدمار الذي تخلفه الحروب السيبرانية يعد تدميرا بدون زهق الدماء أو أنقاض باعتباره حرب خفية أطرافها مجهولي الهوية ونتائجها خطيرة من خلال تدمير المواقع على الأنترنت بالعديد من الفيروسات كما أن سعة هذا المجال تسمح دوما بزيادة عدد المهاجمين وامتداد الصراع في الزمان والمكان.[1]

5- قصور القوانين العالمية للحد من الجرائم السيبرانية

إن غياب القوانين الردعية على المستوى الدولي جعلت من المجرمين في الفضاء السيبراني يشنون هجمات متكررة ومتتالية غير مبالين بالعواقب الناتجة عن أعمالهم العدائية، خاصة في ظل بيئة دولية تتميز بسباق التسلح بخصوص تطوير الأسلحة السيبرانية بغرض كسب ميزة إضافية أي القدرة على شن هجوم ما بالحصول على معلومات سرية قد تساهم في القيام بسياسة استباقية قد تمكن الدولة المهاجمة مثلا من الاطلاع على ما تنوي الدولة الأخرى القيام به. وبهذا بإمكانها إعداد استراتيجية لمواجهة أي قرار أو سياسة قد تهدد من مصالحها حاليا أو حتى مستقبلا.

ويعود قصور القوانين الردعية لمواجهة الهجمات السيبرانية إلى غياب التنسيق الدولي للحد من هذه الظاهرة والبحث عن حلول جذرية بإمكانها التقليل من حدة وتأثير هذه الهجمات في ظل بيئة دولية تعتمد على الفضاء الإلكتروني بشكل كبير. ونظرا لكون الفاعلين في الهجمات السيبرانية صعب التعرف عليهم بسبب قدراتهم على التخفي فإن هذا يثبط عملية القبض عليهم ومحاسبتهم على الأعمال الضارة بالنظم المعلوماتية.

المطلب الثالث: أهم الفاعلين في شن الهجمات السيبرانية:

يمكننا تقسيم الفاعلين في الفضاء السيبراني إلى ثلاثة أقسام ممن يمتلكون القدرة على تحقيق مكاسب بواسطة الهجمات السيبرانية وهم كالتالي:

1- الدول

تعتبر الدول أهم فاعل والأكثر قوة في مجال الفضاء السيبراني، ومنه تبرز أهمية حماية الفضاء السيبراني بالنسبة للدول ذات السيادة في تخصيصها لجزء من الميزانية لحماية أجهزتها الحساسة وأمنها القومي السيبراني من أي اختراقات قد تطالها، كما تسعى معظم دول العالم إلى امتلاك قدرات هجومية وأخرى دفاعية تجعلها في مركز قوة على الصعيد الدولي. ففي نهاية عام 2008استطاعت حولي 180دولة امتلاك ترسانة من الأسلحة السيبرانية ما يوضح لنا التنافس القائم بين الفاعلين الدوليين من أجل تحقيق التفوق والريادة والتحكم في الفضاء السيبراني دفاعا وهجوما.

"ويعد هجوم ستاكسنت (Stuxnet)من أبرز الهجمات التي شنتها الولايات المتحدة الأمريكية والكيان الصهيوني ضد إيران والتي كانت جزءا من هجمات أكبر عرفت باسم" الألعاب الأولمبية "وكان هدف هذه الهجمات تخريب البرنامج النووي الإيراني حيث تم إنزال فيروس على برنامج التشغيل الإلكتروني الذي

[1] على عبد الرحيم العبودي ،"هاجس الحروب السيبرانية وتداعياتها على الأمن والسلم الدوليين"، ***المجلة الأكاديمية العلمية IRAQUI***،م57،(2019)،ص ص 89-118.

يدير عملية تخصيب اليورانيوم في موقع ناتانز النووي"[1] وتسبب ذلك في إتلاف عدد كبير من وحدات الطرد المركزي وقد عرف هذا الهجوم بأنه جد متطور بالنظر إلى قدرته الكبيرة على الاختراق والإتلاف. وقد قامت إيران في المقابل بمحاولات لتطوير أنشطتها السيبراانية لردع هذا الهجوم السيبراني.

ويرى كل من "**ريتشارد كلارك (Richard Clark) وروبرت كناك (Robert knack)في كتابهما عن الحرب الإلكترونية، بأنها الخطر القادم الذي يهدد الأمن القومي للدو ل وأضافا بعدا آخرا يرتبط بمدى اعتماد الدول على الفضاء الإلكتروني في إدارة شؤون الدولة** "[2]ومنه تزيد قوة الدولة في النظام الدولي، كلما كانت قادرة توجيه هجمات سيبرانية إلى خصومها، وكذا على حماية الفضاء السيبراني، مع الاعتماد النسبي على الفضاء الإلكتروني لا الكلي.

اعتمادا على العديد من المعطيات قدم الباحثان تصنيفا لأكثر الدول التي تمتلك قدرات في الجانب الإلكتروني وهي كالتالي الولايات المتحدة الأمريكية ثم روسيا والصين وإيران وكوريا الشمالية. وينظر الكاتبان نظرة سلبية للاعتماد الكبير للدول على الفضاء الإلكتروني في مؤسساتها الرسمية إذ يزيد من احتمالية تعرضها إلى عدة هجمات إلكترونية ومن ثم انكشاف الأمن القومي لهذه الدولة إذ تصبح سهلة للتدمير الذي يمكن أن يطال ببنيتها التحتية.[3]

يقارن الباحثان بين العديد من الدول من حيث اعتمادهم على الفضاء الإلكتروني، فتحتل الولايات المتحدة الأمريكية المرتبة الأولى من حيث قدراتها الهجومية في الفضاء السيبراني إلا أنها في مقابل ذلك أكثر دولة لديها قابلية التعرض للهجمات السيبرانية، وعلى عكس ذلك فدولة الصين استطاعت تحقيق توازن بين البعد الدفاعي والهجومي عن طريق خفض اعتمادها على الفضاء الإلكتروني، مع استعدادها التام لتنفيذ هجمات في الفضاء السيبراني إذا تم المساس بأي من مقوماتها الأساسية.

2- الفواعل من دون الدول:

شهد العالم بعد نهاية الحرب الباردة بروز عدة فواعل أصبحت لها مكانة في النظام الدولي ولم تعد الدولة الفاعل الرئيسي في التفاعلات الدولية، فكما قال بريجنسكي (Brzezinski)"**يبدو أن دور الدولة يتراجع كوحدة أساسية في المجتمع الدولي وفي حياة الفرد**"[4]. ويعرف بريان هوكينغ (Brian Hocking) ومايكل سميث(Smith Michael) الفاعلين من غير الدول بأنهم جماعة أو منظمة تتمتع بالاستقلال أي بمقدار من الحرية عند السعي لتحقيق أهدافها وإحداث فرق تجاه قضية ما"[5]. وتلعب الفواعل اللادولاتية في الفضاء السيبراني دورا هاما إذ أن هذه الهجمات كانت في البداية عبارة عن محاولات فردية ضد الدولة القومية والغرض الرئيسي منها هو

[1] - بونة، مرجع سابق، ص 161.
[2]- شفيق، مرجع سابق، ص 41.
[3] نفس المرجع، ص42.
[4] تغريد صفاء ولبنى خميس مهدي، "أثر السيبرانية في تطور القوة" ***مجلة حمورابي*** ، م3،ع 33،34،(السنة الثامنة شتاء 2020)ص ص145-161.
[5] شهرزاد أدمام،"الفواعل العنيفة من غير الدول، دراسة نظرية في الأطر المفاهمية والنظرية"، ***سياسات عربية*** ،ع8،(أبريل 2014)ص ص 69-82.

الكسب المادي أو كسب الاعتراف أي لفت النظر، ومع تطور البيئة الدولية والدور المتزايد لهذه الفواعل أصبحت لها رؤى ومطالبا وقضايا للدفاع عنها وتأييدها وأبرز هذه الفواعل.

أ-المنظمات غير الحكومية:

تعتمد هذه المنظمات أساسا على التقنيات الحديثة كتكنولوجيا الاتصال غير أنها لا تمتلك قدرات كبيرة مثل الدول، حيث أنها تسعى للتأثير في البيئة الدولية عبر شن هجمات على مواقع إلكترونية مثلا أو حتى الضغط على النظم السياسية لتغيير قرار ما لا يتماشى مع سياساتها ويكون ذلك عن طريق التعبئة بواسطة المجتمع المدني.

وأبرز مثال عن ذلك الضغوطات التي تمارسها منظمات البيئة العالمية على الدول التي لا تعير لها أي اهتمام مثل ما حدث في الولايات المتحدة الأمريكية ورفض التزامها بما جاء به بروتوكول كيوتو الذي يدعو الدول إلى خفض انبعاثات الغازات والحد من التلوث البيئي الذي تم التوقيع عليه في عام 1997. ولكن الولايات المتحدة لم تصادق عليه وانساحبهامن اتفاقية باريس بناءا على قرار اتخذ في 1 يونيو 2017 من قبل الرئيس دونالد ترامب على اعتبار أن الالتزام بهذه الاتفاقيات سوف يؤثر بشكل سلبي على الاقتصاد الأمريكي[1]، هنا قام العديد من النشطاء والمهتمين بقضايا البيئة والمنظمات البيئية بتنظيم مسيرات ومظاهرات احتجاجا على قرار الرئيس ترامب، رغم فشلهم في تغير قرارات الرئيس إلا أنهم مارسو العديد من الضغوطات على صناع القرار في أمريك. بالإضافة إلى الجماعات الإجرامية أي المجرمون (التي سيتم التطرق لها لاحقا)

ب-الشركات متعددة الجنسيات:

لقد أصبحت الشركات متعددة الجنسيات فاعلا يمتلك كل أدوات القوة التي أحيانا تفوق قوة الدول وما ينقصها سوى شرعية ممارسة هذه القوة التي لا تزال مناطة بالدولة ذات السيادة. فمثلا تفوق ميزانية شركة غوغل(Google) أو فيسبوك(Facebook) أو حتى أبل(Apple)ميزانية العديد من الدول الإفريقية ما يجعل منها لاعبا له مكانته في النظام الدولي في عصر العولمة. بالإضافة إلى امتلاك هذه الشركات العملاقة قاعدة بيانات مستخدمي هذه المنصات تمكنها من استغلال هذه البيانات بما يخدم مصالحها من خلال استكشاف واستغلال الأفراد والأسواق بالإضافة إلى اقتصاديات الدول[2].

من أبرز الأمثلة عن قيام شركات متعددة الجنسيات بالتأثير في مجريات العلاقات الدولية حادثة اختراق الحكومة الصينية حسابات بريد البعض من المواطنين الصينين منهم نشطاء سياسيين ورجال أعمال وهنا طالبت الصين غوغل بحجب نتائج البحث التي تعتبر بالنسبة للحكومة غير مصرح بالاطلاع عليها، وهو ما رفضته شركة غوغل نظرا لما يشكله هذا التصرف من تهديد لسمعة الشركة العالمية، بالإضافة إلى أن الحكومة الصينية أرادت الاعتداء على حقوق الملكية الفكرية الخاصة بغوغل(Google) هذا ما جعل الشركة تهدد علنا

[1] ابو علي حسن ،**ترامب وغد مناخي آخر يلوث الكوكب**،https://n9.cl/8cayuu ، تاريخ الإطلاع(2024/05/05).
[2] إيهاب خليفة، **القوة الإلكترونية كيف يمكن أن تدير الدولة شؤونها في عصر الأنترنت** (القاهرة، العربي للنشر والتوزيع 22 ماي 2017)ص68.

الحكومة الصينية بحجب غوغل(Google) عن دولتها في حال واصلت هجماتها، وفي مقابل هذا قامت الصين كرد فعل بتطوير محرك بحث يسمى بايدو(BAIDU) لغرض التخلص من التبعية الأمريكية .[1]

3- المجرمون (cyber criminels)

هم جماعات أو أفراد يستخدمون تكنولوجيا المعلومات بطريقة سيئة عن طريق تنفيد عمليات إجرامية كغسيل الأموال، الاحتيال المالي، قرصنة البرامج، والتجسس والغرض الأساسي لهذه الجماعات هو ربحي بالأساس أي تحقيق مكاسب بطرق غير مشروعة. ومع تطور الوسائل أصبحت أعمالها تمارس في البيئة الافتراضية. ومن أبرز الأمثلة عن هذه الجماعات (الجماعات الأسيوية المعروفة باسم (Asian triads) والجماعة اليابانية ياكوزا (yakuza)وغيرها من الجماعات في شرق أوروبا .[2]

4- الجماعات الإرهابية (terrorist groups)

تعد من أبرز الفواعل في البيئة الدولية بدأ الحديث عنها منذ هجمات الحادي عشر من سبتمبر 2001 ، وتتكون الجماعات الإرهابية من مجموعة أفراد غالبا ما تكون أهدافهم ذات بعد سياسي يسعون أساسا إلى إلحاق الضرر بالبنية التحتية للدول سواء اقتصاديا أو سياسيا أو حتى تجاريا وتتميز هذه الجماعات بامتلاكها مهارات عالية وتعمل بشكل سري وتكون ممولة ولها أهداف أيديولوجية ويعتبر بعض الدارسين للمجال أن الأنترنت أصبحت بمثابة معسكر تدريبي افتراضي(virtual training camp) تمارس فيه هذه الجماعات أنشطتها حتى يتسنى لها التحضير والتنسيق الجيد لتنفيذ الهجمات الإلكترونية .[3]

5- المبتدئون (thrill seekers)

مجموعة من الأفراد أعمارهم صغيرة أي مراهقين في الغالب يقومون بشن هجمات على أنظمة الكمبيوتر والشبكات من أجل المتعة الشخصية سواء كانوا يريدون معرفة مدى البيانات والمعلومات السرية التي يمكنهم سرقتها أو مهتمين بطريقة عمل أنظمة الكومبيوتر. ومن أهم ميزاتهم أنهم لا يسعون لإلحاق ضرر كبير بأهدافهم وفي المقابل قد يستغلون نقاط ضعف البرنامج أو المؤسسة لشن هجمات إلكترونية مستقبلا [4]

6-القراصنة (Hackers)

"وهم أشخاص يمتلكون مهارات في التعامل مع أنظمة الحاسوب والشبكات وتخطي أي إجراء أو أنظمة لحماية تلك الشبكات وتعود بداية القرصنة إلى ستينات القرن الماضي" [5]

---

[1] - خليفة، المكان نفسه.

[2] What Is A Threat Actor? – Types & Examples، https://2u.pw/p7uicmlP، (03/03/2024).

[3] شفيق، مرجع سابق ، ص47.

[4] What Is A Threat Actor? – Types & Examples ،op .cit.

[5] ليتيم فتيحة، ليتيم نادية "الأمن المعلوماتي للحكومة الإلكترونية والقرصنة" ،***مجلة المفكر*** ،(ع12)،(كلية الحقوق والعلوم السياسية، جامعة محمد خضير (الجزائر 2015)ص ص 238-253.

وارتبط ظهورها مع ظهور أول الحواسيب إلا أن أول عملية قرصنة إلكترونية سجلت سنة 1878 بإحدى شركات الهواتف المحلية الأمريكية ويعتبر الخبراء الفترة من 1980 و1989 العصر الذهبي للقرصنة[1]. ويسعى القراصنة إلى اختراق البيانات والملفات والأنظمة بهدف التدمير عن طريق مجموعة الهجمات المعقدة ويكون هدفهم تحقيق الشهرة أو مكاسب مالية. وهناك أيضا نوع آخر وهم قراصنة السياسة (Hacktivism) فما يميزهم عن القراصنة العاديين هو أن أهدافهم ذات بعد سياسي. ويستند هؤلاء على هجمات الحرمان من الخدمة وكذا نشر الفيروسات.

وفي بعض الأحيان قد تتعاون الدول مع المنظمات غير الحكومية أو حتى الجماعات وذلك بواسطة تقديم الدعم التقني والمادي لهم لشن جملة من الهجمات السيبرانية ضد الخصوم نيابة عنها، وذلك حتى تتفادى التورط المباشر. وأبرز مثال عن هذا الهجوم الإلكتروني على إستونيا في 2007 وعلى جورجيا 2008إذ لم تكن للحكومة الروسية يد مباشرة في هذا إلا أنه حسب المحللين فهذه الهجمات تم تنفيذها بواسطة جماعة روسية لها علاقة وطيدة بالكرملين.[2] وللتلخيص لما قيل سابقا بشأن الفواعل يقدم الجدول رقم 2 أدناه.

الجدول رقم 2: أبرز الفواعل في تنفيد الهجمات السيبرانية ودوافعهم الحقيقية.

فواعل الهجمات السيبرانية	دوافع تنفيذ الهجوم
الدولة القومية	دافع جيوسياسي، أمني
الجماعات الإجرامية	تحقيق أرباح
القراصنة	كسب الاعتراف، الشهرة، المال، نصرة قضية ما
الجماعات الإرهابية	دافع أيديولوجي
المبتدئون	متعة شخصية

المصدر: إعداد الطالبة بالإستعانة بالمرجع التالي:

(03/03/2024)، https://2u.pw/p7uicmlP، What Is A Threat Actor? – Types & Examples

المطلب الرابع: أنواع الهجمات السيبرانية

مع التطور الحاصل في تكنولوجيا المعلومات والتقنيات الجديدة التي يشهدها العالم على صعيد تحقيق قدر من التفوق سواء بالنسبة للقدرات الهجومية أو حتى الدفاعية التي من شأنها تحقيق الأمن، ظهرت أشكالا جديدة من الهجمات لم تكن معروفة من قبل بالإضافة إلى الأشكال التقليدية ويمكننا إجمالا حصر أهم أنواع الهجمات السيبرانية في:

[1] المرجع نفسه، ص 242.
[2] شفيق ،مرجع سابق ص 44.

1-هجمات حجب الخدمة:(Denial of Service Attacks)

تعتبر من أخطر أنواع الهجمات السيبرانية والأكثر انتشارا حيث يقوم مجموعة من المهاجمين أو فرد واحد باقتحام الأنظمة أو الخوادم أو الشبكات بهدف شل عملها والسيطرة على بياناتها لمنع وصول المستخدمين إلى المعلومات والبيانات اللازمة على الإنترنت. ومن هنا يصبح هذا النظام غير قادر على تلبية رغبات وحاجيات المستخدم وبهذا غير فعال للغرض الذي أنشئ لأجله.[1]

بشكل عام الغرض الأساسي للمهاجمين هو تعطيل عمل الكمبيوتر أو نظام عمله عن طريق التدخل في الآلية التي يعمل بها وهي التدخل في المعلومات، بالإضافة إلى حرمان المستخدمين من الخدمة التي يقدمها وبهذا تعتبر الوقاية أو الحماية من هذه الهجمات أمرا في غاية الأهمية نظرا لخطورتها على عدة قطاعات في الدولة أهمها الاقتصاد.

ومثال ذلك: أنه أثناء الحرب الأهلية في سوريا قامت جماعات منظمة تعرف باسم الجيش الإلكتروني السوري التي تتكون من قراصنة يدعمون نظام بشار الأسد بهجوم مكثف ضد جماعات معارضة، باستخدام تقنية حجب الخدمات والمعلومات، وقد نجحوا في العديد من عمليات القرصنة. كما استهدفت هذه الجماعة مواقع إخبارية وثقافية غربية، ونجحت في اختراق أكثر من 120 موقعا، وأهم هجماتها كانت ضد حساب تويتر(twiter) لوكالة الأسوشيتد (Associated Press News) ووضع تغريدة زائفة مفادها أنه تم قصف البيت الأبيض وأصيب الرئيس وكنتيجة لذلك سجل هبوط حاد في الأسواق المالية الأمريكية وفي مؤشر داو جونز الصناعي لعدة دقائق[2].

2-هجوم البرامج الضارة (Malware):

هو نوع يعتمد أساسا على البرامج الضارة بأجهزة الحاسوب أو شبكة أو خادم للوصول إلى معلومات تتسم بالسرية. ويتم هذا في الغالب عن طريق برامج تجسس تكون موصولة ببرامج أو تطبيقات عادية، تستعمل من طرف الضحية على أساس أنها برامج شرعية، وهو ما يسمى (حصان طروادة) حيث يعمل هذا البرنامج كواسطة تمر عبرها البرامج الضارة متنكرة على أنها عادية.[3]

"بالإضافة إلى الروابط الإلكترونية غير معروفة المصدر والتي تقوم بتثبيت تلك البرامج الضارة فور النقر عليها"[4]

[1] Jaideep Singh and others، A Detailed Survey and Classification of Commonly Recurring Cyber Attacks،"International Journal of Computer Applications (0975 – 8887)، Volume(141)No.(10،) (May 2016،)p15-16.

[2] بهاء عدنان يحي، **مرجع سابق** ص 410.

[3] أشهر الهجمات السبيرانية وكيفية مواجهتها والحماية منها، https://2u.pw/jiyLTkMT ،تاريخ الإطلاع (2024/05/05).

[4]المكان نفسه.

3-التصيد الاحتيالي (Phishing):

هو نوع من أنواع الاحتيال عن طريق الفضاء الإلكتروني ويتم عن طريق إرسال رسائل بريد إلكتروني تبدو أنها حقيقية، أي مصدرها موثوق. ويكون الهدف الرئيسي لهذه الهجمات الحصول على معلومات شخصية وبيانات تخص الأفراد المستهدفين لغرض إلحاق الضرر. كما يمكن أن تكون عبر موقع إلكتروني غير شرعي يستولي على بيانات مستخدميه[1].

المثال الأول: في سنة 2018ظهرت حملة تصيد متطورة جدا استهدفت أساسا المواطنين الفرنسيين، مفادها إرسال جملة من الرسائل النصية من طرف الخطوط الجوية الفرنسية للاستفادة من تذكرتين مجانيتين، وذلك بمناسبة الذكرى السنوية الخامسة والثمانين على إنشاء الشركة كما هو موضح في الشكل رقم 03أسفله.

الشكل رقم **01: يمثل الرابط هجمات التصيد الإحتيالي المرسل إلى المواطنين الفرنسيين**

المصدر: ساعد بوقرص ، الأمن السيبراني: مخاطر وتهديدات وتحديات تتطلب ممارسات وتوصيات واستراتيجيات خاصة، مجلة الأبحاث في الحماية الاجتماعية ،م(3)،ع(1)،(22جوان 2022)ص ص 61، 77.

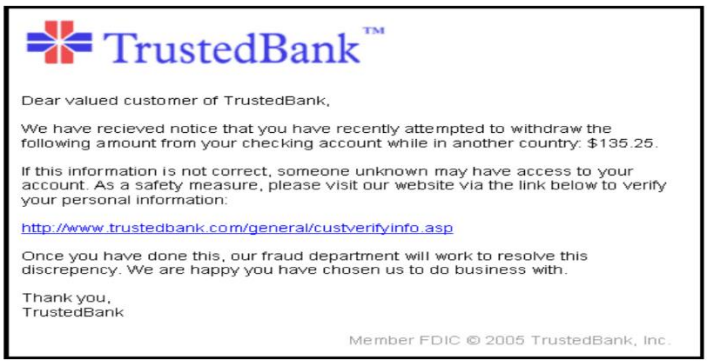
فالملاحظ في هذا الرابط هو وجود اختلاف بسيط بينه وبين الرابط الأصلي التابع للخطوط الجوية الفرنسية وهو النقطة الموجودة تحت حرف a مما يجعل عملية اكتشافها صعبة جدا، وأوقع العديد من الأفراد ضحايا للاحتيال الممارس ضدهم وضد بياناتهم الشخصية وتمت قرصنتها بنجاح.[2]

أما المثال الثاني فهو متعلق بحملة تصيد احتيالي استهدفت زبائن بنك تراست(Trust bank) والحيلة التي استخدمها الهاكرز عبر إضافة حرفين إلى الرابط حيث يصبح (Trusted bank) إذ من الصعب ملاحظة الثغرة أو اكتشافها ويتم بذلك استيلاء المهاجم على كل ما يريد الحصول عليه من الضحية بكل سهولة.

[1] ساعد بوقرص ، الأمن السيبراني: مخاطر وتهديدات وتحديات تتطلب ممارسات وتوصيات واستراتيجيات خاصة، م**جلة الأبحاث في الحماية الاجتماعية** ،م(3)،ع(1)،(22جوان 2022)ص ص 61، 77

[2] **المرجع نفسه**، ص 70.

الشكل رقم02: يمثل البريد الإلكتروني المرسل من قبل منفذي هجمات التصيد الاحتيالي.


TrustedBank™

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

المصدر: ساعد بوقرص ، الأمن السيبراني: مخاطر وتهديدات وتحديات تتطلب ممارسات وتوصيات واستراتيجيات خاصة، مجلة الأبحاث في الحماية الاجتماعية ،م(3)،ع(1)،(22جوان 2022)ص ص 61، 77.

لهذا لا بد من الحذر الشديد عند التعامل مع الملفات والرسائل المرسلة عبر البريد الإلكتروني، أو حتى الروابط للتقليل من مخاطر التصيد الاحتيال، كما يجب نشر الوعي خاصة بين الموظفين في المؤسسات والشركات سواء العمومية أو الخاصة لتجنب الوقوع في مثل هذه المواقف التي قد تكلف المؤسسة الكثير من الخسائر.[1]

4- الهجوم الوسيط (Man-in-the-Middle):

يعد هذا الصنف من الهجمات السيبرانية من الأنواع الأكثر شيوعا ويعتمد أساسا على وجود طرف ثالث وسيط بين العميل والخادم غرضه الأساسي سرقة المعلومات دون علم الشخص المعني ويسمي أيضا هجوم الوصول كما يمكن توضيح كيف تتم العملية عبر المثال الآتي:

يمكن للمهاجم التنصت على مكالمة تتم بين طرفين دون موافقتهما في حين يعتقد الطرفين أنهم يتحدثون مباشرة إلى بعضهم هناك طرف ثالث باستطاعته رؤية كل المحادثات وتغيير محتواها حسب هدفه من هذا التصرف[2]

من أنواعه المعروفة (هجوم التشويش الإلكتروني، سرقة البريد الإلكتروني، والانتحال).

أما عن تصنيف للهجمات السيبرانية حسب أهدافها فيحيلنا إلى ما يلي:

[1] **المرجع نفسه**، ص 71.

[2] Jibi Marian Biju، neethu gopal Majuj Prakash ،"cyber-attacks and its different types"، ***international research journal of engineering technology***، i03،(mars2019)pp4849-4852.

1- الهجمات السبيرانية الدولية:

وهي كل الهجمات التي تتم على مستوى البيئة الدولية وتعرض الأمن الدولي بكل أبعاده عسكريا سياسيا اقتصاديا أو حتى اجتماعيا للخطر، كما تقوم بتهديد البنية التحتية للدول ذات السيادة (الأسواق المالية، المنشئة النووية، والمؤسسات الرسمية للدولة، وكذا قطاعات النقل البري والبحري والجوي)[1]

2- الهجمات السبيرانية الشخصية:

والتي تطال الأفراد غالبا عن طريق الاستيلاء على بياناتهم الشخصية أو تسريبها أو سرقة الأموال واختراق أنظمة المعلومات، وكذا الاعتداء على الملكية الفكرية، بالإضافة إلى الإعلانات غير المرغوبة من طرف المواطنين وخاصة الأطفال لما تحتويه من تهديد وهدم لقيم المجتمع ويمكننا القول أن هذا النوع من الهجمات يكون أكثر خطورة نظرا لأنه يهدد الأفراد بحد ذاتهم وليس دولة كاملة بهياكلها السلطوية.

[1] أحمد عبد الكريم عبد الوهاب، محمود عبد الرحمان خلف، "إشكالية الأمن السبيراني العراقي بين التهديدات السبيرانية والتقنين المقيد للحريات"، ***مجلة قضايا سياسية،لكلية العلوم السياسية جامعة النهرين***، ع60،(2020)،ص ص .1-19.

المبحث الثاني: تأثير الهجمات السيبرانية على الأمن القومي للدول

يعرف الأمن القومي للدولة عموما على أنه سلامة وأمن سيادة الدولة واستقرارها، والحفاظ على حدود رقعتها الجغرافية، وكذا حمايتها من أي تهديد قد يمس مؤسساتها الرسمية أو مواطنيها وبياناتهم الشخصية من أي اعتداء قد يطالها.

المطلب01: دور الهجمات السيبرانية في انكشاف مفهوم الأمن القومي

يشهد العصر الحالي اعتمادا كبيرا على التكنلوجيا الحديثة في كل مناحي الحياة بداية من الأفراد في حياتهم اليومية عبر التطبيقات ووسائل التواصل الاجتماعي وصولا إلى الوسائل الدفاعية للدول ذات السيادة. ورغم المزايا العديدة التي تقدمها هذه التكنلوجيا من سهولة في استخدام وكذا توفير خدمات ذات جودة وتوفير الوقت والدقة، إلا أنها قد تكون بمثابة تهديد كبير للأمن القومي للدول خاصة ما تعلق بمراكز صنع القرار أو الدفاع الوطني، وغيرها من المجالات المتعلقة برسم السياسة الخارجية وأمن الدولة.

1- الهجمات السيبرانية كتهديد جديد:

شهدت الدول العديد من التهديدات الخارجية منها ما هو عسكري كالنزاعات والحروب ومنها ما هو اقتصادي كالركود الاقتصادي والبطالة ومنها ما هو بيئي كالتلوث أما حاليا فالتهديدات أصبحت أكثر خطورة من ذي قبل، نظرا لارتباطها بالفضاء الإلكتروني الذي دخل كل مناحي الحياة، ولم يعد حكرا على مجال دون الآخر ما جعل من الدولة تواجه تحدي أخر، ألا وهو كيفية حماية إقليمها وبياناتها من أي خطر محتمل، قد يرغب في الاستيلاء على هذه البيانات أو محاولة تخريبها أو المساس بها، أو استعمالها كورقة ضغط على هذه الدولة خاصة في ظل بيئة دولية تتميز بالفوضوية أي عدم وجود قانون دولي ملزم قد يفرض على الفاعلين أو يقيد أفعالهم. بالإضافة إلى تحول الفضاء الإلكتروني لوسيط ومصدر جديد للصراع الدولي ذو الأطراف المتنوعة.

ومع هذه التغيرات لم تعد الدولة قادرة على حماية سيادتها بالتركيز على البعد العسكري فقط أي الجيش والأسلحة أو موقعها الجغرافي ومواردها الطبيعية بل يتعدى مفهوم الأمن القومي كل هذا بالتركيز أيضا على البعد التكنولوجي [1]

كما تؤثر الهجمات السبيرانية على البنية التحتية الحيوية للدول: كالبنوك وشبكات الكهرباء والغاز وكذلك المنشآت النووية وذلك عبر شل حركتها أي تعطيل خدمتها ما يؤثر على سيادة الدولة وقدرتها على توفير الحماية والتحكم في مواردها الحيوية. وكمثال عن هذا نجد الاختراقات التي حصلت في البرازيل والمملكة المتحدة للبنية التحتية ما طال بآثاره السلبية على ملايين الأشخاص والمؤسسات والمصالح بالإضافة إلى الاختراقات التي

[1] سليمة طيان، عادل زقاع،" تحول القوة في العلاقات الدولية: محددات ثانوية "، ***المجلة الجزائرية للأمن والتنمية*** ،م12،ع3، (جويلية 2023)، ص ص 191-204.

شهدتها منشأة الطاقة النووية الإيرانية وكذلك ما وقع بين روسيا وجورجيا وانقطاع الاتصال بالأنترنت في إستونيا وغيرها من الأحداث[1].

2- مواطن تأثير الهجمات السيبرانية على الأمن القومي:

يعتمد العديد من المجرمين الدوليين أسلوب الهجمات السيبرانية لسرقة المعلومات والبيانات السرية خاصة في المجال العسكري، هذا ما يؤدي إلى فقدان التفوق الاستخباراتي والاستراتيجي ويعرض الأمن القومي للدول إلى الخطر [2] كما يمكن للهجمات السيبرانية المتطورة أن تعطل أنظمة القيادة والمعدات العسكرية ووسائل التواصل في ظل النزاعات ما يقلل بالضرورة من قدرة الدولة على الهجوم أو حتى على حماية أراضيها.

كما يمكن للجماعات الإرهابية المتطرفة أن تشكل خطرا على الأفراد داخل الدولة أو حتى الحكومات بواسطة تبنيها للأساليب الهجومية عبر الفضاء الإلكتروني عن طريق التهديدات ونشر الذعر والخوف في أوساط المجتمع، أو حتى عن طريق رسائل إلكترونية هدفها كسب التأييد والتعبئة لأكبر فئة ممكنة من أفراد المجتمع، فالتنظيمات الإرهابية ترى أن الفضاء الإلكتروني هو ساحة جديدة للصراع الإيديولوجي، فقد منح لهم فرصة التخفي عن طريق إنشاء صفحات ومجموعات غرضها الأساسي الترويج للأفكار المتطرفة وخلق بيئة آمنة للتواصل والتنسيق بين أعضائها بعيدا عن الرقابة التي تمارسها الأجهزة الرسمية للدولة[3].

وكمثال عن هذا: استعانة تنظيم داعش بحسابات على موقع تويتر(twiter) لغرض التنسيق بين أعضائه للقيام بالعمليات الإرهابية إذ يوجد ما يقارب 70ألف حساب نشط أنشأ لغرض نشر الكراهية والتطرف والمساعدة على تجنيد الشباب خاصة، "**فقد قامت شركة التويتر(twiter) بالتعاون مع مكتب التحقيقات الفيدرالية الأمريكي بإغلاق نحو 125ألف حساب سنة 2015يمتلكها تنظيم داعش لتشجيع الأعمال الإرهابية وتهديد الدول والأفراد.**"[4]

كما يمكن لمواقع التواصل الاجتماعي أن تساهم في خلق النزاعات وزرع الفتن داخل الدولة الواحدة بين فصائل المجتمع عن طريق نشر الدعايات والأخبار الزائفة والتضليل الإلكتروني وأبرز مثال عن ذلك بروز مفهوم جديد في حقل العلاقات الدولية وهو الطائفية السبيرانية.

"وتعرف الطائفية على أنها أمر طبيعي حيث يولد الفرد في مجتمعات متعددة وهو يكن مشاعر الارتباط لها وتكمن المشكلة الأساسية في رفض وممارسة العنف والاضطهاد ضد الطوائف الأخرى المكونة للمجتمع والإحساس بالعلو تجاهها "[5]والجديد هنا هو دخول هذه الصراعات الطائفية إلى الفضاء السيبراني على شكل

---

[1] عبد الكريم، عبد الوهاب، **مرجع سابق** ، ص6.

[2] خالد عبد الغفار البياتي، "الحرب الإلكترونية التهديدات والتحديات في عصر التكنلوجيا الرقمية على الأمن القومي والمجتمعي"، https://www.alnahrain.iq/post/979 ،تاريخ الإطلاع (2024/03/02).

[3] عبد الكريم، عبد الوهاب، مرجع سابق ،ص8.

[4] نفس المرجع، ص9.

[5] إلهام ناصر،الموسوعة السياسية ، ،(2021/11/30)،متوفر على الرابط https://2u.pw/5hV910sV،تاريخ الإطلاع في(2024/04/02).

منشورات وتعليقات وصور وفيديوهات تعمل تأجيج هذه النزعات الطائفية. فسابقا كانت هذه النزاعات تنطلق من الواقع مستقلة عن الفضاء السيبراني، أما حاليا فقد أصبحت شبكة الأنترنت هي المحفز الأول لهذا النوع من الصراعات المجتمعية خاصة عن طريق الصفحات التحريضية على مواقع التواصل الاجتماعي[1]

وهذا ما يولد غياب الألفة والانسجام بين أفراد المجتمع الواحد، بالإضافة إلى انتشار مظاهر العنف والتطرف والاغتراب. وفي بعض الأحيان قد تصل الأمور إلى نزاعات عرقية وطائفية يغديها جملة من الأشخاص مجهولي الهوية في الفضاء الإلكتروني، مما يجعل الدولة في تهديد دائم ومستمر ما لم تستطع ضبط هذه الفئة من المجتمع، على اعتبار أن الأمن المجتمعي لا يمكن فصله عن الأمن القومي. فالدولة التي يكون أفرادها غير منسجمين ويشهدون العديد من الصراعات لا يمكن لها بأي شكل من الأشكال أن تكون آمنة.

المطلب الثاني: توفير الأمن السيبراني

كما ذكر سابقا بأن كل دولة في النظام الدولي تسعى لتحقيق أمنها القومي بجميع أبعاده سياسيا واقتصاديا واجتماعيا، والحفاظ على تراثها وتقاليدها المتوارثة عن الأجيال السابقة التي بالضرورة تمثل هويتها وتاريخها الطويل. بالإضافة إلى حرصها الشديد على تأمين فضائها السيبراني من كل الأخطار والتهديدات التي يمكن لها أن تقوض من سيادة وسلطة الدولة داخل إقليمها أو تجعلها هشة داخليا. وانطلاقا من هذا كان لا بد للدول من وضع استراتيجيات من أجل حماية قواعد البيانات الحساسة عن طريق سن قوانين وكذا توفير التقنيات والوسائل اللازمة لتوفير الأمن السيبراني.

الأمن السيبراني: هو مجموعة الأدوات والتقنيات والتدابير الغرض الأساسي منها حماية الشبكات وأجهزة الكمبيوتر، بالإضافة إلى البرامج والبيانات من أي اختراق أو ضرر أو هجوم قد يطالها وذلك ضمانا للسرية وسلامة البنية التحتية للدول [2]

كما يعرف على أنه: "**مجموع الإجراءات المتخذة للحد أو الدفاع ضد مخاطر الهجمات السيبرانية من خلال الوسائل والأدوات المستخدمة في مواجهة تلك المخاطر**"[3]

ومن هذا يمكن القول إن الأمن السيبراني ظهر كنتيجة حتمية لتزايد التهديدات والمخاطر التي مصدرها الأنترنت، وقد أصبحت هذه التهديدات تستهدف كل الفاعلين الدوليين سواء الدول أو الفواعل اللادولاتية. ولحماية المستخدمين للفضاء الإلكتروني لا بد من اتخاذ مجموعة التدابير الوقائية أو حتى الدفاعية في حال وقع اختراق أو هجوم.

---

[1] عبد الكريم، عبد الوهاب، مرجع سابق ، ص10.

[2] Dan Craigen،Nadia Diakun "Defining Cyber Security"، https://www.timreview.ca/article/835 (06/03/2024)

[3] عادل موسى عوض جاب الله ،"وسائل حماية الأمن السيبراني، دراسة فقهية تأصيلية مقارنة بالنظم المعاصرة "، ***المجلة العلمية لجامعة الأزهر كلية الشريعة والقانون بأسيوط***،م3 ،ع34،(2022).

بناء على هذا هناك العديد من الدول حول العالم استطاعت تحقيق نسب كبيرة في مؤشر القوة السبيرانية التابع لمركز بيلفر (Belfer Center) الذي يسمى إن سي بي آي (NCPI) للعلوم والشؤون الدولية التابع لجامعة هارفرد في الولايات المتحدة الأمريكية ويتم بناء هذا التصنيف على عدة معايير أهمها:

الهجمات الإلكترونية، وقوانين حماية البيانات، والمعايير الفنية، وحوكمة الإنترنت، والبحوث الإلكترونية.

وفي الجدول الآتي توضيع للأهم الدول التي تحتل مراكز عليا في اكتسابها للقوة السبيرانية وحفاظها على بياناتها وأمنها السيبراني[1]

الشكل رقم 03: يمثل تصنيف الدول حسب مؤشر القوة السبير انية.

Belfer Center National Cyber Power Index 2020 "Top 10"		
#	Country	Overall score
1	United States	50.24
2	China	41.47
3	United Kingdom	35.57
4	Russia	28.38
5	Netherlands	24.18
6	France	23.43
7	Germany	22.42
8	Canada	21.50
9	Japan	21.03
10	Australia	20.04

المرجع:

Julia Voo Irfan Hemani Simon Jones Winnona DeSombre Dan Cassidy Anina Schwarzenbach، "National Cyber Power Index 2020" https://2u.pw/vDnDx20t، (02/04/2024).

[1] خالد وليد محمود، **عن مؤشر القوة السيبرانية الوطني 2022**، https://2u.pw/3pUeuMe ، تاريخ الإطلاع في(2024/04/02).

نلاحظ هنا أن الولايات المتحدة الأمريكية تحتل المرتبة الأولى في هذا المؤشر وبعدها الصين في الرتبة الثانية ب47،41 نقطة وبعدها بريطانياب35,57 نقطة، ورابعا روسيا ب28,38نقطة.

المطلب 03: الهجمات السيبرانية وحروب الجيل الخامس

تعتبر الهجمات السيبرانية من الأدوات المستخدمة في إطار حروب الجيل الخامس التي يمكن تعريفها على أنها "**معركة التصورات والمعلومات، حروب ثقافية وأخلاقية، تعمل على تشويه وتزييف تصور الجماهير لإعطاء نظرة مشوهة عن العالم، والسياسة. ففي هذا النوع من الحروب ينتشر العنف بسرية تامة لدرجة أن الضحية لا تدرك حتى أنها ضحية حرب وستخسرها** "[1]بالإضافة إلى أن أهم ما يميز هذه الحروب ويجعلها أخطر من سابقاتها هو سريتها وغالبا لا يتم اكتشافها حتى تتمكن من تحقيق أهدافها المسطرة سابقا من قبل منفذيها. وهو ما ينطبق على الحروب في الفضاء الافتراضي حاليا ومنه فالهجمات السبيبرانية تشكل تهديدا كبيرا على مفهوم الأمن ليس فقط الأمن القومي للدول والمواطنين بل إن تأثيرها يتجاوز ذلك وصولا إلى التأثير على مجرى العلاقات الدولية .

"**فقد أصبح الصراع السيبراني والحروب السيبرانية مهيمنين على القضايا ذات الأهمية في حقل العلاقات الدولية**"[2]. وكتأكيد لهذا حاول العديد من الباحثين تعريف التهديدات والمخاطر غير التقليدية التي يمكنها أن تؤثر على مفهوم الأمن الإنساني باعتباره مفهوم شامل لمجمل الأخطار التي تطال الفرد كوحدة تحليل، والدولة والنظام الدولي إجمالا وإعطاء العديد من الافتراضات الممكنة.

حيث تبرز الأهمية الكبيرة للتكنولوجيا الحديثة من خلال تطور مفهوم الحرب من حرب تقليدية إلى حرب حديثة توظف فيها جميع الوسائل والإمكانيات لتحقيق النصر وإلحاق الهزيمة بالخصم. وفي مقابل ذلك تسعى الفواعل في البيئة الدولية إلى اكتساب ميزة إضافية تمكنهم من صد أي تهديد أو هجوم سيبراني محتمل.

1- أثار الهجمات السيبرانية:

تعتبر الهجمات السيبرانية من أخطر وأعقد الجرائم التي فرضت نفسها على مستوى التفاعلات الدولية وأصبحت تشكل تهديدا حقيقيا للأمن والسلم العالمي:

- ✓ الإرهاب: كما ذكر سابقا أنه من أبرز الفواعل على مستوى البيئة الدولية نظرا للمخاطر التي تنجر عنه ومع التطور التقني والمعلوماتي الحاصل واكب هذا الأخير التكنلوجيا الحديثة عن طريق استغلالها في عمليات التجنيد في صفوف الشباب على مواقع التواصل الاجتماعي، بالإضافة إلى الدعاية ومحاولة تحسين صورة هذه الجماعات، وكسب الشرعية لممارساتها على اعتبارها ذات مصدر ديني ولا يمكن

[1] زينب فريح ،"دراسة في محددات تطور الأجيال الخمس للحرب "،**دفاتر السياسة والقانون** ،م13،ع02،(15 /2021/05)،ص ص 542-555.
[2] سوزي رشاد ،التهديدات الأمنية الهجينة في العلاقات الدولية (السبيرانية والذكاء الاصطناعي نموذجا)،**مجلة وادي النيل للدراسات والبحوث الإنسانية والاجتماعية والتربوية**،م.30،ع.30،(06أكتوبر)،ص ص 663-700.

التنازل عنها بالإضافة إلى إمكانية هذه الجماعات اختراق شبكات الكهرباء والطاقة والمواصلات التي بالضرورة تؤثر على البنية التحتية للدول ،حيث تعتبر ممارسة القوة على الفضاء الإلكتروني بمثابة الإرهاب الجديد.

فمثلا: إذا كان الإرهاب غرضه الأساسي التأثير في مخرجات النظام السياسي لأي دولة أو حتى التأثير في الرأي العام العالمي حول قضية معينة، فهنا يمكننا تسميته بالإرهاب الجديد المكمل للإرهاب التقليدي الذي يعتمد على وسائل الحرب التقليدية [1]ومثال ذلك جماعة سايبر بيركوت (Cyber Berkut) الأوكرانية التي هاجمت سنة 2014 المواقع الإلكترونية لحلف الناتو، مما أدى إلى تعطيلها لعدة ساعات متسببين بذلك في أزمة دولية وتوتر في العلاقات الدبلوماسية آنذاك.[2]

كما تظهر أثار الهجمات السيبرانية على مستوى النظام الدولي من الناحية السياسية على اعتبارها تهديد يطال وحدة الدول بالتفكك كما سبق وذكر أن بإمكان جماعة أن تؤثر على العلاقة بين دولتين أو تكون السبب في أزمة دبلوماسية عن طريق جرائمها السيبرانية ضد دولة أخرى. بالإضافة إلى تشويه سمعة الدول والتقليل من أهميتها وقوتها أمام الرأي العام العالمي، وضعف ثقلها السياسي. [3]كما أن الفيروسات تعتبر الأسلحة الرئيسية في الهجومات السيبرانية حيث تعمل أساسا على تعطيل عمل الشبكات الإلكترونية والخوادم الأساسية ويمكن نشر هذه الفيروسات عبر الرسائل الإلكترونية أو حتى بواسطة نقل الملفات الإلكترونية عبر أداة لحفظ البيانات.[4]

بالإضافة إلى أن الهجمات السيبرانية وغياب الأمن السيبراني ساهم في تقسيم العالم إلى طوائف وعرقيات متضاربة فيما بينها داخل الدولة القومية وحتى على المستوى الخارجي عن طريق الفتن والدعايات التي مصدرها الأنترنت لأغراض تدميرية للأفراد، وكذا الدول. أما في الجانب الاقتصادي فتعد الشركات والبنوك الأكثر استهدافا عبر سرقة بيانات مستخدميها مثل المعلومات الخاصة بالمعاملات المالية، ما يجعل من هذه المؤسسة تفقد ثقة عملائها بسبب عجزها عن حماية بياناتهم وكذا الخسائر المالية التي تستلزم إعادة تهيئة بنية تحتية آمنة أو حتى معالجة القضايا المتعلقة بالابتزاز المالي والتهديد بنشر سندات ووثائق سرية لا يراد الكشف عنها. أما على الصعيد النفسي فالتهديدات السيبرانية تشكل حالة من التوتر والخوف لدى الأفراد، وأبرز مثال عن هذا الأثار النفسية التي تسببت فيها لعبة الحوت الأزرق التي أثارت ضجة في العالم بداية من سنة 2013 في روسيا حيث تتكون أساسا هذه اللعبة من العديد من التحديات لمدة 50 يوما، يمثل التحدي الأخير الانتحار وما سببته من خوف وسط أفراد المجتمع، خاصة وأن هذه اللعبة تم نشرها في العديد من الدول وتقوم بتهديد

[1] إيهاب خليفة، **القوة الإلكترونية وأبعاد التحول في خصائص القوة** (الإسكندرية: وحدة الدراسات المستقبلية ،2014)ص 37.
[2] محمود وآخرون، مرجع سابق.
[3] المكان نفسه
[4] د بونة، مرجع سابق.

مستخدميها وتجعلهم يقدمون على أفعال انتحارية وهذه تعتبر جريمة في حق الإنسانية ويجب أن يعاقب عليها القانون[1].

2- الحروب السيبرانية وخصائصها

لقد أصبحت الأبعاد الإلكترونية واضحة في أغلب التفاعلات الدولية نظرا للمكانة والأهمية التي يكتسيها التحكم في الفضاء الإلكتروني وقدرة الدولة على حماية أمنها السيبراني من عدمه، حيث يعتبر هذا حاليا معيار لقياس قوة الدولة بالإضافة إلى مدى تمكنها من توجيه هجمات ضد خصومها.

كما أن تنفيذ الهجمات السيبرانية غير مرتبط بفترات الحرب والنزاعات فقط، فقد يحدث أيضا في فترات السلم بهدف التجسس.

إن التكنولوجيا الرقمية والإنترنت قد ارتبطت ارتباطا وثيقا بأمن الدولة، أي أن الإشراف عليها والبحث في هذا المجال اختصت به الأجهزة الرسمية للدول ذات السيادة. أي أجهزة الاستخبارات والأمن، حيث أنه، ومع نهاية الحرب الباردة، وانتشار التكنولوجيا الرقمية عالميا، لم تعد حكرا على الدولة وهنا زادت المخاطر التي يمكن أن تتسبب فيها التهديدات ذات المصدر السيبراني.[2]

يعد أمن الفضاء السيبراني من كل ما يمكن أن يهدد أمن المعلومات السرية والبيانات الرقمية من القضايا الأساسية التي تسعى الدول للبحث فيها وحمايتها بالإضافة إلى الاهتمامات المتصاعدة على الصعيد الدولي بضرورة إدراج قضايا الأمن السيبراني ضمن الأجندات العالمية للدول كافة.[3] ولابد من الإشارة إلى أن فترات السلم والحرب غير معروفة في إطار تنفيذ الهجمات السيبرانية أي أنها تتميز بخاصية التخفي ولا يمكن للدولة إدراك حدوثها حتى يتمكن المهاجمون من تحقيق جزء من أهدافهم أو حتى كلها، هذا ما يجعل الدول عاجزة عن إدراك إذا كانت تواجه أخطار الهجمات السيبرانية أو أنها في حالة غياب سلم وغياب التهديد.

كما أنه في فترات السلم تشهد الدول تهديدات سيبرانية خاصة ما تعلق بالهجمات على المؤسسات المالية والشركات وكل ما تعلق بالبنية التحتية عبر شل عمل مولدات الطاقة وكذا وسائل النقل ما يؤثر سلبا على الحياة اليومية للأفراد.

كما أن الأخبار الزائفة التي تبث عادة عبر وسائل التواصل الاجتماعي قد تؤدي إلى إحداث فوضى داخل المجتمع وخاصة مع بروز التقنيات الجديدة المتعلقة بالذكاء الصناعي التي تستطيع حتى فبركة خطابات مرئية لرؤساء دول أو شخصيات معروفة دون أن تترك مجال للشك في مصداقية هذا الخطاب هذا بالضرورة ما يؤدي إلى زعزعة الثقة بين الحاكم والمحكوم وكذلك المساس بالاستقرار السياسي، قد يصل إلى خلق صراعات جديدة ذات خلفية دينية عرقية داخل الدولة الواحدة.

---

[1] محمود وآخرون، مرجع سابق.
[2] شرقي ، مرجع سابق، ص 279.
[3] شلوش، مرجع سابق ، ص 187.

أما بالحديث عن الفترات التي تشهد أزمات دولية ونزاعات فتلعب الهجمات السيبرانية دورا مساعدا بالإضافة إلى وسائل الحرب الأخرى التقليدية (كالعمليات العسكرية أو الحصار الاقتصادي)[1]

فكما هو معروف أن نجاح أي عملية عسكرية مرتبط بمدى تحقيقه للأهداف المرجوة، وأحيانا تكون القوة العسكرية وحدها غير كافية لذلك يجب تزويدها بالقوة السبيرانية لغرض تأمين البنية التحتية أو حتى في إطار الصراع السيبراني الذي يتميز بصعوبة تحديد أطرافه والزيادة الهائلة في أعداده والأثار المترتبة عنه من حرب نفسية وشل لأنظمة الاتصالات لدى العدو وكذا الدعاية.

كما أنه خلال الفترة الأخيرة قد ظهرت طرق بديلة عن المواجهة المباشرة بين الأطراف ألا وهي الحروب عبر شبكات الاتصال والمعلومات.

قد تحول معها مفهوم الصراع خاصة في ظل الاعتماد المتبادل وظهور ما يسمى بعصر القوة النسبية التي تعرف على أنها قدرة الدولة على التأثير على الفواعل الأخرين ليس فقط من خلال استخدام القوة الصلبة بل بواسطة كل الوسائل المتاحة (اقتصاديا، سياسيا ثقافيا) ذلك الأن القوة العسكرية وحدها في العصر الحالي غير كافية لتحقيق ميزة تنافسية وتحقيق أهدافها على مستوى النظام الدولي[2]

وبهذا فقد تغير براديغم الحرب كليا من حروب بين الدول إلى حروب داخل الشعوب أي التحكم في إرادة الشعوب وخياراتهم سواء داخل إقليم الدولة أو عبر صناعة الرأي العام العالمي ،وهنا تكون الحرب النفسية والدعاية هي الأسلحة الرئيسية لهذه الحروب الجديدة وتسمى هذه الحروب الممارسة في الفضاء الإلكتروني بالحروب السيبرانية (cyber war) وتعتبر متعددة الأنماط أهمها:

- ✓ <u>الحرب السيبرانية منخفضة الشدة</u>: حيث يتم استخدام الفضاء السيبراني كساحة للصراع منخفض الشدة الذي يكون ذو طبيعة ممتدة له طابع غير سلمي بخلاف أنه عميق الجذور ومتداخل وله نواحي متعددة ثقافية أو اقتصادية أو اجتماعي وعادة ما يكون مرتبط بالصراعات ذات البعد الديني والاجتماعي طويلة الأمد مثل الصراع العربي الإسرائيلي وكذا الهندي الباكستاني.[3]
- ✓ <u>الحرب السيبرانية متوسطة الشدة</u>: يتحول الصراع في هذا النوع من الحروب إلى ما يعادل الحرب التقليدية من حيث شدتها كما قد يكون بداية لعمل عسكري وتتم هذه الحروب عبر اختراق المواقع الإلكترونية وتخريبها وشن حروب نفسية ضد الخصوم ومثال ذلك هجمات حلف الناتو على يوغسلافيا في سنة 1999[4] حيث" **استهدفت الهجمات الإلكترونية تعطيل شبكات الاتصالات للخصوم، كما برزت أيضًا خلال الحرب بين حزب الله وإسرائيل في عام 2006، وبين روسيا وجورجيا**

[1] رشاد، مرجع سابق، ص 683.
[2] شيماء عويس أبو عبيد، "القوة في العلاقات الدولية: دراسة تأصيلية" ،https://n9.cl/1ln1a تاريخ الاطلاع في(2024/04/09).
[3] رشاد، **مرجع سابق**، ص 685.
[4] - **نفس المرجع**، ص194-195

في 2008، وفي المواجهات بين حركة حماس والاحتلال الإسرائيلي في عامي 2008 و2012"وكذالك 2023.[1]

- ✓ الحرب السيبرانية الساخنة مرتفعة الشدة: يتميز هذا النوع من الحروب بأنه الأكثر خطورة وتعقيدا وتطورا ويكون غير موازي للحرب التقليدية يتم استخدام الروبوتات الألية وطائرات مسيرة وإدارتها عن بعد بغرض تحقيق الهيمنة والتفوق وإخضاع العدو، مثل شن إسرائيل هجمات فيروس ستاكسنت ضد المنشآت النووية الإيرانية بالتعاون مع الولايات المتحدة في عام 2010، وكان قد تم تطوير هذا الفيروس وتجربته في إسرائيل خلال عام 2007.[2]
- ✓ الحرب بالوكالة السيبرانية: عن طريق شن الحروب بشكل غير مباشر عن طريق توظيف فاعلين أخرين تحقق الدول بواسطتهم أهدافها ول يمكن اكتشاف أمرها مثل القراصنة ،الميليشيات السيبرانية، مثل ما حدث في الحرب الروسية الجورجية سنة 2008 وكذا في إطار الحرب بالوكالة بين إيران وإسرائيل[3].

المطلب04: تأثير الهجمات السيبرانية على العلاقات الدولية

يعتبر حقل العلاقات الدولية من أكثر الحقول تشعبا وإلماما بالظواهر الدولية، حيث يحاول وصف وتفسير جميع المتغيرات والمستجدات التي تشهدها البيئة الدولية وأبرزها ما أصبح يعرف بالتهديدات اللاتماثلية التي من بينها الهجمات عبر الفضاء الإلكتروني التي تشهد مؤخرا انتشارا كبيرا. لهذا وجب محاولة إعطاء تصور عن تأثير الذي تمارسه على مفاهيم العلاقات الدولية.

1-تأثير الهجمات السيبرانية على مفهوم القوة

يعتبر مفهوم القوة من أبرز المفاهيم التي يقوم عليها حقل العلاقات الدولية حيث سعت كل نظرية إلى إعطاء تعريف واضح لهذا المفهوم بداية من النظرية الواقعية التي ترى أن السياسة الدولية تتسم بالصراع والنزاعات لغرض اكتساب القوة، حيث أن أهم ما يميز النظام الدولي طبيعته الفوضوية التي بالضرورة تجعل الدول تسعى إلى تحقيق التفوق بالاعتماد على قدراتها وإمكانياتها. فالدول في النظام الدولي تسعى إلى تحقيق البقاء وتعظيم قوتها العسكرية والنهوض باقتصادها [4]أما بالحديث عن "**النظرية اللبرالية فقد ركز أنصارها على القوة الاقتصادية بالإضافة إلى القوة العسكرية وهذين النوعين يمثلان القوة الصلبة بالإضافة إلى**

[1] حسام السبكي، "الحروب السيبرانية" المفهوم والأنماط والتداعيات على الأمن الدولي،https://roayahnews.com/?p=353430 تاريخ الإطلاع في (10 /2024/04).
[2] - المكان نفسه.
[3] صابر غل العنبري، الحرب السيبرانية، معركة بالوكالة بين إيران وإسرائيل،https://2u.pw/kyUjAtqX ،تاريخ الإطلاع في(10 /2024/04).
[4] خليفة، مرجع سابق، ص 14.

بعد آخر تتمكن الدولة من خلاله تحقيق أهدافها ومصالحها بواسطة جاذبية النموذج [1]"أي بواسطة الإقناع وهو ما يسمى القوة الناعمة لجوزيف ناي.

ومع التطور الحاصل خلال القرن الواحد والعشرين في المجال التكنلوجي ظهر ما يعرف "**بالقوة الذكية وتعني الجمع بين القوة الصلبة والناعمة بغية التوصل إلى استراتيجية متكاملة**" [2]مع التركيز أكثر على الوسائل اللامادية أي البعيدة عن القوة العسكرية لغرض تحقيق أهداف استراتيجية وسياسية ويتم ذلك بواسطة عدة وسائل أهمها التأثير الثقافي، التأثير الإعلامي، الدعاية عبر وسائل التواصل الاجتماعي، أي الدفاع عن أمنها السيبراني وحتى قد تتمثل القوة الذكية في استطاعة الدولة رد الهجمات السيبرانية للطرف المعتدي على سيادتها كنوع من فرض الهيمنة وإثبات القوة والقدرة على إلحاق الضرر بالخصم.

وقد أثرت التطورات والمستجدات في الفضاء السيبراني على مفهوم القوة في العلاقات الدولية بشكل جلي تمثل في:

2-تغير مصادر القوة وتعدد فواعلها:

فقد أصبح بالإمكان للفواعل الدولية إحداث ضرر دون تدخل عسكري مباشر أي بالاعتماد على الهجمات السيبرانية ونشر الفيروسات التي تؤثر على البنية التحتية للدول وتجعل الحدود السيادية لها مستباحة ومخترقة. فقد أصبح بإمكان فرد واحد تنفيذ هجوم سيبراني يمس قطاعا حساسا في دولة ما أن يربك الأمن والاستقرار الدولي [3].

3-بروز مفاهيم جديدة في العلاقات الدولية:

انطلاقا من التفاعلات الطارئة على مستوى حقل العلاقات الدولية برزت العديد من المفاهيم الجديدة مثل سباق التسلح السيبراني الذي اشتعل منذ عام 2001بين الولايات المتحدة الأمريكية وإيران، وكذلك بين كوريا الشمالية وكوريا الجنوبية. ومفهوم الهيمنة على الفضاء السيبراني خاصة بعد مقترح عسكرة الفضاء الذي حرص عليه الرئيس الأمريكي دونالد ترامب رغبة في الحفاظ على الهيمنة والتفوق الأمريكي على الدول المنافسة كروسيا والصين. وقد تم هذا عبر إنشاء وكالة تنمية فضائية وقيادة فضائية غرضها الأساسي التصدي لحروب الفضاء السيبرانية. هذا ما يعكس زيادة الاهتمام بمجال الأمن السيبراني وتصاعد وتيرة سباق التسلح بين الدول ذات السيادة والاهتمام أكثر بتطوير أدوات الحرب السيبرانية[4] .

3-تراجع دور القوة الصلبة:

[1] خليفة، مرجع سابق، ص 14.

[2] عادل عنتر علي زعلوك، التطور المنهجي لمفهوم القوة في العلاقات الدولية دراسة مسحية في الأدبيات المعاصرة " **المجلة العلمية لكلية الدراسات الاقتصادية والعلوم السياسية** ،م 08،ع16،(جويلية2023)ص ص 251-276.

[3] رشاد، مرجع سابق ،ص 679.

[4] نفس المرجع، ص 181.

حسب جوزيف ناي هناك خمسة عوامل ساهمت في تراجع دور القوة الصلبة حول العالم وقللت من فاعليتها تمثلت في:

- ✓ مفهوم الاعتماد الاقتصادي المتبادل: لأن الدول التي بينها معاملات اقتصادية لا يمكنها المخاطرة والدخول في حرب قد تكون مدمرة بالنسبة للتطور والنمو الاستقرار الاقتصادي وتحقيق الأمن الغذائي لمواطنيها.[1]
- ✓ بروز فواعل أخرى دون الدول القومية: أي أن القوة توزعت ولم تعد حكرا على الدول ذات السيادة وحدها، بل تشاركها الفواعل الأخرى وأصبحت بطبيعة الحال قادرة على التأثير في البيئة الدولية منها المنظمات الدولية بنوعيها الحكومية وغير الحكومية بالإضافة للشركات متعددة الجنسيات والجماعات الإرهابية.
- ✓ انبعاث النزعات القومية: ما صعب عملية إخضاع الجهات المتنازعة للقوة العسكرية أي أن القوة العسكرية لم تعد تأثر مثلما كانت عليه سابقا نظرا للتوجهات الثقافية والمجتمعية في العالم المعاصر.
- ✓ انتشار التكنولوجيا المعاصرة وتطور أساليب القتال: فمع ظهور الحروب الهجينة وتزايد وتيرة الهجمات السبيرانية وتطور الأسلحة النووية لم تعد القوة العسكرية التقليدية فعالة لوحدها ما لم تقترن بعوامل قوة أخرى.
- ✓ ظهور قضايا تعجز القوة الصلبة عن حلها: أي أنها ذات بعد عالمي أولا وغير مرتبطة بالمخاطر العسكرية بل تخص الأمن الإنساني بأبعاده المختلفة مثل: الفقر، المناخ، الأوبئة. كما أن استخدام القوة حاليا أصبح يثقل كاهل الدول أي أنه مكلف مقارنة بالأساليب الحديثة، التي يمكن لها أن تؤثر نفس التأثير أو أقل بقليل من الحروب التقليدية ولكنها جد فعالة في الكثير من الحالات دون الوصول إلى التصعيد والحرب المباشرة[2].

[1] خليفة، مرجع سابق، ص18.
[2] خليفة، مرجع سابق، ص20.

خلاصة الفصل:

- ✓ لقد سلط هذا الفصل الضوء بداية على فهم طبيعة الهجمات السيبرانية وأهم أنواعها وفواعلها وكذا تبيان الفروقات بينها وبين المفاهيم المشابهة ،بالإضافة إلى إدراك التأثير العميق الذي تحدثه هذه الهجمات خاصة فيما تعلق باختراقها للأمن السيبراني للدول وتهديد بنيتها التحتية واستقرارها.
- ✓ كما أسهمت الهجمات السيبرانية في تغيير العديد من المفاهيم البارزة في حقل العلاقات الدولية وتغيير دلالتها فالقوة أصبحت تحمل أبعادا غير مرتبطة بالجانب الصلب والحروب أصبحت تدار بواسطة الحواسيب بعيدا عن ساحة المعركة التقليدية.
- ✓ انطلاقا من معرفة حجم المخاطر والخسائر التي تتكبدها الدول جراء هذه الهجمات السيبرانية أدرك القارئ أهمية تأمين الفضاء السيبراني وكذا ضرورة نشر الوعي العالمي بخطورة التهديدات الجديدة التي جاءت تزامنا مع التطور التقني والمعلوماتي التي نتج عن ثورة التكنلوجيا الحديثة.

الفصل الثاني

العلاقات الروسية الأوكرانية بين السلم والحرب

تمهيد

تعد العلاقة بين دولة روسيا و أوكرانيا علاقة طويلة الأمد، متعددة الأبعاد منها ما هو تاريخي واقتصادي وثقافي. غير أنها في السنوات الأخيرة صارت تعاني من توتر حاد قاد الدولتان مؤخرا إلى مواجهة عسكرية مباشرة، وبناءا على هذا كان لا بد من البحث في تاريخ هاتين الدولتين واكتشاف الأسباب الحقيقية وراء هذا التوتر، وكذا معرفة مدى نجاعة الهجمات السيبرانية في تحقيق مساعي كل من روسيا وأوكرانيا على الساحة الدولية. والإجابة على سؤال هل تمكنت روسيا من كسب الحرب وتحقيق الغلبة أم أن الصراع سيظل مستمرا؟

وفي هذا الإطار تم إدراج ثلاثة مباحث لمناقشة هذه المسائل:

- ✓ المبحث الأول: تاريخ العلاقات الروسية - الأكرانية.
- ✓ المبحث الثاني: الوسائل المستخدمة في الحرب الروسية- الأوكرانية سنة 2014.
- ✓ المبحث الثالث: استمرار المواجهة في الفضاء السيبراني بين روسيا وأوكرانيا.

المبحث الأول: تاريخ العلاقات الروسية الأوكرانية:

تمتد العلاقات الروسية الأوكرانية إلى العصور القديمة أي أكثر من ألف سنة بداية من تأسيس الدولة السلافية الأولى" كيفان الروس" الإمبراطورية التي أسسها الفايكنغ(viking) في القرن التاسع الميلادي حتى منتصف القرن الثالث عشر في أجزاء ما يعرف اليوم بروسيا وأوكرانيا وبيلاروسيا[1].ويعد الواقع الأوكراني جد معقدا فهو امتداد عبر التاريخ من فترات سلم إلى فترات حرب، بداية من تعرضها للتقسيم من طرف العديد من الإمبراطوريات المختلفة سواء المجرية أو السلوفاكية أو حتى روسيا القيصرية آنذاك وصولا إلى إعلان جمهورية الشعب الأوكراني للمرة الأولى تاريخياً ثم استقلالها وهذا سنة 1917 حيث كانت تضم الأقاليم الشرقية فقط من أوكرانيا الحالية.[2]

المطلب01:العلاقات الروسية الأوكرانية خلال فترة الاتحاد السوفياتي

مع نهاية القرن الثامن عشر حتى بداية القرن العشرين اعتبرت الأراضي الأوكرانية جزءا من الإمبراطوريتين النمساوية ثم المجرية ثم الروسية. كما شارك الأوكرانيون آنذاك في العديد من الحروب حيث عانت أوكرانيا من الدمار الكبير الذي خلفته الحرب العالمية الأولى ثم ضمها قسريا إلى اتحاد الجمهوريات السوفيتية الاشتراكية الذي تأسس في 30 ديسمبر1922 كإحدى الجمهوريات المؤسسة له. ففي الوقت الذي حافظت فيه بولندا على إقليمها وسيادتها فشلت أوكرانيا في الحفاظ على استقلالها وأصبحت تسمى جمهورية أوكرانيا الاشتراكية السوفياتية كما فرض الاتحاد السوفياتي عليها العديد من العقوبات وصادر جميع المنتجات مما أدى إلى انهيار اقتصادي في المنطقة[3]. وبعد نهاية الحرب العالمية الثانية، تم دمج الأقاليم الغربية من أوكرانيا إلى جمهورية الشعب الأوكراني وانضمت أوكرانيا وكان اسمها جمهورية أوكرانيا السوفييتية

---

[1] يارا عبد الجواد، "التوجهات الاستراتيجية لروسيا الاتحادية وعلاقتها مع الغرب"، ***مركز قضايا ونظرات*** ، (جويلية 2022)ص 28.

[2]"روسيا وأوكرانيا الإخوة الأعداء: قصة الخلاف بين روسيا وثاني أكبر جمهوريات الاتحاد السوفياتي ،"في https://2u.pw/0bnI8CoU ،تاريخ الاطلاع(2024/04/23).

[3]– Origins History of Ukraine, https://ukraine.ua/explore/origins-history-of-ukraine/ (24/04/2024).

الاشتراكية إلى روسيا وشكَّلا معاً نواة اتحاد الجمهوريات السوفييتية الاشتراكية، أو الاتحاد السوفييتي كما بات معروفاً إعلامياً."[1]

وبالعودة إلى الفترة التي تلت الثورة البلشفية سنة 1917وتقلد لينين لمقاليد الحكم في روسيا أجرى العديد من التغييرات على مستوى النظام الاقتصادي في البلاد عبر المرور بفترة انتقالية حتى يتمكن الشعب الروسي من قبول النظام الاشتراكي في حين يتم تطبيق النظام الرأسمالي بشكل محدود للنهوض بالاقتصاد وذلك من خلال سياسته المعروفة بالنيب (NEP)أي أنه فرض الضرائب على الفلاحين في روسيا الذين منحوا الحرية في بيع منتجاتهم، كما سمح بإدارة المعامل الكبرى دون تملكها والاستثمار الأجنبي بشرط أن يكون تحت رقابة الدولة بهذا شهد الاقتصاد الروسي نموا ملحوظا.[2]

لكن ما إن استلم ستالين السلطة بعد وفاة لينين سنة 1924 حتى بدأ في عملية تصفية معارضيه سواء من التيار اليساري بزعامة ليون تروتسكي (Leon Trotski) نظرا لتعارض وجهات النظر بينه وبين ستالين ثم بعدها التيار اليميني بقيادة زينوفيف (Zinoviev) وليون كامينيف (Leon Kamenev) واستولى على مقاليد الحكم لغرض تطبيق سياسة النيب التي بدأ في تطبيقها لينين قبل وفاته كمرحلة أولية، ليتم توطيد النظام الاشتراكي داخل روسيا ثم تصديره أخيرا إلى خارج الحدود الروسية.[3] وكانت سياسة النيب بالنسبة لستالين مجرد مرحلة انتقالية الهدف لبلوغ تحويل الاتحاد السوفياتي من دولة زراعية إلى دولة صناعية وتحقيق النمو الاقتصادي والبعد عن التبعية للدول الأجنبية ذات النظام الرأسمالي.[4]

وفي إطار سعي ستالين ذلك سن مجموعة من القوانين التي من شأنها النهوض بالقطاع الصناعي، ودعم الإنتاج المحلي، وقام بالعديد من الإصلاحات كان أبرزها نظام المزارع المشتركة أو الجماعية التي تمكن الجماعات التعاونية من المزارعين من بيع نصف المحصول إلى الحكومة السوفياتية، في حين تتلقى مقابل ذلك مبلغا ماليا تقوم السلطات الرسمية للدولة بتحديده، أما ما تبقى فيتم توزيعه على الفلاحين والعمال حسب نسبة عمل

---

[1] "روسيا وأوكرانيا الإخوة الأعداء: قصة الخلاف بين روسيا وثاني أكبر جمهوريات الاتحاد السوفياتي"، المرجع السابق.

[2] أحمد محمد جاسم، ستار محمد علاوي،" التطورات الداخلية في الاتحاد السوفيتي 1924 – 1939"، ***مجلة ديالى***، ع.57(2013)،ص ص 1-36.

[3] – المكان نفسه..

[4] ماهر الشريف،،السياسة الاقتصادية الجديدة (النيب): استراحة محارب، https://2u.pw/5sPKFPp3،(2024/04/26).

كل فرد منهم[1]وبعد مدة من الزمن "**بدأت الدولة تؤسس نوعاً آخر من المزارع يكون تابعاً لها مباشرة وهي مؤسسات زراعية اشتراكية ...تابعة للدولة وتخصص لزراعة الحبوب والقطن وتربية المواشي وزراعة الأشجار المثمرة والحمضيات وغير ذلك**"[2] كما أن المداخيل أصبحت مضاعفة إلى خزينة الاتحاد السوفياتي أي أن الخطة بدأت في تحقيق أهدافها تدريجيا

وهنا لا بد من الإشارة إلى أن هذه السياسة المنتهجة من قبل الاتحاد السوفياتي لم تلق قبول كبيرا من طرف الفلاحين الذين يمثلون نسبة كبيرة من المجتمع السوفياتي على اعتبارها سياسة جائرة في حقهم، واستغلالية إلى حد كبير لجهودهم واستنزاف لقدراتهم ، خاصة الأوكرانيين باعتبار المنطقة زراعية بامتياز، بل حتى أن فكرة السيطرة على أوكرانيا أساسا كان لاعتبارها مصدر لإمدادات الحبوب للتصدير لاحقا، وتحويل الاتحاد السوفياتي إلى قوة صناعية باستعمال موارده المتاحة فسكان أوكرانيا ينتمي أغلبهم إلى فئة الكولاك وقادرين على إحداث الفرق الاقتصادي.[3] وبعد النجاح النسبي الذي حققته الخطة الخماسية الأولى، بدأ ستالين في تطبيق الخطة الخماسية الثانية 1933-1937 التي كانت تهدف إلى تصفية الكولاك* الذين استطاعوا جمع ثروة لا بأس بها، وأصبحوا بالنسبة لستالين يمثلون طبقة خبيثة من المجتمع وتم اعتقال الكثير منهم ونفى أخرين إلى سيبيريا بعد مصادرة كل أملاكهم.[4]

بالإضافة إلى الفظائع التي لحقت تنفيذ المزارع الجماعية أي التابعة للحكومة السوفياتية مع جزء بسيط للعامل فيها فقد سجل التاريخ موت "**ما يقارب خمسة ملايين مواطن من الجوع، لأنهم رفضوا تنفيذ المشروع بالإضافة إلى أكثر من خمسة ملايين غيرهم نقلوا للعمل في سيبيريا، كما تم بيع القمح المصادر من الفلاحين**

---

[1] –أحمد محمد جاسم ، علاوي ،مرجع سابق ، ص8.

[2] – **نفس المرجع**، ص 11.

***الكولاك:** ظهرت تسمية كولاك أواخر حقبة الإمبراطورية الروسية. وعن طريق كلمة كولاك، يشير المسؤولون الروس حينها لطبقة الفلاحين الذين امتلكوا ما يزيد عن 3.2 هكتار من الأراضي أي كبار ملاك الأراضي وأغلبهم من منطقة أوكرانيا التي تعد من المناطق الزراعية بامتياز وقد سعت هذه الفئة من المجتمع إلى الحفاظ على مكانتها حتى في ضل فترة حكم الستالين التي تميزت بجملة الإصلاحات في المجال الزراعي والصناعي كذلك.

[3] Holocaust and Genocide Studies ,University Of Minnesota , https://2u.pw/twmjSzcO (29/04/2024).

[4]طه عبد الناصر رمضان، اجتثاث الكولاك هكذا أباد السوفييت الآلاف من فلّاحي أوكرانيا، في https://2u.pw/0G4Z9u0O تاريخ الإطلاع (2024/04/27).

للمرابين اليهود الذين تمكنوا من احتكاره " [1]و تعد فترة الثلاثينيات من القرن العشرين من أصعب الفترات خاصة على الشعب الأوكراني بداية من سنة 1930 إلى 1933 حيث تم استخدام كل أساليب القمع ضده بالإضافة إلى عمليات التطهير للمثقفين وأعضاء من الحزب الشيوعي وصل عدد الضحايا حسب الإحصائيات إلى ملايين الأوكرانيين، والغرض من هذه العمليات الإجرامية هو شعور ستالين بالتهديد من سعي الأوكرانيين إلى استقلالهم عن الاتحاد السوفياتي خاصة وأن أوكرانيا تضم فئة كبيرة من المثقفين المتمردين على الحكم الشمولي لستالين، أي أن الزعيم السوفياتي أراد منع الثورة المضادة الوطنية في أوكرانيا[2] بالإضافة إلى المجاعة التي عانى منها الشعب الأوكراني نظير تمرده على السلطة الحاكمة التي أصدرت سنة 1932قانون يجرم أي سرقة للحبوب باعتبارها ملكية اشتراكية، وأن أي محاولة لسرقة ما يزيد عن كيس من القمح يعرض صاحبها إلى الموت رميا بالرصاص. ونتيجة لهذه القوانين لم يعد هناك من الغذاء ما يكفي للعائلات الأوكرانية وازدادت المجاعة في مقابل هذا قام الاتحاد السوفياتي بتصدير أكثر من مليون طن من الحبوب إلى الدول الأوروبية حسب ما تشير إليه الإحصائيات[3]

ويمكن القول أن العلاقة بين أوكرانيا والاتحاد السوفياتي منذ سنة 1920 إلى غاية انفصالها عنه وإعلانها دولة مستقلة سنة 1991 تميزت بكونها متوترة وقائمة على فكرة السيطرة والاستنزاف لثروات الشعب وجهوده، رغبة في بناء اقتصاد سوفياتي قوي وتحقيق النظام الاشتراكي الذي سعى له لينين ومن بعده ستالين وتوسيع النفوذ الروسي في منطقة أوروبا الغربية، والسيطرة على الدويلات المجاورة لضمان حماية إقليمها من أي تدخل يمكن له أن يهدد الأمن والسلم في منطقة أوروبا الغربية سيما خلال الحرب الباردة الممتدة من 1945 إلى غاية انهيار الاتحاد السوفياتي سنة 1991. وقد استقلت أوكرانيا عن الاتحاد السوفياتي عن طريق استفتاء تقرير مصير شعبها، وصوتت الأغلبية الساحقة لصالح الانفصال. وقد قامت كل من روسيا وأوكرانيا بتوقيع اتفاقية شراكة بينهما ثم بعد مدة أي في عام 1994 وقعت اتفاقية شراكة مع حلف الشمال الأطلسي وكان هذا بمثابة بداية قصة التصادم بين روسيا وأوكرانيا.

---

[1] – أحمد محمد جاسم ، علاوي، **مرجع سابق** ، ص.11.

[2] The War in Ukraine — Interwar Soviet Ukraine (1922–1939)، UCONN University of Connecticut, https://2u.pw/PKg4ZBK6 ،(30/04/2024).

[3] –The famine of 1932–33 (Holodomor)،Britannica, https://2u.pw/iee0uxoa ,(29/04/2024).

الشكل 04: يمثل خريطة توضيحية للحدود الروسية الأوكرانية بعد تفكك الاتحاد السوفياتي.

المصدر: "اللحظات المحورية في تاريخ العلاقات بين أوكرانيا وروسيا "،الشرق الأوسط صحيفة العرب الأولى،27مارس 2022، https://2u.pw/fqGSaXh .

المطلب 02: العلاقات الروسية الأوكرانية بعد انهيار الاتحاد السوفييتي

رفض الاتحاد السوفياتي إعلان أوكرانيا استقلالها في البداية، وحاول الإبقاء على هيمنته في المنطقة من خلال محاولة انقلاب سنة 1991، وفشلت في النهاية ليتم اعتماد قانون إعلان الاستقلال في 24أوت من نفس السنة، وبعد المصادقة عليه جرى الاستفتاء الشعبي الذي انتهى بنسبة 90% نعم لاستقلال أوكرانيا.[1]وبعد تفكك الاتحاد السوفياتي ونجاح أوكرانيا في الحصول على استقلالها كدولة ذات سيادة كان لا بد لها من بناء دولة قائمة على أسس تمكنها من الحفاظ على إقليمها من أي اختراق قد يطاله. بالإضافة إلى بناء اقتصاد قوي وكذا إدارة علاقاتها مع روسيا ومحاولة بناء هوية مستقلة عنها على الرغم من التاريخ المشترك الذي جمعهما. وفي المقابل بقيت روسيا تنظر إلى أوكرانيا على أنها جزء من مجال نفوذها في منطقة أوروبا الشرقية، ولا يمكن

[1] –How Ukraine prepared for the declaration of independence as part of the USSR: the adoption of the Declaration of Sovereignty of Ukraine، https://2u.pw/49AHzZwZ ، (03/05/2024).

التخلي عنها لأنها بالنسبة للروسيين جزء من الاتحاد السوفياتي سابقا وفاعل أساسي في معادلة الأمن القومي الروسي حاليا[1].

وقد تباينت مواقف الفصائل المكونة لدولة أوكرانيا بعد انفصالها فمنها فئة الناطقين باللغة الروسية يظهرون دعمهم للاستقلال السياسي لأوكرانيا في حين يؤيدون التقارب الثقافي بين روسيا وأوكرانيا. وعلى العكس من هذا يفضل القوميون الأوكرانيون بناء علاقات قوية مع الدول الأوروبية رغبة في بناء هويتهم المستقلة، بالإضافة إلى الحفاظ على استقلالهم، أي ضمان الأمن لدولة أوكرانيا عن طريق التقارب الأوروبي الأمريكي وبناء علاقات وطيدة مع حلف الناتو في حالة التعرض لأي هجوم من طرف العدو الروسي حسب نظرة القوميين الأوكرانيين. وقد أشار مسح أجري عام 1997 للنخب في أوكرانيا إلى أن% 70 يفضلون الارتباط بالاتحاد الأوروبي على الارتباط بروسيا من جديد، وهو ما يؤكد على الرغبة الملحة لأوكرانيا في بناء هويتها المستقلة عن النهج الروسي وتقاربها مع أوروبا رغبة في حماية مصالحها.[2]

أما في الجانب الاقتصادي فقد كان لتفكك الاتحاد السوفياتي أثرا كبير اعلى الاقتصاد الأوكراني نظرا لأنه كان يعتمد بشكل كبير على التصنيع وخاصة الصناعات الثقيلة التي تم تطويرها بغرض التصدير لروسيا آنذاك رغم أن أوكرانيا كانت دولة زراعية أكثر من كونها صناعية، لكن خطط الزعماء السوفيات فرضت العديد من السياسات الواجب إتباعها من قبل الأوكرانيين لتطوير اقتصاد دول الاتحاد السوفياتي، وتحقيق الاكتفاء الذاتي، هذا ما أدى إلى انهيار جذري لاقتصاد البلاد بعد انفصال أوكرانيا عن الاتحاد السوفياتي.[3]

بالإضافة إلى انخفاض الناتج المحلي الخام سنة 2014 بنسبة 35%مقارنة بعام 1990وقد تحولت أوكرانيا إلى أفقر دولة في أوروبا وشهد الاقتصاد تضخما كبيرا أثر بشكل كبير على المستوى المعيشي للمواطنين الأوكرانيين.[4] ومنه يمكن القول أن تفكك الاتحاد السوفياتي كان بمثابة بداية أزمة اقتصادية داخل أوكرانيا، اتسمت بالتضخم المفرط وانخفاض الناتج المحلي بالإضافة إلى ضعف الهيكل المؤسساتي للدولة الجديدة،

---

[1] علي مفتاح علي شاوش ، "تأثير الأزمة الأوكرانية على العلاقات الروسية الغربية "، ***مجلة جامعة بني وليد للعلوم الإنسانية والتطبيقية*** ، ع 29(2023/09/20) ص ص.339-358.

[2] –المكان نفسه

[3] –. James M. Boughton، 8 After the Fall: Building Nations out of the Soviet Union، https://2u.pw/qX3rAXo9، (03/05/2024).

[4] PEKKA SUTELA، Ukraine's Economy Since 1991، https://n9.cl/6e7t8، (04/05/2024).

وخسارة أكبر شريك اقتصادي وهو روسيا، وهي كلها عقبات واجهت الحكومة الأوكرانية في طريقها إلى ضمان استقلال شعبها وتحقيق النمو الاقتصادي في البلاد، رغم مرورها بفترات نمو إلا أنها لا تزال عرضة للمؤثرات الخارجية في البيئة الدولية وتواجه الكثير من التحديات الاقتصادية.

المطلب 03: القضايا الخلافية في العلاقات الروسية الأوكرانية والتصعيد نحو الحرب.

تميزت العلاقات الروسية-الأوكرانية بالتذبذب فتارة تعرف استقرارا وتارة أخرى تسير في طريق التصعيد وتشهد العديد من الأزمات التي من شأنها أن تكون حاجزا دون بناء علاقات ودية مبنية على حسن الجوار وتحقيق السلم والأمن في المنطقة. فمنذ انفصال أوكرانيا عن الاتحاد السوفياتي بقي جزء من الترسانة السوفياتية النووية في أوكرانيا بلغت أنداك "**حسب الإحصائيات ما يقرب 175 صاروخاً بعيد المدى و أكثر من 1800 رأس نووي** "[1]. وقد تم التوقيع على مذكرة بودابست سنة 1994 بين روسيا بقيادة بوريس يلتسن وأوكرانيا بزعامة ليونيد كرا فتشوك وبيل كلينتون في الجانب الأمريكي، تضمنت تخلي أوكرانيا عن أسلحتها النووية في مقابل ضمانات أمنية تمكنها من الحفاظ على حدودها وعدم المساس بسيادتها واستقلاليتها. وقد تعهدت أمريكا بحمايتها في حال تم غزوها من طرف روسيا. [2]هذا الوعد المقدم من طرف روسيا ولم تستطع الحفاظ عليه من خلال غزوها لشبه جزيرة القرم سنة 2014 شدد من حدة الصراع القائم بين الطرفين، واتجهت العلاقات إلى التصعيد، وبشكل أكثر حدة من خلال غزوها لأوكرانيا سنة 2022 رغبة في الحد من توسع حلف الناتو على حدودها الغربية ،وضمانا لأمن حدودها. ففي العلاقات الدولية أكثر ما تحاول الدولة الحفاظ عليه هو أمنها القومي وعند الشعور باي تهديد يمكن أن يعيق عملية تحقيقه لا بد من التدخل ولو بالقوة العسكرية على حساب أوكرانيا لضمانه.

وبالعودة إلى التاريخ تعتبر روسيا أوكرانيا امتدادا طبيعيا لها بدليل الثقافة المشتركة ووجود ما يمثل 24%من سكان أوكرانيا ذوي أصول روسية، فهي دائما تسعى أن تبقي أوكرانيا تحت رقابتها ولا تنحاز بأي شكل من الأشكال إلى الدول الأوروبية، وذلك استنادا لما صرح به الرئيس الروسي فلاديمير بوتين في خطاب له

[1] ثالث أكبر ترسانة في العالم. كيف جُرّدت أوكرانيا من أسلحتها النووية؟ ، https://2u.pw/RWC0eV7i ، (2024/05/04).

[2] – كلينتون «نادم» لضغطه على أوكرانيا للتخلي عن ترسانتها النووية عام 1994، https://2u.pw/YsQpgJxW ،(2024/05/04).

سنة2005[1]، أي أن روسيا دائما تتحسر على خسارة أوكرانيا باعتبارها منطقة ذات أهمية حيوية لمصالحها الجيوسياسية والاقتصادية، فضلاً عن كونها جزءاً من هويتها التاريخية والثقافية التي لا يمكن تجاهلها في معادلة روسيا للحفاظ على مكانتها في المنطقة. ومن هذا المنطلق شهدت العلاقات الروسية الأوكرانية العديد من الأزمات أهمها:

1-أزمة شبه جزيرة القرم:

بعد انفصال أوكرانيا عن الاتحاد السوفياتي اعتبرت شبه جزيرة القرم جمهورية تتمتع بالحكم الذاتي داخل دولة أوكرانيا وظلت هكذا إلى غاية سنة 2014، بعد الاحتجاجات التي أقيمت في أوكرانيا تمردا على حكم الرئيس فيكتور يانوكوفيتش (Viktor Yanukovych) الموالي لروسيا، تمت الإطاحة به في ثورة يطلق عليها الأوكرانيون ثورة الكرامة ،والمطالبة في نفس الوقت بانضمام دولة أوكرانيا إلى الاتحاد الأوروبي وإلى حلف الشمال الأطلسي للتخلص من التبعية لموسكو وحماية أوكرانيا من أي اعتداء قد يطال أراضيها[2]، وفي ظل كل هذه الأحداث، قامت أوكرانيا بحل البرلمان في شبه جزيرة القرم واستغلت روسيا هروب الرئيس الأوكراني إلى أراضيها وقام الرئيس الروسي فلاديمير بوتين بإلقاء خطاب في شبه جزيرة القرم أكد فيه على التاريخ المشترك للمنطقتين وأحقية روسيا في هذه الأراضي، رغبة في التعبئة وكسب الرأي العام[3]

وخلال الفترة الحرجة التي كانت تمر بها أوكرانيا والفراغ السياسي الحاصل استغلت روسيا هذه النقطة عن طريق إرسالها لمجموعة من الأفراد المسلحين إلى مراكز حكومية في القرم، وتم برمجة استفتاء شعبي في 16 مارس 2014حظي بالأغلبية الساحقة لصالح الانضمام إلى روسيا وتم ضمها. وقد لقي هذا القرار العديد من ردود الفعل الدولية المتباينة منها من أيدت قرار روسيا ومنها ما استنكرت هذا الفعل واعتبرته تعدي على سيادة أوكرانيا واقتطاع من أقاليمها. إن الدول الغربية ليس من مصلحتها ضم روسيا لشبه جزيرة القرم، لذالك قامت بفرض العديد من العقوبات على الدولة الروسية خاصة في الجانب الاقتصادي، وانطلاقا من كل هذه المعطيات يعتبر ضم شبه جزيرة القرم ذو أهمية كبيرة بالنسبة لروسيا نظرا لأنها منطقة استراتيجية تتمكن عبرها روسيا من تصدير الغاز إلى كل دول أوروبا الغربية المستوردة، في حين تعتبرها أوكرانيا تصرف غير شرعي

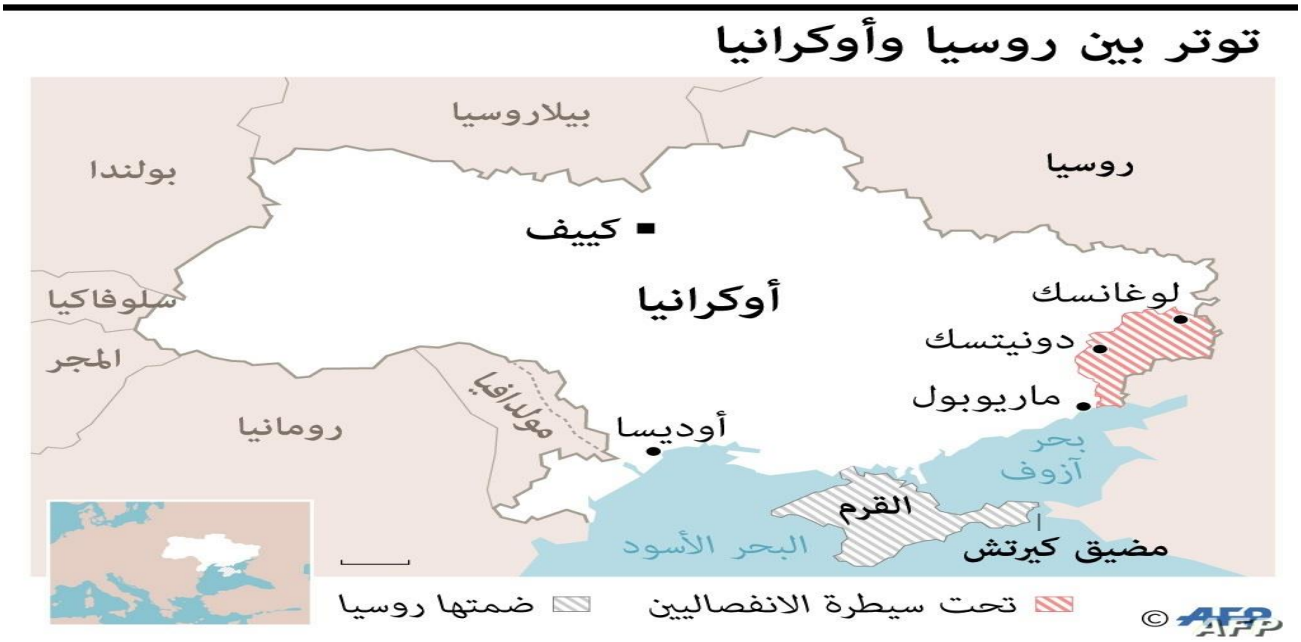
[1] عبد الجواد، مرجع سابق، ص. 28.

[2] خيري فرجاني، **أوكرانيا والأمن القومي الروسي**، (القاهرة: دار البيان،2020) ،ص5.

[3] رامي القليوبي، ثماني سنوات على ضم القرم: حين بدأ ابتلاع أوكرانيا، https://2u.pw/OCFeU7uE ، (2024/05/08).

اقتطاعا من أراضيها أي استغلال وجود نسبة كبيرة من الروس في المنطقة بذريعة ضمها إلى الدولة الروسية وتعد هذه القضية من أبرز القضايا المتنازع حولها بين الدولتين.

الشكل رقم 05: خريطة توضح موقع شبه جزيرة القرم



المصدر: منطقة توتر بين روسيا وأوكرانيا...حقائق عن بحر الأزوف، https://2u.pw/S8p0TeF3 ، (2024/05/12).

2- مسألة توسيع عضوية الناتو:

إن السبب الرئيس الذي أنشئ من أجله حلف الشمال الأطلسي منذ سنة 1949هو ردع التوسع السوفياتي في العالم، أي الدفاع المشترك على اعتبار أن أي تهديد قد يطال سيادة دولة ما عضوة يشكل تهديدا جماعيا، تعهدت الدول العضوة بمواجهته عبر حشد كل إمكانياتها. ومع انهيار الاتحاد السوفياتي وبروز الأحادية القطبية ظل الحلف الأطلسي محافظا على المبادئ التي قام عليها. وبما أن الاتفاقية التأسيسية لهذا الحلف نصت على أن أي دولة أوروبية تتوفر على شروط الانضمام للحلف يمكنها ذلك بناءا على "سياسة الباب المفتوح"، سعت أوكرانيا إلى ذلك رغبة في كسب التأييد والحماية والتقارب مع دول الاتحاد الأوروبي في حالة الهجوم الروسي على أراضيها، وهذا ما شكل بالنسبة لروسيا تهديدا لحدودها وأن وجود الحلف على مستوى الحدود الروسية في أوكرانيا يعد بمثابة محاولة انتهاك لسيادة دولة روسيا وتهديد أمنها القومي. ومن خلال تتبع

تاريخ العلاقات الروسية-الأوكرانية يتضح أن روسيا كلما شعرت بتهديد لمصالحها واستقرارها من قبل الدول الأوروبية عبر السماح للجمهوريات السوفياتية السابقة بالانضمام لهذا الحلف العسكري أو حتى التقارب الأوروبي وصعود أصوات داخل أوكرانيا تنادي بالتخلص من التبعية لروسيا تقوم بانتهاج سياسة تحذير، وفي حال التمرد تقدم على القيام بعمليات عسكرية كرادع لدولة أوكرانيا وحفاظا على أمن حدودها بالدرجة الأولى وأبرز مثال على ذلك غزو القرم في 2014 وكذلك الغزو الروسي للأوكرانيا منذ سنة 2021 إلى يومنا هذا.

3-دعم الانفصاليين في أوكرانيا:

من أهم السياسات التي انتهجها روسيا لاستمرار سيطرتها على منطقة أوكرانيا هي دعم الجماعات الانفصالية داخل الحدود الأوكرانية خاصة في المناطق التي يكون فيها عدد كبير من الناطقين بالروسية، وأغلبها تقع في الجزء الشرقي من البلاد أي المناطق التي لها حدود مع روسيا. وبحلول الأزمة السياسية التي شهدتها أوكرانيا سنة2013 المتمثلة في تعليق الرئيس الأسبق الأوكراني يانوكوفيتش لاتفاقيات الشراكة مع الاتحاد الأوروبي وسط سخط شعبي كبير و عزله عن السلطة، في ظل أزمة داخلية محتدم، قامت روسيا بغزو شبه جزيرة القرم وإعلان انفصال إقليمي اللوغانسك ودونيتسك (Donetsk and Luhansk) عن أوكرانيا وإعلانهما جمهوريتين تابعين لروسيا [1].

وتمت هذه العملية عبر استلاء المتمردين المسلحين في المنطقة الشرقية المدعومين من روسيا على المباني الحكومية وأعلنوا عن الجمهوريتين، حيث أشار الرئيس الروسي فلاديمير بوتين إلى أن هاتين المنطقتين جزء من تاريخ روسيا "**واعتبر أن هذه المناطق لم تكن جزءا من أوكرانيا خلال الحقبة القيصرية بل منحت الحكومة السوفياتية هذه المناطق لأوكرانيا في عشرينات القرن الماضي**"[2] ويعد هذا الانفصال الثاني بعد ضم شبه جزيرة القرم إلى روسيا الاتحادية.

أما عن أهمية منطقتي دونيتسك ولوغانسك(Donetsk and Luhansk) فتمثلان منطقة صناعية بامتياز، يساوي عدد سكانها حوالي 6.5 مليون نسمة وأغلبهم ناطقون بالروسية يعتمدون على التنقيب عن الخامات والمعادن والمواد الكيميائية وتصنيعها ثم تصديرها. ونشير إلى إن اقتصاد هذه المنطقة كان مربوطا بروسيا إلى حد كبير بناءا على هذه المعطيات رأى أصحاب الأعمال الحرفية أن مصالحهم لن تتناسب مع اتجاه

[1] علي سعدي عبد الزهرة جبير، المعهد العراقي للحوار،، https://2u.pw/59R0I7P ،تاريخ الإطلاع (2024/05/09).
[2] – المكان نفسه.

أوكرانيا نحو الدول الغربية لهذا كان لا بد من معارضة توجهات الحكومة الأوكرانية والوقوف ضدها وفي المقابل المطالبة بالاستقلال عنها والانضمام إلى روسيا للحفاظ على مصالحهم[1].

وبخصوص رد فعل أوكرانيا فاعتبرت هذا الأمر غير شرعي ويمس بسيادة وحدود أوكرانيا التاريخية، وبهذا فإن أهم القضايا التي تشكل أسبابا لتوتر العلاقات بين كل من روسيا وأوكرانيا هي قضايا حدودية متعلقة بالبعد التاريخي بالإضافة إلى ارتباطها الوثيق بالتفسير الواقعي للعلاقات الدولية في إطار ما يسمى بالمعضلة الأمنية حيث ترى روسيا أن أي تحرك أو سياسة تنتهجها أوكرانيا تمثل بالضرورة تهديد للأمن القومي لروسيا الاتحادية. رغم مطالبة من الغرب ضمانات عن عدم توسع حلف الناتو شرقا إلا أنها لم تف بوعودها ، وبهذا تقوم روسيا برسم سياسيات خارجية دفاعية عن سيادتها تكون عبر استخدام القوات العسكرية ووسائل حرب أخرى (سيتم الحديث عنها في المبحث الموالي)،حتى تكون في منأى عن وصول حلف الشمال الأطلسي إلى حدودها الغربية وتصبح في خوف وتهديد مستمرين بالإضافة إلى فكرة أن روسيا ترى في أوكرانيا منطقة استراتيجية لا يمكن بأي شكل من الأشكال التخلي عنها أو تسليمها للغرب، وقبول انضمامها إلى الحلف الأطلسي أو الاتحاد الأوروبي بمثابة السماح بانتهاجها نهج يختلف عن تطلعات بوتين ويتعارض مع مصالح دولة روسيا.

[1] مايكل، كوفمان وآخرون "عبر من عمليات روسيا في شبه جزيرة القرم وشرق أوكرانيا"، ***مؤسسة راند***،ص50

المبحث الثاني: الوسائل المستخدمة في الحروب الروسية الأوكرانية سنة 2014

لم تعد القوة العسكرية وشن الحروب على الدول بمثابة الخيار الأمثل الذي تستعمله الدول للدفاع عن مصالحها، بسبب أن الحروب تعتبر جد مكلفة وتستنزف اقتصاد الدولة ويتم تجريمها دوليا. وفي المقابل هناك العديد من الوسائل التي يمكن أن تستخدمها الدول للتعبير عن تطلعاتها والحفاظ والدفاع عن أمنها القومي، ولكن في العديد من المواقف يكون استخدام خيار واحد غير كاف لتحقيق الانتصار والحفاظ على أمن الدولة من أي تهديدات خارجية. لهذا ظهر ما يسمى بالحروب الهجينة التي تستعمل كلا الخيارين العسكري وغير العسكري للدفاع عن أمنها وتحقيق مصالحها في البيئة الدولية.

المطلب 01: الوسائل العسكرية في الحرب الروسية الأوكرانية ودورها في حسم المعارك

أثبت غزو شبه جزيرة القرم للعالم أن روسيا مستعدة لاستعمال القوة العسكرية عندما يتعلق الأمر بمصالحها السياسية نظرا للإمكانيات الكبيرة التي تمتلكها روسيا في إطار تنسيق التحركات السياسية والعسكرية للجماعات المسلحة المناط بها القيام بهذه العمليات العسكرية. وهذا ما جعل أوكرانيا والدول الغربية في حالة توتر دائم على اعتبار عدم توفر معلومات كافية حول حجم الإمكانيات الروسية ومدى استعدادها لتوظيف كل هذه الإمكانيات لتحقيق النصر في هذه العملية العسكرية على أراضي أوكرانيا[1].

ونظرا للاعتماد الكبير لروسيا على عائدات الغاز الطبيعي الذي يتم تصديره إلى دول أوروبا عبر الأراضي الأوكرانية بالإضافة إلى الاعتماد عليه من طرف أوكرانيا بنسبة تفوق 60%،فإن روسيا لا يمكنها بأي شكل من الأشكال أن تتنازل عن دورها في هذه المنطقة ذات الأهمية الاستراتيجية، مع العلم أن روسيا تعتبر أوكرانيا جزء استراتيجيا مهما في مجالها الحيوي نظرا لأنها تشكل منطقة عازلة بينها وبين الغرب، وكذا دول أوروبا الشرقية التي انظمت لحلف الناتو بالإضافة إلى اعتمادها كممر لتمرير الغاز الروسي كنافذة نحو البحر الأسود حيث يوجد الأسطول الروسي المتمركز بقاعدة سيفاستوبول (Sevastopol base)[2].

لهذا يلاحظ من خلال تتبع مسار الصراع الروسي الأوكراني أنه تضمن كل الوسائل والأساليب الممكنة لتحقيق مكاسب وتحقيق أكبر قدر من الأمن لدولة روسيا وإبعادها عن الأطماع الغربية في المنطقة بالإضافة

[1] Johan Nordberg، The Use of Russia's Military in the Crimean Crisis، https://n9.cl/t7glf، (10/05/2024)

[2] نادية ضياء شكارة، **تداعيات الأزمة الأوكرانية على العلاقات الروسية الأوكرانية 2014-2016**، *جامعة النهرين بكلية العلوم السياسية*، م.20، ع."(2017)،ص ص 433-456.

إلى قمع أي محاولة تقارب أوكرانية غربية، حيث تعددت الوسائل والأساليب التي استخدمتها روسيا في إطار حربها على أوكرانيا سنة 2014 في إطار محاولتها لضم شبه جزيرة القرم وإقليمي اللوغانسك دونيتسك ومنها الوسائل العسكرية أي الأسلحة الخفيفة والمدفعيات التي استخدمت ضد دولة أوكرانيا، بالإضافة إلى القوات الخاصة الروسية. كما أن روسيا قد استخدمت مجموعة من المرتزقة والمعارضين للنظام الأوكراني وأغلبهم من الناطقين باللغة الروسية رغبة في التمرد والدفاع على المصالح الروسية داخل أوكرانيا وقدمت لهم في المقابل الدعم اللوجستي والاستخباراتي[1] اللازم لتنفيذ هذه المهام

فالنسبة لدولة روسيا إما أن تحقق هذه العملية العسكرية أهدفها أو ستكون هناك عملية أكبر بإمكانها حسم النتيجة وبهذا سعت إلى أخذ الموافقة من مجلس الاتحاد الروسي وباشرت في العمليات العسكرية على شرق أوكرانيا يوم 27فيفري 2014[2]، وبالإمكان القول أن هذه العملية قد نجحت في تحقيق أهدافها ألا وهي ضم شبه جزيرة القرم إلى روسيا بالإضافة إلى إعلان انفصال الجمهوريتين اللوغانسك دونيتسك.

المطلب 02: نتائج الحرب الروسية الأوكرانية سنة 2014

بداية من سنة 2014 اندلعت الحرب الروسية الأوكرانية بعد غزو روسيا شبه جزيرة القرم كان ذلك بعد الاحتجاجات التي شهدتها شوارع العاصمة كييف من طرف معارضين لسياسة الرئيس فيكتور يانوكوفيتش الذي كان مواليا لروسيا، في الوقت نفسه اشتدت حدة النزاعات في منطقة الدونباسك الشرقية ما جعل الانفصاليون المدعومون من الحكومة الروسية يتدخلون في المنطقة لحماية الأقليات الناطقة باللغة الروسية، ومن هنا اشتد التوتر بين الدولتين.

وانطلاقا من هذا نتج عن الحرب الروسية الأوكرانية في سنة 2014 العديد من الأحداث والمخرجات أهمها ما يلي:

- نتج عن الحرب الروسية الأوكرانية ضم شبه جزيرة القرم إلى روسيا ما نتج عنه إدانة دولية كبيرة لروسيا على اعتبارها غزو لإقليم الدولة المجاورة وهي أوكرانيا.

[1] عصام عبد الشافي، الحرب الروسية–الأوكرانية ومستقبل النظام الدولي، https://studies.aljazeera.net/ar/article/5361 ، (2024/05/09).

[2] – Nordberg ،op.cit.

- استمرار الصراع في منطقة الدونباسك بين كل من الحكومة الأوكرانية والانفصاليين في المنطقة.
- تفاقم حدة الصراع بين كل من روسيا والدول الغربية خاصة بعد فرضهم لعقوبات اقتصادية على الدولة الروسية، واختلافهم في العديد من القضايا منها التدخل في الانتخابات الأوكرانية والهجمات السيبرانية بالإضافة إلى قضية حقوق الإنسان.
- تعزيز الوجود الغربي عبر حلف الناتو في منطقة أوروبا الشرقية أي الحدود الروسية.
- تضرر أوروبا اقتصاديا من خلال ارتفاع أسعار صادرات الغاز باعتبار المنطقة المأزومة هي تلك التي يتم عبرها نقل الغاز إلى أوروبا.
- ارتفاع حصيلة الخسائر البشرية حيث قتل هناك" **14 ألف شخص بين عامي 2014 ونهاية 2021، بحسب المفوضية السامية لحقوق الإنسان، بينهم 3106 مدنيين"**[1].
- اتفاق مينسك: حيث أنه في ظل استمرارا النزاع في منطقة الدو نباس كان لا بد من إيجاد حل أو اتفاق يمكن الطرفين من حل النزاع القائم ووقف روسيا إطلاق النار، وسمي هذا الاتفاق بمينسك كان في يناير 2015، الذي ضم كل من منظمة الأمن والتعاون في أوروبا بالإضافة إلى طرفي النزاع القائم روسيا وأوكرانيا بغرض الوصول إلى اتفاق لوقف إطلاق النار "**وُضِعَت صيغة تفاوض أخرى في الشهر نفسه في شكل "رباعية نورما ندي"، التي شملت أوكرانيا وروسيا بصفتهما الأطراف، مع ألمانيا وفرنسا بصفتهما وسطاء"**[2]

وقد تم الاتفاق على وقف إطلاق النار وكذا إجراء انتخابات في أوكرانيا مع إعطاء وضع خاص لبعض الأقاليم في أوكرانيا. غير أن الاتفاقية فشلت والسبب الرئيس في فشل اتفاقية مينسك للسلام هو إطلاق أوكرانيا حملات سميت بحملات محاربة الإرهاب بعد الانتخابات الرئاسية، بالإضافة إلى توجيه الانفصاليين للعديد من الهجمات العسكرية على مراكز هامة في أوكرانيا مدعومين من روسيا على حسب ما صرحت به الحكومة الأوكرانية آنذاك. في حين نفت روسيا وجود أي علاقة مع هذه الجماعات. قد هزمت أوكرانيا مرة أخرى في منطقة تدعى" ديبا لتسيفي" وتم الاتفاق مجددا على عقد اتفاقية سلام أخرى في

[1] إليك حصاد خسائر الحرب الأوكرانية بالمليارات والأرواح، https://2u.pw/EG6650pd ، (2024/05/17).

[2] روسيا وأوكرانيا قصة خلاف الإخوة الأعداء قصة خلاف بين روسيا وثاني أكبر جمهوريات الاتحاد السوفياتي، **مرجع سابق.**

المنطقة سميت بمينسك الثانية وهي اتفاقية لم تنفذ بنودها كاملة. ومع الهجمات التي شهدتها أوكرانيا في سنة 2021 أكدت هذه الاتفاقية فشلها في تحقيق الأمن والحفاظ على السلم في المنطقة[1].

[1] عبد الجواد، **مرجع سابق**، ص36.

المبحث الثالث: استمرار المواجهة في الفضاء السيبراني بين روسيا وأكرانيا

إن المواجهة في الفضاء السيبراني بين الدول تشهد تزايدا وحدة عما كانت عليه من قبل نظرا لعدة عوامل وعليه فالحرب الروسية الأوكرانية تعتبر من أبرز المواقف التي تم استعمال فيها جميع أساليب الحرب بداية من الحرب التقليدية إلى الجديدة بواسطة أساليب هجينة.

المطلب 01: الهجمات السيبرانية في الحرب الروسية الأوكرانية 2014

على الرغم من أن الأسلحة التقليدية تتفوق بميزة تحقيق الإجبار وإلحاق أضرار مادية واسعة النطاق بالخصم على المستوى العسكري والاقتصادي أو حتى الاجتماعي، إلا أن السلاح الإلكتروني يتميز بالعديد من الخصائص منها عنصر المباغتة أي المفاجأة، وكذلك القدرة على التأثير على الاتصال المجتمعي بأقل التكاليف وبفعالية أكبر، وكذا تهيئة الساحة للهجمات العسكرية عبر اختراق شبكات الاتصال مثلا، وهذا ما جعل الدول تعتمد بالإضافة إلى الحروب المباشرة على حروب الفضاء السيبراني.

لذلك سعت روسيا منذ نهاية الحرب الباردة إلى تطوير وتحسين كفاءة ترسانتها السيبرانية في توجيه هجمات وتحقيق الأهداف المرجوة منها، وقد أكد التاريخ هذا من خلال ملاحظة وتحليل التحركات الروسية بداية من هجماتها على إستونيا في سنة 2007 ثم الهجمات التي مست جورجيا بعد تطوير القدرات الهجومية الروسية سنة 2008وصولا إلى الحرب الروسية الأوكرانية بداية من سنة 2014،فقد استخدمت روسيا الهجمات السيبرانية كجزء من استراتيجيتها الهجومية والردعية في الحروب، وذلك بالاعتماد على أساليب متعددة منها جمع المعلومات الاستخباراتية، القرصنة، واستخدام البرامج الضارة بالإضافة إلى استهداف البنية التحتية وتم تطوير كل هذه الآليات من طرف روسيا رغبة في تحقيق التفوق وكسب ميزة على خصومها وحسم الصراع الدائر في المنطقة لصالحها.

وفي الوقت الذي شهدت فيه أوكرانيا حركة الميدان الأوروبي المؤيدة لانضمامها إلى الشراكة الأوروبية وتم قمعها بعنف، تعرضت مواقع المؤسسات الأوكرانية لهجمات سيبرانية من نوع(DDos) * وكان ذلك مع بداية سنة 2014ويرجح أن روسيا كانت السبب في هذا الهجوم[1]. ففي 27 و28فيفري2014 تم قطع الاتصالات

[1] Risk and Resilience Team, "ETH Zürich Hotspot Analysis: Cyber and Information warfare in the Ukrainian conflict ،"،Center ***for Security Studies (CSS)***، (Zürich, October 2018)،p07.

*هو نوع من الهجمات الإلكترونية التي تهدف إلى تعطيل مواقع الويب أو خدمة الشبكة عن طريق إغراقها بحركة مرور وهمية.

في شبه جزيرة القرم مع العالم الخارجي عبر العبث بكابلات الألياف الضوئية من طرف مهاجمين مدعومين من روسيا (جنود لا يرتدون الزي الرسمي)، وتزامن هذا مع المظاهرات في العديد من المناطق في دولة أوكرانيا[1] أي أن هذا الهجوم كان بمثابة عملية روسية منظمة هدفها عزل هذه المنطقة والاستيلاء عليها. وفي 13 مارس تم شن هجمات سيبرانية مباشرة على مؤسسات حكومية أوكرانية وشل عملها لمدة ثمانية دقائق بهدف زعزعة الاستقرار وكذا صرف انتباه الرأي العام عن وجود تدخل عسكري في شبه جزيرة القرم[2].

كما شهدت أوكرانيا قيام هاكر موالي لروسيا يدعى (cyber bukut) باختراق خوادم لجنة الانتخابات المركزية الأوكرانية وإصابتها ببرامج ضارة، حيث تمكن فريق الاستجابة للطوارئ السيبرانية من إزالة هذه البرامج من الشبكة في الوقت المناسب قبل الانتخابات، وكان هذا بتاريخ 24 ماي 2014. ورغم ذلك استطاعت روسيا شن هجوم آخر في فترة الانتخاب تمكن من تعطيل عملية فرز الأصوات وأخّر عملية الإعلان عن نتائج هذه الانتخابات التي فاز بها المرشح بترو بورشينكو(Petro porshinko)[3]. وعرفت شركة توزيع الكهرباء المسماة (Kyivoblenergo) انقطاع خدمتها للعملاء في23ديسمبر2015 وكان ذلك بسبب دخول طرف ثالث إلى أنظمة الحاسوب الخاصة بالشركة، حيث قام بفصل العديد من المحطات الفرعية عنها لتزويد الطاقة في مناطق عديدة. وفي غضون ثلاثة ساعات أدى هذا الهجوم إلى العديد من الخسائر أهمها فقدان الشركة لما يقارب 225000عميل. وبعد مدة قصيرة تم الإعلان من طرف الحكومة على أن انقطاع التيار الكهربائي كان بسبب هجوم تسببت فيه دولة روسيا[4]، كما تبعه هجوم آخر سنة 2016 على شبكة الكهرباء الأوكرانية وتسبب في الكثير من الخسائر.

وعموما تميزت الهجمات السيبرانية في الحرب الروسية الأوكرانية بالعديد من الخصائص أهمها استخدام روسيا لبرمجيات خبيثة استهدفت بشكل مباشر أجهزة الكمبيوتر التابعة للحكومة الأوكرانية قبل

---

[1]–Loc.cit.

[2] Jakub Przetacznik with Simon Tarp ova،"Russia's war on Ukraine: Timeline of cyber-attacks ", ***European Parliamentary Research Service,*** (June 2022), p03

[3]–Risk and Resilience Team، op.cit, p.p 8-9.

[4]– Robert M. Lee, SANS ،Michael J. Asante," SANS، Tim Conway, SANS، "Analysis of the Cyber Attack on the
Ukrainian Power Grid Defense Use Case", ***Electricity Informayion Sharing and Analysis Center***,(March 18, 2016).

غزو القرم وأثناء وبعد انتهاء العمليات العسكرية، أي بشكل متواصل بهدف إحداث عطب في أنظمتها الدفاعية والبنكية أيضا، بالإضافة إلى استهدافها لإمدادات الطاقة الموجودة في العاصمة كييف[1].

كما استخدمت روسيا فيروس سمي "سنايك" (Snake)ضد أوكرانيا سنة 2014. وعلى حسب ما توصل إليه الخبراء في هذا المجال فإن عمر نشاط هذا الفيروس الضار يقارب العشرين سنة وتم نشره فيما يقرب من 50 دولة عبر العالم ويعتبر هذا البرنامج الضار الأكثر تطورا في ترسانة جهاز الأمن الفيدرالي الروسي[2].بالإضافة إلى جملة من الهجمات السيبرانية المتقطعة بداية من فترة حكم الرئيس يانوكوفيتش (Viktor Yanukovych) إلى فترة الإطاحة به، والإعلان عن رئيس جديد للدولة حيث تم تنفيذ العديد من هجمات قطع الموزع لخدمة المواقع الإلكترونية التابعة للحكومة، التي استطاعت تعطيل النظام الإلكتروني لجمع وفرز الأصوات الانتخابية مما أثر بشكل سلبي على العملية الانتخابية وجعل الفرز يتم يدويا وبهذا تأخرت الحكومة الأوكرانية في الإعلان عن نتائج الانتخابات[3]

والواقع أن الهجمات السيبرانية الروسية جمعت بين مزيج من حملات التجسس المتطورة وحملات البرمجيات الخبيثة الإجرامية، بالإضافة إلى حملات معلومات متعددة على شرق أوكرانيا، وذلك عبر استعمال وسائل التواصل الاجتماعي أهمها: كونتاكتي(Vkontakti) وأودنوكالسنيكي (Odnoklassniki) والتي يتم تشغيلها على خوادم روسية، استطاعت روسيا بذلك حجب صفحات ومنشورات كل المتمردين والمعارضين لسياستها في الأراضي الأوكرانية[4].

وهكذا لم تقتصر الحرب على أوكرانيا سنة 2014 على التدخلات العسكرية الروسية داخل الأراضي الأوكرانية بل تبعتها هجمات أخرى عبر الفضاء السيبراني، وذلك في ظل نقص الخبرة وبطء الاستجابة التي

---

[1] الحرب السيبرانية الروسية الأوكرانية ، الأساليب ، المخاطر وطرق المواجهة، https://2u.pw/LKKTtHYr ، تاريخ الإطلاع(2024/05/11).

[2] Florian Bayard، Snake, le redoutable malware espion de la Russie, a été détruit, 20 ans après sa création، https://2u.pw/ItwHOtS5، (12/05/2024)

[3] كوفمان وآخرون، مرجع ***سابق***، ص.51.

* كونتا كتي، وأودنوكالسنيكي: مواقع تواصل اجتماعي تستعمل على نطاق واسع من طرف المواطنين الروس وكذلك من قبل الجمهوريات السالقة للاتحاد السوفياتي مثل أوكراني وجورجيا.

[4] كوفمان وآخرون، **مرجع سابق**، ص. ص. 50-61.

تتميز بها أوكرانيا وعجزها عن مواجهة المخاطر السيبرانية وعدم توفير الأمن السيبراني لمؤسساتها[1]. وعلى هذا الأساس قامت روسيا بالعديد من الهجمات السيبرانية التي مست قطاعات حساسة في دولة أوكرانيا سواء القطاع العسكري، أو حتى البنية التحتية للدولة كشبكات الكهرباء والماء وأنظمة البنوك ...وغيرها.[2]وحسب الدراسات في ذات المجال"**تم تسجيل 30 حادثة سيبرانية ثنائية بين روسيا وأوكرانيا بين عامي 2000 و2020، من بينها 93% قامت بها روسيا، وتركزت غالبية هجمات موسكو بنسبة 57% على جهات فاعلة خاصة وغيرحكومية كما استهدفت 11% فقط أهدافاً عسكرية حكومية داخل أوكرانيا لأغراض التعطيل أو التجسس** "[3].

ومن هنا يمكن القول أن الهجمات السيبرانية ساهمت إلى جانب القوة العسكرية في حسم الحرب الدائرة بين روسيا وأوكرانيا وضم روسيا لشبه جزيرة القرم، والاعتراف باستقلالية الجمهوريتين المنفصلتين من قبل أوكرانيا. غير أن ضم روسيا لشبه جزيرة القرم ودعم الانفصاليين في شرق أوكرانيا لا يعني انتهاء الصراع التاريخي القائم بين البلدين بل تبعه استمرار صراع من نوع آخر، حيث شهدت البيئة الدولية العديد من المستجدات والمتغيرات التي كان لها دور في الحرب الجديدة القائمة بين كل من روسيا وأوكرانيا المدعمة من دول أوروبا الغربية والولايات المتحدة الأمريكية. فقد استمرت الهجمات السيبرانية الروسية ففي عام **2017 "وقع هجوم (Not petya) الذي نفذته جماعة لها ارتباط مع الاستخبارات العسكرية الروسية ضد أوكرانيا ونتج عنه إصابة ما يقارب 10%من أنظمة الكمبيوتر الإلكترونية بحزمة من البرامج الضارة، ويعد هذا الهجوم الأكثرتدميرا حول العالم وكلف الشركات العالمية ما يقارب 10 مليار دولار من الخسائر حسب التقديرات الأمريكية"[4]**. وقد تسبب هذا الهجوم في تعطيل المطارات والسكك الحديدية والعديد من البنوك بالإضافة إلى أنه فيروس مس العديد من الشركات متعددة الجنسيات مثل شركة الأدوية العملاقة (Merck) وكذلك شركة(TNT Express)[5] . كما يذكر "**هجوم 15 يناير 2022حيث كشفت شركة (Microsoft)عن**

---

[1]على حسين حميد، أنغام عادل حبيب، "ملامح توظيف الفضاء السيبراني في عالمنا المعاصر(الحرب الروسية الأوكرانية نموذجا)"،***القضايا السياسية***،ع72،(03/31 /2023)،ص ص.150-172.

[2]شفيق، ***مرجع سابق***، ص184.

[3] "حدود تأثير العمليات السيبرانية في الحرب الروسية الأوكرانية"،https://2u.pw/gYXUoPi ، (2024/05/16).

[4] حميد، حبيب، ***مرجع سابق***.ص160.

[5]باسم علي خريسات، ماهي الهجمات السيبرانية الروسية الجارية في أوكرانيا: اقتراح حول مستقبل الحرب السيبرانية https://2u.pw/3dvYw0yk تاريخ الاطلاع في (2024/05/19).

برامج ضارة متخفية في شكل برامج فدية تسمى(Whisper Gate تستهدف العشرات من المنظمات غير الربحية والمؤسسات الخاصة بتكنلوجيا المعلومات[1]"

المطلب02 : أهداف الهجمات السيبرانية الروسية على أوكرانيا وتأثيرها على الأمن القومي لأوكرانيا

كان من أهم أهداف الهجمات السيبرانية الروسية ضد أوكرانيا تدمير بنيتها التحتية: وذلك عبر شل عمل مختلف المؤسسات ذات الأهمية بالنسبة للدولة، والتي لها تأثير مباشر على المجتمع ومن ثم إثبات فشل دولة أوكرانيا في حماية أمن مؤسساتها ومواطنيها، على غرار ما حدث خلال الهجمات التي شهدتها شركة الكهرباء الأوكرانية والتي أدت إلى حرمان عدد هائل من المواطنين من الكهرباء سنة 2015وما تلاها من اضطرابات شهدتها وزارة الدفاع الأوكراني خلال الحرب.

كما استهدفت روسيا جمع البيانات والمعلومات، إذ تقوم الاستراتيجية الروسية على الاستفادة من أي معلومة سرية لا يراد الكشف عنها بواسطة أجهزة الاستخبارات رغبة في استخدامها أثناء التحركات الميدانية للقوات العسكرية في الحدود الأوكرانية، أو كورقة ضغط يمكن توظيفها في المفاوضات مع أوكرانيا[2]. وكثيرا ما سعت روسيا من وراء تلك الهجمات إلى اختبار قدراتها الهجومية، ومدى جاهزيتها سيبرانيا لمواجهة أي أخطار خارجية وتحقيق مكاسب استراتيجية بإثبات قوتها على الساحة الدولية.

ومن الأهداف الروسية كذلك الحرب النفسية والخداع الاستراتيجي إذ سعت روسيا من خلال الهجمات السيبرانية إلى إضعاف الروح المعنوية للشعب الأوكراني، والتأثير على قرارات صانع القرار عبر نشر المعلومات المضللة، والتلاعب بالمعلومات أي التأثير على مخرجات وسائل الإعلام، وكذا تقويض الدعم الموجه للأوكرانيين عن طريق محاولة عزلها عن العالم للانفراد بتدمير ما أمكن تدميره من الأراضي الأوكرانية[3].

---

[1]– حبيب، مرجع سابق.ص160.

[2]محمود جمال، كيف استخدمت روسيا الهجمات الإلكترونية في حربها مع أوكرانيا؟ ، https://2u.pw/LzgKqf4X تاريخ الاطلاع، (2024/05/19).

[3] عبد المنعم علي، حدود تأثير العمليات السيبرانية في الحرب الروسية الأوكرانية،https://2u.pw/gYXUoPi ، تاريخ الاطلاع، (2024/05/19).

وانطلاقا من مجمل الأهداف التي تسعى روسيا إلى تحقيقها من خلال حربها السيبرانية ضد أوكرانيا منذ 2014 يمكن القول أن استهداف شبكات الطاقة وسلاسل التوريد بالإضافة إلى شل عمل القطاعات العامة كالنقل مثلا بإمكانه أن يحدث العديد من الأزمات والاحتجاجات والمشاكل الداخلية التي بالضرورة تؤدي إلى حدوث أزمات وقلاقل داخل الدولة الأوكرانية وأزمات سياسية وتمرد من قبل المواطنين خاصة إذا طالت هذه الفترة التي تشهد هجوما سيبرانيا، بحيث يفقد المواطنون الثقة فيمن يرأسهم على اعتبار أنهم عاجزون عن حماية بياناتهم وتأمينها من الأخطار الخارجية. وبما أنّ أول هدف للدولة القومية هو السعي لتأمين إقليمها ووحدتها من أي اعتداء قد يطالهما أصبح الفضاء السيبراني ذو أهمية كبرى منذ الثورة في مجال تكنولوجيا المعلومات والتطور التقني الهائل. وفي حالة أوكرانيا فإن الدولة أظهرت عجزها عن تطوير الوسائل التي تكفل أمنها السيبراني كمتغير جديد في البيئة الدولية، ما يجعلها دولة هشة غير قادرة على مواجهة الأخطار الخارجية وبالتالي لم تستطع لوحدها ضمان أمنها القومي.

لقد استطاعت روسيا عن طريق شن مجموعة من الهجمات السيبرانية تحقيق العديد من الأهداف المرجوة من الحرب الروسية الأوكرانية بدء بتسهيل عملية الغزو الروسي للقرم عن طريق التجسس على المعلومات الاستخباراتية وتقديم الدعم للجيش وتسهيل تحركاته في المنطقة، وصولا إلى حسم الحرب ضد أوكرانيا وضم شبه جزيرة القرم إلى روسيا، باستخدام الحرب الهجينة التي تعرف على أنها: "**الدمج بين انواع مختلفة من الحروب تتضمن الحرب التقليدية والحرب غير تقليدية والحرب الناعمة والهجمات السيبرانية، التي تعد من أخطر الحروب التي تعرض الأمن الوطني للتهديد المباشر، لكونها لا تخضع لأي قانون أخلاقي أو أي قانون آخر**"[1]. كما كانت فرصة روسية لتوجيه تحذير و ردع لدولة أوكرانيا والدول الغربية الداعمة لها، وتثبيط أي محاولة للاعتداء على سيادة روسيا أو المساس بأمن حدودها. وبالفعل استطاعت الهجمات السيبرانية الروسية خلق مشاكل اقتصادية داخل دولة أوكرانيا عبر شل حركة البنوك والمعاملات المالية، ولو لفترة محدودة مما أدى إلى إعاقة التجارة والنشاطات الاستثمارية في المنطقة وإلى تراجع النمو الاقتصادي للبلد.

[1] تمارة علاء عبد الزهرة، "الحرب الهجينة"، ***مركز النهرين للدراسات الاستراتيجية***، https://2u.pw/jcUGCjF3. تاريخ الاطلاع، (2024/05/19).

المطلب03: ردود أوكرانيا على هذه الهجمات

سعت أوكرانيا إلى استثمار كل مجهوداتها في عملية تأمين البنية التحتية الأوكرانية ما جعلها تخصص جزءا كبيرا من الميزانية الحكومية لتعزيز قدراتها السيبرانية سواء الدفاعية أو حتى الهجومية، وذلك عن طريق الدعم المقدم لها من طرف الدول الغربية بزعامة الولايات المتحدة الأمريكية وحتى متطوعين من جميع أنحاء العالم. ومن أهم ما قامت به أوكرانيا ما يلي:

- تعزيز البنية التحتية لدولة أوكرانيا أي محاولة حماية شبكات الكهرباء الاتصالات والبنوك من أي اختراق قد يطالها مستقبلا.
- تشكيل جيش إلكتروني لمواجهة الهجمات السيبرانية الروسية يتكون أساسا من خبراء أوروبيين بالإضافة إلى متطوعين.
- القيام بمجموعة من الهجمات المضادة التي كانت محدودة التأثير مست مواقع عسكرية وحكومية للدولة الروسية[1]. ومن أبرز الهجمات السيبرانية التي استهدفت روسيا كانت قيام "**مجموعة من القراصنة الأوكرانيين بتسريب رسائل بريد إلكتروني مخترقة من مستشار الرئيسي فلاديمير بوتين فلاديسلاف سوركوف (Vladislav Surkov)كشفت هذه الرسائل أن الرئيس على تواصل مع القادة الانفصاليين الموالين لروسيا في أوكرانيا**" وكان ذلك بتاريخ 25 أكتوبر 2016[2].
- وما يمكن ملاحظته هو أن الهجمات السيبرانية الروسية سنة 2014 ضد أوكرانيا كانت بمثابة الإدراك الحقيقي للتأثير العميق الذي يمكن أن تتسبب فيه هذه الهجمات وبوصفها أداة من أدوات الحروب الحديثة وبإمكانها تحقيق مكاسب حيث لم تقتصر الحرب الروسية الأوكرانية على الحرب السيبرانية فقط فالإضافة إليها تم استخدام العديد من الوسائل أهمها كان الدعاية ونشر المعلومات المغلوطة بغرض التأثير على الرأي العام، كما استخدمت روسيا وسائل التواصل الاجتماعي كأدات لمراقبة ومتابعة كل النقاشات القائمة في الفضاء الافتراضي وإدارتها وقد أنشأت روسيا لهذا الهدف فرق للرصد والمتابعة للأنترنت متخصصة "**على مدار الساعة في فترتي عمل متتابعتين تصل كل منهما إلى**

[1] James Andrew Lewis، Cyber War and Ukraine، https://2u.pw/FDs6xoGa، (12/05/2024).

[2] Risk and Resilience Team،**op.cit.**

12 ساعة، وينبغي أن يستوفى كل فرد منهم حصة يومية قدرها 135 تعليقاً بحد أدنى 200 حرف لكل تعليق للرد على الآراء والتعليقات العدائية الموجهة للسياسات الروسية"[1]

[1]أماني عصام، "استخدام روسيا للقوة السيبرانية في إدارة تفاعلاتها الدولية"، ***مجلة كلية الاقتصاد والعلوم السياسية لجامعة حلوان***، م.22، ع.04، (أكتوبر 2021)،ص ص 167-190.

خلاصة الفصل:

لم تعد الحرب التقليدية كافية لتحقيق أهداف السياسة الخارجية للدول في ظل التطور التكنلوجي وتغير مفاهيم القوة. فبالإضافة إلى ضرورة اكتساب الدول لمقومات القوة الصلبة صار إلزاما عليها التحكم في الفضاء السيبراني، وامتلاك قدر من القوة السيبرانية لغرض الدفاع عن أمنها السيبراني من أي هجمات أو اختراق قد يطاله، أو حتى تنفيذ هجمات ضد خصومها ما تعلق الأمر بمصالحها الحيوية.

الجدير بالذكر أن تزايد الهجمات السيبرانية بين الدول يؤدي إلى التصعيد وقد يتحول إلى حرب مباشرة أي مواجهة عسكرية مثل ما هو الحال في الحرب الروسية الأوكرانية سواء الأولى سنة 2014 والتي أدت إلى غزو شبه جزيرة القرم أو حتى الحرب الدائرة حاليا بين الدولتين.

الفصل الثالث

الهجمات السيبرانية في الحرب بين روسيا وأوكرانيا منذ 2021 وسبل التصدي لها

تمهيد

أصبحت التهديدات السيبرانية تشكل عائقا كبيرا بالنسبة للدول في تحقيق الاستقرار والتطور نظرا لنتائجها الوخيمة على اقتصاديات الدول ومنشأتها الحيوية، وفي ظل بروز متغيرات دولية عديدة لم تستطع الدول مواجهة هذه المخاطر بشكل منفرد، رغم محاولاتها اعتماد استراتيجيات للحد من آثار هذه الهجمات السيبرانية.

إلا أنه أصبح من الضروري استحداث آليات تعاونية وتنسيقية يشرف عليها المجتمع الدولي للتقليل من المخاطر ذات المصدر السيبراني.

وتم تقسيم هذا الفصل إلى مبحثين يتناول المبحث الأول استخدام الهجمات السيبرانية من قبل روسيا وأوكرانيا. ويعالج الثاني دور المجتمع الدولي والمنظمات الدولية للحد من الهجمات السيبرانية.

المبحث الأول: استخدام الهجمات السيبرانية من قبل روسيا وأوكرانيا

كما سبق وأشرنا استخدمت روسيا في حربها ضد أوكرانيا كل الوسائل سواء العسكرية وغير العسكرية في شكل حرب هجينة لتحقيق النصر والحصول على المكاسب المرجوة من هذه الحرب. ومن أهم الوسائل غير العسكرية الهجمات السيبرانية سواء في حرب ضم شبه جزيرة القرم أو حتى في حربها الثانية من سنة 2022. وكرد فعل قامت أوكرانيا بدورها بتنفيذ العديد من الهجمات السيبرانية كاستراتيجية دفاعية ضد ما أسمته بالغزو والاختراق لسيادتها.

المطلب الأول: الإستراتيجية الأوكرانية في مواجهة التهديدات السيبرانية

شهدت أوكرانيا قبيل الغزو الروسي الذي كان بشكل علني يوم 23 فيفري 2022 العديد من محاولات إطلاق هجمات سيبرانية كإجراء تحذيري وردعي صاحب بداية العمليات العسكرية على الحدود الأوكرانية، ومنذ نهاية سنة 2021 سعت روسيا إلى توجيه العديد من الفيروسات والبرامج الضارة ضد العديد من القطاعات الحيوية المرتبطة بالفضاء الإلكتروني داخل دولة أوكرانيا كان أهمها:

الجدول رقم03 : يمثل أبرز الهجمات السيبرانية الروسية ضد أوكرانيا.

تاريخ الهجوم	نوع الهجوم والهدف منه
14 يناير 2022	تعطيل العديد من المواقع التابعة للحكومة الأوكرانية منها الموقع الرسمي لوزارة الخارجية ووزارة الصحة.
23 فيفري 2022	برامج ضارة مدمرة لحذف وإتلاف البيانات على الكمبيوتر أو الشبكات ضد البنوك، المراكز الحكومية أوكرانيا هجمات الحرمان من الخدمة.
28 فيفري2022	هجمات حجب الخدمة على مستوى البنوك ومراكز توليد الطاقة.
07 مارس 2022	التصيد الاحتيالي ضد المواطنين والمؤسسات الخدماتية.

16مارس 2022	قرصنة محطة تلفزيون "أوكرانيا 24 ساعة" وبث خطاب ملفق للرئيس زيلنسكي يدعو فيه المواطنين إلى الاستسلام.
7 ماي 2022	هجوم إلكتروني ضد مجلس مدينة أوديسا الأوكرانية بالتوازي مع هجوم صاروخي على منطقة سكنية.

المصدر:

Przetacznik with Tarp ova، op.cit, p0

نلاحظ من خلال الجدول أعلاه أن دولة أوكرانيا قد تلقت العديد من الهجمات السيبرانية التي مست تقريبا جميع القطاعات الحيوية للبلاد منذ بداية حرب 2022، وعلى هذا الأساس كان لا بد لها من اعتماد استراتيجية تمكنها من التعامل مع هذه التهديدات الجديدة وتقليل الخسائر التي قد تنجم عنها وكذا محاولة استحداث أساليب تمكنها من الحفاظ على أمنها السيبراني، وأمن إقليمها ومجابهة الهجمات الروسية بهجمات مضادة لتحقيق التوازن وتعديل موازين القوى.

رغم أن أوكرانيا تمكنت من تشكيل جيش سيبراني بغرض الهجوم والدفاع في آن واحد إلا أنها تبنت في الغالب استراتيجية دفاعية ردعية للتصدي لمختلف الهجمات ذات المصدر الروسي، وقد أثبتت من خلال استراتيجية الردع الشامل القائمة على تعزيز القدرات الدفاعية وبناء تحالفات مع دول أخرى ومنظمات دولية أن هذه الاستراتيجية بإمكانها التصدي للهجمات السيبرانية[1]. كما استخدمت أوكرانيا خلال حربها السيبرانية ضد روسيا الدعاية السياسية والعسكرية بغرض إضعاف العدو من جهة، وأعدت برامج تكوين الكوادر التي بإمكانها تولي إدارة المنظومة السيبرانية الأوكرانية الدفاعية من جهة أخرى، مستفيدة من خبرتها خلال حرب القرم في كيفية التعامل مع الغزو الروسي لسنة 2022.

كما نشرت أوكرانيا حملات دعائية عديدة لبث روح المقاومة في أوساط الشعب ولدى الجيش لتأكيد سرديتها في الحرب مع روسيا، مع الإصرار على تبيان الحقائق والمعاناة التي يعيشها الأوكرانيون للعالم، وهو ما أدى إلى تعاطف كبير معهم من قبل المجتمع الدولي وخاصة الدول الأوروبية التي صارت تتساهل في استقبال الأوكرانيين اللاجئين، ودعمت الدولة الأوكرانية بكل ما يحتاجونه خلال هذه الحرب من مؤونة وأسلحة. وفي هذا الإطار أنشأت أوكرانيا العديد من الوكالات السبيرانية المتخصصة والاستعانة بخبرات الدول الأوروبية

[1] نبيل عودة، "العمليات السيبرانية في الحرب الروسية الأوكرانية طبيعتها وأنماطها"، **الشرق للأبحاث الاستراتيجية**،(20سبتمبر2022)،ص 05.

وأمريكال مواجهة التهديدات السيبرانية و **"من هذه الوكالات كان فريق الاستجابة لطوارئ الكمبيوتر الأوكراني المعروف بـ.CERT، الذي أسهمت شراكته مع الكيانات الدولية مثل ميكروسوفت في رصد فايروس (Foxblade)و إبطال مفعوله"**[1].

من الأساليب الوقائية التي اعتمدتها الحكومة الأوكرانية كان نقل المعدات والنسخ الاحتياطية لقاعدة البيانات إلى مناطق أكثر أمنا في أوكرانيا، بحيث لا تستطيع القوات الروسية الوصول إليها بالإضافة إلى إنشاء نظام حماية البنية التحتية للدولة من أي هجمات قد تطالها[2]. كما قامت دولة أوكرانيا بتجنيد العديد من المتطوعين أي الهاكرز من جميع أنحاء العالم بالإضافة إلى الاستعانة بالشركات الخاصة للقيام بهجمات سيبرانية مضادة للهجمات الروسية، ما نتج عنه فيما بعد ما يسمى بالجيش السيبراني الأوكراني. **وحسب نائب وزير التحول الرقمي الأوكراني فإن وجود هذا الجيش في أوكرانيا كان ممكنا لعدة عوامل كالبنية الرقمية الأوكرانية المتطورة، والأنظمة الإلكترونية، ورأس المال البشري المدرب، وعدالة القضية الأوكرانية**[3].وعبر العديد من النشطاء في عمليات الغزو السيبراني تعاطفهم مع الأوكرانيين ووعدوا بتقديم كل الدعم اللازم لمساندة الجانب الأوكراني في الحرب.

كما أن أوكرانيا قد استعانت بمجموعة "من **القراصنة المعروفين باسم أنونيموس (Anonymous)، والتي أعلنت الحرب الرقمية ضد وسائل الإعلام الروسية المملوكة للدولة ونجحوا في اختراق محطات البث الروسية الكبرى ومنها "روسيا 24" و"القناة 1" و"موسكو 24"، واخترقت موقع "روسيا اليوم" لمدة 12 دقيقة"**[4]

المطلب 02: الاستراتيجية روسيا في مواجهة التهديدات السيبرانية

تعتبر الحرب القائمة بين روسيا وأوكرانيا ذات أهمية كبيرة بالنسبة للمنظرين والدارسين في هذا المجال نظرا لأنها ستساهم في تغيير الكثير من الافتراضات والمسلمات على مستوى النظام الدولي من حيث اعتمادها على القوة السيبرانية بالإضافة إلى القوة التقليدية العسكرية، على اعتبار أن كلا الطرفين لديهما قدرات كافية في مجال الدفاع السيبراني والهجمات السيبرانية. بداية من دولة روسيا التي تعتمد كثيرا على الأدوات السيبرانية

[1] المكان نفسه.

[2] The Ukrainian Digital Resistance: cyber resilience and digital diplomacy at work، https://2u.pw/0yaVjR20 (03/03/2024).

[3]عودة، مرجع سابق، ص 15.

[4] عز الدين أبو عيشة، "الهاكرز"... كنائب الاقتحام الإلكتروني في الحرب الروسية الأوكرانية، https://n9.cl/1g9tn ،تاريخ الاطلاع(2024/05/20).

في سياستها الخارجية وصولا إلى أوكرانيا التي ومنذ هجمات 2014 سعت جاهدة إلى علاج مكامن الضعف استراتيجيتها الدفاعية ضد روسيا[1]

لقد تمكنت أوكرانيا من تنفيذ العديد من الهجمات ضد روسيا منذ بداية الحرب أهمها كان "**قرصنة سيبرانية ضد الموقع الرسمي لرئيس روسيا فلاديمير بوتين وإخراجه عن الخدمة لمدة تسع ساعات، كما أوقفت عمل موقع البرلمان الروسي "الكرملين" وكذلك الموقع الإلكتروني لمجلس الأمن الروسي، وبسبب الهجمات الإلكترونية خرجت بورصة موسكو من التداول**[2]" أكثر من مرة، وكانت هذه الهجمات السيبرانية كرد فعل ضد الهجمات السيبرانية الروسية ضد البنية التحتية الأوكرانية والعديد من المراكز الحكومية.

الواقع أن روسيا رائدة في مجال الأمن السيبراني، حيث من أهم المؤسسات المسؤولة عن الأمن الإلكتروني في روسيا هي مجلس الأمن، وجهاز الأمن الفيدرالي، جهاز الحرس الفيدرالي، والجهاز الفيدرالي للتحكم التقني، ووزارة الاتصالات وتكنولوجيا المعلومات وتنقسم المهام ما بين الإدارات المختلفة في الأنشطة المتعلقة بالأمن الإلكتروني[3]. والواقع أن الاهتمام بالمجال الإلكتروني في السياسة الخارجية الروسية ليس بجديد إذ يعود إلى سنة 2000، وقد منح الأمن السيبراني أهمية كبرى، باعتباره يحقق المصالح القومية للدولة ويعزز الاستقرار في جوانب عدة منها الاجتماعي والسياسي وحتى الاقتصادي بالإضافة إلى دورها البارز في إطار الجهود الدولية الرامية إلى إبرام اتفاقيات تسعى للحد من المخاطر التي تنتج عن سباق التسلح الإلكتروني ومواجهة مخاطره الكبيرة، **وبلغ الانفاق العسكري الروسي على حرب الفضاء الإلكتروني 127 مليون دولار من إجمالي إنفاق عسكري** "[4].

في 10 سبتمبر 2018 أنشأت روسيا جهاز الأمن الفيدرالي الروسي وهو مركز وطني لغرض مجابهة الهجمات السيبرانية، عبر تعزيز وسائل الدفاع وتأمين البنية التحتية، وكذا الكشف المبكر والوقاية من هذه الهجمات، وتبادل الخبرات بين الهيئات المتخصصة في الأمن السيبراني. ولتحقيق الأمن السيبراني قامت الحكومة الروسية بفصل أجهزة الدولة عن الأنترنت بشكل كلي لمدة بغرض زيادة فاعليتها في مجابهة الهجمات السيبرانية والقرصنة ذات المصدر الأجنبي[5].

[1] **المكان نفسه.**
[2]- **المكان نفسه.**
[3]- **المكان نفسه.**
[4]عصام، مرجع سابق، ص173.
[5]-**نفس المرجع**، ص169.

كما أبرزت الحرب الروسية الأوكرانية منذ 2022 الأهمية الكبيرة لوسائل الإعلام على اعتبارها الوسيلة التي تنقل عبرها الحرب من العالم الواقعي إلى الافتراضي أي من التقليدي إلى العصري، وهو ما يعرف بالحرب الإعلامية الروسية ضد أوكرانيا. وفي المقابل تسعى الدول الأوروبية وأمريكا بوصفها دول داعمة لدولة أوكرانيا تشويه صورة الدولة الروسية وسياستها الخارجية بصفة عامة، وذلك بتوظيف عدة أساليب منها حملة الشبكات الإعلامية العالمية مثل سي أن أن(CNN) ونيويورك تايمز (NEW YORK TIMES)...وغيرها ، والتي سعت إلى تأليب الرأي العام العالمي ضد ما أسمته بالعدوان الروسي ضد دولة أوكرانيا. كما تم منع بث القنوات الروسية في الدول الأوروبية كقناة روسيا اليوم (RT)وسبوتنيك(SPUTNIK) ، رغبة في التضييق على روسيا والإبقاء على الرأي الواحد لدى المواطن الغربي وحرمانه من معرفة الصورة الكاملة لما يحصل في المنطقة عن طريق تزويده بالأخبار من مصدر واحد متحيز[1].

كما برز دور وسائل التواصل الاجتماعي في الحرب الروسية الأوكرانية بشكل واضح باعتبارها أداة قوية في يد المتحكمين فيها لغرض الدعاية ودعم أوكرانيا، وذلك من خلال تصريح الناطق الرسمي باسم شركة ميتا في يوم 10 مارس 2022 عبر منصة التويتر (twiter)بمنشور يؤكد فيه على أن الشركة ستسمح باستعمال مختلف التعابير والعبارات السياسية العنيفة التي كانت مرفوضة سابقا للوقوف مع الأوكرانيين، ودعمهم معنويا في حربهم ضد روسيا. وكرد فعل قامت الحكومة الروسية بالتنديد بتصنيف ميتا (Meta)على أنها منظمة متطرفة تهدف إلى نشر العدوان والعنف ضد مواطني دولة روسيا، بالإضافة إصدار الرئيس بوتين قرارا بحظر تطبيق الأنستغرام (Instagram)التابع لشركة ميتا (Meta)في دولة روسيا يوم 14 مارس 2022[2]. كما استخدمت الحرب السيبرانية بالوكالة التي تعرف على أنها استعانة الحكومة الروسية ا بفواعل أخرين مثل الجماعات الإجرامية والقراصنة، عبر تقديم الدعم المالي والحماية القانونية لهذه الجماعات من أي ملاحقة قضائية. بالإضافة إلى توفير أحدث الأجهزة والتقنيات وتدريبهم على أسس تكفل تنفيذ الاستراتيجية الروسية في هذه الحرب. ويعد الدافع الأساسي لتوظيف الدول لهذه الجماعات هو سهولة إنكارها للتهم الموجهة ضدها وكذا حماية نفسها من أي انتقام من طرف خصومها[3].

والملاحظ في إطار غزو روسيا لدولة أوكرانيا أن روسيا استعملت كل أنواع الهجمات السيبرانية المتاحة تزامنا مع العمليات العسكرية، رغبة في كسب ميزة إضافية عن الأعداء وحسم نتيجة الحرب لصالحها، نظرا الأن

[1] محمود محمد علي، **كيف تم توظيف الإعلام في الحرب الروسية الأوكرانية**، (لقاهرة: دار المعارف،**2022**) ،ص9-11.

[2] -المكان نفسه.

[3] عبدالله عيسى الشريف، من الردع إلى المرونة: تغيرات الحرب السيبرانية بالوكالة بين روسيا وأوكرانيا، https://2u.pw/UzUrqF4y ، (2024/05/20).

الاستراتيجية الروسية تقوم أساسا على الجمع بين العناصر العسكرية والسياسية والسيبرانية والإعلامية لتحقيق النصر في الحروب.

المطلب الثالث: مدى فعالية الهجمات السيبرانية في تحقيق أهداف الحرب الروسية الأوكرانية

لقد نتج عن الحرب الروسية الأوكرانية منذ 2022 العديد من التداعيات على المستوى العالمي سواء في الجانب الاقتصادي والسياسي أو حتى على مستوى التنظير في العلاقات الدولية وتغير مفاهيم الحرب من تقليدية إلى جديدة باستعمال كل الأساليب والوسائل التي من الممكن الاستفادة منها لتغيير معادلة الحرب. وقامت دولة روسيا بشن العديد من العمليات العسكرية في المنطقة التي تهدف إلى وقف توسع حلف الناتو، ومنع انضمام أوكرانيا إليه نظرا الأن هذا بالضرورة يجعل منطقة غرب روسيا تحتوي على قواعد عسكرية تهدد السلم في المنطقة، وتنعكس بالسلب على الأمن القومي الروسي، كما استعملت الهجمات السيبرانية واستطاعت روسيا تحقيق العديد من المكاسب بالنسبة منذ بدايتها قبل ثلاثة سنوات من تاريخ اندلاع الحرب العسكرية. وذلك بواسطة اعتمادها كاستراتيجية هجومية ومساعدة للعمليات العسكرية الروسية على الأراضي الأوكرانية، منها البرامج الضارة التي مست الأقمار الصناعية الأوكرانية، وأدت إلى تعطيل أكثر من ثلاثين ألف اتصال حول أوروبا وليس في أوكرانيا، بالإضافة إلى أنه تم اكتشاف العديد من الفيروسيات والبرامج الضارة التي مست الدول الداعمة لأوكرانيا في حربها مع روسيا مثل الولايات المتحدة الأمريكية والتي اكتشفت وجود برامج ضارة على مستوى البنية التحتية المرتبطة بتوليد وتوفير الكهرباء والغرض[1] الأساسي لهذه الهجمات كان عزل أوكرانيا عن تلقيها الدعم الخارجي، بالإضافة إلى استعراض القدرات والإمكانيات الروسية على مستوى الفضاء السيبراني.

وكانت الهجمات السيبرانية التي شنتها روسيا ضد دولة أوكرانيا وحلفائها من الدول الأوروبية فعالة في إبراز قوة روسيا وقدرتها، كما أثبتت هشاشة أنظمة الدفاع الأوكرانية خاصة في السنة الأولى، إذ تمكنت من زرع الخوف بين المواطنين وانعدام ثقتهم في الحكومة الأوكرانية بالإضافة إلى الحصول على العديد من المعلومات التي مكنت الجيش الروسي من تحقيق العديد من الانتصارات في ساحة المعركة. وعلى الرغم من استخدام روسيا للهجمات الصاروخية وكذا التفجيرات وتهجير المواطنين والتلويح باستخدام السلاح النووي إلا أنها لم تستخدم الحرب السيبرانية الشاملة المكلفة ضد أوكرانيا أو مؤيديها من الدول الأوروبية، بل اقتصرت على تنفيد هجمات

[1]-Grace B. Mueller., Benjamin Jensen., Brandon Valeriano., Ryan C. Maness & Jose M. Macias. "Cyber Operations during the Russo-Ukrainian War: From Strange Patterns to Alternative Futures،" *Center for Strategic and International Studies*. JULY 2023.

سيبرانية مست قطاعات حيوية، وكان لها دور استخباراتي تجسسي غرضه الحصول على المعلومة والحرب النفسية، أكثر من كونها عاملا حاسما في الحرب بين الطرفين.

والواقع أن عدد الهجمات منذ بداية الحرب في تزايد مستمر فحسب الإحصائيات شهدت أوكرانيا خلال السنة الأولى 47 هجوما سيبرانيا، لتزداد بنسبة 75% ، ومع ذلك فهي لا تزال أداة قسرية ضعيفة في إطار الحرب، أي لا يمكن بواسطتها إخضاع العدو خاصة في ظل تحسن الدفاع الأوكراني وتطويره للآليات التي يمكن من خلالها الحد من تأثير هذه الهجمات على المراكز الحيوية والحساسة خاصة المتعلقة بسيادة الدولة خاصة.[1]

[1] عبد المنعم، **مرجع سابق**.

المبحث الثاني: دور المجتمع الدولي والمنظمات الدولية للحد من الهجمات السيبرانية

نظرا لتعقيدات الهجمات السيبرانية بسبب تعدد فواعلها وتطور الاستراتيجيات والوسائل التي تتم عبرها تواجه الدول العديد من المشاكل في التصدي لها سيما بشكل منفرد في ظل تزايد أثارها المدمرة على اقتصاديات الدول وبنيتها التحتية، لذلك كان لا بد من التفكير في قوانين وآليات يتم بواسطتها التعامل مع هذه التحديات وتحقيق الأمن السيبراني، وتطوير أساليب جديدة للوقاية منها وتفادي الخسائر التي تنجم عنها. ومنه سعى المجتمع الدولي من منظمات دولية وإقليمية إلى إبرام العديد من الاتفاقيات لمواجهة جرائم الفضاء السيبراني سواء ذات البعد الدولي أو الإقليمي.

المطلب الأول: أهم الاتفاقيات المبرمة للحفاظ على الأمن السيبراني للدول

تعود أولى الجهود الدولية التي سعت إلى مواجهة الهجمات السيبرانية والجرائم في الفضاء الإلكتروني إلى سنوات الثمانينات، حيث تمت مناقشة كيفية إيجاد تشريع قانوني على مستوى الأنتربول الدولي سنة 1981يمكن من خلاله مواجهة الجرائم السيبرانية التي أصبحت تهدد الفواعل في البيئة الدولية. وقد شهد الاهتمام بهذا المجال تطورا بطيئا آنذاك ، إلا أنه ومع نهاية الحرب الباردة أحرز تقدما ملحوظا. فبعد انهيار الاتحاد السوفياتي وانفراد الولايات المتحدة الأمريكية بزعامة النظام الدولي برزت أخطارا دولية غير مرتبطة بالقوة العسكرية منها الجريمة المنظمة العابرة للحدود، وكذا الإرهاب وتزايد مستوى التهديدات ذات المصدر السيبراني التي أصبحت تهدد سيادة الدول، واحتلت الصدارة في اهتمامات أجندات الأمن الدولي.

وهنا كان لا بد من تعميق الدراسات والأبحاث في هذا المجال بداية من إنشاء معهد قانون الفضاء الإلكتروني بجامعة جورج تاون الأمريكية سنة 1991 الذي يضم ثلاثن مختصا غرضهم البحث عن كيفية التعامل مع الفضاء الإلكتروني في ظل تزايد المخاطر والتهديدات المرتبطة به وكيفية حمايته[1]. كم تم فيما بعد إبرام العديد من الاتفاقيات الدولية المختصة في محاربة الجريمة الإلكترونية والحد من الهجمات السيبرانية، وتحقيق الأمن السيبراني، ويمكن تقسيم هذه الاتفاقيات كما يلي:

[1] عبد الصادق، **مرجع سابق**،ص350-351.

1- الاتفاقيات الدولية:

أ- اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية المعروفة باتفاقية بودابست:

تعتبر هذه الاتفاقية بمثابة أول محاولة ذات بعد قانوني لمواجهة الهجمات والأخطار ذات المصدر السيبراني، وتم عقدها بالعاصمة المجرية بودابست من طرف المجلس الأوروبي يوم 11 أوت 2001 كما تمت المصادقة عليها يوم 23أوت، وبمشاركة العديد من الدول الأوروبية الأعضاء، وغير الأعضاء وهي أول اتفاقية متعددة الأطراف وملزمة لأطرافها[1]. وقد نصت الاتفاقية على قائمة بأهم الجرائم الإلكترونية التي يجب على الدول تجريمها ومعاقبة مرتكبيها بأشد العقوبات، نظرا لخطورتها وتأثيرها الجسيم على الأمن السيبراني والقومي. ومن أهم هذه الجرائم الإرهاب وتزوير بطاقات الدفع الإلكتروني وجرائم الأخلاق مثل دعارة الأطفال. كما تعمل هذه الاتفاقية على سن قوانين جديدة وموحدة للعمل بها داخل الدول وتعزيز التعاون الدولي.

وأسست الاتفاقية على التنسيق بين أجهزة الشرطة والحكومات بمساعدة العديد من المختصين في مجال الأمن السيبراني، وتمت صياغة نص نهائي ورسمي لهذه الاتفاقية من قبل عدد من الخبراء في المجلس الأوروبي المتخصص في الجريمة الإلكترونية بمساعدة العديد من الدول الرائدة في المجال مثل الولايات المتحدة الأمريكية[2]. كما أن قامت هذه الاتفاقية حددت أهم الجرائم التي يجب أن توفر لها التشريعات الوطنية الإجراءات العقابية اللازمة. ومن الجرائم التي نصت عليها:

- ✓ الجرائم الواقعة على مستوى الفضاء السيبراني منها الاحتيال والنصب، سرقة البيانات، القرصنة.
- ✓ جرائم التعدي على حقوق الملكية الفكرية وحقوق النشر.
- ✓ حيازة أو نشر برامج ضارة يمكن من خلالها زعزعة الأمن السيبراني.
- ✓ التعدي على الحقوق الأساسية للأفراد أي حقوق الإنسان وحمايته من أي أخطار قد تعيق تحقيق الأمن والاستقرار في الدولة، مع إمكانية الدول غير الأعضاء الاستعانة بها بغرض إعداد التشريعات الوطنية.

[1] قطاف سليمان، بوقرين عبدالحليم، "الآليات القانونية الموضوعية لمكافحة الجرائم السيبرانية في ضل اتفاقية بودابست"، ***المجلة الأكاديمية للبحوث القانونية والسياسية***، م.6ع.(2022)،ص ص 334-358.

[2] قطاف سليمان، بوقرين عبدالحليم، "مواجهة الجرائم السيبرانية في ضوء الاتفاقيات الدولية"، ***مجلة البحوث القانونية والإقتصادية***،م.5،ع2،(2020)،ص ص62-87.

وقد بلغ عدد الدول الموقعة عليا هذه الاتفاقية 26 دولة من أصل 43 دولة عضوة في مجلس أوروبا، كما يمكن لأي دولة في العالم الانضمام إلى هذه الاتفاقية فهي ليست حكرا على الدول الأوروبية[1].

ب- اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية:

وتعرف على أنها معاهدة دولية جاءت لمكافحة الجرائم العابرة للحدود ذات التأثير العالمي، انعقدت من طرف الجمعية العامة لمنظمة الأمم المتحدة يوم 15 نوفمبر سنة 2000، ودخلت حيز التنفيذ في 19 سبتمبر2003 وشاركت فيها حتى الأن أكثر من 190حول العالم، وتنص هذه المعاهدة الدولية على الحد من الجرائم العابرة للحدود، وإلزام الدول باتخاذ الإجراءات اللازمة للتقليل من هذه الجرائم أو القضاء عليها، و منها تجارة المخدرات والتهريب وغسيل الأموال، والتهديدات السيبرانية التي أصبحت عائقا كبيرا في تحقيق الأمن القومي للدول والحفاظ على أمنها السيبراني[2] ,وتتمثل الأهداف الرئيسية لهذه الاتفاقية أساسا في:

- ✓ تشجيع التعاون بين الدول من خلال المساعدة في التحقيقات وكشف المعلومات والمجرمين لتسليمهم للعدالة.
- ✓ اتخاذ تدابير الحد من مخاطر وتهديدات الجرائم العابرة للحدود، وتأمين البنية التحتية للدول لغرض حمايتها من هجمات سيبرانية التي يمكن أن تهدد استقرارها[3].
- ✓ حماية ضحايا الجريمة العابرة للحدود وتقديم الدعم اللازم لهم.

ج- مؤتمر فيينا حول التعاون الأمني الدولي

تم إنشاء هذا المؤتمر منذ سنة 1923 أهم ما تم إصداره ما سمي باللجنة الدولية لشرطة الجنائية والتي تقوم بالتنسيق بين الدول الأوروبية في مجال مكافحة الجريمة المنظمة، ومع اندلاع الحرب العالمية الثانية جمدت نشاطاته إلى غاية نهايتها أين تم عقد مؤتمر دولي جديد في جوان من سنة 1946 تم الاتفاق من قبل الأعضاء 16على إنشاء المنظمة الدولية للشرطة الجنائية (INTERPOL) وتعتبر بديلا عن اللجنة الدولية للشرطة الجنائية وتقوم على أسس التعاون بين الأعضاء بغرض الوصول إلى المجرمين المبحوث عنهم،

[1] وفاء لطفي "الجهود الدولية في مجال مكافحة جرائم الإرهاب السيبراني التجربة الماليزية نموذجا "، ***مجلة كلية الاقتصاد والعلوم السياسية لجامعة القاهرة*** .23،(يناير 2022) ص ص151-172.

[2] United Nations، Office on Drugs and Crime ، ***United Nations Convention against Transnational Organized Crime and the Protocols Thereto***,15November 2000,p.p 1-2

[3] -بيدي أمال، "جهود الأمم المتحدة لمواجهة الجريمة السيبرانية"، **مجلة البحوث في الحقوق والعلوم السياسية**K،م.08،ع.01،(2022)،ص ص299-316.

وكذلك محاربة كل ما له علاقة بالجريمة العابرة للحدود ومنها الهجمات السيبرانية والقرصنة نظرا لأهميتها الكبيرة ولتأثيرها على الأمن الدولي[1].

2-الاتفاقيات على المستوى الإقليمي

أ-اتفاقية الاتحاد الإفريقي حول الأمن السيبراني أو اتفاقية مالابو 2014:

"لقد ظل الاتحاد الأوروبي لما يقارب الثلاثين سنة يتغنى بإصداره الاتفاقية الوحيدة في مجال مكافحة الجريمة الإلكترونية"[2] وبناء على هذا سعى الاتحاد الإفريقي إلى الاهتمام بهذا الجانب نظرا للأهمية الكبيرة التي يكتسيها، بداية بالموافقة من طرف رؤساء الدول والحكومات الإفريقية على إنشاء الاتحاد الإفريقي استنادا إلى اتفاقية سرت بطرابلس 09 سبتمبر 1999 كبديل عن منظمة الوحدة الإفريقية ومحاولة لتلافي كل نقاط الضعف التي عانت منها المنظمة سابقا منذ إنشاءها سنة 1963. وعلى هذا الأساس تمثل الغرض الرئيسي للمنظمة هو تقديم ألية مؤسساتية لدول القارة حتى يتسنى لها مواجهة التهديدات الأمنية والاقتصادية والاجتماعية خاصة مع بداية الألفية حيث تم عقد العديد من القمم لمناقشة هذه القضايا ومحاولة الوصول إلى حلول جذرية للقضاء عليها منها قمة لوساكا لزامبيا في سنة 2001، وقمة دوربان بجنوب إفريقيا سنة 2002. ومن بين المواضيع التي طرحت في هذا الإطار ضرورة تنسيق الجهود في عدة مجالات أهمها قطاع التكنولوجيا والاتصالات الحديثة كما تواصلت الاهتمامات بهذا القطاع، وضرورة تأمينه وكذا التسهيلات في ما يخص التعاملات الرقمية داخل الدول الإفريقية وصولا إلى اتفاقية مالابو لسنة 2014، التي تعرف على أنها نص قانوني استراتيجي جاء انطلاقا من تزايد التهديدات على مستوى الفضاء السيبراني بالنسبة للدول الإفريقية، هدفه حماية بيانات الأفراد وكذلك مواجهة الجرائم الإلكتروني العابرة للحدود[3].

[1] اعز الدين مبرك، محمد أمين محري ، الآليات القانونية لحماية البيانات الرقمية، https://2u.pw/4zayYM2i ، تم الاطلاع يوم(2024/05/20).

[2] مريم لوكال، قراءة في اتفاقية الاتحاد الإفريقي حول الأمن السيبراني وحماية المعطيات ذات الطابع الشخصي لسنة 2014، **مجلة الدراسات القانونية والاقتصادية**، لجامعة أمحمد بوقرة،م04.ع03،ص ص657-673.

[3] المكان نفسه.

وتتمثل الأهداف الرئيسية لهذه الاتفاقية فيما يلي:

- ✓ تعزيز التعاون الدولي بين دول القارة الإفريقية بغرض التنسيق بينها وتبادل المعلومات للوصول إلى حلول للمشاكل التي يعاني منها الفضاء السيبراني في هذه الدول، مثل تسليم المتورطين في جرائم المعلوماتية وكذا تقديم المساعدة القانونية
- ✓ تكييف التشريعات الوطنية للدول الأعضاء خاصة في مجال تكنولوجيا المعلومات والاتصال مع ضمان حقوق وحريات الأفراد[1].
- ✓ التنمية الرقمية في دول القارة ومساعدة الدول على الاستفادة قدر الإمكان من مزايا وإيجابيات التكنولوجيا الحديثة.

وإضافة إلى هذه الجهود تم إنشاء جهاز الأفريبول في 13 ديسمبر 2015بالجزائر ويتكون من قوات الأمن الوطني ل 21 دولة إفريقية مهمته الأساسية كجهاز أمني إفريقي هو مكافحة الجرائم العابرة للحدود على رأسها الجرائم المرتبطة بالفضاء السيبراني[2]

ب-اتفاقية جامعة الدول العربية لمكافحة الجريمة السيبرانية

لقد سعت الدول العربية إلى تعزيز التعاون في المجال السيبراني واستحداث قانون يمكن من خلاله محاربة الجرائم السيبرانية في إطار جامعة الدول العربية عن طريق التوقيع على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات يوم 21ديسمبر 2010، والتي نصت على ضرورة حشد الجهود لمكافحة التهديدات والأخطار ذات المصدر الإلكتروني وتوفير الأمن السيبراني خاصة بالنسبة للمواطنين والبنى التحتية للدول المشاركة في هذه الاتفاقية[3].

كما أكد مجلس جامعة الدول العربية بالنسبة للدول المصادقة على الاتفاقية على ضرورة مكافحة جرائم المعلومات، "**وإلى مواءاة الأمانة الفنية للمجلس بما تم اتخاذه من إجراءات المواءمة لتشريعاتها مع أحكام الاتفاقية، وتجريم كل صور الجرائم الإلكترونية... ومنع الإرهابيين من استخدام الأنترنت، وتعزيز التعاون بين المنظمات الدولية والإقليمية ومواجهة كافة أشكال الإرهاب الإلكتروني[4]**"

[1] المرجع نفسه، ص.361.
[2] مبرك، محري ،مرجع سابق.
[3] قطاف ، بوقرين ع، "مواجهة الجرائم السيبرانية في ضوء الاتفاقيات الدولية،مرجع سابق، ص 81.
[4] المكان نفسه.

إذن، ركزت هذه الاتفاقية على الأهمية الكبيرة لتكثيف جهود الدول والتعاون في إطار مكافحة جرائم المعلوماتية، مع الدول وكذلك المنظمات المتخصصة في هذا الشأن ومنع الإرهابين من استخدام وسائل التكنلوجيا الحديثة لتكثيف عملياتهم، وحماية كل المناطق ذات الأهمية الاستراتيجية مثل الموانئ والمطارات والحدود[1].

المطلب 02:آليات مواجهة التهديدات السيبرانية بالنسبة للمنظمات الدولية

لقد أدى النمو المتواصل للتهديدات السيبرانية إلى زيادة الاهتمام بضرورة استحداث آليات بإمكانها تحقيق الأمن السيبراني، ومنه قد سعت العديد من المنظمات الدولية إلى إيجاد استراتيجية أو إطار قانوني ذو بعد عالمي حتى تتمكن من مواجهة هذه المخاطر العابرة للحدود.

1- آليات منظمة الأمم المتحدة لمواجهة التهديدات السيبرانية

لقد برز اهتمام كبير من قبل منظمة الأمم المتحدة والجمعية العامة بكامل القضايا التي لها علاقة بالتطور التكنلوجي والأمن الإلكتروني وقامت بناء على هذا بمحاولات عديدة رغبة في مواجهة التهديدات القائمة والمحتملة، وكذا إعادة تعريف العديد من المفاهيم وربطها مع متغيرات البيئة الدولية الجديدة. وعلى هذا الأساس تعد دورتي جنيف 2003و دورة تونس 2005 من أبرز الجهود الدولية المتعلقة بالقمة العالمية لمجتمع المعلومات برعاية الأمم المتحدة[2].

وابتداء من 2015 تمكن الخبراء في منظمة الأمم المتحدة من وضع العديد من المعايير والضوابط التي بإمكانها مواجهة الهجمات ذات المصدر السيبراني، ولم يتم الاتفاق على هذه الضوابط من قبل جميع الأعضاء داخل المنظمة حتى سنة 2021. ومن أهم ما نصت عليه تلك الضوابط تجريم أي استعمال سلبي للفضاء السيبراني بغرض زعزعة الأمن والاستقرار، وذلك عن طريق تعهد تقدمه الدول لمنع أي ممارسات تدخل في إطار الممارسات الخبيثة ذات المصدر الإلكتروني، من هجمات سيبرانية وقرصنة وغيرها[3].

لقد أكدت منظمة الأمم المتحدة على الأهمية الكبيرة للتعاون الدولي وتكثيف جهود الفاعلين الدوليين بغرض صد الهجمات السيبرانية والمساعدة على كشف الفاعلين في هذا المجال عبر تبادل المعلومات وتكثيف عمل اجهاز المخابرات لكل دولة على حدا، بالإضافة إلى تبادل الخبرات لغرض تحسين الاستجابة لهذه التهديدات

[1] المكان نفسه.

[2] عبد الصادق،مرجع سابق،ص331.

[3] James Andrew Lewis, "Creating Accountability for Global Cyber Norms", Center for Strategic and International Studies (CSIS), February 23, 2022.

ومواجهتها كما يمكن للدول أن تقوم باستحداث أساليب جديدة تمكنها من حماية أمنها السيبراني وكذا التنبؤ بأي أخطار أو هجمات سيبرانية. بالإضافة إلى وضع الدول التشريعات القانونية للتحقيق في الجرائم السيبرانية وملاحقة مرتكبيها ويتم ذلك على عدة أصعدة وطنيا وإقليميا ودوليا بواسطة المنظمات التي تهتم بهذا الشأن[1].

والواقع أن هذه المشاريع لا يمكن أن تخضع لعملية المساءلة* نظرا لكون مجلس الأمن لا يتحرك إلا في حال استخدام القوة بالمفهوم التقليدي[2]. وهنا ظهر جدل كبير بين الدارسين في مجال العلاقات الدولية حول إمكانية اعتبار الأسلحة السيبرانية أسلحة تقليدية تنطبق عليها نفس معايير القوة الصلبة، ومدى إمكانية إخضاعها لقيود الاتفاقيات الدولية لحظر التسلح ومنع استعمال القوة في العلاقات الدولية أو التهديد باستخدامها، كما ورد في ميثاق الأمم المتحدة في المادة 02 الفقرة 04: "**يمتنع أعضاء الهيئة جميعا في علاقاتهم الدولية عن التهديد باستعمال القوة أو استخدامها ضد سلامة الأراضي أو الاستقلال السياسي ألية دولة أو على أي وجه آخر لا يتفق ومقاصد الأمم المتحدة**"[3].

وهنا لم يتم إعطاء تعريف واضح للقوة الأمر الذي جعل المختصين يتساءلون إذا كانت التهديدات السيبرانية تندرج في إطار استعمال القوة المذكورة في الميثاق أم أنها لا ترقى لذلك بناء على تأثيرها المحدود حيث لم تشهد العلاقات الدولية دمارا شاملا أو حروبا دامية بسبب قرصنة أو تجسس إلكتروني قام به أحد الفاعلين في البيئة الدولية ما يجعل مسألة الحسم في هذا الأمر صعبة نوعا ما. وهنا ظهر اتجاهان:

الاتجاه الأول: يؤكد أنصاره على أن التفسير يجب أن يكون ضيقا على حسب ما ورد في الميثاق والتهديدات غير العسكرية غير مذكورة فيه أي أنه لا ينطبق عليها ويستندون في ذلك إلى تجريم القوة المسلحة حسب ما نصت عليه ديباجة الميثاق، بالإضافة إلى" **استبعاد اقتراح البرازيل اعتبار إجراءات الضغوط الاقتصادية ضمن الاستخدام غير المشروع للقوة** "[4] وهو ما يعني أن أنصار هذا التوجه يفسرون ميثاق الأمم المتحدة تفسيرا حرفيا ولا يمكن للتهديدات السيبرانية أن تكون بمثابة استخدام للقوة المراد حظرها، نظرا لأنها لا تحدث

[1] أحمد ناصر ريسي، التعاون الدولي السبيل لمواجهة الجريمة السيبرانية، https://2u.pw/tNdLEdoN تم الاطلاع في يوم(2024/05/27).

* تعرف المساءلة الدولية على أنها مسؤولية الدول والجهات الفاعلة عن أفعالها وتصرفاتها على مستوى البيئة الدولية. ويقصد بها هنا ضرورة تحمل المسؤولين عن تنفيذ الهجوم السيبراني عواقب ونتائج هذا الهجوم من إدانة وعقوبات ضدهم، ويتم تقديرها على حسب الضرر الذي تسببت فيه هذه الهجمات. ونظرا لصعوبة اكتشاف الجهات الفاعلة في الهجوم السيبراني وصعوبة إثبات الجريمة عليها فتستحيل إدانة المجرمين.

[2] Loc.cit.

[3] أميرة عبد العظيم، محمد عبد الجواد، "الدفاع الشرعي وإشكالية الرد على الهجمات السيبرانية في ضوء ميثاق الأمم المتحدة"، ***مجلة روح القوانين لكلية الحقوق بجامعة طنطا***، ع.08،ص ص 881-934.

[4] المكان نفسه.

خسائر بشرية ومادية هائلة وتعد ذات تأثير محدود مثلها مثل الإكراه السياسي أو الاقتصادي رغم أنها تعد تهديدا كبيرا للأمن الدولي[1]

الاتجاه الثاني: يشير أنصار هذا الاتجاه إلى أن أي أعمال تخريبية أو انتقامية سواء كانت باستعمال القوة العسكرية أو دونها اعتمادا على الاقتصاد أو حتى الفضاء السيبراني عبر شن الهجمات السيبرانية والاستيلاء على البيانات تدخل في نطاق القوة التي حظر استعمالها في ميثاق الأمم المتحدة في إطار المادة 02ف 04، بل إن ممارسة ضغوط اقتصادية على سبيل المثال بإمكانه أن يؤدي إلى نتائج وخيمة على الأمن الدولي. ويمكن القول أن هذا الاتجاه يعتبر موسعا لمفهوم استخدام القوة، حيث يشير إجمالا إلى أن الهجمات السيبرانية يمكنها إحداث أضرار جسيمة ومادية ملموسة. وتستعمل القوة خاصة ما تعلق بتعطيل أنظمة حواسيب الدولة أو ما تعلق بالمنشأة الحيوية المرتبطة ارتباطا مباشرا بالفضاء الإلكتروني[2].

ورغبة في الخروج من هذا الجدل القائم بين المفكرين اقترح المفكر الألماني كارل شميت (Carl shmit) عددا من المؤشرات التي يمكن من خلالها اختبار هذه الهجمات، إذا كانت قد استخدمت القوة ويمكن إدراجها فيما نص عليه ميثاق الأمم المتحدة واعتمد في تصنيفه هذا حجم التأثير الذي تحدثه هذه الهجمات ومن بين المعايير المستخدمة لحساب شدة التأثير نجد خمسة معايير وهي[3]:

- ✓ شدة الهجوم: أي حجم تأثيره على الأفراد والمنشأة والخسائر المادية التي انجرت عنه، بالإضافة إلى شكل الضرر على الممتلكات.
- ✓ الضرر الفوري: أي أن تأثيره يكون قابل للملاحظة بعد مدة وجيزة من تنفيذ الهجوم
- ✓ يمكن قياس حجم الضرر.
- ✓ أن يكون عابرا للحدود الدولية.
- ✓ مشابه للهجوم العسكري في آثاره[4].

وانطلاقا من المعطيات المذكورة سابقا، يمكن القول أن المفاهيم في العلاقات الدولية تشهد تطورا مستمرا ومتزامنا والمستجدات الحاصلة في البيئة الدولية. وعلى هذا الأساس يعتبر المفهوم الضيق للقوة غير مناسب لإعطاء تصور شامل للتهديدات الجديدة، وخاصة ما تعلق بالهجمات السيبرانية التي تشهدها الدول، والتي

[1] المكان نفسه.
[2] انفس المرجع ،ص917.
[3] - نفس المرجع ، ص118
[4] المرجع نفسه ، ص 181

تمنع الدول من حقهم في الرد أو حتى تجريم الفاعلين وردعهم. وعلى هذا الأساس يعتبر التحليل الذي جاء به المفكر كارل شميت (Carl Schmitt) الأصح في تصنيف التهديدات غير العسكرية كونه يركز على الآثار التي خلفها هذا الاعتداء أو الهجوم بغض النظر عن كونه لا يعتمد على الأسلحة التقليدية، وهو ما يعد أكثر تناسبا مع الواقع الدولي ومستجداته بالإضافة إلى أنه بمثابة التطور الطبيعي لمفهوم القوة من كونها قوة تقليدية إلى قوة جديدة بالاعتماد على الوسائل التكنولوجية الحديثة وحتى الذكاء الصناعي في الحروب بوصفه ثورة العصر الحالي.

2 - أليات مواجهة التهديدات السيبرانية بالنسبة لمنظمة الشرطة الجنائية الدولية:

منظمة الشرطة الدولية هي منظمة دولية أنشئت سنة 1923 تتكون من 196 دولة عضوة هدفها الأساسي التحقيق في الجرائم العابرة للحدود، ومحاربتها عن طريق التنسيق وتوحيد جهود الدول الأعضاء، بالإضافة إلى أنها تسعى لمنع الجرائم السيبرانية نظرا لتأثيرها الكبير على المستوى الوطني والإقليمي والدولي، بغرض كشفها والتحقيق فيها ثم تقديم المجرمين إلى العدالة [1]. ومن هذا تعتبر هذه المنظمة بمثابة جهاز شرطة عالمي يسعى لمحاربة كل ما يمكنه أن يؤثر على الأمن الدولي، محاولا إيجاد سبل للتصدي لهذه التهديدات العابرة للحدود والتي لا تقوى الدول على مواجهتها بشكل منفرد بل وجب التنسيق للتصدي لها.

وقد اعتمدت هذه المنظمة في إطار مكافحة الجرائم السيبرانية على العديد من الأساليب والوسائل أهمها:

- تنسيق التعاون الشرطي بين الدول حيث تعتبر أكبر منظمة شرطية في العالم لها مكاتب في جميع أنحاء العالم، وتقوم بمكافحة كل ما تعلق بالجرائم العابرة للحدود كالتهريب، وتجارة المخدرات، وكذا الهجمات السيبرانية[2].
- تقوم هذه المنظمة الدولية بمساعدة الدول على فهم وتحليل الهجمات السيبرانية، والكشف عن مصادرها وأطرافها. كما تساهم في جمع معلومات استباقية لمساعدتها على التنبؤ بحدوث جرائم إلكترونية التي بإمكانها زعزعة الاستقرار في دولة ما أو ضرب بنيتها التحتية[3].
- اتخاذ جملة من الإجراءات التي بإمكانها كشف المجرمين، والتنسيق مع أجهزة إنفاذ القانون بالاعتماد على **"نموذج المكتب الإقليمي لمكافحة الجرائم السيبرانية والوصول إلى مقاضاة الفاعلين".**

[1] أسامة غريبي، "المنظمة الدولية للشرطة الجنائية (الإنتربول) ودورها في مكافحة الجريمة المنظمة"، ***مجلة دراسات وأبحاث***، م.03 ،ع. 03،(2011/03/15)ص ص154-173.
[2] ما هو الإنتربول؟، https://www.interpol.int/ar/3/3 ، تم الاطلاع في 2024/05/27).
[3] الإنتربول مكافحة الجريمة السيبرانية الاستراتيجية العالمية 2022-2025، https://2u.pw/HNC0EVaD ،تم الاطلاع،(2024/06/02).

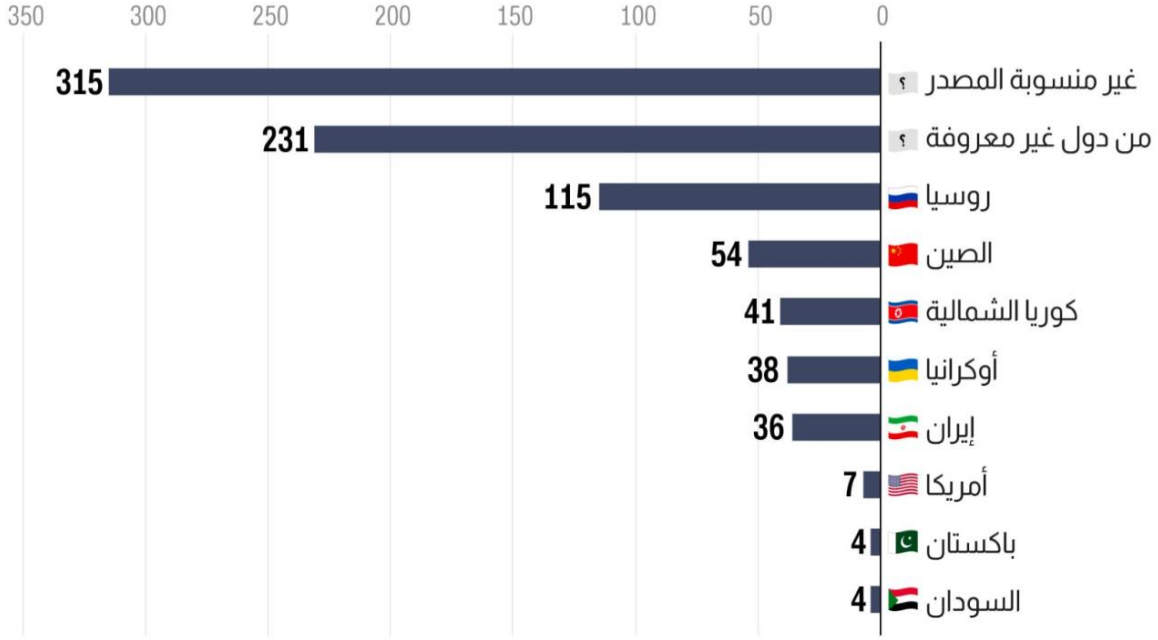
- كما تسعى هذه المنظمة إلى وضع اتفاقيات حول الجرائم السيبرانية وإمكانية استحداث طرق وقوانين جديدة بإمكانها الحد من تأثير هذه التهديدات الجديدة.

تعتبر هذه المنظمات الدولية من أبرز الجهود الدولية التي وضعت آليات لمحاربة الجرائم السيبرانية ذات التأثير على كل الفواعل في البيئة الدولية، وحاولت استحداث أساليب تمكنها من القضاء عليها أو حتى التقليل من خسائرها.

المطلب الثالث: مستقبل الهجمات السيبرانية وطبيعة التحولات على ظاهرة الحرب

تشهد الهجمات السيبرانية تزايدا رهيبا وتطورا هائلا في السنوات الأخيرة، خاصة مع التطورات الحاصلة في مجال التكنولوجيات الجديدة المرتبطة بالفضاء الإلكتروني، واستحداث تقنيات جديدة بإمكانها إحداث ثورة في هذا المجال. ويشير العديد من الخبراء والمختصين إلى أن نسبة الهجمات منذ سنتين تشهد ارتفاعا كبيرا، استنادا على فحص بعض الإحصائيات حيث وصل إجمالي الهجمات السيبرانية 895 عملية سيبرانية سنة 2023وهي مقسمة كالتالي:

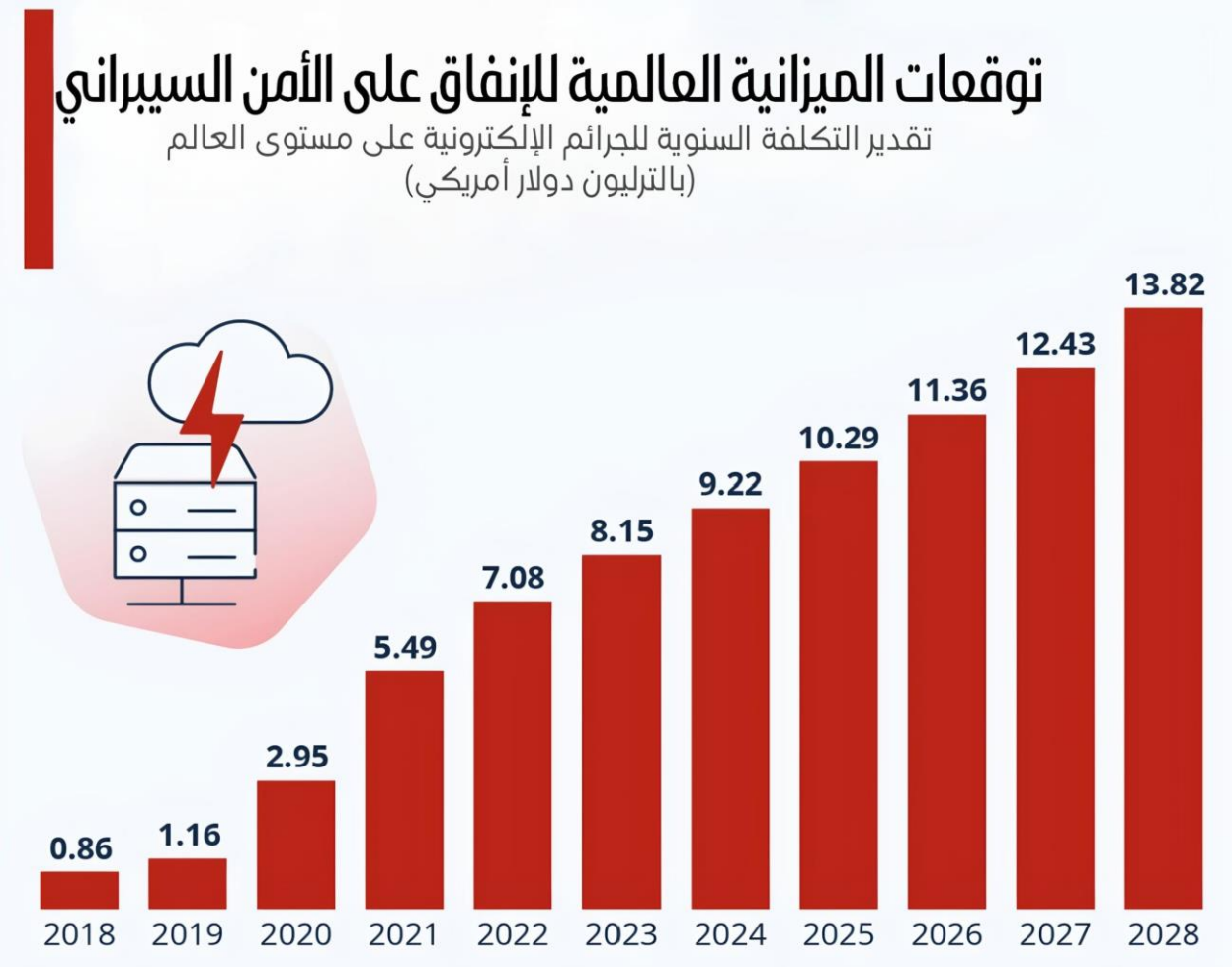
الشكل06: عدد العمليات السيبرانية من قبل البلدان المشتبه بها لسنة 2023.



المصدر: العمليات السيبرانية الأعلى المسجلة وفقًا للدول المستهدفة في عام 2023،في https://2u.pw/oz90jmX6، تاريخ الاطلاع(01 /2024/06).

ومن خلال الشكل يمكننا أن نلاحظ أن عدد الهجمات السيبرانية لعام 2023 شهد ارتفاعا رهيبا مقارنة بالعام السابق. ولهذا وجب على الدول حول العالم تخصيص ميزانيات أكبر لغرض تحقيق الأمن السيبراني، وحماية بيانات مواطنيها. وحسب توقعات الخبراء حول الجرائم الإلكترونية، فإن السنوات المقبلة سترتفع التكلفة العالمية المخصصة لمكافحة الجرائم الإلكترونية من 9,22تريليون دولار عام 2024إلى 13,82ترليون دولار بحلول عام 2028[1].

الشكل رقم07: توقعات الميزانية العالمية للإنفاق على الأمن السيبراني.



المصدر: Anna Fleck, Cybercrime Expected To Skyrocket in Coming Years, https://2u.pw/MySqctx8 .(2024/06/02).

[1]Anna Fleck, Cybercrime Expected To Skyrocket in Coming Years, https://2u.pw/MySqctx8 ,(02/06/2024).

وبناءا على هذا فالهجمات السيبرانية حسب المعطيات الحالية في تزايد مستمر ومن المتوقع أن تزداد تعقيدا وخطورة في المستقبل نظرا للعديد من العوامل أهمها:

- ✓ تقنية الذكاء الاصطناعي: حيث يتم استخدام الميزات التي يوفرها الذكاء الاصطناعي لتنفيذ هجمات سيبرانية أكثر قوة وتعقيدا، وتحقيق مكاسب ضد الخصوم عبر استغلاله في إنشاء هجمات يصعب اكتشافها أو التصدي لها عبر استحداث برامج ضارة أكثر ذكاء تعمل على تدمير المراكز الحيوية ذات الأهمية ويمكنها بذلك التهرب من الرقابة والوصول إلى غايتها بكل أريحية[1].
- ✓ التغيير الحاصل في ظاهرة الحرب، من كونها حرب تعتمد على وسائل تقليدية محدودة التأثير إلى أساليب أكثر تطورا منها طائرات المسيرة الصغيرة القادرة على الانتشار السريع دون أثر، بالإضافة إلى الروبوتات ذاتية التحكم التي تستخدم لمحاربة الجماعات الإرهابية من طرف الدول الكبرى كالولايات المتحدة الأمريكية.
- ✓ الهجمات الهجينة: حيث أصبح الحديث عن الهجمات الهجينة التي بدورها تعتمد على الأساليب التقليدية والحديثة على حد سواء، لتحقيق أهدافها في البيئة الدولية أي أن القوة العسكرية وحدها لم تعد كافية وصار إلزاما على الدول التفكير في وسائل أخرى لتدعيم سياساتها ومواجهة خصومها[2].
- ✓ تأثير الهجمات السيبرانية على اقتصاد الدول: حيث أن الهجمات السيبرانية لا تقتصر على صناعات محددة بل تستهدف حتى القطاعات الحيوية لعمل الاقتصاد العالمي، فالبنوك والمؤسسات المالية والإنتاجية وأنظمة الطاقة والنقل تعتبر الأكثر استهدافا من قبل المهاجمين، ونتيجة للارتباط الكبير بين هذه القطاعات واعتمادها على التكنولوجيا الحديثة.

ورغم المزايا والخدمات التي توفرها إلا أنه في ظل تزايد نسبة الهجمات السيبرانية التي تشنها الدول ضد خصومها صار لابد من التفكير في أساليب لتحقيق الأمن السيبراني[3].

كما أن الحروب قد تأثرت كثيرا بالتزايد الرهيب للهجمات السيبرانية وأبرز مثال على ذلك الحرب الروسية الأوكرانية الهجينة التي استعملت فيها الدولة الروسية كل الأساليب والوسائل العسكرية والسيبرانية على حد سواء، رغبة في تحقيق النصر وتتميز الحروب الجديدة بهذه الخاصية نظرا الأن القوة العسكرية لم

[1] رشاد، **مرجع سابق**، ص 693

[2] تقنيات الأمن السيبراني والتحديات المستقبلية، https://2u.pw/LwUrexj ، تم الاطلاع في يوم(2024/06/03).

[3] كيف يهدد تطور الهجمات السيبرانية الاقتصاد العالمي ؟، https://2u.pw/yOPUNPtP ، تم الإطلاع في يوم(2024/60/04).

تعد كافية لتحقيق أهداف الحرب خاصة في ظل المتغيرات الدولية الجديدة، والتقنيات التي ظهرت على الصعيد التكنولوجي أهمها الذكاء الاصطناعي.

واستنادا على توقعات الخبراء والمختصين ستتزايد التهديدات السيبرانية التي بدورها ستلزم الدول بتطوير وتحديث آليات الدفاع وحماية بياناتها من أي تدمير قد يطالها. وما يمكن قوله هو أن الحرب أصبحت في شكلها الجديد متعددة الأبعاد والوسائل، بالإضافة إلى القوة العسكرية كمحدد رئيسي لا يمكن الاستغناء عنه أو حتى تهميشه نظرا لأهميته في حسم النزاعات والحروب. وأصبح الحديث عن الحرب الهجينة أي المختلطة التي تستند إلى كل الوسائل لتحقيق النصر وحسب ما تشهده الساحة الدولية تعد الأنجح والأقدر على مواجهة المخاطر الدولية واكتساب مكانة دولية.

خلاصة الفصل:

ختاما لهذا الفصل يمكن القول أن الاستراتيجية الروسية في الحرب الدائرة حاليا بتبنيها مبدأ الحرب الهجينة كانت ناجحة إلى حد فرض نفوذها وإبراز قوتها للعالم ككل. ومع تزايد حدة الهجمات السيبرانية في العالم اليوم صار من العاجل استحداث آليات للتصدي لهذه التهديدات العابرة للحدود، وذلك لا يتم إلا بواسطة حشد جهود الدول، وكذا المنظمات الدولية للوصول إلى تشريعات وقوانين بإمكانها الحد من هذه الجرائم. ورغم صعوبة إثباتها إلا أن المحاولات تبقى قائمة في سبيل تحقيق الأمن السيبراني.

يتضمن التعاون في المجال السيبراني مساعدة الدول التي ليس لها إمكانيات كافية على تأمين فضائها السيبراني عن طريق تقديم مساعدات مالية سواء من قبل المنظمات الدولية أو حتى المؤسسات المالية الدولية مثل البنك العالمي، وصندوق النقد الدولي لمساعدتها على بناء قدرات دفاعية تمكنها من تجاوز الأخطار الإلكترونية.

الخاتمة

ختاما لهذه الدراسة أصبحت الهجمات السيبرانية تشكل تهديدا حقيقيا على الدول والمنظمات الدولية وكذلك الأفراد، والمؤسسات، وتعد محددا حاضرا بقوة في الساحة الدولية خاصة باعتبارها وسيلة حرب جديدة تعتمدها الدول جنبا إلى جنب مع الوسيلة العسكرية. فحسب ما توصلت إليه هذه الدراسة لا يمكن للدول بأي شكل من الأشكال أن تستغني عن القوة العسكرية واكتفائها بتطوير أليات الدفاع والهجوم السيبراني. وتظل القوة العسكرية ذات أهمية إضافة إلى المحددات الأخرى مثل الاقتصاد والإعلام والتحكم في التكنولوجيا. ولعل أبرز مثال عن ذلك هو الحرب الروسية الأوكرانية المستمرة، حيث أنه على الرغم من تنفيذ روسيا للعديد من الهجمات السيبرانية ضد البنية التحتية الأوكرانية قبيل البدء في شن العمليات العسكرية، إلا أنها لم تستطع تحقيق أهدافها من الحرب ومنع انضمام أوكرانيا إلى حلف الشمال الأطلسي، أي أن القوة السيبرانية بإمكانها التأثير في مسار الحرب وليس حسمها أو تحقيق انتصارات ومكاسب ذات أهمية استراتيجية.

وبناء على هذه الدراسة تم التوصل إلى النتائج التالية:

- ✓ لقد ساهم الفضاء السيبراني كمتغير جديد في العلاقات الدولية في إعادة إعطاء تعريف جديد للعديد من المفاهيم مثل القوة، الحرب، والأمن وأصبحت تحمل أبعادا أخرى.
- ✓ تشهد البيئة الدولية تزايدا مستمرا في عدد الهجمات السيبرانية، بالإضافة إلى التطور في طرق وأساليب تنفيذها خاصة ما تعلق باستعمال التقنيات الحديثة مثل الذكاء الاصطناعي.

- ✓ إن الدول الأكثر اعتمادا على الفضاء السيبراني تعد الأكثر استهدافا من طرف المهاجمين وتكون معرضة للمساس بأمن بياناتها، وتشهد نسبا مرتفعة في تلقيها للهجمات نظرا لانكشاف بياناتها مما يسهل عملية التلاعب بها، واستعمالها لأغراض غير قانونية كالتجسس.
- ✓ شهدت الحروب الروسية الأوكرانية من 2014 إلى 2021 تطورا في أساليبها ووسائلها انطلاقا من اعتبار الهجمات السيبرانية جزء من الاستراتيجية الروسية الحربية واستحداث آليات تمكنها من تحقيق النصر، وصولا إلى دولة أوكرانيا في محاولاتها لتأمين بنيتها التحتية ضد أي اختراق أو هجوم قد يطالها وذلك بمساعدة من الدول الغربية.
- ✓ خلال دراسة الحرب الروسية الأوكرانية يتضح أن الهجمات السيبرانية لوحدها لم تحقق أهداف السياسة الخارجية الروسية ولذلك تم استعمال القوة العسكرية في الحرب القائمة حاليا بين الدولتين.

- ✓ رغم الجهود المبذولة من قبل المنظمات الدولية إلا أن الفضـــاء الســـيبراني يبقى مجالا مفتوحا لهيمنة القوى الكبرى وتحقيق مصـــالحها في البيئة الدولي،ة نظرا لغياب آليات بإمكانها كشـــف المجرمين، وغياب المســـاءلة وصـــعوبة إثبات الجرائم الســـيبرانية على مرتكبيها خاصـــة في ظل تطور أســـاليب التخفي وبروز الحرب السيبرانية بالوكالة.

<u>وعليه يمكن تقديم الاقتراحات التالية:</u>

- ✓ يجب على الدول التخلص من التبعية في المجال التكنلوجي والاســتثمار في تطوير برمجيات محلية لكل دولة على حدا رغبة في حماية الأمن الســـيبراني، ولتجنب الاعتماد على البرمجيات الأجنبية التي قد تكون معرضة للاختراق والتجسس.
- ✓ تعزيز مبادئ التعاون وإقامة شـــراكات بين الدول في مجال مكافحة الجرائم الســـيبرانية، وتبادل الخبرات بين الفواعل. بالإضـافة إلى إمكانية تقديم مسـاعدات مالية للدول الضـعيفة حتى تتمكن من تطوير وتحديث أجهزتها الدفاعية ضد هذه الهجمات.
- ✓ تطوير ســـياســـيات واســـتراتيجيات وطنية تمكن الدول من مواجهة التهديدات القادمة من الفضـــاء السيبراني، وكذا التفكير في خطط تمكنها من الاستجابة السريعة في حالة الطوارئ.
- ✓ اعتماد نســخ احتياطية للبيانات المهمة الخاصـــة بالدول، والمنظمات الدولية يمكن الاعتماد عليها في حالة ما إذا تم إتلاف النسخ الأصلية وذلك لضمان استمرار نشاطاتها وعدم الرضوخ لأي مهاجم في حال طلب فدية لاسترجاع البيانات المسروقة.
- ✓ ضرورة تعزيز الدول لأنظمة الدفاع السيبراني لأن النظام الدولي يشهد تزايدا ملحوظا في عدد الحروب الهجينة التي يتم فيها الاعتماد بكثرة على توجيه هجمات سيبرانية مدمرة لمنظومة دفاع الخصم.

المصادروالمراجع

أولا باللغة العربية:

✓ الكتب:

_ بدوي عبد الرحمان. **مناهج البحث العلمي**. الكويت: وكالة المطبوعة، ط.03. 1977.

_ خيري فرجاني. **أوكرانيا والأمن القومي الروسي**. القاهرة: دار البيان،2020.

_ شفيق، نوران. **أثر التهديدات الإلكترونية على العلاقات الدولية**. "دراسة في أبعاد الأمن الإلكتروني القاهرة مصر، المكتب العربي للمعارف،2016.

_ عبد الرحمان بدوي، مناهج البحث العلمي، (الكويت: وكالة المطبوعة، ط.03(1977،، ص.05.

_ عبد الصادق، عادل. **الإرهاب الإلكتروني القوة في العلاقات الدولية نمط جديد وتحديات مختلفة**.مصر، مركز الأهرام للدراسات السياسية والاستراتيجية 2009.

_ محمود محمد علي. **كيف تم توظيف الإعلام في الحرب الروسية الأوكرانية**. لقاهرة: دار المعارف،2022.

_خليفة، إيهاب. **القوة الإلكترونية كيف يمكن أن تدير الدولة شؤونها في عصر الأنترنت**. القاهرة، العربي للنشر والتوزيع 22 ماي 2017.

_محمد شلبي. **المنهجية في التحليل السياسي مفاهيم –مناهج –إقترابات**. الجزائر :ديوان المطبوعات الجامعية،1997

✓ المقالات في المجلات العلمية:

_ لطفي وفاء "الجهود الدولية في مجال مكافحة جرائم الإرهاب السيبراني التجربة الماليزية نموذجا "، مجلة كلية الاقتصاد والعلوم السياسية لجامعة القاهرة .23،(يناير 2022) ص ص151-172.

_ عبد الكريم عبد الوهاب أحمد، خلف عبد الرحمان محمود، "إشكالية الأمن السبيراني العراقي بين التهديدات السبيرانية والتقنين المقيد للحريات"، مجلة قضايا سياسية لكلية العلوم السياسية جامعة النهرين،ع60،(2020)، ص ص .1-19.

_ أدمام شهرزاد ،"الفواعل العنيفة من غير الدول ،دراسة نظرية في الأطر المفاهمية والنظرية" ،سياسات عربية ،ع8،(أبريل 2014) ص ص 69-82.

_ أسماء حداد،" الحروب الهجينة :أوكرانيا أنموذجا"مجلة مدارات سياسية ،ديسمبر (2017)،ص ص129,114

_ بوطلاعة وداد بوكورو منال،" الهجمات السيبرانية على البنية التحتية الحرجة "،دراسة في ضوء القانون الدولي العام، صادرة عن مخبرالدستورالجزائري والدراسات القانونية والاستشرافية، جامعة الأخوة منتوري قسنطينة 1،منشورة في مجلة حقوق الإنسان والحريات العامة، ع 07،ع02، (2022) ص ص ،322-355.

_ بوقرص ساعد، الأمن السيبراني: مخاطر وتهديدات وتحديات تتطلب ممارسات وتوصيات واستراتيجيات خاصة، مجلة الأبحاث في الحماية الاجتماعية ،م.03 ع.01،(22جوان 2022) ص ص 61، 77.

_ بيدي أمال، "جهود الأمم المتحدة لمواجهة الجريمة السيبرانية"، مجلة البحوث في الحقوق والعلوم السياسية،م.08،ع.01،(2022)،ص ص299-316.

_ تغريد صفاء ولبنى خميس مهدي، "أثر السبيرانية في تطور القوة" ،مجلة حمورابي ،م3،ع 34,33،(السنة الثامنة شتاء 2020) ص ص145-161.

_ حميد علي حسين ، أنغام عادل حبيب، "ملامح توظيف الفضاء السيبراني في عالمنا المعاصر(الحرب الروسية الأوكرانية نموذجا)"،القضايا السياسية،ع72،(03/31 /2023)،ص ص.150-172.

_ حناشي نجيم، "البحث العلمي مناهجه وأساليبه العلمية"، مجلة دراسات لجامعة عبد الرحمان ميرة ببجاية،م.11،ع.01،(ماي 2022)،ص ص665-682

_ حناشي نجيم، "البحث العلمي مناهجه وأساليبه العلمية"، مجلة دراسات لجامعة عبد الرحمان ميرة ببجاية،م.11،ع.01،(ماي 2022)، ص ص665-682.

_ سليمة طيان، عادل زقاع،" تحول القوة في العلاقات الدولية: محددات ثانوية "،المجلة الجزائرية للأمن والتنمية ،م12،ع3،(جويلية 2023) ص ص 191-204.

_ سمير باي، "التهديدات الأمنية السيبرانية: دراسة في انعكاسات الحرب لإلكترونية على الأمن القومي للدول واستراتيجيات المقاومة، مجلة الرسالة للدراسات والبحوث الإنسانية، م.08،ع.02،(جوان 2023)،ص ص 189-200.

_ سمير باي، "التهديدات الأمنية السيبرانية: دراسة في انعكاسات الحرب لإلكترونية على الأمن القومي للدول واستراتيجيات المقاومة، مجلة الرسالة للدراسات والبحوث الإنسانية، م.08،ع.02،(جوان 2023)،ص ص 189-200.

_ شكارة نادية ضياء، "تداعيات الأزمة الأوكرانية على العلاقات الروسية الأوكرانية 2014-2016"،جامعة النهرين بكلية العلوم السياسية،م.20،ع."(2017)،ص ص 433-456.

_ شويرب الجيلالي ومراد فائزة "مفهوم الحروب السبيرانية والأمن السبيراني "مجلة الحقوق والحريات ،م 11،ع1،(2023)ص ص 157-178.

_ عبد العظيم أميرة ، محمد عبد الجواد، "الدفاع الشرعي وإشكالية الرد على الهجمات السيبرانية في ضوء ميثاق الأمم المتحدة"، مجلة روح القوانين لكلية الحقوق بجامعة طنطا، ع.08،ص ص 881-934.

_ عبد الكريم محمد زهير،" الإرهاب السبيراني وأزمة عالمية جديدة"، مجلة القضايا السياسية،ع 64(يناير 2021)، 277-294، متاحة على الرابط التالي : https://political-encyclopedia.org/library/1561/download .

_ عدنان يحي بهاء ،تأثير التهديدات السبيرانية في الصراعات الإقليمية (نماذج مختارة)،مجلة كلية التربية للبنات للعلوم الإنسانية ،ع. 32،ص ص 399-420.

_ علي مفتاح علي شاوش ،"تأثير الأزمة الأوكرانية على العلاقات الروسية الغربية "،مجلة جامعة بني وليد للعلوم الإنسانية والتطبيقية ،ع 29(2023/09/20) ص ص.339-358.

_ عنتر عادل علي زعلوك، التطور المنهجي لمفهوم القوة في العلاقات الدولية دراسة مسحية في الأدبيات المعاصرة "المجلة العلمية لكلية الدراسات الاقتصادية والعلوم السياسية ،م 08،ع16،(جويلية2023)ص ص 251-276.

_ عوض جاب الله موسى عادل،"وسائل حماية الأمن السبيراني، دراسة فقهية تأصيلية مقارنة بالنظم المعاصرة "،المجلة العلمية لجامعة الأزهر كلية الشريعة والقانون بأسيوط،م3 ،ع34،(2022). زينب فريح ،"دراسة في

محددات تطور الأجيال الخمس للحرب "،دفاتر السياسة والقانون ،م13،ع02،(15 /2021/05)، ص ص 542-555.

_ قطاف سليمان، بوقرين عبدالحليم، "الأليات القانونية الموضوعية لمكافحة الجرائم السيبرانية في ضل اتفاقية بودابست"، المجلة الأكاديمية للبحوث القانونية والسياسية ،م.6،ع،(2022)،ص ص 334-358.

_ قطاف سليمان، بوقرين عبدالحليم، "مواجهة الجرائم السيبرانية في ضوء الاتفاقيات الدولية"، مجلة البحوث القانونية والإقتصادية، م.5،ع2،(2020)،ص ص62-87.

_ لوكال مريم ،قراءة في اتفاقية الاتحاد الإفريقي حول الأمن السيبراني وحماية المعطيات ذات الطابع الشخصي لسنة 2014،مجلة الدراسات القانونية والاقتصادية لجامعة أمحمد بوقرة،م04.ع.03،ص ص657-673.

_ ليتيم فتيحة، ليتيم نادية "الأمن المعلوماتي للحكومة الإلكترونية والقرصنة" ،مجلة المفكر ، ع12، كلية الحقوق والعلوم السياسية، جامعة محمد خضير (الجزائر 2015) ص ص 238-253.

_ لين هربرت، "النزاع السيبراني والقانون الدولي الإنساني "،المجلة الدولية للصليب الأحمر .94،(2012)) ص ص 515-531.

_ محمد ياسين بونة أحمد، "الهجمات السبيرانية :الحرب الرقمية التي تجاوزت الحدود الجغرافية"، مجلة شمال إفريقيا للنشر العلمي،م1،ع4،(ديسمبر2023) ص ص.154-168.

_ محمود خالد وليد، "الهجمات عبر الأنترنت ساحة صراع الإلكتروني الجديدة"، سياسات العربية ،ع5(نوفمبر 2013) ص ص 115-125.

_ محمود علي عبدالرحمن، "الفضاء الكتروني وأثره علي مفاهيم القوة والأمن والصراع في العلاقات الدولية"، مجلة كلية السياسة والاقتصاد،م.16،ع15،(جويلية 2022) ص ص.423-443.

_أحمد محمد جاسم، ستار محمد علاوي،" التطورات الداخلية في الاتحاد السوفيتي 1924 – 1939، مجلة ديالي، ع.57(2013) ،ص ص 1-36.

_أسامة غريبي، "المنظمة الدولية للشرطة الجنائية (الإنتربول) ودورها في مكافحة الجريمة المنظمة"، مجلة دراسات وأبحاث،م.03 ،ع. 03،(2011/03/15)ص ص154-173.

_أماني عصام، "استخدام روسيا للقوة السيبرانية في إدارة تفاعلاتها الدولية"، مجلة كلية الاقتصاد والعلوم السياسية لجامعة حلوان، م.22، ع.04، (أكتوبر2021)،ص ص 167-190.

_سوزي رشاد ،التهديدات الأمنية الهجينة في العلاقات الدولية (السيبرانية و الذكاء الاصطناعي نموذجا)،وادي النيل للدراسات والبحوث الإنسانية والاجتماعية والتربوية (06أكتوبر)،ص ص 663-700.

_شرقي عبد الغاني"التهديدات السيبرانية وإشكالية السيادة ،مجلة السياسة العالمية،م7،ع2، ص 270-286.

_شلوش نورة ،"القرصنة الإلكترونية في الفضاء السيبراني التهديد المتصاعد للأمن الدول"، مجلة مركز بابل للدراسات الإنسانية،م.8،ع.2،(2018) ص ص .185-206..

_عبودي على عبد الرحيم،"هاجس الحروب السيبرانية وتداعياتها على الأمن والسلم الدوليين"، المجلة الأكاديمية العلميةIRAQUI ،م57،(2019) ص ص 89-118.

✓ **<u>الرسائل الجامعية:</u>**

_ عقون نورة ، واقع الفضاء السيبراني وإشكالية الدفاع الوطني في الجزائر، مذكرة تخرج للاستكمال متطلبات نيل شهادة الماستر في ميدان الحقوق والعلوم السياسية، (جامعة قاصدي مرباح ورقلة كلية الحقوق والعلوم السياسية، 2018، 2019ص ص 14.

_ هندي أية ،التهديدات السيبرانية وأثرها على الأمن القومي الجزائري ،مذكرة للاستكمال متطلبات نيل شهادة الماستر في العلوم السياسية والعلاقات الدولية (جامعة الجزائر 03كلية العلوم السياسية والعلاقات الدولية ،2022-2023)ص 33.

✓ **المقالات الصادرة عن مراكزدراسات:**

_ مايكل، كوفمان وآخرون "عبر من عمليات روسيا في شبه جزيرة القرم وشرق أوكرانيا"، مؤسسة راند،ص50.

_عبد الصادق عادل الإرهاب الإلكتروني القوة في العلاقات الدولية نمط جديد وتحديات مختلفة (مصر مركز الأهرام للدراسات السياسية والاستراتيجية 2009)، ص 106.

يارا عبد الجواد، "التوجهات الاستراتيجية لروسيا الاتحادية وعلاقتها مع الغرب"، مركز قضايا ونظرات ،(جويلية 2022)ص 28.

✓ **المو اقع الإلكترونية:**

_ الشريف ماهر، السياسة الاقتصادية الجديدة (النيب): استراحة محارب، https://2u.pw/5sPKFPp3، (2024/04/26).

_ عبد المنعم علي، حدود تأثير العمليات السيبرانية في الحرب الروسية الأوكرانية، https://2u.pw/gYXUoPi ، تاريخ الاطلاع، (2024/05/19).

_ كيف يهدد تطور الهجمات السيبرانية الاقتصاد العالمي؟، https://2u.pw/yOPUNPtP ،تاريخ الإطلاع في يوم(2024/60/05).

_ مبرك عز الدين، محمد أمين مهري ،لآليات القانونية لحماية البيانات الرقمية، https://2u.pw/4zayYM2i ، تاريخ الاطلاع يوم(2024/05/20).

_ القليوبي رامي، ثماني سنوات على ضم القرم: حين بدأ ابتلاع أوكرانيا، https://2u.pw/OCFeU7uE ، (2024/05/08).

_ ما هو الإنتربول؟، https://www.interpol.int/ar/3/3 ، تاريخ الاطلاع في 2024/05/27).

_ محمود خالد وليد، عن مؤشرالقوة السيبرانية الوطني 2022، https://2u.pw/3pUeuMe، تاريخ الإطلاع في(2024/04/02).

_ أبو عبيد شيماء عويس، "القوة في العلاقات الدولية: دراسة تأصيلية"، https://n9.cl/1ln1 ، تاريخ الإطلاع في(2024/04/09).

_ أشهر الهجمات السبيرانية وكيفية مواجهتها والحماية منها ، https://2u.pw/jiyLTkMT ، تاريخ الإطلاع (2024/05/05).

_ الإنتربول مكافحة الجريمة السيبرانية الاستراتيجية العالمية 2022-2025، https://2u.pw/HNC0EVaD ،تاريخ الاطلاع،(2024/06/02).

_ البدري كيرو،" مفهوم الأمن السيبراني ونشأته وتطوره "،في https://n9.cl/bikmb ،بتاريخ الإطلاع (2024/04/15)

_ البياتي خالد عبد الغفار، "الحرب الإلكترونية التهديدات والتحديات في عصر التكنلوجيا الرقمية على الأمن القومي والمجتمعي"، https://www.alnahrain.iq/post/979 ،تاريخ الإطلاع(2024/03/02).

_ الحرب السيبرانية الروسية الأوكرانية ، الأساليب ، المخاطر وطرق المواجهة، https://2u.pw/LKKTtHYr ، تاريخ الإطلاع (2024/05/11).

_ السبكي حسام، "الحروب السيبرانية" المفهوم والأنماط والتداعيات على الأمن الدولي، https://roayahnews.com/?p=353430 تاريخ الإطلاع في (10 /2024/04).

_ الطبر أية، تعريف المنهج التاريخي، https://n9.cl/ofoxko ،تاريخ الاطلاع(2024/06/06).

_ العمليات السيبرانية الأعلى المسجلة وفقًا للدول المستهدفة في عام 2023،في https://2u.pw/oz90jmX6 ، تاريخ الاطلاع(01 /2024/06).

_ العنبري صابر غل ، الحرب السيبرانية، معركة بالوكالة بين إيران وإسرائيل، https://2u.pw/kyUjAtqX ،تاريخ الإطلاع في(10 /2024/04).

_ إليك حصاد خسائر الحرب الأوكرانية بالمليارات والأرواح، https://2u.pw/EG6650pd ، تاريخ الإطلاع (2024/05/17).

_ أية الطبر، تعريف المنهج التاريخي، https://n9.cl/ofoxko ،تاريخ الاطلاع(2024/06/06).

_ تريسي إسراء، هجمة إلكترونية تشلّ مؤسسات الدولة بأكملها. قصة "تمثال الأحرار" الذي أشعل الحرب السيبرانية بين أستونيا وروسيا، https://2u.pw/SH8u9dg ، تاريخ الإطلاع (2024/05/10)

_ تعريف المنهج الوصفي التحليلي ، https://n9.cl/wop07 ،تاريخ الاطلاع،(2024/06/05).

_ ثالث أكبر ترسانة في العالم. كيف جُرّدت أوكرانيا من أسلحتها النووية؟ ، https://2u.pw/RWC0eV7i ، تاريخ الإطلاع(2024/05/04).

_ حدود تأثيرالعمليات السيبرانية في الحرب الروسية الأوكرانية"، https://2u.pw/gYXUoPi ، تاريخ الإطلاع (2024/05/16).

_ روسيا وأوكرانيا الإخوة الأعداء: قصة الخلاف بين روسيا وثاني أكبر جمهوريات الاتحاد السوفياتي ،"في https://2u.pw/0bnI8CoU ،تاريخ الاطلاع(2024/04/23).

_ عبد الزهرة تمارة علاء ، "الحرب الهجينة"، مركز النهرين للدراسات الاستراتيجية، https://2u.pw/jcUGCjF3 . تاريخ الاطلاع، (2024/05/19).

_ عبد الناصر طه رمضان، اجتثاث الكولاك هكذا أباد السوفييت الآلاف من فلّاحي أوكرانيا، في https://2u.pw/0G4Z9u0O تاريخ الإطلاع (2024/04/27)

_ كلينتون «نادم» لضغطه على أوكرانيا للتخلي عن ترسانتها النووية عام 1994، https://2u.pw/YsQpgJx

_ منطقة توتر بين روسيا وأوكرانيا...حقائق عن بحر الأزوف ، https://2u.pw/S8p0TeF3 ، (2024/05/12).

__ أهم أدوات جمع البيانات في البحث العلمي، https://n9.cl/q3idh ،تاريخ الإطلاع،(2024/06/06).

_أبو عيشة عز الدين، "الهاكرز"... كتائب الاقتحام الإلكتروني في الحرب الروسية الأوكرانية، https://n9.cl/1g9tn ،تاريخ الاطلاع(2024/05/20).

_الشريف عبدالله عيسى، من الردع إلى المرونة: تغيرات الحرب السيبرانية بالوكالة بين روسيا وأوكرانيا، https://2u.pw/UzUrqF4y ، (2024/05/20).

_تقنيات الأمن السيبراني والتحديات المستقبلية، https://2u.pw/LwUrex j ، تاريخ الإطلاع في يوم(2024/60/03).

_جمال محمود، كيف استخدمت روسيا الهجمات الإلكترونية في حربها مع أوكرانيا؟ ، https://2u.pw/LzgKqf4X تاريخ الاطلاع، (2024/05/19ال).

_خريسات باسم علي ، ماهي الهجمات السيبرانية الروسية الجارية في أوكرانيا:اقتراح حول مستقبل الحرب السيبرانية https://2u.pw/3dvYw0yk تاريخ الاطلاع في (2024/05/19).

_ريسي أحمد ناصر، التعاون الدولي السبيل لمواجهة الجريمة السيبرانية، https://2u.pw/tNdLEdoN تاريخ الاطلاع في يوم(2024/05/27).

_عبد الشافي عصام،الحرب الروسية-الأوكرانية ومستقبل النظام الدولي، https://studies.aljazeera.net/ar/article/5361 ، (2024/05/09).

_هاني حسن محمود وأخرون،"أثر التهديدات السبيرانية على الأمن القومي:دراسة حالة ماليزيا 2015,2022"،في https://democraticac.de/?p=90955 تاريخ الاطلاع (2024/03/10)

ثانيا: المراجع باللغة الإنجليزية:

- ✓ **Books:**

_Jakub Przetacznik with Simon Tarp ova", Russia's war on Ukraine: Timeline of cyber-attacks" , **European Parliamentary Research Service**, (June 2022),p03.

_ JOSEPH .NYE ,"cyber power" ، **Cambridge :Harvard Kennedy schoolbelfer center for science and international affaires**,(may 2010):p4.

_ Risk and Resilience Team, "ETH Zürich Hotspot Analysis: Cyber and Information warfare in the Ukrainian conflict,", Center **for Security Studies (CSS)** ,(Zürich, October 2018),p07.

_ United Nations , "Office on Drugs and Crime" ,**United Nations Convention against Transnational Organized Crime and the Protocols Thereto**,(15November 2000),P 1-2

- ✓ **Scientific articles**

_ Grace B. Mueller., Benjamin Jensen., Brandon Valeriano., Ryan C. Maness & Jose M. Macias. "Cyber Operations during the Russo-Ukrainian War: From Strange Patterns to Alternative Futures ،"**Center for Strategic and International Studies** ،(JULY 2023).

_ Jaideep Singh and others, A Detailed Survey and Classification of Commonly Recurring Cyber Attacks", International Journal of Computer Applications (0975 – 8887), Volume. 141 No.)10(May 2016) ,p15-16.

_ James Andrew Lewis, "Creating Accountability for Global Cyber Norms", **Center for Strategic and International Studies (CSIS)**, February 23, 2022.

_ Robert M. Lee, SANS, Michael J. Asante," SANS, Tim Conway, SANS, "Analysis of the Cyber Attack on the Ukrainian Power Grid Defense Use Case", **ELECTRICITY INFORMAYIONSHARING AND ANALYSIS CENTER**,(March 18, 2016).

Web sites :

_Anna Fleck, Cybercrime Expected To Skyrocket in Coming Years, https://2u.pw/MySqctx8 ,(02/06/2024).

_ Dan craigen,nadia diakun "defining cyber security", https://2u.pw/Jo5QnLe4 (06/03/2024)

_ Dan craigen,nadia diakun "defining cyber security", https://2u.pw/Jo5QnLe4 (06/03/2024)

_ Florian Bayard, Snake, le redoutable malware espion de la Russie, a été détruit, 20 ans après sa création , https://2u.pw/ItwHOtS5 , (12/05/2024)

_ How Ukraine prepared for the declaration of independence as part of the USSR: the adoption of the Declaration of Sovereignty of Ukraine, https://2u.pw/49AHzZwZ , (03/05/2024).

_ Johan Nordberg, The Use of Russia's Military in the Crimean Crisis, https://n9.cl/t7glf , (10/05/2024)

_ Mr. James M. Boughton, 8 After the Fall: Building Nations out of the Soviet Union, https://2u.pw/qX3rAXo9 , (03/05/2024).

_ ORIGINS HISTORY OF UKRAINE, IN https://2u.pw/ggpP19l4

_ PEKKA SUTELA, Ukraine's Economy Since 1991, https://n9.cl/6e7t8 , (04/05/2024).

_ The famine of 1932–33 (Holodomor),Britannica, https://2u.pw/iee0uxoa ,(29/04/2024).

_ The War in Ukraine — Interwar Soviet Ukraine (1922-1939), UCONN /university of Connecticut, https://2u.pw/PKg4ZBK6 ,(30/04/2024).

_ What Is A Threat Actor? – Types & Examples, https://2u.pw/p7uicmlP ,(03/03/2024).

قائمة المصادر والمراجع

أولا باللغة العربية:

✓ الكتب:

_ بدوي عبد الرحمان. **مناهج البحث العلمي**. الكويت: وكالة المطبوعة، ط.03. 1977.

_خليفة، إيهاب. **القوة الإلكترونية كيف يمكن أن تدير الدولة شؤونها في عصر الأنترنت**. القاهرة, العربي للنشر والتوزيع 22 ماي 2017.

_خيري فرجاني. **أوكرانيا والأمن القومي الروسي**. القاهرة: دار البيان,2020.

_شفيق، نوران. **أثر التهديدات الإلكترونية على العلاقات الدولية**. "دراسة في أبعاد الأمن الإلكتروني القاهرة مصر، المكتب العربي للمعارف,2016.

_عبد الرحمان بدوي، مناهج البحث العلمي، (الكويت: وكالة المطبوعة، ط.03(1977,، ص.05.

_عبد الصادق، عادل. **الإرهاب الإلكتروني القوة في العلاقات الدولية نمط جديد وتحديات مختلفة**.مصر، مركز الأهرام للدراسات السياسية والاستراتيجية 2009.

_محمد شلبي. **المنهجية في التحليل السياسي مفاهيم –مناهج –إقترابات**. الجزائر :ديوان المطبوعات الجامعية,1997

_محمود محمد علي. **كيف تم توظيف الإعلام في الحرب الروسية الأوكرانية**. لقاهرة: دار المعارف،2022.

✓ المقالات في المجلات العلمية:

_ أسماء حداد," الحروب الهجينة :أوكرانيا أنموذجا"مجلة مدارات سياسية ,ديسمبر (2017),ص ص129,114

_أحمد محمد جاسم، ستار محمد علاوي،" التطورات الداخلية في الاتحاد السوفيتي 1924 – 1939، مجلة ديالي، ع.57(2013) ،ص ص 1-36.

_أسامة غريبي, "المنظمة الدولية للشرطة الجنائية (الإنتربول) ودورها في مكافحة الجريمة المنظمة", مجلة دراسات وأبحاث,م.03 ,ع. 03,(2011/03/15)ص ص154-173.

_أماني عصام، "استخدام روسيا للقوة السيبرانية في إدارة تفاعلاتها الدولية"، مجلة كلية الاقتصاد والعلوم السياسية لجامعة حلوان، م.22, ع.04, (أكتوبر2021),ص ص 167-190.

_بوطلاعة وداد بوكورو منال،" الهجمات السيبرانية على البنية التحتية الحرجة ",دراسة في ضوء القانون الدولي العام، صادرة عن مخبرالدستورالجزائري والدراسات القانونية والاستشرافية، جامعة الأخوة منتوري قسنطينة 1,منشورة في مجلة حقوق الإنسان والحريات العامة, ع 07,ع02, (2022) ص ص ,322-355.

_بوقرص ساعد, الأمن السيبراني: مخاطر وتهديدات وتحديات تتطلب ممارسات وتوصيات واستراتيجيات خاصة, مجلة الأبحاث في الحماية الاجتماعية ,م.03 ع.01,(22جوان 2022) ص ص 61, 77.

_بيدي أمال، "جهود الأمم المتحدة لمواجهة الجريمة السيبرانية", مجلة البحوث في الحقوق والعلوم السياسية,م.08,ع.01,(2022),ص ص299-316.

_ تغريد صفاء ولبنى خميس مهدي, ‘‘أثر السبيرانية في تطور القوة" ,مجلة حمورابي ,م3,ع 34,33,(السنة الثامنة شتاء 2020) ص ص145-161.

_حميد علي حسين ، أنغام عادل حبيب، ‘‘ملامح توظيف الفضاء السيبراني في عالمنا المعاصر(الحرب الروسية الأوكرانية نموذجا)",القضايا السياسية,ع72,(03/31 /2023),ص ص.150-172.

_حناشي نجيم، ‘‘البحث العلمي مناهجه وأساليبه العلمية", مجلة دراسات لجامعة عبد الرحمان ميرة ببجاية,م.11,ع.01,(ماي 2022),ص ص665-682

_سليمة طيان، عادل زقاع،’’ تحول القوة في العلاقات الدولية: محددات ثانوية ",المجلة الجزائرية للأمن والتنمية ,م12,ع3,(جويلية 2023) ص ص 191-204.

_سمير باي، ‘‘التهديدات الأمنية السيبرانية: دراسة في انعكاسات الحرب لإلكترونية على الأمن القومي للدول واستراتيجيات المقاومة، مجلة الرسالة للدراسات والبحوث الإنسانية، م.08,ع.02,(جوان 2023),ص ص 189-200.

_سوزي رشاد ,التهديدات الأمنية الهجينة في العلاقات الدولية (السبيرانية و الذكاء الاصطناعي نموذجا),وادي النيل للدراسات والبحوث الإنسانية والاجتماعية والتربوية (06أكتوبر),ص ص 663-700.

شرقي عبد الغاني‘‘التهديدات السبيرانية وإشكالية السيادة ,مجلة السياسة العالمية,م7,ع2, ص 270-286.

_شكارة نادية ضياء, "تداعيات الأزمة الأوكرانية على العلاقات الروسية الأوكرانية 2014-2016",جامعة النهرين بكلية العلوم السياسية,م.20,ع."(2017),ص ص 433-456.

_شلوش نورة ,"القرصنة الإلكترونية في الفضاء السبيراني التهديد المتصاعد للأمن الدول", مجلة مركز بابل للدراسات الإنسانية,م.8,ع.2,(2018) ص ص .185-206..

_ أدمام شهرزاد ،"الفواعل العنيفة من غير الدول ,دراسة نظرية في الأطر المفاهمية والنظرية" ,سياسات عربية ,ع8,(أبريل 2014) ص ص 69-82.

_شويرب الجيلالي ومراد فائزة "مفهوم الحروب السبيرانية والأمن السبيراني "مجلة الحقوق والحريات ,م 11,ع1,(2023)ص ص 157-178.

_عبد العظيم أميرة ، محمد عبد الجواد، "الدفاع الشرعي وإشكالية الرد على الهجمات السيبرانية في ضوء ميثاق الأمم المتحدة", مجلة روح القوانين لكلية الحقوق بجامعة طنطا, ع.08,ص ص 881-934.

_عبد الكريم عبد الوهاب أحمد, خلف عبد الرحمان محمود, "إشكالية الأمن السبيراني العراقي بين التهديدات السبيرانية والتقنين المقيد للحريات", مجلة قضايا سياسية لكلية العلوم السياسية جامعة النهرين,ع60,(2020)، ص ص .1-19.

_عبد الكريم محمد زهير," الإرهاب السبيراني وأزمة عالمية جديدة", مجلة القضايا السياسية,ع 64(يناير 2021), 277-294, متاحة على الرابط التالي : https://political-encyclopedia.org/library/1561/download .

_عبودي على عبد الرحيم,"هاجس الحروب السبيرانية وتداعياتها على الأمن والسلم الدوليين", المجلة الأكاديمية العلميةIRAQUI ,م57,(2019) ص ص 89-118.

_عدنان يحيي بهاء ،تأثير التهديدات السبيرانية في الصراعات الإقليمية (نماذج مختارة),مجلة كلية التربية للبنات للعلوم الإنسانية ,ع. 32,ص ص 399-420.

_علي مفتاح علي شاوش ,"تأثير الأزمة الأوكرانية على العلاقات الروسية الغربية ",مجلة جامعة بني وليد للعلوم الإنسانية والتطبيقية ,ع 29(2023/09/20) ص ص.339-358.

_عنتر عادل علي زعلوك، التطور المنهجي لمفهوم القوة في العلاقات الدولية دراسة مسحية في الأدبيات المعاصرة "المجلة العلمية لكلية الدراسات الاقتصادية والعلوم السياسية ,م 08,ع16,(جويلية2023)ص ص 251-276.

_عوض جاب الله موسى عادل,"وسائل حماية الأمن السبيراني, دراسة فقهية تأصيلية مقارنة بالنظم المعاصرة ",المجلة العلمية لجامعة الأزهر كلية الشريعة والقانون بأسيوط,م3 ,ع34,(2022). زينب فريح ,"دراسة في محددات تطور الأجيال الخمس للحرب ",دفاتر السياسة والقانون ,م13,ع02,(15 /2021/05)، ص ص 542-555.

_قطاف سليمان، بوقرين عبدالحليم، "الأليات القانونية الموضوعية لمكافحة الجرائم السيبرانية في ضل اتفاقية بودابست", المجلة الأكاديمية للبحوث القانونية والسياسية ,م.6,ع,(2022),ص ص 334-358.

_قطاف سليمان، بوقرين عبدالحليم، "مواجهة الجرائم السيبرانية في ضوء الاتفاقيات الدولية"، مجلة البحوث القانونية والإقتصادية،م.5,ع2,(2020),ص ص62-87.

_لطفي وفاء ‘‘الجهود الدولية في مجال مكافحة جرائم الإرهاب السيبراني التجربة الماليزية نموذجا ‘‘، مجلة كلية الاقتصاد والعلوم السياسية لجامعة القاهرة .23,(يناير 2022) ص ص151-172.

_لوكال مريم ,قراءة في اتفاقية الاتحاد الإفريقي حول الأمن السيبراني وحماية المعطيات ذات الطابع الشخصي لسنة 2014,مجلة الدراسات القانونية والاقتصادية لجامعة أمحمد بوقرة,م04.ع.03,ص ص657-673.

_ليتيم فتيحة، ليتيم نادية ‘‘الأمن المعلوماتي للحكومة الإلكترونية والقرصنة" ,مجلة المفكر , ع12, كلية الحقوق والعلوم السياسية, جامعة محمد خضير (الجزائر 2015) ص ص 238-253.

_لين هربرت، "النزاع السيبراني والقانون الدولي الإنساني ",المجلة الدولية للصليب الأحمر .94,(2012)) ص ص 515-531.

_محمد ياسين بونة أحمد, ‘‘الهجمات السبيرانية :الحرب الرقمية التي تجاوزت الحدود الجغرافية", مجلة شمال إفريقيا للنشر العلمي,م1,ع4,(ديسمبر 2023) ص ص.154-168.

_محمود خالد وليد، "الهجمات عبر الأنترنت ساحة صراع الإلكتروني الجديدة"، سياسات العربية ،ع5(نوفمبر 2013) ص ص 115-125.

_محمود علي عبدالرحمن، "الفضاء الكتروني وأثره علي مفاهيم القوة والأمن والصراع في العلاقات الدولية", مجلة كلية السياسة والاقتصاد,م.16,ع15,(جويلية 2022) ص ص.423-443.

_ حناشي نجيم ، ‘‘البحث العلمي مناهجه وأساليبه العلمية", مجلة دراسات لجامعة عبد الرحمان ميرة ببجاية,م.11,ع.01,(ماي 2022)، ص ص665-682.

✓ **الرسائل الجامعية:**

_هندي أية، التهديدات السبيرانية وأثرها على الأمن القومي الجزائري ,مذكرة للاستكمال متطلبات نيل شهادة الماستر في العلوم السياسية والعلاقات الدولية (جامعة الجزائر 03كلية العلوم السياسية والعلاقات الدولية ,2022-2023)ص 33.

_عقون نورة ،واقع الفضاء السيبراني وإشكالية الدفاع الوطني في الجزائر، مذكرة تخرج للاستكمال متطلبات نيل شهادة الماستر في ميدان الحقوق والعلوم السياسية، (جامعة قاصدي مرباح ورقلة كلية الحقوق والعلوم السياسية, 2018, 2019ص ص 14.

✓ **المقالات الصادرة عن مراكز دراسات:**

_عبد الصادق عادل الإرهاب الإلكتروني القوة في العلاقات الدولية نمط جديد وتحديات مختلفة (مصر مركز الأهرام للدراسات السياسية والاستراتيجية 2009)، ص 106.

_مايكل، كوفمان وآخرون "عبر من عمليات روسيا في شبه جزيرة القرم وشرق أوكرانيا", مؤسسة راند,ص50.

يارا عبد الجواد، "التوجهات الاستراتيجية لروسيا الاتحادية وعلاقتها مع الغرب", مركز قضايا ونظرات ,(جويلية 2022)ص 28.

✓ **المواقع الإلكترونية:**

_أبو عبيد شيماء عويس, "القوة في العلاقات الدولية: دراسة تأصيلية", https://n9.cl/1ln1 , تاريخ الإطلاع في(2024/04/09).

_أبو عيشة عز الدين، "الهاكرز"... كتائب الاقتحام الإلكتروني في الحرب الروسية الأوكرانية, https://n9.cl/1g9tn ,تاريخ الاطلاع(2024/05/20).

_أشهر الهجمات السيبرانية وكيفية مواجهتها والحماية منها , https://2u.pw/jiyLTkMT , تاريخ الإطلاع (2024/05/05).

_إليك حصاد خسائر الحرب الأوكرانية بالمليارات والأرواح, https://2u.pw/EG6650pd , تاريخ الإطلاع (2024/05/17).

_الإنتربول مكافحة الجريمة السيبرانية الاستراتيجية العالمية 2022-2025, https://2u.pw/HNC0EVaD ,تاريخ الاطلاع,(2024/06/02).

_أهم أدوات جمع البيانات في البحث العلمي, https://n9.cl/q3idh ,تاريخ الإطلاع,(2024/06/06).

_أية الطبر، تعريف المنهج التاريخي، https://n9.cl/ofoxko ,تاريخ الاطلاع(2024/06/06).

_البدري كيرو،" مفهوم الأمن السبيراني ونشأته وتطوره ",في https://n9.cl/bikmb ,بتاريخ الإطلاع (2024/04/15)

_البياتي خالد عبد الغفار ، "الحرب الإلكترونية التهديدات والتحديات في عصر التكنلوجيا الرقمية على الأمن القومي والمجتمعي"، https://www.alnahrain.iq/post/979 ,تاريخ الإطلاع(2024/03/02).

_تريسي إسراء، هجمة إلكترونية تشلّ مؤسسات الدولة بأكملها. قصة "تمثال الأحرار" الذي أشعل الحرب السيبرانية بين أستونيا وروسيا، https://2u.pw/SH8u9dg , تاريخ الإطلاع (2024/05/10)

_تعريف المنهج الوصفي التحليلي , https://n9.cl/wop07 ,تاريخ الاطلاع,(2024/06/05).

_تقنيات الأمن السيبراني والتحديات المستقبلية, https://2u.pw/LwUrex j , تاريخ الإطلاع في يوم(2024/60/03).

_ثالث أكبر ترسانة في العالم. كيف جُرّدت أوكرانيا من أسلحتها النووية؟ , https://2u.pw/RWC0eV7i , تاريخ الإطلاع(2024/05/04).

_جمال محمود، كيف استخدمت روسيا الهجمات الإلكترونية في حربها مع أوكرانيا؟ ، https://2u.pw/LzgKqf4X تاريخ الاطلاع, (2024/05/19ال).

_حدود تأثيرالعمليات السيبرانية في الحرب الروسية الأوكرانية", https://2u.pw/gYXUoPi , تاريخ الإطلاع (2024/05/16).

_الحرب السيبرانية الروسية الأوكرانية , الأساليب ، المخاطر وطرق المواجهة, https://2u.pw/LKKTtHYr , تاريخ الإطلاع (2024/05/11).

_خريسات باسم علي ، ماهي الهجمات السيبرانية الروسية الجارية في أوكرانيا:اقتراح حول مستقبل الحرب السيبرانية https://2u.pw/3dvYw0yk تاريخ الاطلاع في (2024/05/19).

_روسيا وأوكرانيا الإخوة الأعداء: قصة الخلاف بين روسيا وثاني أكبر جمهوريات الاتحاد السوفياتي ,"في https://2u.pw/0bnI8CoU ,تاريخ الاطلاع(2024/04/23).

_ريسي أحمد ناصر، التعاون الدولي السبيل لمواجهة الجريمة السيبرانية, https://2u.pw/tNdLEdoN تاريخ الاطلاع في يوم(2024/05/27).

_السبكي حسام ، "الحروب السيبرانية" المفهوم والأنماط والتداعيات على الأمن الدولي, https://roayahnews.com/?p=353430 تاريخ الإطلاع في (10 /2024/04).

_الشريف عبدالله عيسى ، من الردع إلى المرونة: تغيرات الحرب السيبرانية بالوكالة بين روسيا وأوكرانيا، https://2u.pw/UzUrqF4y ، (2024/05/20).

_الشريف ماهر, السياسة الاقتصادية الجديدة (النيب): استراحة محارب, https://2u.pw/5sPKFPp3, (2024/04/26).

_الطبر أية ، تعريف المنهج التاريخي، https://n9.cl/ofoxko ,تاريخ الاطلاع(2024/06/06).

_عبد الزهرة تمارة علاء ، "الحرب الهجينة", مركز النهرين للدراسات الاستراتيجية, https://2u.pw/jcUGCjF3 . تاريخ الاطلاع, (2024/05/19).

_عبد الشافي عصام ,الحرب الروسية-الأوكرانية ومستقبل النظام الدولي, https://studies.aljazeera.net/ar/article/5361 , (2024/05/09).

_عبد المنعم علي، حدود تأثير العمليات السيبرانية في الحرب الروسية الأوكرانية، https://2u.pw/gYXUoPi ، تاريخ الاطلاع, (2024/05/19).

_عبد الناصر طه رمضان، اجتثاث الكولاك هكذا أباد السوفييت الآلاف من فلّاحي أوكرانيا، في https://2u.pw/0G4Z9u0O تاريخ الإطلاع (2024/04/27)

_العمليات السيبرانية الأعلى المسجلة وفقًا للدول المستهدفة في عام 2023,في https://2u.pw/oz90jmX6 , تاريخ الاطلاع(01 /2024/06).

_العنبري صابر غل ، الحرب السيبرانية، معركة بالوكالة بين إيران وإسرائيل, https://2u.pw/kyUjAtqX ,تاريخ الإطلاع في(10 /2024/04).

_القليوبي رامي، ثماني سنوات على ضم القرم: حين بدأ ابتلاع أوكرانيا, https://2u.pw/OCFeU7uE , (2024/05/08).

_ كلينتون «نادم» لضغطه على أوكرانيا للتخلي عن ترسانتها النووية عام 1994, https://2u.pw/YsQpgJx

_كيف يهدد تطور الهجمات السيبرانية الاقتصاد العالمي؟, https://2u.pw/yOPUNPtP ,تاريخ الإطلاع في يوم(2024/60/05).

_ما هو الإنتربول؟, https://www.interpol.int/ar/3/3 , تاريخ الاطلاع في (2024/05/27).

_ مبرك عز الدين، محمد أمين مهري ,لآليات القانونية لحماية البيانات الرقمية, https://2u.pw/4zayYM2i , تاريخ الاطلاع يوم(2024/05/20).

_محمود خالد وليد, عن مؤشرالقوة السيبرانية الوطني 2022, https://2u.pw/3pUeuMe, تاريخ الإطلاع في(2024/04/02).

_منطقة توتر بين روسيا وأوكرانيا...حقائق عن بحر الأزوف , https://2u.pw/S8p0TeF3 , (2024/05/12).

_هاني حسن محمود وأخرون،"أثر التهديدات السبيرانية على الأمن القومي:دراسة حالة ماليزيا في2015,2022",https://democraticac.de/?p=90955 تاريخ الاطلاع (2024/03/10)

ثانيا المراجع باللغة الإنجليزية:

- ✓ **Books:**

_Jakub Przetacznik with Simon Tarp ova", Russia's war on Ukraine: Timeline of cyber-attacks" , **European Parliamentary Research Service**, (June 2022),p03.

_ JOSEPH .NYE ,"cyber power" , **Cambridge :Harvard Kennedy schoolbelfer center for science and international affaires**,(may 2010):p4.

_ Risk and Resilience Team, "ETH Zürich Hotspot Analysis: Cyber and Information warfare in the Ukrainian conflict,", Center **for Security Studies (CSS)** ,(Zürich, October 2018),p07.

_ United Nations , "Office on Drugs and Crime" ,**United Nations Convention against Transnational Organized Crime and the Protocols Thereto**,(15November 2000),P 1-2

- ✓ **Scientific articles**

_ Grace B. Mueller., Benjamin Jensen., Brandon Valeriano., Ryan C. Maness & Jose M. Macias. "Cyber Operations during the Russo-Ukrainian War: From Strange Patterns to Alternative Futures ،"**Center for Strategic and International Studies** ،(JULY 2023).

_Jaideep Singh and others, A Detailed Survey and Classification of Commonly Recurring Cyber Attacks", International Journal of Computer Applications (0975 – 8887), Volume. 141 No.)10(May 2016) ,p15-16.

_ James Andrew Lewis, "Creating Accountability for Global Cyber Norms", **Center for Strategic and International Studies (CSIS)**, February 23, 2022.

_ Robert M. Lee, SANS, Michael J. Asante," SANS, Tim Conway, SANS, "Analysis of the Cyber Attack on the Ukrainian Power Grid Defense Use Case", **ELECTRICITY INFORMAYIONSHARING AND ANALYSIS CENTER**,(March 18, 2016).

Web sites :

_Anna Fleck, Cybercrime Expected To Skyrocket in Coming Years, https://2u.pw/MySqctx8 ,(02/06/2024).

_Dan craigen,nadia diakun "defining cyber security", https://2u.pw/Jo5QnLe4 (06/03/2024)

_ Florian Bayard, Snake, le redoutable malware espion de la Russie, a été détruit, 20 ans après sa création , https://2u.pw/ItwHOtS5 , (12/05/2024)

_How Ukraine prepared for the declaration of independence as part of the USSR: the adoption of the Declaration of Sovereignty of Ukraine, https://2u.pw/49AHzZwZ , (03/05/2024).

_ Johan Nordberg, The Use of Russia's Military in the Crimean Crisis, https://n9.cl/t7glf , (10/05/2024)

_Mr. James M. Boughton, 8 After the Fall: Building Nations out of the Soviet Union, https://2u.pw/qX3rAXo9 , (03/05/2024).

_ORIGINS HISTORY OF UKRAINE, IN https://2u.pw/ggpP19l4

_PEKKA SUTELA, Ukraine's Economy Since 1991, https://n9.cl/6e7t8 , (04/05/2024).

_The famine of 1932–33 (Holodomor),Britannica, https://2u.pw/iee0uxoa ,(29/04/2024).

_ The War in Ukraine — Interwar Soviet Ukraine (1922-1939), UCONN /university of Connecticut, https://2u.pw/PKg4ZBK6 ,(30/04/2024).

_ What Is A Threat Actor? – Types & Examples, https://2u.pw/p7uicmlP ,(03/03/2024).

فهرس الجداول

1. الجداول

2. الأشكال

فهرس المحتويات