اسم المقال: ملامح توظيف الفضاء السيبراني في عالمنا المعاصر (الحرب الروسية – الأوكرانية انموذجاً)
اسم الكاتب: أ.د. علي حسين حميد، انغام عادل حبيب
رابط ثابت: https://political-encyclopedia.org/library/1568
تاريخ الاسترداد: 2025/05/07 11:03 +03

E-ISSN : 2790-2404
P- ISSN 2070-9250
Qadaya siyasiyyat

Ministry of Higher Education
& Scientific Research
Al-Nahrain University
College of Political Science

وزارة التعليم العالي والبحث العلمي
جامعة النهرين
كلية العلوم السياسية

قضايا سياسية

Political Issues

مجلة فصلية محكمة

Arab Impact Factor
معامل التأثير العربي
2022:(2.11)
معامل تأثير (Arcif)
2022:(0.1712)

العدد ٧٢
Issue 72

كانون الثاني - شباط - اذار / ٢٠٢٣
Jan. - .Feb - .Mar. / 2023

جامعة النهرين
كلية العلوم السياسية

E-ISSN 2790-2404
P- ISSN 2070-9250
(معامل التأثير العربي 2022) : 2.11
(معامل ارسيفArcif 2022) : 0.1712
DOI prefix: 10.58298

قضايا سياسية
Political Issues

مجلة فصلية محكمة تعنى بنشر الأبحاث والدراسات السياسية العراقية والعربية والدولية
http://pissue.iq

قواعد النشر

- لغة المجلة هي اللغة العربية والانكليزية على أن يراعى الوضوح وسلامة النص.
- ترحب المجلة بنشر البحوث والدراسات السياسية النظرية والتطبيقية ولا سيما التي تجعل من قضايا المنطقة والعالم محط اهتمامها، ماضياً وحاضراً ومستقبلاً، وعلى وفق الآتي:
- أن لا يزيد عدد صفحات البحث أو الدراسة عن (25) صفحة مطبوعة بثلاث نسخ مرفقة مع قرص مرن (CD)، مع مراعاة حجم الخط (14) والتباعد (1,15) ونوع الخط Simplified Arabic على ان تكون الهوامش اسفل كل صفحة مطبوعة بالطريقة الالكترونية وبحجم خط (11) ونوع الخط Simplified Arabic وتجمع بقائمة منفصلة عن المصادر في نهاية البحث.
- أن تعتمد الأصول العلمية المتعارف عليها في إعداد البحوث والدراسات وكتابتها وبخاصة التوثيق بحيث تتضمن:

بالنسبة للكتاب الآتي: أسم المؤلف، عنوان الكتاب، مكان النشر، الأسم الكامل للناشر، تاريخ النشر، أرقام الصفحات.

اما بالنسبة للمقالة: فتتضمن أسم الكاتب، عنوان المقالة، اسم الدورية، مكان صدورها، عددها، تاريخها، وأرقام الصفحات.

- أن تتصف البحوث والدراسات بالموضوعية والدقة العلمية.
- أن تعتمد الترقيم العشري للعناوين الأساسية والفرعية او التنصيف المعياري العام.
- يرفق مع كل بحث او دراسة ملخصين (احدهما باللغة العربية والآخر باللغة الانكليزية) وقائمة بالمراجع والمصادر المعتمدة.
- تخضع جميع البحوث المقبولة للنشر الى نظام الاستلال الالكتروني في كلية العلوم السياسية – جامعة النهرين.
- يرفق مع كل بحث ودراسة سيرة ذاتية مختصرة للباحث.
- تقوم المجلة بإخطار الباحثين بإجازة بحوثهم أو دراساتهم بعد عرضها على محكمين تختارهم على نحو سري من بين أصحاب الاختصاص.
- يجوز للمجلة أن تطلب إجراء تعديلات شكلية أو شاملة على البحث أو الدراسة قبل إجازتها للنشر بما يتماشى مع أهدافها.
- لا تلتزم المجلة بإعادة البحوث والدراسات التي يعتذر عن نشرها.

- ترحب المجلة بالمناقشات الموضوعية لما ينشر فيها أو في غيرها من الدوريات وبأية ردود فكرية أو تصويب، وكذلك ترحب بنشر التقارير عن المؤتمرات والندوات ذات العلاقة ومراجعات الكتب وملخصات الرسائل الجامعية التي تتم إجازتها على أن تكون من إعداد أصحابها.

توجه جميع المراسلات إلى رئيس التحرير على العنوان الآتي

مجلة قضايا سياسية، كلية العلوم السياسية، جامعة النهرين–بغداد – الجادرية.

E.mail: pirj@ced.nahrainuniv.edu.iq

www.Pol-Nahrain.org

الرقم الدولي ISSN 2070-9250

جدول المحتويات

ملامح توظيف الفضاء السيبراني في عالمنا المعاصر (الحرب الروسية – الأوكرانية انموذجا)[▽]

The aspects of employing cyberspace in our contemporary world

(The Russian–Ukrainian war as a model)

أد. علي حسين حميد* أنغام عادل حبيب **

Dr. ALI HUSSEIN HAMEED Angham Adil Habeeb

الملخص:

لم يقتصر تأثير اختراق الثورة التكنولوجية مجالات الحياة المختلفة على التفاعلات السياسية والاقتصادية والمجتمعية للدول والافراد، بل امتدت لخلق ساحة جديدة من الحروب غير التقليدية، بعيدا عن ساحات البر والبحر والجو، الا وهي ساحة الفضاء السيبراني التي توافرت فيها عوامل عديدة حفزت الفواعل الدولية وغير الدولية على استخدامها كإحدى أدوات التنافس والهيمنة والصراع والإرهاب غير التقليدي، لدرجة قد تنقل العالم من الهجمات الالكترونية المختلفة الى "حرب سيبرانية" Cyber War.

تعد روسيا من أوائل الدول التي استغلت الفضاء السيبراني في المجال العسكري، اذ اهتمت بتطوير وزيادة قدراتها الهجومية في هذا المجال منذ عام 1998، وتعتمد الاستراتيجية الروسية في نزاعها مع أوكرانيا على الأسلحة الالكترونية الهجومية باعتبارها انها قوة مضاعفة في الحروب، بمعنى انها تزيد من القدرات القتالية للدولة اذا ما استخدمت الى جانب قدرات عسكرية أخرى، كما تعتمد هذه الاستراتيجية على محاولة تعطيل البنية التحتية المعلوماتية للخصم والاتصالات العسكرية والمدنية له قبل الشروع في العمليات العسكرية.

الكلمات المفتاحية: (الأمن السيبراني، الحرب السيبرانية، العمليات السيبرانية ، السيناريوهات المستقبلية)

Abstract:

The impact of the technological revolution's penetration into the various spheres of life was not limited to the political, economic and societal

▽ تاريخ التقديم : 2023/2/18 تاريخ القبول: 2023/3/16 تاريخ النشر: 2023/3/31

* كلية العلوم السياسية/جامعة النهرين dr.alihussien@nahrainuniv.iq

** باحثة ماجستير/كلية العلوم السياسية/جامعة النهرين Anghamadil232@gmail.com

interactions of states and individuals. Rather, it extended to the creation of a new arena of unconventional wars, far from the arenas of land, sea and air. The new arena of conflict is the cyber domain. The latter presented a new set of elements that incentivised state and non-state actors to use them as a tool of competition, domination, conflict, and unconventional terrorism, to the extent that it may move the world from various electronic attacks to a “cyber war.” Russia is among the first countries to use cyber capabilities in the military field, as it has been interested in developing and increasing its offensive capabilities in this field since 1998. The Russian strategy in its conflict with Ukraine relies on offensive electronic weapons as a power multiplier in wars, meaning that it increases the combat capabilities of the state if it is used alongside other military capabilities. This strategy also relies on hindering the opponent's information infrastructure and its military and civil communications before embarking on military operations.

Key Words: (Cyber security, cyber warfare, cyber operations, future scenarios)

المقدمة:

عرف العالم منذ القدم مجموعة من الازمات والحروب الدولية، اذ لم تخلو حقبة تاريخية من الحروب التي غذتها في كثير من الأحيان الاطماع الاستعمارية لبعض الدول، وأفرزتها أزمات دبلوماسية واقتصادية وسياسية وإيديولوجية أحيانا أخرى.

من الصواب القول، ان الحرب ظاهرة بشرية معقدة للغاية ومتعددة الابعاد والمستويات والموضوعات والفواعل والنطاقات، ولكن بصورة عامة فالمعنى الشائع للحرب هو استخدام القوة المفرطة لتحقيق اهداف الدولة والحفاظ على امنها وردع اعدائها، فهي اعلى مستويات ممارسة القوة سواء كانت قوة عسكرية او اقتصادية لتحقيق النفوذ وفرض الارادة، فالحروب هي النقيض الحتمي للسلام والأمن ووسيلة لتنفيذ سياسة الدول بوساطة العنف والاكراه، فقد تعددت أشكال الحروب وأنواعها ووسائلها، إذ لم يعد مفهوم

الحرب مقتصرا على الحروب النظامية العسكرية التي تنشأ بين دولتين او اكثر، بل اصبحنا امام حروب جديدة الا وهي الحروب السيبرانية التي تعد ظاهرة جديدة في العلاقات الدولية الراهنة، باعتبارها ذلك الوجه السلبي لاستخدام التطبيقات التكنولوجية والمعلوماتية، بل أضحت من بين المخاطر والتهديدات الأمنية الجديدة التي تتجاوز في تداعياتها وأبعادها الحدود السياسية والجغرافية للدول، فكان للتطور المتسارع في التقنيات الذكية وتزايد الاعتماد على التكنولوجيا في الحياة اليومية، وضيق الفجوة بين التقنيات الميدانية والعسكرية في الفضاء السيبراني، ما جعل ظاهرة الحروب السيبرانية تتشكل ويعاد تشكيلها بصورة مستمرة.

من معاني القول،الحرب السيبرانية ،هي :" تنفيذ والاستعداد لتنفيذ العمليات العسكرية وفقا للمبادىء المعلوماتية، عن طريق تعطيل – ان لم يكن تدمير – نظم المعلومات والاتصالات على أوسع نطاق "، كما يشمل مفهوم الحرب السيبرانية ابعادا غير مادية تتمثل في "تدمير العقيدة العسكرية للعدو والتي تمثل الأساس الذي يعتمد عليه لتحديد هويته وخططه وتصرفاته وأهدافه والتحديات التي يواجهها"، وذلك عبر معرفة كل شيء عن العدو ومنعه في الوقت نفسه من معرفة أي شيء عن الطرف الاخر، وتحويل ميزان المعرفة ليكون في صالح هذا الطرف. بمعنى اخر ، الحرب السيبرانية هي عملية " توظيف المعرفة بهدف الاقتصاد في توظيف رأس المال والعمالة" او حتى في حالة عدم تكافؤهما مع الخصم.

أهمية البحث: تأتي أهمية البحث من كونها تتطرق لموضوع في غاية الأهمية في الوقت الراهن، وتشمل أساسا الاجرام السيبراني في احدى اشكاله وهي الحرب السيبرانية، اذ يعد الأمن الركيزة الأساسية للمجتمع بحيث لا يمكن تصور نمو أي نشاط دون تحقيق الأمن، فقد افرزت ثورة المعلومات والتكنولوجيا تحولات عميقة في مفهوم الأمن ومضامينه وابعاده، كما ساهمت في تحول عدد من الظواهر والتهديدات وفي مقدمتها الحروب، وان دراسة العمليات السيبرانية في الحرب الدائرة بين روسيا وأوكرانيا تعد أمرا جوهريا لتعزيز فهمنا لظاهرة الحرب في عصر الانترنت، حيث باتت الوسائل والأدوات الالكترونية مرتبطة بشكل عضوي في أي عمل حربي.

مشكلة البحث: تنبع مشكلة البحث من الآتي:

تطرح بين الحين والأخر جملة من الاتهامات المتبادلة بين طرفي الصراع، روسيا وأوكرانيا حول الاستهداف السيبراني ضد المواقع الحيوية والبنى التحتية لكل طرف مما يسبب إنهاك وإبطاء في تلك المؤسسات الحيوية، فارتأينا ان نبحث في ذلك الصراع وتلك الاتهامات لمعرفة حقيقة تلك الهجمات

السيبرانية، ولمعرفة المسار الاستراتيجي لتلك الهجمات السيبرانية سنطرح ادناه عدة تساؤلات، وهي كالاتي:

– ما تأثيرات الفضاء السيبراني في تغير طبيعة وخصائص الأمن والصراع في البيئة الاستراتيجية العالمية؟

– ما الحرب السيبرانية من حيث مفهومها وأشكالها وخصائصها؟

– ما تداعيات الحرب السيبرانية على تفاعلات السياسة الدولية؟

– ما ملامح توظيف الفضاء السيبراني من قبل روسيا في المواجهة الأوكرانية؟

– ما سيناريوهات الحرب السيبرانية الروسية – الأوكرانية؟

فرضية البحث: تنطلق فرضية البحث من الآتي: تعد الحرب السيبرانية أداة من أدوات الجيل الخامس للحروب التي تستهدف المواقع الحيوية والبنى التحتية للطرف المستهدف من الجهة القائمة بتلك الهجمات السيبرانية بواسطة أسلحتها من الفايروسات والبرامجيات التدميرية وهذا ما نجده بين طرفي الصراع روسيا وأوكرانيا، وان تصاعد مخاطر الحروب السيبرانية بات يشكل تهديدا جديا لأمن الدول، فضلا عن الأمن الدولي.

الاطار المنهجي للبحث: من اجل ان تكون دراستنا ضمن المنهج العلمي البحثي الصحيح وجب علينا ان نستخدم عدد من المناهج العلمية فكان المنهج الوصفي ومنهج التحليل النظمي مناهج الدراسة، من اجل التعرف على طبيعة العمليات العسكرية التي شنتها روسيا والتعرف أنماط تلك العمليات والتكتيكات التي اتبعت في تنفيذها.

تقسيمات الدراسة: تضمن البحث فضلا عن المقدمة والخاتمة ستة محاور: تضمن المحور الأول: مفهوم الأمن السيبراني في البيئة الاستراتيجية العالمية، اما المحور الثاني: تناول مفهوم الحرب السيبرانية وخصائصها وأشكالها وتداعياتها على التفاعلات السياسية الدولية، وتناول المحور الثالث: التاريخ السيبراني للحرب الروسية – الأوكرانية، اما المحور الرابع: تناول الغزو السيبراني الروسي لأوكرانيا في العام 2022، بينما تناول المحور الخامس: العمليات السيبرانية في الحرب الروسية – الأوكرانية (طبيعة التوظيف والأدوات المستخدمة)، اما المحور السادس: تناول السيناريوهات المستقبلية للحرب السيبرانية الروسية – الأوكرانية.

أولا: الامن السيبراني في البيئة الاستراتيجية العالمية

تمثل البيئة الاستراتيجية العالمية المجال الحيوي الذي يتعايش فيه مفهوم الامن السيبراني ، وان أهمية هذا المفهوم داخل الدراسات السياسية جاءت نتيجة ظروف عالمية ذات صبغة سياسية وعسكرية مع احداث 11 أيلول ، ففي العصر السيبراني حدث تغيير في مفهوم الأمن وظهرت مصالح جديدة وتهديدات سيبرانية ، اذ اصبح الأمن السيبراني رافد أساسي من روافد الأمن القومي مما دفع العديد من الدول تتصارع في سبيل الحصول على مستويات عالية لتعزيز قدراتها الدفاعية او الهجومية وذلك عن طريق تبني استراتيجيات وطنية للأمن السيبراني[1]، اذ اصبح مفهوم الامن السيبراني يمثل ظاهرة مركبة متعددة الابعاد والظواهر ، ولابد من الاخذ بعين الاعتبار ان مسألة إيجاد تعريف واضح ومحدد لمفهوم الامن السيبراني داخل البيئة الاستراتيجية المعاصرة تظل مسألة بالغة التعقيد ؛ نتيجة تنوع وتعدد المدارس الفكرية التي تناولت هذا المفهوم من جوانب فكرية وعلمية مختلفة ناهيك عن استمرار حدوث العديد من المتغيرات العالمية التي افرزتها متغيرات البيئة الاستراتيجية والتي بدورها ساهمت على عدم الاتفاق على مفهوم اجرائي محدد.

ويمكن ذكر اهم الأسباب التي ساهمت في احداث عدم الاتفاق على إيجاد تعريف جامع لمفهوم الامن السيبراني على النحو الاتي:[2]

– ان مفهوم الامن السيبراني مفهوم معقد ومركب وهذا مما جعل الباحثين السياسيين يتصرفوا لمفاهيم أكثر مرونة.

– وجود التشابك بين مفهوم الامن السيبراني ومفهوم القوة والذي اوجدته البيئة الاستراتيجية ولاسيما بعد ظهور المدرسة الواقعية والتي رسمت في البيئة الاستراتيجية العالمية فكرة التنافس من اجل القوة، بحيث ينبغي النظر لمفهوم الامن السيبراني على انه اداة لطلب القوة او أداة لتعظيمها.

– ظهور موجة من المثاليين ترفض طرح المدرسة الواقعية وتطرح هدفا اخر للأمن القومي وهو السلام.

– دور رجال السياسة في تعميق مفهوم الامن السيبراني بهدف الحصول على منارة أكبر لغرض الصراع الخارجي او الاستهلاك الداخلي.

---

[1] عادل عبد الصادق، الإرهاب السيبراني والأمن القومي في بيئة متغيرة، المركز العربي لأبحاث الفضاء الاليكتروني، دوريات – مفاهيم استراتيجية، متوفرة على الرابط الالكتروني الاتي:
https://accronline.com/article_detail.aspx?id=31557

[2] احمد سالم المنتصر، تجليات جديدة في مفهوم الامن الالكتروني " السيبراني " (دراسة مقارنة)، ط1، منشورات دار البيان للطباعة والنشر، 2017، ص71.

ومن المفيد بالطرح ،القول ان الأمن السيبراني:يمثل امن وحماية الشبكات والأنظمة المعلوماتية والبيانات والأجهزة التي تتصل بالأنترنت، فالمجال المتعلق بمعايير وإجراءات الحماية التي يتم اتخاذها والالتزام بها لمواجهة التهديدات او على الأقل الحد من اثارها يسمى **بالأمن السيبراني**[1]. والامن السيبراني حسب تعريف الاتحاد الدولي للاتصالات في تقريره حول اتجاهات الإصلاح في الاتصالات للعام 2010-2011 هو " مجموعة المهمات كالإجراءات الأمنية والمبادئ التوجيهية ومقاربات إدارة المخاطر والتدريبات والتقنيات التي يمكن استخدامها لحماية البيئة السيبرانية وموجودات المؤسسات والمستخدمين ".[2] وعليه ، ان أثر الفضاء السيبراني في تغير طبيعة وخصائص الأمن والصراع والقوة في البيئة العالمية، يتم عبر متغيرات ثلاث،على النحو الاتي:[3]

المتغير الأول : يرتبط هذا المتغير بكون ان الأمن السيبراني لم يقتصر على البعد التقني فقط بل تعداه لأبعاد أخرى ، في ظل تراجع سيادة الدولة وتزايد علاقة الأمن والتكنولوجيا بصفة عامة لاسيما مع إمكانية تعرض مصالح الدول الاستراتيجية الى اخطار وتهديدات ، حيث فرضت تلك التطورات إعادة التفكير بمفهوم " الأمن القومي للدولة " الذي يعني بحماية القيم الأساسية للمجتمع وابعاد مصادر التهديد عنها ، ومن جهة أخرى ان تحول الفضاء السيبراني الى ساحة عالمية عابرة للحدود ، جعل الأمن السيبراني الداخلي للدول يرتبط عضويا بأمن الفضاء السيبراني ، وهذا ما يشكل الأساس للأمن الجماعي العالمي لاسيما مع وجود مخاطر تهدد جميع الفاعلين بمجتمع المعلومات العالمي.

المتغير الثاني: جعل هذا المتغير الفضاء السيبراني يلعب دورا مهما في تعظيم القوة او الاستحواذ على العناصر الأساسية لها في العلاقات الدولية، اذ أصبح التفوق بذلك المجال عنصرا حيويا في تنفيذ العمليات الفعالة في الأرض والبحر والجو والفضاء، والاعتماد على القدرة القتالية في الفضاء السيبراني على نظم التحكم والسيطرة التكنولوجية. كما ساهمت " القوة السيبرانية " في تدعيم القوة الناعمة للدولة، اذ بات الفضاء السيبراني مسرحا لشن الهجمات التخريبية المرتبطة بنشر المعلومات المضللة والتأثير بالرأي العام والنشاط الاستخباراتي السري والحرب النفسية، كما ساهم ذلك من زيادة إنفاق الدول على سياسات الدفاع السيبراني وحماية شبكاتها الوطنية من التهديدات وبناء المؤسسات الوطنية لحمايتها السيبرانية.

المتغير الثالث : ارتبط هذا المتغير بعلاقة الفضاء السيبراني ببروز أنماط جديدة من التهديدات ، كمجال تنشأ فيه الصراعات بين الفاعلين المختلفين تعبيرا عن تعارض القيم والمصالح سواء بين الفاعلين من غير الدول او الفاعلين الدوليين ، ويأتي ذلك من كون الفضاء السيبراني عابرا للحدود وسهولة الدخول اليه ، مما أدى اتساع دائرة الصراعات

---

[1] منى الأشقر جبور، السيبرانية هاجس العصر، بيروت، المركز العربي للبحوث القانونية والقضائية، 2017، ص35.

[2] الاتحاد الدولي للاتصالات، اتجاهات الإصلاح في الاتصالات، جنيف: الاتحاد الدولي للاتصالات، 2008، ص18.

[3] عادل عبد الصادق، الإرهاب السيبراني والأمن القومي في بيئة متغيرة، مرجع سبق ذكره.

السيبرانية والزيادة من عدد الفاعلين والمهاجمين ، وظهور صراع امتلاك أدوات الحماية والهجوم والدفاع وارتباط ذلك بحيازة الهيمنة السيبرانية والقوة السيبرانية والتأثير السيبراني ضمن المستويين المحلي والدولي ، من اجل الحصول على مكاسب تقنية او اقتصادية او سياسية او الاستحواذ على أسواق التجارة العالمية.

وان اهم الأسباب التي ساعدت على ظهور مفهوم الامن السيبراني داخل البيئة الاستراتيجية العالمية تتمثل بما يلي:[1]

1. توسع مفهوم المصلحة الوطنية وذلك من خلال حماية الترتيبات الداخلية التي تدفع نحو زيادة معدل الرفاهية، وعن طريق ضمان الرفاهية عبر ضمان حماية مصادر الموارد الطبيعية.

2.زيادة شعور الدول الوطنية لاسيما النامية بتنوع التهديدات السيبرانية الخارجية.

3.زيادة إحساس الدول الوطنية المعاصرة بالتوتر والقلق الذي من الممكن ان يتحول الى مظاهر عديدة لحالات عدم الاستقرار وعدم الامن؛ بسبب قصور عمليات انتاج وتوزيع السلع والخدمات.

4.زيادة معدلات العنف وتصاعد حدة النزاعات والصراعات داخل البيئة الاستراتيجية العالمية.

ثانيا: الحرب السيبرانية (المفهوم، الأشكال، الخصائص، التداعيات)

يشير "نيلز ميلزر" الى ان الحرب السيبرانية هي "تلك الحرب التي تجري في الفضاء السيبراني من خلال الأساليب والوسائل السيبرانية"[2]، كما تعرف الحرب السيبرانية بأنها" اعمال هجومية ودفاعية، متكافئة وغير متكافئة، تحدث في الشبكات الرقمية من قبل الدول او جهات فاعلة شبيهة بالدولة او ما دون الدولة، وتشتمل على مخاطر تصيب البنية التحتية الوطنية المهمة والأنظمة العسكرية"[3]، وهذا النوع من الحروب يتطلب درجة عالية من الترابط بين الشبكات الرقمية والبنية التحتية من جانب المدافع، والتقدم التكنولوجي من جانب المهاجم[4]، كما يمكن فهم الحروب السيبرانية على انها تهديد مستقبلي وليس تهديدا حاليا، كما تتناسب مع نموذج حرب المعلومات[5].

---

[1] مرعي علي الرمحي، الحرب السيبرانية ومتطلبات الامن القومي الجديدة، ط1، المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية، المانيا – برلين، 2022، ص 7.

[2] Melzer, Nils. "Cyberwarfare and international law", 2011, p.4

[3] Shane M, Coughlan. "Is there a common understanding of what constitutes cyber warfare?, The University of Birmingham School of Politics and international Studies, 30 September 2003, p.2

[4] Ibid.

[5] Ibid.

ويعرف حلف الناتو NATO الحرب السيبرانية بانها" ذلك القسم العسكري الذي يستخدم الكترونيات تهتم بالإجراءات التي تتخذ لمنع العدو من استخدام طاقته الكهرومغناطيسية الفعالة والإجراءات التي تتخذ لحماية طاقتنا الكهرومغناطيسية المنبثقة الفعالة"

[1] كذلك تعرف الحرب السيبرانية على انها" عمليات عسكرية ضمن الفضاء السيبراني تحمل طابعا معلوماتيا"، ويمكن ان تتخذ ثلاثة اشكال أساسية:

– جمع المعلومات الاستخباراتية من شبكة وبيانات العدو حول خططه وانتشاره وتوجهاته العامة وما ينوي القيام به.

– مهاجمة أنظمة الكمبيوتر والبيانات الحساسة للعدو خاصة تلك المرتبطة بالبنى التحتية والمؤسسات ومراكز الاتصال واضعاف قياداته العسكرية والسياسية.

– حماية البيانات الالكترونية والدفاع عن الشبكات الخاصة بالدولة والوقوف دون اتلافها او التعرض لها.[2]

وتنطوي الحرب السيبرانية على عدة خصائص، منها:[3]

1– **حروب لا تناظرية:** ان الحروب السيبرانية هي تلك الحروب التي تحتاج الى تكاليف بسيطة لصنع الأدوات اللازمة، كما لا تحتاج الى دولة أخرى تقوم بتصنيع الأسلحة المكلفة كالمقاتلات المتطورة والطائرات، من اجل فرض تهديدا حقيقيا خطيرا على دولة أخرى.

2– **تمتع المهاجم بأفضلية واضحة:** في هذا النوع من الحروب يتمتع المهاجم بأفضلية واضحة كبيرة على المدافع، فهي تتميز بالمرونة والمراوغة والسرعة وبيئة يتمتع بها المهاجم بأفضلية يصعب على عقلية التحصن لوحدها من ان تنجح، اذ يجعل التحصن هذا الطرف عرضة للمزيد من محاولات الاختراق والضغط.

---

[1] رائد طيران، جاسم محمد البصيلي، الحرب الالكترونية أسسها واثرها في الحروب، المؤسسة العربية للدراسات والنشر، بيروت ، ط2، 1989، ص 30.

[2] جون باسيت، الحروب المستقبلية في القرن الحادي والعشرين، مركز الامارات للدراسات والبحوث الاستراتيجية، أبو ظبي، 2014، ص57.

[3] حكيم غريب، صبرينة شرقي، تداعيات الحرب الالكترونية على العلاقات الدولية: دراسة في الهجوم الالكتروني على ايران (فيروس ستكنست)، مجلة دفاتر السياسة والقانون، المجلد12، العدد2، 2020، ص ص 96–97.

– فشل نماذج الردع: لم يعد مفهوم الردع الذي تم تطبيقه في الحرب الباردة له جدوى في هذا النوع من الحروب، فالردع بالعقاب او الانتقام لا ينطبق على الحروب السيبرانية، حيث من المستحيل تحديد الهجمات السيبرانية ذات الزخم العالي ومنها ما يحتاج الى اشهر لرصدها وهذا ما يلغي مفعول الردع بالانتقام، كما هناك الكثير من الحالات التي لا يمكن تتبع مصدرها وحتى وان تمت متابعة مصدرها فأنها قد تعود لفاعلين غير حكوميين لن يكون لديهم قواعد او أصول حتى يتم الرد عليها.

3– **تعدي المخاطر الأهداف العسكرية:** ان مخاطر الحروب السيبرانية لا ينحصر فقط باستهداف المواقع العسكرية، حيث هناك جهود متزايدة تستهدف البنى التحتية والحساسة للبلدان المستهدفة، كالقدرة على استهداف الطاقة وشبكات الكهرباء والمنشآت الحساسة المائية او النفطية او الصناعية واستهداف شبكات النقل والنظام المالي وغيرها من الاعمال التي تؤدي الى انفجارات او دمار او اضرار مادية حقيقية.

4– **حرب رقمية:** فهي حروب ذات تقنية متطورة جسدت قمة التطور الذي وصلت اليه ثورة المعلومات وبوابتها الالكترونية، التي شكلت الأداة المحورية والميدان الرئيس لها، كما كانت بسبب ذلك عرضة للتنوع والابتكار والتطور المستمر في وسائلها وتقنياتها، بسبب ارتباطها بقمة الهرم التقني للمصالح الحيوية للدول والحضارة الإنسانية.

وسببت الحروب السيبرانية العديد من المخاطر والتداعيات على تفاعلات السياسة الدولية، ويمكن طرح ابرزها على النحو الاتي:[1]

1– **تصاعد المخاطر السيبرانية:** لاسيما مع قابلية المنشآت المدنية والعسكرية في الدول للهجوم، وهذا ما يؤثر على وظائف تلك المنشآت وان التحكم في تنفيذ هذا الهجوم يعد أداة سيطرة استراتيجية.

2– **تعزيز القوة وانتشارها:** عمل الفضاء السيبراني على إعادة تشكيل قدرة الأطراف المؤثرة، وادى ذلك الى انتشار القوة بين فاعلين متعددين.

3– **عسكرة الفضاء السيبراني:** في هذا الاطار برزت العديد من الاتجاهات، مثل التطور في مجال سياسات الدفاع والامن السيبراني، وتصاعد القدرات في سباق التسلح السيبراني، وتبني السياسات الدفاعية

[1] عادل عبد الصادق، الحروب السيبرانية: تصاعد القدرات والتحديات للأمن العالمي، المركز العربي لأبحاث الفضاء الالكتروني، متوفرة على الرابط الالكتروني الاتي: https://accronline.com/article_detail.aspx?id=28395

السيبرانية لدى الأجهزة المعنية بالدفاع والامن في الدول، وتزايد الاستثمار في مجال تطوير أدوات الحرب السيبرانية داخل الجيوش الحديثة.

4- إدماج الفضاء السيبراني ضمن الأمن القومي للدول: ويتم ذلك عبر تحديث الجيوش وتشكيل وحدات متخصصة في الحروب السيبرانية، وإقامة هيئات وطنية للأمن والدفاع السيبراني والقيام بالتدريب واجراء المناورات لتعزيز الدفاعات السيبرانية.

5- الاستعداد لحروب المستقبل: تتبنى العديد من الدول استراتيجية حرب المعلومات باعتبارها حربا للمستقبل، وترى الدول الكبرى ان من يحدد مصير تلك المعركة المستقبلية ليس من يمتلك القوة فقط، وانما القادر على شل القوة والتشويش على المعلومة.

ثالثا : تاريخ الحرب السيبرانية الروسية – الأوكرانية

لطالما أدرك المحللون السياسيون أن المواجهة العسكرية الروسية – الأوكرانية، إذا حدثت، قد يكون لها تداعياتها السيبرانية، حيث يدرك المتخصصون في السيبرانية أن وراء الصراع الأوكراني الروسي حرباً سيبرانية، بدأت معاركها بالفعل وتضاعف ضحاياها منذ عام 2014.

بينما تعاني أوكرانيا من نقص الخبرة في مجال الأمن السيبراني وضعف التنظيم وقدرة الاستجابة المحدودة ونقص التنسيق بين الوكالات الإلكترونية ذات الصلة، تدرك كييف قوة القدرات السيبرانية الروسية، وهي حاليا في سباق مع الزمن لتقليص الفجوة وتحسين الوسائل للدفاع والردع السيبراني بالتعاون مع الحلفاء، وخاصة الولايات المتحدة والاتحاد الأوروبي.

تتعرض أوكرانيا لهجمات سيبرانية متواصلة من قراصنة روس مدعومين من الكرملين منذ أن ضمت موسكو شبه جزيرة القرم في عام 2014، حيث أصبح التجسس الإلكتروني واختراق الشبكات وقواعد البيانات والخوادم وتعطيل مرافق الطاقة والاتصالات ونشر الشائعات والمعلومات المضللة جزءاً من الصراع بين روسيا وأوكرانيا.

وقعت أبرز الهجمات السيبرانية الروسية ضد أوكرانيا خلال عامي 2014 و 2015 وشملت:[1]

- خلال عام 2014، تمكن المهاجمون السيبرانيون الروس من الوصول الى نظام عد الأصوات في أوكرانيا عشية الانتخابات العامة، مما أدى الى تدمير السجلات الإلكترونية وإجبار السلطات الأوكرانية على فرز الأصوات يدوياً.
- في العام التالي 2015، أثناء عملية نسبت الى مجموعة مرتبطة بالاستخبارات الروسية، تسبب هجوم إلكتروني في انقطاع التيار الكهربائي لعدة ساعات في غرب أوكرانيا وجزء من كييف. كان هذا أول تعتيم معروف ناجم عن هجوم سيبراني.
- خلال عام 2017، وقع هجوم NotPetya الذي نفذته نفس المجموعة المرتبطة بالاستخبارات العسكرية الروسية ونجح في إصابة ما يقرب من 10% من جميع أنظمة الكمبيوتر الإلكترونية بحزمة برامج ضارة قبل أن تنتشر في جميع أنحاء العالم في واحدة من أكثر الهجمات السيبرانية تدميرا في التاريخ، كلفت الشركات في جميع أنحاء العالم ما يقرب من 10 مليارات دولار من الخسائر، وفقا لتقديرات أمريكية.
- في 15 يناير 2022، كشفت Microsoft عن برامج ضارة متخفية في شكل برنامج فدية تسمى WhisperGate، تستهدف العشرات من المنظمات الحكومية وغير الهادفة للربح ومؤسسات تكنولوجيا المعلومات الموجودة في أوكرانيا.
- في 19 يناير 2022، أدى هجوم إلكتروني الى تعطيل وظائف معينة في GAC للشئون العالمية بكندا، بعد أن مد المسئولون الكنديون دعمهم لأوكرانيا.
- وفي أوائل فبراير 2022، كشفت مايكروسوفت عن استهداف المكاتب العسكرية الأوكرانية والشبكات الحكومية من قبل مجموعة "أكتينيوم"، التي يعتقد أنها مرتبطة بأجهزة الأمن الروسية. بدأ هذا الاستهداف منذ أكتوبر 2021 ويهدف الى التجسس وجمع المعلومات الاستخباراتية.

[1] أحمد فتحي، الحروب السيبرانية: الازمة الروسية الأوكرانية نموذجا، مركز آتون للدراسات، القاهرة، ط1، 2023، ص ص 82 – 84.

رابعا : الغزو السيبراني الروسي لأوكرانيا 2022

يعد الفضاء السيبراني أمراً محورياً في خطة روسيا الخاصة بأوكرانيا قبل الغزو، فقد حذر عضو البرلمان الأوروبي بارت جروثيس في 23فبراير 2022، من أن روسيا قد تطلق حملة تضليل منسقة في دول البلطيق ودول الاتحاد الأوروبي المجاورة الأخرى. أوكرانيا نفسها معرضة لخطر حملات التضليل الجماعي عبر وسائل التواصل الاجتماعي والقنوات الأخرى على الإنترنت، والهجمات السيبرانية الكبرى التي تكون أكثر تخريباً وزعزعة للاستقرار من تلك التي نظمها مؤخراً قراصنة مرتبطون بالدولة الروسية ضد الحكومة الأوكرانية والأهداف التجارية.

وبحسب تقارير صحفية، استعدت الحكومة في كييف لنقل بيانات حساسة الى خارج البلاد عقب اعتراف روسيا باستقلال جمهوريتي لوغانيسك ودونيتسك عن أوكرانيا، استعداداً لغزو القوات الروسية للعاصمة. أرسل فريق الاستجابة الإلكترونية السريع التابع للاتحاد الأوروبي عشرة خبراء إلكترونيين من ست دول أوروبية لمساعدة أوكرانيا، وسيكون فيسبوك وشركات التواصل الاجتماعي الأخرى في حالة تأهب قصوى لمنع إساءة استخدام منصاتهم من قبل روسيا في حملات تضليل، لكنه سيكون من الصعب احتواء المعلومات المضللة عبر التطبيقات المشفرة الشهيرة مثل تليجرام واتس أب. بينما مجتمعات المعلومات المغلقة مثل روسيا معزولة أكثر من الديمقراطيات المفتوحة عن حملات المعلومات المضادة. من المرجح أن تحدث هجمات سيبرانية مضادة من قبل الدول الغربية، ولكنها ستكون متناسبة وسرية.[1]

وقبل الغزو الروسي لأوكرانيا بيوم واحد، عان العديد من المؤسسات الحكومية والمصرفية في أوكرانيا من جولة أخرى من هجمات رفض الخدمات الموزعة. وفقا لمحققي الأمن السيبراني، كانت هذه الهجمات في الواقع غطاء لتثبيت برنامج ضار متطور لمسح البيانات يسمى **Hermetica Wiper** على الأنظمة المستهدفة. كما تأثر بعض الأنظمة في لاتفيا وليتوانيا نتيجة هجمات وقعت في منتصف يناير 2022،

[1] Oxford Analytica (2022), 'Cyberspace will be central to Russia's Ukraine plan', Expert Briefings.
https://doi.org/10.1108/OXAN-ES267528

وتضمنت هجمات فدية مزيفة وتشويه مواقع حكومية من قبل قراصنة روس بمثابة غطاء لتثبيت برنامج ضار مشابه يسمى **WhisperGate**.[1]

وتعمل الدول الغربية (الولايات المتحدة والناتو بشكل رئيسي) على تكثيف استراتيجيتها لمكافحة الهجمات السيبرانية، حيث نصحت حكومة المملكة المتحدة شركات البنية التحتية الحيوية في المملكة بتشديد أمن الشبكة، وكشف تقرير استشاري مشترك بين الولايات المتحدة والمملكة المتحدة عن معلومات فنية حول البرمجيات الخبيثة الروسية الصنع "**Cyclops,Blink**" لتفادي استخدامها، مؤكدا أن خيار الهجوم السيبراني مطروح على الطاولة.

وكررت وزارة الدفاع الأمريكية[2]، أن استراتيجيتها الإلكترونية تركز الان على "الأربعة الكبار" – روسيا والصين وإيران وكوريا الشمالية – بدلا من الصين في المقام الأول. ومن المحتمل أن يكون الهجوم السيبراني الروسي المباشر ضد هدف غربي تصعيداً للغاية بالنسبة للكرملين، ولكن الأهداف الغربية تواجه خطراً جسيماً من فشل متتال، مثل ذلك الذي أحدثته البرامج الضارة **NotPetya** الروسية الصنع في عام 2017.

بينما أفادت الحكومة البولندية أن نظام مقاصة المدفوعات الوطني وشبكة البريد الإلكتروني الحكومية قد شهدا ارتفاعاً في الهجمات السيبرانية خلال الأيام التي سبقت الغزو الروسي لأوكرانيا، ولكن لم تنسب وارسو الهجمات رسميا الى أي جهة فاعلة، ومع ذلك أشارت الى أن التورط الروسي شبه مؤكد.[3]

على الرغم من أن الحكومة والمؤسسات المالية الأوكرانية كانت على ما يبدو الأهداف الرئيسية للقرصنة الروسية الأخيرة، فإن الأضرار البولندية – وخروقات الشبكات في لاتفيا وليتوانيا – تظهر أن نطاق الحملة السيبرانية الروسية ونطاقها يمتدان الى ما هو أبعد من أوكرانيا.

---

[1] Oxford Analytica (2022), "Russian invasion raises risk of cascading cyberattack", Expert Briefings.
https://doi.org/10.1108/OXAN-ES267563

[2] Ibid.

[3] Oxford Analytica (2022), "Russian cyber warfare could result in casualties", Expert Briefings. https://doi.org/10.1108/OXAN-ES267581

ويهدف النشاط السيبراني لروسيا الى الضغط على أعضاء الناتو في جواره المباشر، جزئيا لتشتيت انتباه صانعي السياسة الأوروبيين لتوتر الوحدة بينهم. الهجمات السيبرانية الغربية المضادة ضد الأهداف الروسية ممكنة، لكنها ستزيد من خطر الانتقام غير المتناسب من روسيا. مع احتمالية وقوع إصابات في صفوف المدنيين في أوكرانيا أو داخل الاتحاد الأوروبي جراء هجوم سيبراني روسي شامل كرد انتقامي من استهداف روسيا إلكترونياً.

خامسا : العمليات السيبرانية في الحرب الروسية-الأوكرانية(2021-2022)

1.طبيعة التوظيف

بدأت تلك الهجمات في مارس 2021 في اختراق مبكر للأنظمة الأوكرانية وصولا الى معلومات استخبارية ذات صلة بالشراكات العسكرية الأوكرانية وسلاسل الامداد في الداخل والخارج الاوكراني من اجل جمع اكبر قدر من المعلومات الممكنة عن أعضاء حلف الناتو. من بعد ذلك تعرضت أوكرانيا لهجوم سيبراني في 2022/1/14، اذ استهدف نحو 70 موقعا الكترونيا تابع لهيئات حكومية وسفارات اجنبية وقد شمل ذلك مجلس الامن والدفاع ومجلس الوزراء ووزارتي الخارجية والتعليم والعديد من الوزارات، ناهيك عن المواقع الالكترونية لسفارة الولايات المتحدة الامريكية والمملكة المتحدة والسويد كما استهدف موقع "Diia" الالكتروني (وهو نظام أساسي يضم دوائر حكومية اوكرانية، يخزن بيانات شخصية خاصة باللقاح وشهاداته) بجانب مكتب تأمين المركبات وخدمات الطوارئ. وعقب مضي ما يقارب الشهر على هذا الهجوم السيبراني وتبعا لمركز الامن السيبراني الاوكراني وهيئة رقابة الاتصالات الأوكرانية ووزير التحول الرقمي: ميخائيلو فيدروف " تعرض موقع وزارة الدفاع الأوكرانية الالكتروني في يومي 15 – 2/16/ 2022 لهجوم سيبراني غير مسبوق استمر ساعات عدة لتظهر رسالة عليه تشير الى تعطله وخضوعه لصيانة تقنية، اذ نجح المهاجمون من اكتشاف نقاط ضعف التعليمات البرمجية مما دفع أوكرانيا الى الاستعانة بشبكات أمريكية لمجابهة ما اطلقت عليه " **القرصنة الالكترونية** ".[1]

وفي 2022/2/23 تعرضت عدة مواقع الكترونية لعدد من الوزارات الحكومية ومؤسسات الخدمة المالية لموجة من هجمات رفض الخدمة الموزعة لتتوقف 10 مواقع الكترونية اوكرانية عن العمل بما في ذلك المواقع الالكترونية لوزارات الدفاع والخارجية والصحة والثقافة، كما اكتشف خبراء الامن السيبراني برنامجا خبيثا يتمكن من مسح بيانات

[1] أحمد فتحي، الحروب السيبرانية: الازمة الروسية الأوكرانية نموذجا، مصدر سبق ذكره، ص 108.

أجهزة الحاسب الآلي الذي يستهدفه، فقد اكدت شركة "Symantec Threat Intelligence " إصابة ما يقارب 50 حاسبا آليا في احدى المؤسسات المالية الأوكرانية ببرنامج ضار ماسح للبيانات.[1]

اما في 2022/2/25 أصدرت قوة الدفاع الالكتروني الأوكرانية تحذيرا على منصات التواصل الاجتماعي قائلة فيه: " لقد بدأ هجوم تصيد ضد الاوكرانيين! تتلقى عناوين البريد الالكتروني للمواطنين رسائل مرفقة بملفات ذات طبيعة غير مؤكدة " ، حيث القت السلطات اللوم على مجموعة من المتسللين تحمل الاسم الرمزي (UNC1151) وقد وصف أعضاؤها بانهم ضباط في الجيش البيلاروسي في **مينسك** ، كما اكد مسئولو الامن السيبراني الاوكرانيون وفريق استجابة حالات الطوارئ الحاسوبية **(CERT)** ان قراصنة من بيلاروسيا يسرقون كلمات المرور لاقتحام البريد الالكتروني للجنود الاوكرانيين ، كما يستخدمون دفاتر العناوين المخترقة لأرسال المزيد من الرسائل الضارة والوصول الى اكبر كم من المعلومات المتاحة.[2]

ومروراً في شهر ابريل من عام 2022 تمكنت أوكرانيا من احباط هجوم سيبراني استهدف واحدة من اكبر منشآت الطاقة التي شنتها مجموعة "**ساندوورم**"، فكان الهدف من هذا الهجوم هو حرمان ملايين الاوكرانيين من الكهرباء عن طريق برنامج خبيث يطلق عليه اسم "**اندستروير2**" وهو النسخة المحدثة من برنامج خبيث استخدم عام 2015 ضد المنشآت الكهربائية في البلاد، وحرم مئات الآلاف من المنازل الأوكرانية من الكهرباء. ومنذ بداية الحرب الروسية–الأوكرانية حتى أوائل شهر يوليو 2022 بلغ عدد الهجمات السيبرانية التي امكن رصدها على أوكرانيا نحو 40 هجوما، حيث 32% منها استهدف البنية التحتية الحيوية المؤثرة على المواطنين المدنيين والحكومة الأوكرانية والجيش الاوكراني والاقتصاد القومي، اذ اعتمدت تلك الهجمات على التصيد الاحتيالي ونقاط الضعف المحتملة واستهداف مقدمي الخدمات التكنولوجية، كما تعددت البرامج الضارة المستخدمة بتعدد الهجمات السيبرانية تجنبا لاحتمالات اكتشافها.[3]

وفي 2022/8/16 تعرضت مؤسسة الطاقة النووية الأوكرانية لهجوم سيبراني روسي على موقعها بالتوازي مع تصاعد حدة التوتر حول محطة زابوريجيا النووية في جنوب أوكرانيا ، حيث استخدمت مجموعة " الجيش السيبراني الشعبي " الروسية حوالي اكثر من 7 ملايين روبوت انترنت لمهاجمة الموقع الالكتروني لمدة ثلاث ساعات ، بعد ان دعت القناة المعنونة " الجيش السيبراني الشعبي " على تطبيق "انستجرام" متابعيها الى مهاجمة الموقع الالكتروني

[1] المصدر نفسه، ص109.
[2] أحمد فتحي، مصدر سبق ذكره، ص110.
[3] المصدر نفسه، ص111.

لمؤسسة الطاقة النووية الأوكرانية ، ثم عادت توجيه المتابعين الى هدف جديد هو " المعهد الاوكراني للذكرى القومية " الذي عانى من بطء شديد.[1]

2.ادوات التوظيف

وظف الجانبان الروسي والأوكراني جملة من الأدوات لإدارة الصراع المستمر بينهما في الفضاء السيبراني:[2]

أ.القراصنة الاوكرانيون: طالبت الحكومة الأوكرانية بحشد القراصنة الوطنيين المتطوعين في البلاد للمساعدة في حماية البنية التحتية الحيوية من ناحية والقيام بمهام التجسس السيبراني ضد الجانب الروسي من ناحية ثانية ، وقد ظهرت طلبات التطوع على منتديات القراصنة منذ 2022/2/24 بالاستعانة بعدد من شركات الامن السيبراني في العاصمة كييف ، وفي مقدمتها شركة " Cyber Unit Technologies " استجابة لطلب بعض المسئولين بوزارة الدفاع الأوكرانية ، وقد ورد في الرسائل المنشورة على تلك المنتديات نصا : " المجتمع الالكتروني الاوكراني! حان الوقت للمشاركة في الدفاع السيبراني عن بلدنا "، وقد طلب من خبراء الامن السيبراني والمتسللين ذكر تخصصاتهم من اجل توزيعهم على وحدات سيبرانية دفاعية (للدفاع عن وحدات البنية التحتية مثل محطات الطاقة وشبكات الكهرباء وأنظمة المياه وغير ذلك) وهجومية (لمساعدة الجيش الاوكراني من اجراء عمليات التجسس السيبرانية ضد القوات الروسية)، وبالفعل لقد تقدم مئات المتقدمين لتتولى أوكرانيا مسئولية التحقق من انتماءاتهم كي لا يندس العملاء الروس بينهم.

ب.القراصنة الروس: اتجه بعض القراصنة الروس الى تشكيل فرق خاصة كي يتسببوا في المزيد من الاضرار السيبرانية لأوكرانيا، ووفقا لهيئة الإذاعة البريطانية " بي بي سي " تسببت فرقة مكونة من 6 قراصنة في اغلاق عدد من المواقع الحكومية الأوكرانية مؤقتا، كما استغلت تلك الفرقة احدى صفحات الويب العسكرية الأوكرانية غير المتصلة بالأنترنت وارسلت عبر البريد الالكتروني 20 تهديدا يفيد بوجود قنابل في المدارس الأوكرانية، واخترقت القيادة المباشرة لفريق الاستجابة السريع التابع للسلطات الأوكرانية وارسلت رسائل بريد الكتروني رسمية باستخدام بريد الكتروني للحكومة الأوكرانية ينتهي ب (mail.@.gov.ua) لشن هجمات تصيد مستهدفة بهدف العثور على أي نقاط ضعف ممكنة.

---

[1] رغدة البهي، المعارك السيبرانية في الحرب الروسية–الأوكرانية، مجلة شئون عسكرية، المركز المصري للفكر والدراسات الاستراتيجية، العدد الأول، اكتوبر 2022، ص 60 ص61.

[2] المصدر السابق، ص61 ص62.

ج.مجموعة برامج الفدية "كونتي" Conti Ransomware: في 2022/2/25 تعهدت تلك المجموعة التي تتخذ من روسيا مقرا لها باستخدام برامج الفدية لابتزاز الشركات الامريكية والأوروبية وجني ملايين الدولارات ومهاجمة أعداء الكرملين اذا ردوا على الحرب الروسية–الأوكرانية، كما اكدت تلك المجموعة دعمها الكامل لحكومة الرئيس الروسي " فلاديمير بوتين " متعهدة باستخدام كافة مواردها الممكنة لاستهداف البنى التحتية للعدو متى يقرر شن هجوم سيبراني على روسيا او القيام بأي أنشطة حربية ضدها. وفي سياق متصل اكدت " كيمبرلي جودي " مديرة شركة " مانديانت الامريكية للأمن السيبراني " ان جزءا من مجموعة " كونتي " موجود في روسيا، وانها تملك علاقات وثيقة بأجهزة المخابرات الروسية، فيما أشار " بريت كالو " محلل التهديدات في شركة Emsisoft النيوزيلندية للأمن السيبراني الى أهمية مراقبة الدفاعات السيبرانية الامريكية، لان الهجمات السيبرانية ضد أوكرانيا قد تنتشر في الخارج.

د.وسائل التواصل الاجتماعي: جزئيا، قيدت روسيا الوصول الى موقع التواصل الاجتماعي " فيسبوك " من اجل حماية الاعلام الروسي، في ظل تواطؤ الأول في انتهاك حقوق الانسان والحريات الأساسية وتحديدا حقوق وحريات المواطنين الروس، وترجع تلك القيود الروسية الى القيود التي فرضها " فيسبوك " على حسابات تابعة لوسائل الاعلام المدعومة من الكرملين، ومنها " وكالة الانباء الحكومية RIA Novosti و " قناة Zvezda التلفزيونية الحكومية والمواقع الإخبارية الموالية للكرملين .Lenta.ru و Gazeta.ru " من ناحية، ورفض روسيا إيقاف التحقيق المستقل في وقائع حربها ضد أوكرانيا من ناحية ثانية. وقد اكدت " الدائرة الاتحادية لرقابة الاتصالات وتقنية المعلومات والاعلام " Roskomnadzor ان التقييد الجزئي سيدخل حيز التنفيذ في 2022/2/25 دون ان توضح الإجراءات المرتقبة، كما طالبت برفع القيود المفروضة على الحسابات الروسية التي تضمنت وضع علامة على محتواها تفيد بعدم إمكانية الاعتماد عليها، ومن الجدير بالذكر ان شركة " ميتا " انشات مركز عمليات خاصا للتعامل مع المحتوى الخاص بأوكرانيا الذي يحرض على العنف او يتضمن خطابات كراهية.

ذ.البرمجيات الخبيثة: أعلن تقرير استخباراتي أمريكي – بريطاني ان فريقا روسيا يسمى Sandworm يشن هجمات سيبرانية منذ عام 2019 لصالح الحكومة الروسية ، وقد كشف التقرير الذي نشرته وكالة الأمن السيبراني وأمن البنية التحتية الامريكية CISA ان الفريق الروسي طور برمجية خبيثة تستهدف أجهزة شركة Watchguard المتخصصة في أنظمة جدران الحماية البرمجية والتي تتمثل أهميتها في حماية الشبكات الالكترونية من أي هجمات سيبرانية خارجية ، كما أشاروا الى ان البرمجية الخبيثة قد طورت منذ عام 2019 وما زالت فعالة وقادرة على النفاذ عبر أجهزة الشركة المستخدمة على نطاق واسع في قطاع الاعمال والقطاع الحكومي. ويصبح بإمكان المخترقين النفاذ الى داخل الشبكات الرقمية بمجرد تغلب البرمجية الخبيثة على أنظمة الحماية المستخدمة في الشبكات الالكترونية، ما

يسمح بزرعها مباشرة داخل الحواسيب الشخصية وما يتصل بها من شبكات الكترونية، اذ تتمثل خطورة هذه الهجمات في توجيه مئات او الآف الطلبات الى موقع ما، ما يؤدي الى زيادة العبء على خوادمه الى درجة غير محتملة وصولا الى فقدان اتصالها بالإنترنت، ما يجعل الوصول اليها امرا متعذرا ان لم يكن مستحيلا.

و.أجهزة الاستخبارات الروسية: تعود بعض الهجمات السيبرانية التي استهدفت أوكرانيا في 2022/4/6 الى " سترونتيوم " Strontium ذات الصلة بوحدة (Gru) ، وهي وكالة المخابرات العسكرية الخارجية لهيئة الاكان العامة للقوات المسلحة للاتحاد الروسي ، وقد تمكنت شركة " مايكروسوفت " من السيطرة على سبعة نطاقات انترنت استخدمت في شن تلك الهجمات التي استهدفت المؤسسات الأوكرانية ، بما في ذلك المؤسسات الإعلامية والمؤسسات الحكومية ومراكز الفكر في كل من الولايات المتحدة والاتحاد الأوروبي ، من اجل الوصول الى الأنظمة المستهدفة وتوفير الدعم التكتيكي للحرب وتسريب المعلومات الحساسة ، فمنذ بداية الحرب كثفت وكالات الاستخبارات الروسية جهودها لاختراق شبكات الكمبيوتر الحكومية لكل من الولايات المتحدة والدول الحليفة (128 منظمة ، نصفها وكالات حكومية ، و 12% منها وكالات غير حكومية في 42 دولة) وبعض القطاعات التي قد تحتوي على معلومات قيمة ذات صلة بالحرب " كالحكومات ومراكز الفكر " لجمع المعلومات الاستخباراتية والتجسس.

3.ملامح توظيف الفضاء السيبراني من قبل روسيا في المواجهة الأوكرانية

يمكن الوقوف على ابرز ملامح توظيف روسيا للفضاء السيبراني في مواجهة أوكرانيا من خلال النظر الى النقاط التالية:[1]

أ.تزامن الهجمات: ارتبط توظيف روسيا للهجمات السيبرانية ارتباطا وثيقا بعملياتها العسكرية التي استهدفت الخدمات والمؤسسات الحيوية الأوكرانية لدعم الأهداف الاستراتيجية والتكتيكية للجيش الروسي ، فقد شنت روسيا هجوما سيبرانيا في 2022/2/23 في اليوم السابق للعملية العسكرية باستخدام برامج ضارة ماسحة للبيانات Wiper تعرف باسم FoxBlade لمحو البيانات الموجودة على الشبكات الحكومية الأوكرانية ، كما هاجمت شبكة اتصالات الأقمار الصناعية " فياسات " بهدف شل الجيش الاوكراني ، بجانب احدى شركات البث الكبرى في أوائل مارس 2022 ، أي بالتزامن مع اعلان الجيش الروسي عن نيته تدمير اهداف التضليل الأوكرانية ، وتوجيه ضربة صاروخية ضد

[1] رغدة البهي، مصدر سبق ذكره، ص62 ص63.

احد الأبراج التلفزيونية في كييف ، وبينما حاصرت القات الروسية مدينة ماريوبول بدأ الاوكرانيون يتلقون بريدا الكترونيا ظهر فيه احد الأشخاص مرتديا زي سكان المدينة متهما الحكومة الأوكرانية كذبا بالتخلي عن مواطنيها.

ب.الدعاية المضللة: وظفت روسيا سلاح المعلومات المضللة ، فيما وصفته بعض التحليلات بانها " الحرب الروسية _ الأوكرانية الهجينة " عبر الرسائل النصية والبريد الالكتروني التي زعمت ان أجهزة الصراف الآلي معطلة تارة وان القوات الأوكرانية استسلمت على نطاق واسع تارة أخرى ، وقد حذر المسئولون في مدونة Zero Hedge من مقاطع فيديو كاذبة ومقالات دعائية وظفتها وسائل الاعلام الروسية عن انفجارات كاذبة مفبركة مصحوبة بصور الجثث والمباني العسكرية المدمرة ، فباستخدام البيانات الضخمة والذكاء الاصطناعي وعدد من الخبراء قدرت نسبة انتشار الدعاية والاخبار الروسية المضللة منذ بدء الحرب حتى أوائل شهر يوليو 2022 بنحو 216% في أوكرانيا و 82% في الولايات المتحدة ، وذلك في صورة روايات مختلفة تلقي اللوم على واشنطن و كييف في بدء الحرب ، وتعتمد روسيا في ذلك على وسائل التواصل الاجتماعي والمنصات الرقمية لإطلاق روايتها على نطاق واسع باستخدام مواقع الويب التي تديرها الحكومة الروسية ، فتضخم سردياتها تارة ، وتعتم على هجماتها العسكرية ضد الأهداف الأوكرانية تارة أخرى.

ج.الدول الأكثر استهدافاً: منذ بداية الحرب الروسية – الأوكرانية حتى أوائل شهر يوليو 2022 يمكن القول ان دول حلف الناتو تعرضت للنصيب الأكبر من الهجمات السيبرانية الروسية ومنها النرويج والدنمارك و لاتفيا وليتوانيا وبولندا والسويد وتركيا ، اذ ركزت الهجمات على الحكومات الرسمية بجانب مؤسسات الفكر والرأي وشركات تكنولوجيا المعلومات وموردي الطاقة ما يعكس في مجمله تعدد نقاط الضعف الجماعية الأوروبية ، وقد أتت بولندا (مركز تقديم المساعدات الإنسانية والعسكرية لأوكرانيا) في المرتبة الثانية عقب الولايات المتحدة . كما تسببت احدى هجمات الحرمان من الخدمة في توقف خدمات موقعي وزارتي الخارجية والدفاع الفنلنديتين، بينما تحدث الرئيس الأوكراني " فولوديمير زيلينسكي " امام البرلمان الفنلندي في 2022/4/8 عبر تقنية الفيديو بالتزامن مع اشتباه فنلندا في اختراق طائرة حكومية روسية اجواءها الجوية.

د.القدرات الروسية: تتمتع جماعات القرصنة ووكالات الاستخبارات الروسية بقدرات متطورة مكنتها من تطوير البرامج الضارة ، وزرع التعليمات البرمجية والتجسس على معلومات حساسة ، وتنفيذ عمليات سيبرانية ذات تأثير عالمي لدعم جهودها العسكرية وشن هجمات سيبرانية أوسع نطاقا واكثر دقة على عشرات الدول فيما لا يتجاوز 6 اشهر ، كما استهدفت روسيا 4 فئات مختلفة هي : الشعب الروسي (لدعم مجهودها الحربي) ، والمواطنون الأوكرانيون (لتقويض الثقة بقدرة البلاد على المقاومة) ، والمواطنون الأمريكيون والأوروبيون (لصرف النظر عن

السياسات العسكرية الروسية) ، ومواطنو دول عدم الانحياز (للحفاظ على دعمهم في الأمم المتحدة وفي أماكن أخرى).

سادسا: سيناريوهات الحرب السيبرانية الروسية–الاوكرانية

بدأت مخاوف تصاعد حدة الصراع السيبراني بين روسيا وأوكرانيا تتجه نحو التزايد، ويمكن الوقوف عليها بالنظر الى السيناريوهات المحتملة التالية:[1]

1.استهداف البنى التحتية: ان التهديدات السيبرانية التي تستهدف البنى التحتية تخلف اضرارا تفوق تلك التي تنجم عن القصف العسكري، اذ شهدت الأعوام الماضية أمثلة عدة كانقطاع التيار الكهربائي بمدينة جوهانسبرج، واستهداف أجهزة الطرد المركزي بالمفاعلات النووية الإيرانية، وتوقف خدمات شركة أرامكو النفطية، وتوقف خط الأنابيب التابع لشركة "كولونيل بايبلاين"، وقد ينصرف تصاعد التوتر الروسي–الاوكراني الى هجمات سيبرانية محتملة على البنية التحتية، قياسا على استهداف وزارات الدفاع والمالية وشبكات الكهرباء في عام 2016، خصوصا مع انخفاض التكلفة المادية وتراجع الادانات الدولية لهذا النوع من التهديدات.

2.استهداف المعلومات الحيوية: بدأت أوكرانيا تتخوف من استهداف بياناتها ووثائقها الرسمية الحكومية، لما لها من قيمة استراتيجية استخبارية كبرى يتحدد على أساسها تحرك القوات الروسية العسكرية، وتحسبا لذلك بدأت أوكرانيا بوضع خطة استراتيجية من اجل حماية البنية التحتية لتكنولوجيا المعلومات، وشحن المعدات والنسخ الاحتياطية الى مناطق آمنة في الداخل الاوكراني بعيدا عن القوات الروسية، كما تلقت أوكرانيا عروضا لاستضافة بياناتها الحساسة والنقل المادي للخوادم وأجهزة التخزين القابلة للإزالة من قبل العديد من الدول لاسيما الدول الاوربية القريبة جغرافيا.

3.الخروج عن السيطرة: بدأ خبراء الأمن السيبراني يتخوفون من انتشار تهديدات سيبرانية محتملة على مستوى العالم يمكن ان تخرج عن نطاق السيطرة بكل سهولة وفي أي وقت ولا تتقيد بالحدود الدولية ،

[1] رغدة البهي، سيناريوهات الحرب السيبرانية بين روسيا وأوكرانيا، المركز المصري للفكر والدراسات الاستراتيجية، السنة الثالثة، العدد38، 2022، ص32 ص33

لاسيما بعد تفشي البرامج الضارة واطلاق القراصنة الروس فايروس (Notpetya) في عام 2017، الذي استهدف الشركات الأوكرانية الخاصة لتتجاوز تكلفته الاقتصادية مليارات الدولارات.

4.استهداف الدول الحليفة لأوكرانيا: تتخوف كلا من أمريكا وبريطانيا وكندا من امتداد دائرة الصراع السيبراني اليها، وتوجد العديد من الشواهد التي تدل على ذلك منها تعرض خدمة الانترنت الفضائي (KA-SAT) المقدمة من شركة ViaSa الامريكية الى هجوم سيبراني اسفر عنه قطع خدمة الانترنت لدى عدد كبير من مستخدميها خصوصا مع اتساع قاعدة العملاء الاوكرانيين، وتعطل الأنظمة الالكترونية لمطار لندن هيثرو، وتحذيرات البنك المركزي الأوربي من هجمات سيبرانية على عدد من المصارف الأوروبية، وتحذيرات مكتب التحقيقات الفيدرالي الأمريكي FBI من التعرض لهجمات سيبرانية على خلفية العقوبات الامريكية على روسيا.

الخاتمة:

الحكمة العسكرية التي تقول "أول ضحية في الحرب هي الحقيقة" ستبقى قائمة. الحرب السيبرانية ستظل واحدة من الأدوات الرئيسية المستخدمة في الحروب القادمة، فالتهديدات السيبرانية والهجمات التخريبية والمدمرة الأخرى المحتملة ستستمر مع تقدم النزاع في أوكرانيا، فالحرب السيبرانية ستكون جزءا مأساويا من حروب المستقبل وستتضمن محاربة الأعداء عن بعد باستخدام فئات جديدة من الأسلحة مثل الفيروسات، والبرامج الضارة، والبرامج التي تغير هدف تشغيل النظام، او حتى توقف تشغيل النظام بالكامل، وستكون الهجمات السيبرانية ساحة المعركة الجديدة غير المرئية التي لا يمكن التنبؤ بها، فالأساليب متجددة ومفتوحة للإبداع والابتكار وإنتاج الأفكار وصراع العقول، ومن المؤكد أننا أمام حروب جديدة ليس لها سوابق في التاريخ، وفي بداية عصر جديد لن يكون فيه مكان الا لمن يبحث ويبتكر في مجال الفضاء السيبراني، اما للدفاع عن بنيته المعلوماتية وفضائه السيبراني، واما للهجوم على الأعداء المحتملين حال اقتضت الضرورة.

فالكثير من الدول بدأ يفكر في انشاء "جيوش رقمية" لتأهيل اكبر عدد من الكوادر القادرة على الابداع في هذا الفضاء الواسع، فالعقول المبدعة هي التي يمكن ان تغير قواعد حروب المستقبل وتنتزع انتصارا بتكاليف اقل من تكلفة الأسلحة التقليدية واسلحة الدمار الشامل، وتلحق اكبر الأضرار غير المرئية بالعدو

المحتمل، وقد تتغير موازين القوى العسكرية في المستقبل اذ يمكن لدولة لا تمتلك الكفاية من القوة الصلبة "العسكرية" ان تستخدم قوتها العقلية والإبداعية في الفضاء السيبراني لتتفوق على اعدائها.

المصادر:

1. Ahmed Salem Al-Muntaser, New Manifestations in the Concept of "Cyber" Electronic Security (Comparative Study), 1st Edition, Dar Al-Bayan Publications for Printing and Publishing, 2017.

2. Mona Al-Ashkar Jabbour, Cyber Obsession of the Age, Beirut, Arab Center for Legal and Judicial Research, 2017.

3. International Telecommunication Union, Telecommunication Reform Trends, Geneva: International Telecommunication Union, 2008.

4. Marai Ali Al-Ramahi, Cyberwar and New National Security Requirements, 1st Edition, Arab Democratic Center for Strategic, Political and Economic Studies, Germany - Berlin, 2022.

5. Pioneer of Aviation, Jassim Muhammad Al-Busaili, Electronic War: Its Foundations and Impact on Wars, The Arab Institute for Studies and Publishing, Beirut, 2nd Edition, 1989.

6. John Bassett, Future Wars in the Twenty-First Century, Emirates Center for Strategic Studies and Research, Abu Dhabi, 2014.

7. Hakim Gharib, Sabrina Sharqi, The Repercussions of Electronic Warfare on International Relations: A Study of the Electronic Attack on Iran (StackNest Virus), Journal of Policy and Law Notebooks, Volume 12, Issue 2, 2020.

8. Raghda Al-Bahi, Cyber Battles in the Russian-Ukrainian War, Journal of Military Affairs, Egyptian Center for Thought and Strategic Studies, Issue 1,

October 2022. Ahmed Fathi, Cyber Wars: The Russian-Ukrainian Crisis as a Model, Aton Center for Studies, Cairo, 1st Edition, 2023

9. Raghda Elbehi, Scenarios of Cyber War between Russia and Ukraine, Egyptian Center for Thought and Strategic Studies, 2022, available at the following online link: https://ecss.com.eg/author/raghda-elbehi/

10. Adel Abdel Sadiq, Cyber Wars: Escalating Capabilities and Challenges to Global Security, Arab Center for Cyberspace Research, available at the following electronic link: https://accronline.com/article_detail.aspx?id=28395

11. Adel Abdel Sadiq, Cyberterrorism and National Security in a Changing Environment, Arab Center for Cyberspace Research, Periodicals - Strategic Concepts, available at the following electronic link: https://accronline.com/article_detail.aspx?id=31557

12. Melzer, Nils. "Cyberwarfare and international law", 2011

13. Shane M, Coughlan. "Is there a common understanding of what constitutes cyber warfare?, The University of Birmingham School of Politics and international Studies, 30 September 2003 .

14. Oxford Analytica (2022), 'Cyberspace will be central to Russia's Ukraine plan', Expert Briefings.
https://doi.org/10.1108/OXAN-ES267528

15. Oxford Analytica (2022), "Russian invasion raises risk of cascading cyberattack", Expert Briefings.
https://doi.org/10.1108/OXAN-ES267563

16. Oxford Analytica (2022), "Russian cyber warfare could result in casualties", Expert Briefings. https://doi.org/10.1108/OXAN-ES267581