Innovations Journal of Humanities and Social Studies (IJHSS): Vol 4, No 1, 2026

DOI: https://doi.org/10.61856/4eg54316

Scientific Events Gate

Innovations Journal of Humanities and Social Studies

IJHSS

https://eventsgate.org/ijhss

e-ISSN: 2976-3312

التجربة الروسية في الحروب السيبرانية "الحرب الأوكرانية نموذجاً 2014-2022"

سميرة سدراتي – د.ليندة زموري

جامعة قاصدي مرباح ورقلة – الدولة - الجزائر

Sarahkhalfaoui02@gmail.com - l.zemouri@yahoo.fr

الملخص في ظلّ الثورة التكنولوجية المتسارعة التي يشهدها العصر الحديث، اخترقت التحولات الرقمية مختلف أوجه التفاعلات الاجتماعية والاقتصادية والسياسية، ولم تقتصر آثارها على المجالات المدنية فحسب، بل امتدّت لتطال طبيعة الحروب ذاتها، حيث أضحت الصراعات المعاصرة تتخذ أشكالًا غير تقليدية، يُدار جزء كبير منها في الفضاء السيبراني بوصفه أداة مركزية من أدوات الصراع والتنافس والهيمنة الدولية. وفي هذا السياق، برزت روسيا كفاعل دولي وظّف المجال السيبراني توظيفًا استراتيجيًا، مجنِّدةً قدراتها التقنية والاستخباراتية والعسكرية لجعل الفضاء السيبراني أحد عناصر القوة والردع في سياستها الأمنية. وتُعدّ الحروب السيبرانية اليوم من أبرز سمات الصراعات السياسية والاقتصادية والتجارية بين الدول، إذ تستهدف البنى التحتية الحيوية، والمنشآت والمؤسسات الحكومية، والشبكات الصناعية، ومراكز البحث والمعرفة، بما يؤدي إلى إرباك الدول وتهديد أمنها القومي. وتهدف هذه الدراسة إلى تقديم رؤية تحليلية واضحة حول مفهوم الحروب السيبرانية، مع التركيز على الحرب الروسية الأوكرانية بوصفها نموذجًا معاصرًا، وتحليل النتائج المترتبة عنها على المستويين الأمني والسياسي. وقد اعتمدت الدراسة على منهج تحليل المضمون للكشف عن أنماط واستراتيجيات الحرب السيبرانية التي انتهجتها روسيا ضمن مقاربتها الأمنية في مواجهتها مع أوكرانيا، سعيًا للحفاظ على أمنها وتعزيز مكانتها وهيمنتها الدولية. ومن أبرز النتائج المتوصل إليها أن الفضاء السيبراني أصبح ساحة جديدة ومفتوحة للصراع الدولي، يتم من خلالها تنفيذ أعمال تخريبية وتدميرية، ولا سيما الهجمات على أنظمة المعلومات والشبكات، بما يشكّل تهديدًا مباشرًا لأمن الدول واستقرارها.

الكلمات المفتاحية: الحرب السيبرانية، الأمن السيبراني، روسيا، الثورة التكنولوجية، الإستراتيجية الروسية.

The Russian Experience in Cyberwars "The Ukrainian War as a Model (2014-2022)"

Sedrati Samira - Dr. zemouri linda

Kassidi merbah university ouargla - Algeria

Sarahkhalfaoui02@gmail.com - l.zemouri@yahoo.fr

Received 02\|08\|2025 - Accepted 22\|10\|2025 Available online 15\|01\|2026

Abstract: In light of the rapid technological revolution characterizing the modern era, digital transformations have penetrated all forms of social, economic, and political interaction. Their impact has not been limited to civilian spheres but has extended to the very nature of warfare itself, as contemporary conflicts have increasingly assumed non-traditional forms, with a significant part being conducted in cyberspace as a central instrument of international conflict, competition, and dominance. In this context, Russia has emerged as a key international actor that has strategically exploited the cyber domain, mobilizing its technical, intelligence, and military capabilities to make cyberspace a core element of power and deterrence within its security doctrine. Cyber warfare has thus become one of the most prominent features of political, economic, and commercial conflicts among states, targeting critical infrastructure, governmental facilities and institutions, industrial networks, and research and knowledge centers, thereby disrupting state functions and threatening national security. This study aims to provide a clear analytical perspective on cyber warfare, with particular emphasis on the Russian–Ukrainian war as a contemporary case study, and to examine the consequences arising

DOI: https://doi.org/10.61856/4eg54316

from it at both the security and political levels. The study adopts a content analysis approach to identify and analyze the patterns and strategies of cyber warfare employed by Russia within its security strategy in the confrontation with Ukraine, with the objective of preserving its security and reinforcing its international influence and dominance. Among the most significant findings is that cyberspace has become a new and open arena for international conflict, through which destructive and disruptive actions are carried out, particularly attacks on information systems and networks, posing a direct threat to state security and stability.

Keywords: Cyber Security, Russia, Technological Revolution, Russian Strategy.

المقدمة:

لقد أحدثتِ التطورات السريعة التي عرفها القرن الحادي و العشرون خاصة ما تعلق بالثورة التكنولوجية و انعكاساتها على جميع مناحي الحياة (الاجتماعية ،و الاقتصادية ،و السياسية و الثقافية) لاسيما في المجالين العسكري و الأمني، أحدثت تغيراً في منطق الحرب التي انتقلت من ميادين القتال الكلاسيكية (البر ،و البحر ،و الجو و الفضاء) إلى شبكات الإنترنت و العالم السيبراني.

أسفرت الثورة في مجال التكنولوجيا و المعلوماتية إلى بروز الفضاء السيبراني ليكون أحد ميادين التنافس و الصراع بين القوى الكبرى، وأصبحت الحروب في الوقت الراهن غير تقليدية بل تُدار في الفضاء السيبراني أداةٌ من أدوات الصراع و التنافس و الهيمنة الدولية . لذلك تتسابق الدول لتعزيز أمنها السيبراني في مواجهة أي هجمات محتملة، فقد أصبح الأمن السيبراني قمة أولويات الأمن القومي للدول الكبرى، وقد لوحظ أن كافة الدول تمتلك فِرقاً للاستجابة السريعة كما أنها مرتبطة باتفاقيات للتعاون الدولي في المجال السيبراني كما استحدثت قوانين لحماية الأمن الإلكتروني.

و لذلك استخدمت روسيا كل قدراتها في المجال السيبراني لتجعل هذا الفضاء أحد عناصر القوة و الردع في استراتيجياتها الأمنية و في إدارة حروبها، خاصة الحرب الروسية الأوكرانية.

أهمية الدراسة :

- تبرز أهمية البحث من الناحية العلمية في كونه عبارة عن دراسة تشخيصية وتحليلية لما يعيشه العالم اليوم في ظل التطور التكنولوجي وبروز الفضاء الإلكتروني الذي أصبح قوة في أيدي من يمتلكونه بما يخدم مصالحهم دون غيرهم.

- تساعد هذه الدراسة في فهم الإستراتيجية التي تتبعها روسيا في الفضاء السيبراني بما في ذلك أساليب الدفاع و الهجوم و جمع المعلومات الاستخباراتية .

أهداف الدراسة:

- البحث عن الإستراتيجية التي خلفتها القوة السيبرانية في الدول خاصة في إستراتيجياتها الأمنية.

- التعرف الى الظاهرة واقعياً بدراسة حالة روسيا و محاولة فهم، وإبراز الظروف التي شجعت ونمت الظاهرة.

- تحليل الحروب السيبرانية و تحديد خصائصها و مكانتها في منظومة الصراع الدولي .

- المساهمة في فهم تأثير البيئة الجيوسياسية على تطور أساليب الحروب السيبرانية خاصةً في الصراعات ذات البعد الدولي من الحرب الروسية – الأوكرانية.

- توضيح العلاقة الوثيقة بين العمليات العسكرية التقليدية و العمليات السيبرانية في نموذج الحرب الهجينة.

منهج الدراسة:

تعتمد الدراسة على المناهج الآتية :

- المنهج الوصفي التحليلي الذي يهدف إلى تحقيق الفهم الدقيق و الوصفي بالأبعاد الحقيقية للظواهر و الموضوعات، وذلك من خلال وصف وتحليل مفهوم الأمن السيبراني و تحليله، و واقع التجربة الروسية مروراً بالإستراتيجيات و آليات الأمن الروسي في ظل الحرب الأوكرانية.
- المنهج التاريخي ،و الذي من خلاله يمكننا الرجوع إلى جذور و بدايات الموضوع الأولية، و بداياته والمحطات التاريخية و الأحداث المهمة لمساعدتنا على فهم الموضوع.

DOI: https://doi.org/10.61856/4eg54316

- منهج دراسة الحالة، وفيه يُركّزُ على حالة معينة يقوم الباحث بدراستها، و ستُدرسُ هذه الحالة بشكل مستفيض وواف، يُناقشُ كل المتغيرات و الظواهر المرتبطة به بالوصف الكامل و التحليل من خلال تسليط الضوء على الأمن السيبراني انطلاقاً من تجربة الحرب السيبرانية الروسية الأوكرانية، و استناداً إلى هذا المنهج يمكن تفسير و قياس الدور العملي المباشر للقدرات السيبرانية في النزاعات المسلحة و تفسيره تفسيراً واضحاً.

مشكلة الدراسة:

إنَّ الحروب السيبرانية تُعدُّ من حروب المستقبل لأنها تستخدم فيها تكنولوجيات قتالية تختلف عن الحروب التقليدية وتستعمل فيها أساليب يصعب تعقبها، وهي الإستراتيجية التي نفذتها روسيا في حربها على أوكرانيا و لتحليل موضوع الدراسة نطرح الإشكال المتمثل في السُّؤال الرئيسي الأتي : إلى أي مدى شكلت الهجمات السيبرانية الروسية ضد أوكرانيا نموذجاً جديداً من الحروب الهجينة ؟ و كيف أصبح الأمن السيبراني جزءًا من أمن الدولة ؟

ويتفرع من الإشكال السابق الأسئلة الفرعية الآتية :

1-ما المقصود بالأمن السيبراني ؟

2-ما هو واقع التجربة الروسية ؟

3-كيف وظفت روسيا قدراتها السيبرانية في الحرب الأوكرانية و ما مدى تأثير هذه العمليات على مجريات الصراع و نتائجه ؟

4-ما أبرز الدروس المستقاة التي يمكن توظيفها في تطوير إستراتيجيات الأمن السيبراني للدول ؟

فرضيات الدراسة:

-إن القدرات السيبرانية الروسية تشكل عنصراً حاسماً في الحرب و الصراعات منها الحرب الأوكرانية . و قد أسهمت في التأثير على مسار الصراع ونتائجه من خلال استهداف البنية التحتية الحيوية و تعطيل القدرات الدفاعية الأوكرانية.

الإطار النظري للدراسة:

تُعُّد النظرية الواقعية (و نشأت النظرية الواقعية من خلال أعمال' توماس هوبز 'و 'نيكولو ميكافيلي' باعتبارها منهجاً في العلاقات الدولية، و قد عرفها 'جوناثان هاسلام ' أستاذ تاريخ العلاقات الدولية بجامعة كمبريدج أنها : " عبارة عن مجموعة من الأفكار التي تدور حول المقترحات الأساسية الأربعة و هي السياسة الجماعية ،و الأنانية ،و الفوضى و القوة السياسية " . (araj, 2022) وتُعدُّ المدرسة الواقعية اتجاهاً من الاتجاهات الفكرية و السياسية التي تتناول العلاقات الدولية من منظور يركز على القوة و المصالح الوطنية و التفاعلات الدولية على أساس أنها محور لفهم السياسة الدولية.

و ترتكز الواقعية على التنافس بين الدول وتُعدُّ التهديدات الأمنية السيبرانية أداة لكسب المزيد من المصالح السياسية و الاقتصادية، حيث بات التفوق السيبراني هدف تسعى إليه جميع دول العالم لتحقيق السيادة و النفوذ و الأهداف السياسية، و أصبح يطلق على عمليات ارتكاب أفعال الاختراق السلم و الأمن الدوليين بحجة التفوق السيبراني أو الردع الافتراضي، مثل الهجوم السيبراني الروسي على أوكرانيا عام 2015 الذي أدى إلى انقطاع الكهرباء على ربع مليون أوكراني.

التحديد الزماني و المكاني للدراسة :

تطبق الدراسة على روسيا و استخدامها للفضاء السيبراني في حربها على أوكرانيا، و تبدأ فترة الدراسة من سنة 2014 بداية الهجوم الروسي على أوكرانيا إلى غاية غزو روسيا لأوكرانيا في فبراير 2022 .

هيكلة الدراسة: و سيُناقشُ ذلك من خلال المباحث الآتية:

المبحث الأول :مفهوم الأمن السيبراني .

المبحث الثاني : واقع التجربة الروسية .

المبحث الثالث : آليات الحماية الروسية في ظل الحرب الأوكرانية و إستراتيجياتها.

المبحث الرابع : نتائج استخدام روسيا للحرب السيبرانية على أوكرانيا.

DOI: https://doi.org/10.61856/4eg54316

الدراسات السابقة

أُطّلِعَ على بعض الدراسات السابقة التي لها علاقة بالموضوع، نوجزها فيما يأتي :

-أولاً : دراسة شريطي و بن عزوز (shriti & hatem, 2023) بعنوان " الإستراتيجية الروسية في الحروب السيبرانية : قراءة في نموذج الصراع السيبراني الروسي مع بعض الدول "، و تهدف هذه الدراسة إلى تقديم نماذج عالمية من الحروب السيبرانية بين الدول و خاصة التي خاضتها روسيا مع بعض الدول مثل (استونيا 2007، و جورجيا 2008، و قيرغيرستان و أوكرانيا)، و خلصت الدراسة إلى انه كلما زادت رقمنة القطاعات العامة زادت حرب المعلومات.

-ثانياً : دراسة نورهان **(hani, 2025)** بعنوان " توظيف التهديدات السيبرانية في الحرب الروسية الأوكرانية "، وتسلط الضوء على أنماط التهديد السيبراني الروسي و تطور استخدامه كوسيلة حرب موازية للعمليات العسكرية التقليدية . و خلصت هذه الدراسة إلى أن الحرب الروسية الأوكرانية سببها الفضاء السيبراني الذي أصبح مجالاً متكاملاً لا يقل أهمية عن ميادين الحروب التقليدية.

-ثالثاً : دراسة توماس لاشان (lachan, 2024) بعنوان " "الحرب الهجينة' ...جبهة حرب روسية خفية ضد الغرب" وتهدف هذه الدراسة إلى تسليط الضوء على كل الأدوات التي تستعمل في الحروب الهجينة و التي تعتد على التكنولوجيات الحديثة في الحرب بين البلدين روسيا و أوكرانيا .و تشير هذه الدراسة إلى أن روسيا تقوم بالعديد من الأعمال التخريبية في أوروبا نتيجة هذه الحروب الهجينة.

التعقيب على الدراسات السابقة :

استفادت هذه الدراسة من الدراسات السابقة في إعداد مضمونها، و تشابهت الدراسة الحالية مع الدراسات السابقة في دراسة الحرب السيبرانية، و تختلف عن الدراسات السابقة في دراستها الحرب السيبرانية بين روسيا و أوكرانيا فقط وقد حُلِّلتِ الأدوات والآليات المستعملة بين الطرفين في هذه الحروب الحديثة، و خلصت الدراسة إلى أن الأمن السيبراني ساهم في ظهور فواعل جديدة بالنظام الدولي، كما عزز من دور القوى العظمى و مدها بأدوات حديثة لتحقيق أهدافها وخلق تحديات حديثة أمام بعض الدول .

أولاً : مفهوم الأمن السيبراني:

يُعدُّ مفهوم الأمن السيبراني من المفاهيم الحديثة التي ظهرت مع انفجار الثورة المعلوماتية و التكنولوجية في العصر الحالي، وقد حاول الباحثون و العلماء و العديد من الهيئات و المنظمات الدولية تقديم تعريف واضح و شامل للأمن السيبراني . وقبل التطرق لتعريفه نُوضح المقصود بكل من الفضاء السيبراني، و الحرب السيبرانية لارتباطهما به.

1 - تعريف الفضاء السيبراني:

هناك تعريفات عديدة للمجال الافتراضي أو حيز السايبر فقد عرفته الوكالة الفرنسية لأمن أنظمة الإعلام (ANSSI) بأنه :" فضاء التواصل المشكل من خلال الربط البيئي العالمي لمعدات المعالجة الآلية للمعطيات الرقمية **".** (zuriga, 2019, p. 1017) هذا التعريف ركز على الجانب التقني و أغفل الجانب البشري، و الذي يُعد أساساً في الفضاء السيبراني. كما عرفه الاتحاد الدولي للاتصالاتInternational Telecommunication Unlon و هي وكالة الأمم المتحدة المتخصصة في مجال تكنولوجيات المعلومات و الاتصالات يعرف الحيز الافتراضي بأنه "الحيز المادي وغير المادي الذي ينشأ أو يتكون من جزء أو من كل العناصر الآتية : (حواسيب، وأجهزة ممكنة، وشبكات، ومعلومات محوسبة، و برامج و مضامين، ومعطيات مرور و رقابة، و الذين يستخدمون كل ذلك) . (mahmoud, 2013, p. 116) وهناك من يعرف المجال الافتراضي بأنه " ساحة الحرب الخامسة بعد البر و البحر والجو و الفضاء الخارجي". و هناك توجه يرى فيه واحداً من سبعة مجالات، إلى جانب الجو و الفضاء و البحر و البر و الحيزين الإلكترو- مغناطيسي و الإنساني. (mahmoud, 2013)

من خلال كل هذه التعريفات السابقة يمكننا تقديم تعريف شامل للفضاء السيبراني بأنه " عبارة عن بيئة تفاعلية حديثة، تشمل عناصر مادية و غير مادية، مكونة من مجموعة من الأجهزة الرقمية، و أنظمة الشبكات ،و البرمجيات، و المستخدمين سواء مشغلين أو مستعملين".

2-تعريف الحرب السيبرانية :

تُعَرَّفُ الحرب السيبرانية بأنها " تلك الإجراءات التي تتخذها الدولة من أجل الهجوم على البنية التحتية للعدو بهدف التأثير و الإضرار بها و الدفاع عن نظم المعلومات الخاصة بالدولة المهاجمة و إذا سببت الهجومات السيبرانية نزاعاً مسلحاً بوصفها

DOI: https://doi.org/10.61856/4eg54316

عملية إلكترونية سواء هجومية أو دفاعية قد يخلق إصابات أو قتل أشخاص أو الإضرار بممتلكات ". (alyazeed, 2024) كما تُعرَّفُ الحرب السيبرانية بأنَّها " هجوم متعمد يهدف إلى تعطيل عمل أو خداع أو إضعاف أو تدمير أنظمة الكومبيوتر و شبكات الاتصال و المعلومات و كل البرامج الموجودة في الأنظمة أو الشبكات التي تمر من خلالها ". (waheb, 2017, p. 21) وتُعرّفُ أيضاً بأنَّها "حرب غير محدودة المجال، و غامضة الأهداف، وهي حروب أقل تكلفة من الحرب التقليدية، و كما تعد أكثر ضرراً منها لتشعب أهدافها و تعدد أغراضها، و عادة ما ينتج عنها إصابات و قتل المدنيين و المستهدفين و تضر بمنشآت الدولة " . (alyazeed, 2024)، وهناك تعريف آخر للحرب السيبرانية يرى بأنها :"عبارة عن أعمال هجومية و دفاعية، متكافئة و غير متكافئة، تنفذ في الشبكات الرقمية من طرف الدول أو جهات فاعلة مماثلة للدول (أو ما دون الدولة)، و تتضمن مخاطر تصيب البنية التحتية الوطنية المهمة و الأنظمة العسكرية ". (odeh, 2022, p. 7)

3-تعريف الأمن السيبراني

يُعرَّفُ الأمن السيبراني بأنه: " مزيج من الأساليب و العمليات و الأدوات و السلوكيات التي تحمي أنظمة الكومبيوتر و الشبكات و البيانات من الهجمات الإلكترونية و الوصول غير المصرح " . (fortient) كما يستخدم هذا المصطلح للإشارة إلى مجموعة من الظروف و الأحداث المتعلقة بتحسين سلامة نظام معين لإدارة المعلومات أو البنية التحتية . (schiliro, 2022, p. 2) بالنسبة للأكاديميين يعرفه كل من pekka Neittaanmati ,Marti lehol بأنه :" مجموعة من الإجراءات التي اتخذت في الدفاع ضد هجمات قراصنة الكومبيوتر و عواقبها و يتضمن تنفيذ التدابير المضادة المطلوبة " . (bouzaida, 2019, p. 1266) أما أستاذ الاتصالات في جامعة كاليفورنيا ريتشارد كمرر Richard.A Kemmerer، فيُعرّفُ الأمن السيبراني بأنه : "مجموعة وسائل دفاعية من شأنها كشف وإحباط المحاولات التي يقوم بها القراصنة " . و قد أيده في الطرح واحد من أهم المختصين في الميدان، و هو الأستاذ إدوارد أموروزو Edward Amoroso، الذي عرَّفَ الأمن السيبراني "تلك الوسائل التي من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات ". (bouzaida, 2019)

وبالنسبة للدوائر الحكومية فتُعرّف وزارة الدفاع الأمريكية الأمن السيبراني بأنه : "مجموعة من الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكالها (الإلكترونية و المادية) .من مختلف الجرائم، والهجمات، والتخريب ،و التجسس و الحوادث .أما وكالة الأمن الرقمي الأوروبية فعَرَّفتهُ بأنه " قدرة النظام المعلوماتي على مقاومة الاختراق أو الحوادث غير المتوقعة، التي تستهدف البيانات المتداولة أو المخزنة وفق إطار توافقي ". أما تعريف الاتحاد الدولي للاتصالات و الذي يُعدُّ بمثابة أرضية إجماع لمختلف التوجهات الفكرية و المهنية فهو :"مجموعة المهمات، مثل تجميع وسائل، وسياسات، وإجراءات أمنية، و مبادئ وتوجيهات، و مقاربات لإدارة المخاطر، وتدريبات، وممارسات فضلى، وتقنيات يمكن استخدامها لحماية البيئة السيبرانية و موجودات المؤسسات والمستخدمين ".(bouzaida, 2019)

ومن خلال هذه التعريفات السابقة يمكننا إعطاء تعريف شامل للأمن السيبراني أو الالكتروني و هو أنَّ مجمل القوانين ،و الأدوات ،و النصوص ،و المفاهيم و الميكانيزمات الأمنية و طرق تسيير الأخطار و الممارسات التقنية المتعلقة بتكنولوجيات المعلومات و الاتصالات المستخدمة لحماية مصالح الدول و الأشخاص، ليبقى الهدف في الأخير، هو قدرة هذه الأدوات على مقاومة التهديدات المتعمدة من طرف قراصنة المعلومات أو غير المتعمدة من طرف المستخدمين، و بالتالي التحرر من الأضرار الناجمة عن تعطيل أو سوء استخدام تكنولوجيا المعلومات و الاتصالات .

4-أبعاد الأمن السيبراني :

يتكون الأمن السيبراني من عدة أبعاد و هي : (البعد العسكري، والبعد الاقتصادي، والبعد الاجتماعي، والبعد القانوني، والبعد السياسي). (samir, 2017, pp. (260,263))

أ-البعد العسكري : تكمن الميزة النسبية للقوة السيبرانية في قدرتها على ربط الوحدات العسكرية بعضها ببعض عبر الشبكات العسكرية في الفضاء الإلكتروني .

ب-البعد الاقتصادي : استخدام الكمبيوتر و شبكة الانترنت في تطوير الصناعات و تحريك الاقتصاد، زاد من أهمية ضرورة توفير الأمن السيبراني لضمان حماية هذه المعلومات.

ج- البعد الاجتماعي : يجب تعميم المفهوم الصحيح للأمن إلى كل المشتركين في الشبكة المعلوماتية الدولية، إذ يُعدُّ خطوة أساسية لتقوية مستوى الأمن.

د-البعد القانوني : تزايد النشاط الفردي و المؤسساتي و الحكومي في الفضاء السيبراني، يستدعي وجود ترسانة قانونية تنسجم مع التطورات الحاصلة.

DOI: https://doi.org/10.61856/4eg54316

ه-البعد السياسي: التسريبات المختلفة للوثائق المهمة و الحساسة التي تؤدي إلى مشكلات كبيرة، تستدعي الاهتمام بالبعد السياسي للأمن السيبراني.

ثانياً : واقع التجربة الروسية

تتعرض أوكرانيا لهجمات متعددة و مستمرة من قراصنة روس مدعومين من الكرملين منذ أن قامت موسكو بضم شبه جزيرة القرم خلال عام 2014، حيث أصبح التجسس السيبراني، و القيام باختراق الشبكات و قواعد البيانات و الخوادم و إيقاف تشغيل مرافق الطاقة و الاتصالات وترويج الشائعات و المعلومات المضللة جانب من جوانب الصراع بين روسيا و أوكرانيا. (mohi, 2022)، و تضمنت المراحل الآتية :

1-المرحلة الأولى من العام 2014 – 2017:

- تمكن المهاجمون السيبرانيون الروس خلال عام 2014 من الوصول إلى النظام الخاص بفرز الأصوات في أوكرانيا قبيل الانتخابات العامة، مما أدى إلى إتلاف السجلات الإلكترونية و أجبرت السلطات الأوكرانية إلى فرز بطاقة الاقتراع بالطريقة اليدوية. (odeh, 2022, p. 10)

- في العام التالي أي في 2015، تتسبب هجوم سيبراني في انقطاع التيار الكهربائي لبضع ساعات بغرب أوكرانيا و جزء من كييف، في عملية منسوبة إلى مجموعة لها علاقة بالمخابرات العسكرية الروسية، و يُعدُّ هذا الانقطاع أول انقطاع معروف للتيار الكهربائي تسبب فيه هجوم سيبراني.(odeh, 2022)

- و في سنة 2017 وقع هجوم نوت بتيا Not pety . قامت به المجموعة نفسها المرتبطة بالمخابرات العسكرية الروسية و قد نجح هذا الهجوم في إصابة ما يقارب من 10 بالمئة من جميع أنظمة الكومبيوتر الأوكرانية بحزمة برامجيات خبيثة قبل أن تنتشر في كل أنحاء العالم في واحدة من أشد الهجمات السيبرانية تدميراً في التاريخ ؛ حيث كلفة الشركات في جميع أنحاء العالم خسائر قاربت من 10مليارات دولار، وفقا لتقدير أمريكي.(alyazeed, 2024)

2-المرحلة الثانية :من 2018الى 2021 :

-وقعت محاولتان هجوميتان إلكترونيتان كبيرتان في عامي 2018 و2021 استهدف الهجوم الأول المحطة الأولى لتقطير الكلود تعمل في 23 مقاطعة أوكرانية . بينما استهدف الهجوم الثاني المواقع الإلكترونية لجهاز الأمن الأوكراني، وقد فشل الهجوم بسبب نظام التفاعل الإلكتروني الذي تستخدمه الهيئات التنفيذية الحكومية لكنه نجح في إلحاق الضرر بالنظام. (przetazink & simona, 2022)

3-المرحلة الثانية : من 2021 إلى انطلاق غزو روسيا لأوكرانيا:

-كشفت مايكرسوفت في مطلع فبراير 2022 عن استهداف مجموعة اكتينيوم Actinium التي يُعتقد أن لها علاقة بأجهزة الأمن الروسية ،و الوحدات الإدارية العسكرية و الشبكات الحكومية الأوكرانية، و بدأ هذا الاستهداف منذ أكتوبر 2021 ،و الغرض منه هو التجسس و جمع المعلومات. **(mohi, 2022)**

قامت روسيا بجملة من العمليات (Infektion) تدار من داخل روسيا، مثل (عمليات التزوير ،و التدخل ،و الهجمات ضد منتقدي الكرملين) على وسائل التواصل الاجتماعي، كما استخدمت حسابات ووثائق مزورة لإثارة الصراع بين الدول الغربية و استهدفت على الخصوص أوكرانيا، وقبل تسعة أشهر فقط من بداية الغزو الروسي أُنتجَ مالا يقل عن 2500 محتوى بسبع لغات، عبر أكثر من 300 منصة. (almoqarani, 2022)فمثلًا، نُشِرت تقارير وصور روسية في العديد من وسائل التواصل الاجتماعي وعلى الفضائيات الروسية وبلغات عديدة، وروايات مثل الادّعاء بوجود مختبرات تابعة « للبنتاغون» تُقوم بأبحاثً عن الأسلحة البيولوجية في أوكرانيا. كما ادّعى المتحدث باسم وزارة الدفاع الروسية " إيغور كوناشينكوف " في 06 مارس، أن العملية العسكرية الروسية في أوكرانيا قد أظهرت أدلة على قيام مختبرات تابعة « للبنتاغون» في أوكرانيا بالقيام بأبحاث حول الأسلحة البيولوجية. كما قامت حسابات تابعة لروسيا لاحقًا بتهويل هذا الادّعاء، و القول إنَّ هذه المختبرات البيولوجية تُموَّل من الولايات المتحدة، و لا تُوجَد في أوكرانيا فقط، بل في كل أنحاء العالم أيضًا. وروسيا لا تزال تقوم بتحقيقات حول الموضوع، وتزعم أنها بصدد تقديم أدلة أكثر حول هذا الموضوع، و لحد الآن لم يظهر ما يؤكد ما تدعيه روسيا. (almoqarani, 2022)

3-أهداف الحرب السيبرانية الروسية على أوكرانيا:

استهدفت روسيا جراء توظيفها للحرب الإلكترونية على أوكرانيا عدة أهداف، و من أبرزها ما يأتي : (ali, 2024)

DOI: https://doi.org/10.61856/4eg54316

-إدخال الحرب النفسية و الخداع الإستراتيجي في أوكرانيا.

-الإخلال بمعادلة الدعم الغربي لأوكرانيا، وذلك من خلال اختراق البنية التحتية الغربية و خاصة الأمريكية.

-السعي إلى تقويض الثقة في النظام الأوكراني و إحداث شعور بنقص السيطرة.

-التركيز على تآكل الثقة العالمية في أوكرانيا بالاعتماد على الدعاية الحاسوبية.

ثالثاً : آليات الحماية السيبرانية الروسية في ظل الحرب الأوكرانية واستراتيجيات:

تعتمد الإستراتيجية الروسية في الحروب السيبرانية على تخريب البنية التحتية و تعطيل كل الاتصالات و قطع الخدمات للخصم، ولتجسيد ذلك تركز روسيا على وكالات متخصصة في الأمن السيبراني، و كل جهاز له مهامه الخاصة، وتستخدم هذه الأجهزة مجموعة من الأدوات و الآليات في حرب المعلومات، كالتضليل المعلوماتي، والقرصنة والاختراق، و التأثير في الرأي العام، وقطع الخدمات.

1-الإستراتيجية السيبرانية الروسية:

تغير تصور مفهوم الحرب لدى القيادة الروسية من كونه خياراً يركز على القوات المسلحة و العنف التقليدي إلى كونه خياراً يعتمد بالأساس على المزج بين الطرق العسكرية و الأساليب الحديثة المتنوعة و التي تعرف اليوم بحرب الجيل الخامس، (و تعرف حروب الجيل الخامس بأنها: " حروب بلا قيود تكون في فترة زمنية ممتدة تستهدف هزم الخصم و تفجير الدولة داخليًّا، و هذا بتركيزها على التناقضات الداخلية و المجتمعية و محاولة تعميق هذه التناقضات باستخدام كل أنواع الأدوات و المواجهات العسكرية و غيرها، إضافة إلى توظيف الحرب الاقتصادية و المعلوماتية و النفسية ") . (sehel, 2023, p. 11) و قد برز هذا النوع من الحروب خاصة بعد ظهور ميدان الفضاء السيبراني كمفهوم غريب في روسيا، و تعتمد الإستراتجية الروسية في الحرب السيبرانية على محاولة إيقاف البنية التحتية المعلوماتية للخصم و تعطيل الاتصالات المدنية و العسكرية له قبل البدء في العمليات العسكرية، و يستخدم الروس عبارة أمن المعلومات Informatsionnauya besopastnost بدلا عن الأمن المعلوماتي، كما قدمت وزارة الدفاع الروسية تعريفًا خاصًّا لمفهوم حرب المعلومات:" بأنها عبارة عن المواجهة بين دولتين أو أكثر في مجال المعلومات بغرض إلحاق الضرر بنظم المعلومات و العمليات و الأنظمة التحتية و غيرها من الهياكل، و إضعاف النظم السياسية و الاقتصادية و الاجتماعية، و إحداث الضرر النفسي للسكان بهدف زعزعة استقرار الدولة والمجتمع، وكذا إلزام الدولة على اتخاذ قرارات لفائدة الكيان المعارض". (hark, 2021)

يُعدُّ المفهوم الروسي لأمن المعلومات هو امتلاك روسيا لبرامج ووكالات خاصة في مراقبة الاتصالات و الشبكات و مختلف وسائل الإعلام، بالتالي الحكومة الروسية تسيطر على كل شيء داخل روسيا . إضافة لذلك روسيا لا تمتلك عقيدة واضحة للأمن السيبراني، حيث تعمل على مواجهة التهديدات القادمة من الفضاء السيبراني بهدف حماية أمنها القومي . ففي نظرهم أن موسكو تُشنُّ صراعاً وجوديًّا مستمرًّا مع قوى داخلية و أخرى خارجية تسعى إلى تهديد أمنها في عالم المعلومات، فهم يرون أن الفضاء الإلكتروني عبارة عن تهديد وفرص يمكن استخدامها بصورة إيجابية لخدمة أهدافها القومية. (hark, 2021)

2-الوكالات الروسية المتخصصة في الأمن السيبراني:

تمتلك روسيا أربع وكالات رئيسة متخصصة في حروب المعلومات وهي : دائرة الحماية الاتحادية (FSO)، و جهاز الأمن الاتحادي (FSB) و جهاز الاستخبارات الخارجية (SVR)، و جهاز الاستخبارات العسكرية (GRU)، كل هذه المنظمات سابقة الذكر وباستثناء جهاز الاستخبارات العسكري GRU هي نتيجة تفكك جهاز الاستخبارات السوفيتي أو ما كان يعرف بالـ KGB و تخضع وكالات FSO و FSBو SVR للرئيس . بينما تُعدُّ وحدة GRU جزءًا تابعًا لوزارة الدفاع باعتبارها هيئة الاستخبارات العسكرية الأساسية و المركزية لهيئة الأركان العامة . **(hark, 2021)**

و يتخصص كل جهاز من الأجهزة السالفة الذكر بمهام معينة و التي يمكن تصنيفها في الأتي :

أ-دائرة الحماية الاتحادية (FSO) (service federal de securité): و هي الجهاز الذي يضمن الأمن الإلكتروني للموظفين الحكوميين و قيادات الدولة، و تتركز مهمتها في القيام بالدفاع عن الشبكات الحكومية ،إذ تُعدُّ مختصة بالعمليات الهجومية.

DOI: https://doi.org/10.61856/4eg54316

ب-جهاز الأمن الاتحادي (FSB) (federal security services of the Russian federation): و هو الجهاز الذي توكل له مسؤولية عن الأمن الداخلي للدولة، و جميع الاتصالات التي تُجرى عبر متعاملي الاتصالات الروسية، تُحوَّلُ إلى جهاز الأمن الاتحادي FSB و هو ما يبرز سيطرة الدولة الروسية على أنظمة الاتصالات ومراقبة حدودها.

أنشأت روسيا جيش يسمى المتصدين يسمى (fancy bear) تابعًا لوكالة الأمن الاتحادي الروسي يتكون من آلاف الموظفين، يخصص له كل سنة حوالي 300 مليون دولار من الميزانية الخاصة بالدفاع الروسية . و يُعدُّ خامس أقوى جيوش العالم الإلكترونية بعد كل من الولايات المتحدة الأمريكية، الصين، بريطانيا و كوريا الشمالية على التوالي، تتركز مهامه في الأتي : (rokoli & ahlem, 2022, p. 140)

-يقوم بالتجسس على الخصوم.

- القيام بهجمات إلكترونية تسبب الضرر بالبنى التحتية والاقتصادية و كذا المواقع الإلكترونية في الدول المعادية.

- القيام بحروب معلوماتية في وسائل الإعلام وعن طريق الشبكات الاجتماعية و ذلك باختراق الحسابات و البريد الإلكتروني و فتح حسابات مزيفة على شبكة المعلومات الدولية، و إنشاء الآلاف من الحسابات الوهمية على مواقع التواصل الاجتماعي للإجابة على الآلاف من التعليقات و المقالات و ترويج الشائعات و إخفاء الحقائق بهدف دعم الموقف الروسي و توجيه الرأي العام ضد خصوم روسيا.

ج-جهاز الاستخبارات الخارجية (SVR) (forign intelligence service) : هو عبارة عن جهاز الاستخبارات الخارجية الرئيسي في روسيا، و هو الجهاز المسؤول عن جمع الاستخبارات الأجنبية باستعمال الطرق البشرية و الإشارات الإلكترونية و السيبرانية و يشارُ إلى قراصنة الاستخبارات الخارجية الروسية أحيانا باسم APT 29 أو Cozy Bear أو The Dukes، و هذا الجهاز تابع للرئيس، و هو المكلف بتوفير المعلومات الاستخباراتية و العمليات و القيام بعمليات التحليل نيابة عن الرئيس الروسي و عن الجمعية الاتحادية للاتحاد الروسي و كذا الحكومة . كما تقوم بتنفيذ استخبارات الإشارات الاسترتيجية و تشغيل أنظمة الأقمار الصناعية التجارية و العسكرية و الاتصالات الثابتة و اللاسلكية.(hark, 2021)

د-جهاز الاستخبارات العسكري (main derectorat of the general staff of the armed forces of the Russian federation) GRU: و تسمى أيضًا المديرية الرئيسة لهيئة الأركان العامة، و هو نظام استخبارات يستعمل بشكل كلي جميع قوى، ووسائل الاستخبارات تقريبا، على أساس أنها تقوم بالعديد من الأنشطة الاستخباراتية، كما هذا الجهاز يشرف على العديد من معاهد البحث التي تقوم بتطوير أدوات القرصنة و البرامج الخبيثة، وفي اغلب الأحيان تنسب الولايات المتحدة الأمريكية أن الجهة المسؤلة عن الهجمات السيبرانيية التي تتعرض لها إلى جهاز الاستخبارات الروسي GRU. (shriti & hatem, 2023, p. 97)

و تُعدُّ هذه الأجهزة الأربعة مراكز أمن المعلومات في روسيا، كما تتميز هذه الأجهزة باحترافية كبيرة، و قد ظهر ذلك في عدة حروب منها الحرب السيبرانية الروسية على استونيا ،و جورجيا، وأوكرانيا، و التأثير على الانتخابات الأمريكية في سنة 2016 و غيرها . كما تُعدُّ روسيا من أوائل الدول التي تُزامن بين الحرب التقليدية و الحرب السيبرانية، و قد قامت بذلك في جورجيا سنة 2008 و أوكرانيا . و هذا يدل على أن صناع القرار في روسيا يعلمون جيداً حجم المكاسب التي يمكن أن تحققها الدولة من خلال استغلال الفضاء السيبراني. (hark, 2021)

3-الأدوات التي تعتمد عليها روسيا في الحرب الإلكترونية:

تستخدم روسيا في حروب المعلوماتية حسب دراسة قام بها ديفيد سميث David j.Smith بأنّ الاستخبارات تستخدم، التجسس المضاد، والخديعة ،و التضليل ،و القيام بتدمير الاتصالات و الأنظمة التي تدعم الملاحة ،و الضغوط النفسية، والدعاية، و تخريب نظم المعلومات.(rokoli & ahlem, 2022, p. 140)

هذا، و الحرب المعلوماتية الروسية تعتمد على أداتين رئيستين :

أولاً:التضليل المعلوماتي : تعتمد روسيا على توظيف الوسائل الإعلامية و الدعائية المتنوعة بهدف خلق روايات مضللة للآخرين و مشوهة للحقائق، و ذلك لخدمة مصالحها على حساب الأطراف الغربية، و يبرز هذا الأسلوب في تعامل وسائل الإعلام الروسية مع الوقائع و الأحداث السياسية التي شنتها الدول الغربية. (bessyouni, 2017)

ثانيًا:القرصنة الإلكترونية : يُعدُّ الهجوم على البنية التحية للدول الأخرى جزءًا جد مهم من إستراتيجية حرب المعلومات الروسية . على اعتبار انه آلية للحد من فعاليات الخصم، و تشتيت انتباهه وتضليله، بالإضافة لذلك فاعلية عمليات القرصنة

DOI: https://doi.org/10.61856/4eg54316

في تفريق نظام القيادة لدى الدول المتعارضة مع روسيا، والسيطرة عليها و لو لفترة محدودة من الزمن. (bessyouni, 2017)

خلال الفترة التي كانت فيها الدول الغربية تتهم روسيا بالتورط في القيام بعمليات القرصنة الإلكترونية، كانت روسيا تسعى لصياغة نموذج حديث من العلاقات، يسمى تيم مور Time Maurer يُوظّف فيه وكلاء سيبرانيين Cyber Proscy Actors، ينتمون لمنظمات و مجموعات متخصصة بالقرصنة أهمها APT 29/APT 28 و هو ما يسمح لروسيا بتحقيق مصالحها، والتنصل من الاتهامات الغربية الموجهة لها. (rokoli & ahlem, 2022)

و تهدف روسيا من خلال حرب المعلومات إلى ما يأتي:

1- زعزعة قدرة الخصم و إضعافه على المواجهة بالاعتماد على عمليات القرصنة.

2- تضليل القوى المناهضة بنشر معلومات و حقائق مغلوطة حول العدو، و خلق صورة إيجابية حول حلفائها.

3- السعي لإثارة مشاكل داخلية في الدول المناهضة لروسيا .

4- جاءت كرد لمواجهة العقوبات التي فرضتها الدول الأوروبية على روسيا سنة 2014، و التي تتمثل في حظر التأشيرات، و تجميد الأصول، و فرض قيود صارمة تجارية و اقتصادية . و ذلك ردًّا على تدخل روسيا في أوكرانيا 2014 . و القيام بضم شبه جزيرة القرم إليها بعد الاستفتاء الذي قامت به في شهر مارس من العام نفسه. (rokoli & ahlem, 2022, p. 141)

4-آليات الحرب السيبرانية الروسية الأوكرانية:

أ-الاختراق و خلق الفوضى في أوكرانيا:

كانت البداية باحتجاجات الميدان الأوروبي في كييف 2013 للمطالبة بانضمام أوكرانيا إلى الاتحاد الأوروبي بعد ما عُلِّقَت حكومة الرئيس فيكتور يانوكوفيتش (و هو الرئيس الرابع لأوكرانيا من سنة 2010 حتى عزله عام 2014)، و تَمّت المصادقة على اتفاقية الشراكة مع الاتحاد الأوروبي، و ازدادت وتيرة الاحتجاجات مع بداية 2014 و نتج عنها مقتل العديد من المحتجين و القوى الحكومية، اشتدت الاشتباكات بين قوات الأمن و المحتجين من 20 فبراير، و في ظل تلك الظروف المتوترة صوت مجلس النواب الأوكراني على إقالة الرئيس يانوكوفيتش في 22 فبراير. (mohamed, 2021)

و بعد الثورة الأوكرانية سنة 2014 التي أطاحت بالرئيس فيكتور يانوكوفيتش و حكومته، قام محتجون، ينتمي معظمهم للقومية الروسية، بالإعتراض على الأحداث الواقعة في كييف وطالبوا بمزيد من التكامل مع روسيا، بالإضافة إلى ذلك المطالبة بحكم ذاتي موسع أو استقلال شبه جزيرة القرم عن أوكرانيا . على الجانب الأخر تظاهرة مجموعة أخرى لتأييد الثورة، و في الأول مارس من العام نفسه، وافق جميع أعضاء مجلس الاتحاد الروسي على طلب الرئيس الروسي فلاديمير بوتين تدخل القوات الروسية في أوكرانيا . و في الثاني من مارس استدعى مجلس الأمن القومي الأوكراني جميع قوات الاحتياط المسلحة، وتصاعدت موجة التوتر في القرم بين الأطراف المساندة لروسيا و المساندة لأوكرانيا. (mohemed asyed, 2022)

لم يرق هذا التغيير في كييف للعديد من السكان في مناطق الجنوب و شرق البلاد و في يوم 23 شباط أُلغيَ قانون اللغة للأقليات (و الذي يشمل الروسية) و إعلان اللغة الأوكرانية لغة رسميةً و حيدة للبلاد، باعتبارها جزءًا من نتائج الثورة الأوكرانية، فجاء هذا القرار ليزيد من حدة التوترات في تلك الأقاليم المستاءة أصلا من التغيرات التي تحدث في عاصمتهم، و قد رأت تلك الأقاليم و بالخصوص في شبه جزيرة القرم أن قرار إلغاء قانون اللغات هو دليل على أن المحتجين في كييف يتبعون أجندة معادية لروسيا، و يتبنون توجه عنصري. (mohemed asyed, 2022)

و في الثاني عشر من مارس أجري استفتاء في شبه جزيرة القرم للانفصال عن أوكرانيا و الانضمام لروسيا، و جاءت نتائج الاستفتاء تأييدا لانضمام لروسيا بنسبة 95 % و قد استعملت روسيا عدة آليات لتحقيق أهدافها في تلك الأزمة من خلال استغلال الفضاء الإلكتروني انطلاقًا من محاولة التأثير على الرأي العام الروسي و صولاً إلى بلوغ مرحلة اختراق الانتخابات الأوكرانية. (mohamed, 2021)

ب-التأثير في الرأي العام الروسي و الأوكراني:

DOI: https://doi.org/10.61856/4eg54316

سبقت العمليات العسكرية الروسية في شبه جزيرة القرم حملة معلومة واسعة، وقد ركزت هذه الحملة بشكل أساسي على الرأي العام الروسي في الداخل، و استهدفت بشكل ثانوي السكان المقيمين في شبه جزيرة القرم . وقد حافظت وسائل الإعلام الروسية على بعض التقارير الإعلامية للأحداث في شبه جزيرة القرم و الرأي العام الروسي الذي يتابعها، مع تفاقم حدة تلاعب روسيا بالمعلومات التي كانت موجهة إلى المواطنين الروس، محذرة إياهم من خطر بناء روابط وثيقة مع الاتحاد الأوروبي EU. (mohamed, 2021)

و في تلك الفترة، شاهد أغلبية الشعب في شرق أوكرانيا و شبه جزيرة القرم التلفزيون الروسي، حيث حصلت الأغلبية الساحقة من الشعب الروسي على أخبارهم من وسائل الإعلام المتلفزة ووسائل التواصل الاجتماعي، و قد أغلقت القوات الروسية تسع محطات تلفزيونية أوكرانية في التاسع من مارس متيحة الوصول إلى القنوات الروسية فقط . وأصبح بالإمكان الوصول إلى القنوات من أوكرانيا عن طريق أجهزة استقبال الأقمار الاصطناعية. (hani, 2025)

و عندما سقطت حكومة يانوكوفيتش في بداية عام 2014 أصبحت التصريحات الروسية بخصوص الأحداث في أوكرانيا أكثر حدة، وقد ركزت حملة المعلومات الروسية على ثلاثة أهداف أساسية : (mohamed, 2021)

أولاً: القيام بتشويه سمعة الحكومة الجديدة في أوكرانيا.

ثانيًا : التأكيد على جسامة الخطر المحدق بالروس في أوكرانيا.

ثالثًا: ضمان الدعم الواسع لعودة شبه جزيرة القرم للعيش في سلام في كنف الوطن الأم روسيا.

بالإضافة إلى ذلك فقد أدت حملة تعبئة الشعب في شبه جزيرة القرم لمكافحة حركة الميدان دورًا مهمًا في اتصالات روسيا الإستراتيجية، و انطلقت هذه الحملة من سكان شبه جزيرة القرم الذين يتحدّثونَ اللغة الروسية، على الرغم من زعم بعضهم أن الحكومة الروسية هي من كانت وراءها.

كان التأثير في الرأي العام بارزًا في الحرب الروسية الأوكرانية، أثناء الغزو الروسي لأوكرانيا في الرابع و العشرين من فبراير 2022، من خلال بث الذعر و الأخبار الكاذبة حول السيطرة الكلية لروسيا على كييف و نجاح العمليات البرية و سقوط العديد من الطائرات الأوكرانية، مما يؤثر في الخصم و يتسبب في إضعافه و العمل على هزيمته نفسيًا. (alyazeed, 2024)

ج- نشر معلومات مضللة و مغلوطة

استغلت موسكو بفعالية وسائل التواصل الاجتماعي لحشد دعم داخلي و نشر كميات كبيرة وهائلة من المعلومات المضللة حول احتجاجات الميدان و توجهات الحكومة الجديدة في كييف .و قد كشف تحليل العمليات عن العديد من المعلومات عن روسيا، في الصراع الأوكراني، و قد ركزت حملتها الدعائية على خمسة عناصر هي: (kofman & katya, 2017, pp. (28,29))

- التأثير الكبير و الطويل الأمد (إعادة المواضيع نفسها مرارًا و تكرارًا) .

- نشر المعلومات المرغوب بها (التلاعب في نشر الرسائل لاستغلال مخاوف الروس في أوكرانيا).

- العمل على التحريك العاطفي (استخدام مواضيع تحرك مشاعر الروس العرقيين و يتصرفون بدافع غضب غير عقلاني).

- الوضوح(القيام بعرض الصراع الأوكراني بعبارة و مصطلحات بسيطة من الخير و الشر).

-الجلاء المفترض (مطابقة كل الرسائل الدعائية مع الخرافات و الأساطير الروسية التي يُصدَّقُ في أوساط الشعب على نطاق واسع).

و قد ساعدت جميع وسائل الإعلام الروسية المرئية و الإلكترونية في ضمان الموافقة الداخلية و تسريع عملية الانتقال من صراع مربك إلى استيلاء على أراض مقبولة من الناحية السياسية . و قد استخدم بوتين تلك الوسائل بهدف تحقيق تأثير كبير في استعراض الحجج التاريخية و العاطفية عن كيفية انتماء شبه جزيرة القرم إلى روسيا في خطاب له بتاريخ 18 مارس 2014. (rokoli & ahlem, 2022)

DOI: https://doi.org/10.61856/4eg54316

و قد ركزت الحملة المعلوماتية الروسية على جمهورها الداخلي أكثر من تركيزها على الرأي العام الأوكراني داخل شبه جزيرة القرم و خارجها . و هذا بالنظر إلى قرب شبه جزيرة القرم من روسيا فقد كانت هذه المقاربة كافية و فعالة و يمكن إعادة تجسيدها في أماكن أخرى في جميع حدود روسيا.(kofman & katya, 2017, p. 30)

د- الاختراق و قطع الخدمة و التلاعب في البيانات و في الانتخابات الأوكرانية

شنّت روسيا العديد من حملات المعلومات على شرق أوكرانيا، بالإضافة إلى هجمات إلكترونية بين الحين و الأخر، و حتى قبل الإطاحة بالرئيس يانوكوفيتش، عانى الميدان الأوروبي في خاركيف الذي كان له الدور الأساسي في تنظيم المنتدى الأوكراني للميادين الأوروبية العام الأول، عانى من هجوم قطع موزع الخدمة الرئيسي Denial of service (D DOS) Distributed في فبراير، و بعد تنحية بيانوكوفيتش، استهدفت عمليات القطع الموزع للخدمة المواقع الإلكترونية المرتبطة بالحكومة، ولم تكن الهجمات الأولية بهدف التعطيل إلى حد كبير، ولكن القراصنة الإلكترونيين استطاعوا في أكتوبر 2014 من تعطيل النظام الإلكتروني الخاص بجمع نتائج الانتخابات، واختراق كل الحواسيب المسجل عليها بيانات التصويت و الاقتراع، في محاولة للتلاعب بالنتائج و إثارة الفوضى، مما اضطرهم إلى القيام بفرز الأصوات يدويا، وتسبب ذلك في تأخير إعلان النتائج . (mohamed, 2021)

و قد رُكِّزَ أيضًا على وسائل التواصل الاجتماعي و أصبحت محط تركيز حملة المعلومات، و بما أن منصتي وسائل التواصل الاجتماعي " كونتاكنتي و ادنوكلاسنيكي" الأكثر شعبية في أوكرانيا كانتا تُستضافان من خوادم روسية، إلا أن السلطات الروسية قادرة على حجب هذه الصفحات الموالية للميدان و إرغام مزودي الخدمات على تشارك معلومات شخصية خاصة الذين نقروا "إعجاب " LIKE لها. (hani, 2025)

ومع زيادة حدة التصعيد و العنف على الأرض أصبحت كونتاكنتي و أدنوكلاسنيكي أداة تساعد في طلب المساهمات و التجنيد في روسيا لمجموعة مثل " مكافحة الميدان Anti Maidan"، و " ميليشيا دونباس الشعبية " Donabas peopl's Millita و " صندوق مساعدة نوفوروسيا " Fund to Help Nouvorossiya . العنصر المهم في حملة المعلومات الروسية يتمثل في إعادة إحياء مصطلح نوفوروسيا (روسيا الجديدة) . و ذكر بوتين هذا المصطلح في خطاب ألقاه في 17 أبريل 2014 ذاكرًا فيه أن شرق أوكرانيا وجنوبها بما في ذلك المناطق الناطقة بالروسية بشكل أساسي – كانت تاريخيًا جزءًا من الإمبراطورية الروسية . وقد كان تفسير بوتين لمفهوم تاريخ نوفوروسيا يخدمه ذاتيا. (mohamed, 2021)

رابعًا-نتائج استخدام روسيا للحرب السيبرانية على أوكرانيا:

استطاعت روسيا من خلال الحرب السيبرانية من تحقيق أهداف تكتيكية مكنتها من الوصول إلى أهداف إستراتيجية و هي :

أ-التأثير في الرأي العام الأوكراني و إضعاف الروح المعنوية للسكان

سعت الهجومات السيبرانية الروسية على أوكرانيا إلى تقويض الثقة في كييف و إحداث الشعور بنقص سيطرة الدولة، ما يؤدي إلى تأليب المواطنين الأوكرانيين على دولتهم، و ذلك لفشلها في حماية المجتمع، و من ثم يتم يُزَعزع استقرار الحكومة و يؤدي إلى انهيارها ما يتيح لروسيا السيطرة على كييف أو الضغط لتقديم تنازلات. (ali, 2024)

ب-استهدفت الهجومات السيبرانية الروسية على أوكرانيا ضرب البنى التحتية و نتج عنها خسائر اقتصادية فادحة .

استخدام العمليات السيبرانية قد ينتج عنها خسائر اقتصادية كبيرة، عندما تستهدف البنى التحتية الرئيسة في الدولة مثل ضرب شركات الطاقة الكهربائية في أوكرانيا سنة 2015 من قبل روسيا فقد تسبب في حرمان أكثر من ربع مليون أوكرانيًا من الكهرباء في المنطقة الغربية ،و أدى إلى خسائر فادحة أضرت بالبلاد ،كما استهدفت عملية سيبرانية أخرى في العام التالي البنوك و مؤسسات النقل و الخدمات العامة الأوكرانية، هذه العمليات من شانها أن تؤثر في قوة الاستثمارات لعدم الاستقرار في البلاد و بالتالي هز الثقة في الاقتصاد الأوكراني. (alyazeed, 2024)

ج-إضعاف الثقة في الحكومة الأوكرانية من خلال اختراق شبكة اتصالات الأقمار الصناعية و الاتصالات العسكرية الأوكرانية و تعطيلهما.

تكررت العمليات السيبرانية الروسية ضد أوكرانيا، و من ذلك معاودة الهجوم على الشركة الكهربائية سنة 2016، و استهداف قراصنة روس القوات الصاروخية و المدفعية الأوكرانية ما أدى إلى دمار 80 % من قوات الهاوتزر الأوكرانية D.30. بالإضافة إلى حدوث أكبر عملية اختراق في أوكرانيا تسمى هجوم(whisper gate) في بداية العمليات العسكرية في 24 فبراير 2022. (alyazeed, 2024)

DOI: https://doi.org/10.61856/4eg54316

النتائج ومناقشتها:

أولاً:نتائج الدراسة

بعد دراسة التجربة الروسية في الحرب السيبرانية المتمثلة في الحرب الأوكرانية توصّل البحث إلى النتائج الآتية:

- الحروب الحديثة أصبحت تدار عبر الفضاء السيبراني و يمكن أن تؤدي إلى نتائج سريعة دون خسائر كبيرة.

- تنتج من الحروب الإلكترونية مخاطر كثيرة مهددة للأمن القومي فتداعيتها العسكرية و الاقتصادية و الاجتماعية و الثقافية و حتى النفسية تؤثر في استقرار الدولة و المجتمع كما هو الحال في أوكرانيا وقبل ذلك جزيرة القرم التي كانت تابعة لأوكرانيا.

- الحروب السيبرانية لن تتوقف، خاصة مع امتلاك الدول العظمى للتكنولوجية و التي تُمثِّل الوسيلة الوحيدة لتحقيق أهداف إستراتيجية دون تكبد خسائر.

- ظهور نوع جديد من التهديدات، و هو ما فرض على الدول تبني استراتيجيات دفاعية خاصة في ظل امتلاك لبعضهم القدرة الهجومية في المجال الإلكتروني . و بناءًا على ذلك فإنَّ الفضاء السيبراني في العصر الحالي أصبح المجال الذي يساعد الدول على تحقيق مصالحها القومية في مختلف المجالات، وبالتالي أي هجوم على أي قطاع يؤدي إلى عدم توازن استراتيجي و بالتالي إمكانية حدوث حرب سيبرانية.

- أصبح الفضاء السيبراني ساحة جديدة للصراع، و ذلك من خلال استخدامه في أعمال تدميرية و تخريبية، كتخريب أنظمة المعلومات و الشبكات الذي يهدد أمن الدول.

- أظهرت حرب روسيا على أوكرانيا أن الكلمة و الصورة والأرقام يمكن أن تكون سلاحًا فعالاً يدعم المعارك التي تجري على الأرض، و لها تأثير في البنية الذهنية و النفسية للمدني و العسكري.

- الحرب الأوكرانية أظهرت لنا أن مفهوم حرب المعلومات يتنامى و يتعقد و يوظف بطريقة غير مسبوقة هذا المفهوم قد يكون هجوميًا أو دفاعيًا، و تندرج تحته الحرب الإلكترونية، وحرب القيادة و السيطرة، وحرب قرصنة المعلومات، و حرب العمليات النفسية و حرب المعلومات الاقتصادية، وهكذا أصبحت حروب المعلومات متعددة المستويات و الأهداف و الأدوات و المجالات، و تخضع لاستراتيجيات الحرب.

- هناك عدة أسباب يمكن أن تفسر بشكل ممكن و أقرب للمنطق سبب قلة العمليات الإلكترونية في الصراع الروسي الأوكراني الأخير بعكس التوقعات، ربما لأن الأوكرانيين قاموا بعمل جيد في تقوية دفاعاتهم الرقمية لمستوى جيد من القوة بمساعدة حلفائهم الأمريكيين و الأوروبيين، و من جهة أخرى قد تُعدُّ الصواريخ أدوات أسرع و أكثر فاعلية لتحقيق الأهداف الإستراتيجية.

ثانيًا-مناقشة النتائج

ساهم الأمن السيبراني في بروز فاعلين جدد بالنظام الدولي، وعزز من دور القوى العظمى و زودها بأدوات حديثة لتحقيق أهدافها و خلق تحديات جديدة أمام دول أخرى.

-القوة السيبرانية أصبحت ساحة لتغلب القوى العظمى و بديل للقوة التقليدية، في ظل غياب الإنذار المبكر للصراعات السيبرانية

-أصبح السباق نحو التسلح السيبراني أشبه بحرب الكل ضد الكل، فالجميع يتسلح ليحمي نفسه، و الكل ضد التهديدات السيبرانية و مخاطرها.

خاتمة

DOI: https://doi.org/10.61856/4eg54316

في ختام الدراسة يتضح جليًا أن الحرب السيبرانية الروسية الأوكرانية لم تكن مواجهة في فضاء رقمي عابر، بل تُعدُّ نموذجا متطورًا من الحروب الحديثة، فقد كشفت هذه التجربة أن الفضاء السيبراني أصبح ساحة إستراتيجية لا تقل خطورة عن الحرب التقليدية، حيث يمكن من خلاله إضعاف القوة الاقتصادية و السياسية و العسكرية للدول محل الاستهداف، كما أوضحت الدراسة أن الاعتماد المتنامي على التكنولوجيات الحديثة و البنى التحتية يجعل من الدول أكثر عرضة لخطر الاختراقات و الهجمات التدميرية. ومن خلال ذلك نقول إنَّ الحرب الروسية الأوكرانية فتحت آفاقًا جديدة لبحث و دراسة أمن المعلومات و السيادة الرقمية، الأمر الذي يُحتّم على الدول ضرورة تحديث استراتيجيات دفاعية وهجومية معتدلة، و توسيع نطاق التعاون الدولي للتصدي لهذا النمط من الصراعات.

References

Arabic References

Ali, A. A. (2024). *Taktikat mutabaddila: Hudud taʾthir al-ʿamaliyyat al-saybiraniyya fi al-ḥarb al-rusiyya al-ukraniyya*. Al-Mustaqbal lil-Abḥāth wa al-Dirāsāt al-Mutaqaddima. Retrieved August 24, 2025, from https://futureuae.com

Almoqarani, A. B. (2022). *Ḥurub al-maʿlumat fi al-azma al-ukraniyya*. Al-Maʿhad al-Duwali lil-Dirāsāt al-Iraniyya (Rasanah). Retrieved November 24, 2024, from https://rasanah-iiis.org

Alyazeed, A. A. (2024). *Al-ʿamaliyyat al-saybiraniyya bayna Rusia wa Ukraine: Qirāʾa fi al-asbāb wa al-natāʾij*. Al-Markaz al-Dimuqrati al-ʿArabi. Retrieved July 25, 2025, from https://democraticac.de

Araj, H. N. (2022). *Naẓariyyat al-waqāʿiyya al-bunyawiyya fi al-dirāsāt al-amniyya: Dirāsa li-ḥālat al-ghazw al-amriki lil-ʿIrāq 2003*. Al-Markaz al-Dimuqrati al-ʿArabi. Retrieved August 29, 2025, from https://democraticac.de

Bessyouni, M. (2017). *ʿAqidat Gerasimov: Al-dawāfiʿ al-istirātijiyya al-rusiyya li-ḥarb al-maʿlumat didda al-duwal al-gharbiyya*. Markaz al-Mustaqbal lil-Abḥāth wa al-Dirāsāt al-Mutaqaddima. Retrieved August 29, 2025, from https://futureuae.com

Bouzaida, J. (2019). Al-istirātijiyya al-jazāʾiriyya fi muwājahat al-jarāʾim al-saybiraniyya: Al-taḥaddiyāt wa al-āfāq al-mustaqbaliyya. *Majallat al-ʿUlūm al-Qānūniyya wa al-Siyāsiyya*, 10(1), 1262–1293.

Hani, N. (2025). *Tawẓif al-tahdīdāt al-saybiraniyya fi al-ḥarb al-rusiyya al-ukraniyya*. Markaz Raʾā lil-Dirāsāt al-Istirātijiyya. Retrieved July 30, 2025, from https://rcssegypt.com

Hark, F. (2021). Al-faḍāʾ al-saybirani wa al-taḥawwul fi shakl al-ḥurūb: Dirāsat ḥālat Rusia. In *Al-Muʾtamar al-Duwali al-Iftirāḍi al-Awwal lil-Amn al-Saybirani fi al-Alfiyya al-Thālitha* (p. 13).

Kofman, M., & Katya, M. (2017). *Cyber operations by Russia in Crimea and Eastern Ukraine*. Arroyo Center, RAND Corporation.

Lachan, T. (2024). Al-ḥarb al-hajīna: Jabhat ḥurūb Rusia al-khafiyya didda al-gharb. *Deutsche Welle*. Retrieved July 30, 2025, from https://www.dw.com

DOI: https://doi.org/10.61856/4eg54316

Mahmoud, K. W. (2013). Al-hajamāt ʿabr al-internet: Saḥat al-ṣirāʿ al-iliktruni al-jadid. *Al-Markaz al-ʿArabi lil-Abḥāth wa Dirāsāt al-Siyāsāt*, (5), 116.

Mohamed, A. E. (2021). Istikhdām Rusia lil-quwwa al-saybiraniyya fi idārat tafāʿulātihā al-duwaliyya. *Dirāsāt*, 2(2).

Mohemed Asyed, M. A. (2022). *Tadaʿiyyāt al-azma al-ukraniyya ʿalā al-ʿalāqāt al-rusiyya al-gharbiyya (February 2014–April 2022)*. Al-Markaz al-Dimuqrati al-ʿArabi. Retrieved August 29, 2025, from https://democraticac.de

Mohi, A. (2022). *Al-Wafd*. Retrieved September 24, 2024, from https://www.alwafd.news

Odeh, N. (2022). Al-ʿamaliyyat al-saybiraniyya fi al-ḥarb al-rusiyya al-ukraniyya: Ṭabīʿatuhā wa anmāṭuhā – taḥlīl. *Al-Sharq Strategic Research*, 34.

Rokoli, K., & Ahlem, G. (2022). Al-ḥarb al-iliktruniyya bayna al-wilāyāt al-muttaḥida al-amrīkiyya wa Rusia. *Majallat Acadimiya lil-ʿUlūm al-Siyāsiyya*, 6(2).

Samir, B. (2017). *Al-amn al-saybirani (Cybersecurity) fi al-Jazāʾir: Al-siyāsāt wa al-muʾassasāt*. *Al-Majalla al-Jazāʾiriyya lil-Amn al-Insāni*, (4).

Sehel, A. A. (2023). Al-ṣirāʿ fi al-ʿaṣr al-raqami: Min al-akhbār al-zāʾifa ilā ḥurūb al-jīl al-khāmis – muqāraba mafāhīmiyya. *Miṣdāqiyya*, 5(2), 1–16.

Shriti, O., & Hatem, B. A. (2023). Al-istirātijiyya al-rusiyya fi al-ḥarb al-saybiraniyya: Qirāʾa fi namūdhaj al-ṣirāʿ al-saybirani maʿa baʿḍ al-duwal. *Majallat al-Bayān lil-Dirāsāt al-Qānūniyya*, 8(2), 90–102.

Zuriga, I. (2019). Al-faḍāʾ al-saybirani fi mafāhīm al-quwwa. *Majallat al-ʿUlūm al-Qānūniyya wa al-Siyāsiyya*, 10(1), 1017.

English References

Fortinet. (D.T.). *What is cybersecurity?* Retrieved from https://www.fortinet.com

Przetacznik, J., & Simona, T. (2022). *Russia's war on Ukraine: Timeline of cyber-attacks*. European Parliamentary Research Service.

Schiliro, F. (2022). *Toward a contemporary definition of cybersecurity*. Australian Defence Force Academy.