

أثر التهديدات السيبرانية على الأمن الوطني:
دراسة على ضوء الحرب الروسية الأوكرانية

**The Effect of Cyber Threats on National Security:
An Examination the Lens of the Russo-Ukrainian
War**

بن فليس نجود*، جامعة بسكرة
Noudjoud.benflis@univ-biskra.dz

تاريخ الاستلام: 2025/04/15 تاريخ القبول: 2025/05/27
ملخص:

استهدفت الدراسة تحليل أثر التهديدات السيبرانية على أمن الدول خاصة وأنها تندرج ضمن التهديدات الجديدة العابرة للحدود، وذلك بالتركيز على الحرب الروسية الأوكرانية التي قدمت مشهدا متعدد الجوانب لتحليل الأبعاد السيبرانية للحرب المعاصرة وارتداداتها داخليا وخارجيا، والتعرف على الأدوات السيبرانية المستخدمة في نطاق هاته الحرب. وبغية تحقيق هدف الدراسة فقد اعتمدت على المنهج الوصفي التحليلي من خلال الوصف الدقيق والمعمق لطبيعة التهديدات السيبرانية والتعرف على مخرجاتها على الأمن الوطني، وكذا الاستعانة بمنهج دراسة الحالة باستعراض الحرب الروسية الأوكرانية في بعدها السيبراني.

وقد توصلت الدراسة إلى أن الحرب الروسية الأوكرانية جسدت نموذجا للعمليات السيبرانية المعاصرة، ودفعت إلى إعادة النظر في الاستراتيجيات العالمية في المجالات التقنية بغية تطويرها ليس من منطلق التنافس التكنولوجي في العالم فقط وإنما حماية لمصالح جيوسياسية، كما ستشهد هاته الحرب تصعيدات مستقبلية نظرا لعدم تنازل أطرافها عن أجنداتها السيبرانية وامتداد التأثيرات لتشمل دول حلف الناتو والاتحاد الأوروبي.

*المؤلف المراسل

جويلية 2025

المجلة الجزائرية للأمن الإنساني

الكلمات المفتاحية: التهديدات السيبرانية – الأمن الوطني – الحرب الروسية الأوكرانية.

Abstract

The study aimed to analyze the impact of cyber threats on the national security of countries. It addressed the emerging cyber threats within the context of the Russian-Ukrainian war by focusing on analyzing the multi-faceted cyber aspects presented by the war, both internally and externally, and identifying the cyber tools used in the theater of war. The study aimed to achieve an accurate and in-depth description of the nature of cyber threats and to identify their repercussions on national security. It also sought to benefit from the case study of the Russian-Ukrainian war in understanding the nature of these threats in its aftermath.

The study concluded that the Russo-Ukrainian War exemplified a paradigm for contemporary cyber operations and necessitated a re-evaluation of global strategies in technological domains. This imperative for development arises not solely from the perspective of global technological competition but also from the need to safeguard geopolitical interests. Furthermore, this conflict is anticipated to undergo continued evolution.

Keywords: Cyber threats , National security, Russia-Ukraine war.

مقدمة:

إن بروز التهديدات الجديدة ضمن السياقات التحولية التي فرضتها متغيرات المرحلة الجديدة، أدى إلى إعادة صياغة نمط التفاعلات وكيفية التعاطي مع الطبيعة المعقدة والمتشابكة لهاته التهديدات ومخرجاتها التي تنعكس على مكونات النظام الدولي من القمة إلى القاعدة. وتصنف التهديدات السيبرانية كأساليب جديدة تهدد الأمن الوطني للدول، وتستخدم في سبيل تحقيق المصالح الإستراتيجية وتغيير التوازنات الدولية، فإلى جانب الآليات العسكرية المادية أصبحت بعض القوى تعمل على تعزيز قدراتها السيبرانية وتوظيفها لتحقيق معادلات ربحية، وهو ما أشار إليه الجنرال فاليري غيراسيموف "رئيس هيئة الأركان العامة الروسية" في مقال نشر في إحدى المجلات

مؤكدًا على تنامي الوسائل غير العسكرية لتحقيق الأهداف السياسية والإستراتيجية، ونجاحها في الاستخدام التقليدي للقوة" (Azharu) وتعتبر الحرب الروسية الأوكرانية أحد أكثر النماذج قدرة على تفسير الطبيعة الدينامكية والمرنة للتهديدات السيبرانية، والتأثيرات المحتملة لاستخدام القوة السيبرانية في سبيل تقويض دور وفعالية الطرف الآخر في الحرب من خلال ضرب البنية التحتية الرقمية، وتسخير ترسانة استخباراتية لخرق قواعد البيانات وزرع الفيروسات، بهدف شل جميع مؤسسات الدول (إداريا، صحيا، تعليميا، طاقويا).

إشكالية الدراسة:

نظرا للتأثيرات التي أحدثتها الهجمات السيبرانية المتبادلة بين الطرفين، بدرجات متفاوتة، وتباينات في مخرجاتها على العديد من الأصعدة سعت الدراسة لفهم وتحليل عميق لأثر هاته التهديدات، وانعكاساتها داخليا على طرقي الحرب، وامتداداتها الخارجية لتشمل دول حلف الناتو والاتحاد الأوروبي، وعليه. جاءت إشكالية الدراسة كالتالي:

كيف أثرت التهديدات السيبرانية على الأمن الوطني لأطراف الحرب الروسية الأوكرانية؟

فرضيات الدراسة:

وكمحاولة للإجابة عن السؤال المركزي المطروح تم وضع الفرضيتين التاليتين:

- 1- لعبت التهديدات السيبرانية دورا مهما في الحرب الروسية الأوكرانية من خلال إحداث ضرر بالغ ومتبادل في البنية التحتية الحيوية لكلا الطرفين.
- 2- بالرغم من الاستخدام المكثف للتهديدات السيبرانية، إلا أن تأثيرها في الأمن الوطني لطرفي الحرب الروسية الأوكرانية كان محدودا.

أهداف الدراسة:

❖ تحليل نمط التهديدات السيبرانية التي تعرض لها طرفي الحرب الروسية الأوكرانية أثناء فترة الصراع.

❖ التعرف على حدود التأثير المتبادل بين الطرفين، ومدى فعالية التقنيات المستخدمة في الدفاع والهجوم، والامتدادات الخارجية لبعض الفواعل كحلف الناتو والاتحاد الأوروبي.

المقاربة النظرية:

من أجل التحليل المعمق للموضوع تم الاعتماد على بعض المقاربات النظرية والمتمثلة في: مقارنة الدور، والمقاربة المؤسسية الجديدة. تمت الاسـتعانة بمقاربة الدور؛ من خلال إبراز دور الأطراف الفاعلة في الحرب السيبرانية الروسية الأوكرانية (الدولة الروسية، الأوكرانية، الدول والمنظمات الدولية الداعمة لأوكرانيا، مجموعات القرصنة التي تتبادل الهجمات، القطاع الخاص، الرأي العام) ومختلف التفاعلات التي حصلت بين هاته الفواعل، كمحاولة للتكيف مع مواجهة الهجمات والمعلومات المضللة. والمقاربة المؤسسية الجديدة؛ التي تركز على دور المؤسسات في تشكيل سلوك الجهات الفاعلة، وتؤثر على قدرة الدول على حفظ أمنها الوطني، وبالعودة إلى موضوع الدراسة فإننا قمنا بإبراز دور هاته المؤسسات كحلف الناتو والاتحاد الأوروبي والمنظمات الغير حكومية التي أدانت الهجوم الروسي، على مستوى دولي، والمؤسسات الداخلية لفواعل الحرب الرئيسية . ومن أجل فهم أبعاد الموضوع، والتعرف على التأثيرات التي أفرزتها رهانات المرحلة الجديدة كالقوة السيبرانية، وبالتركيز على الحرب الروسية الأوكرانية تمت هندسة الدراسة بالشكل التالي:

أولاً: التهديدات السيبرانية في مقابل التهديدات المادية: تأثيرات جديدة على أمن الدول.

ثانياً: الحرب الروسية الأوكرانية: توظيف الأدوات السيبرانية الروسية واستراتيجيات الدفاع الأوكراني.

ثالثاً: التأثيرات المحتملة للاختراقات السيبرانية ضمن الحرب الروسية الأوكرانية.

رابعاً: مآلات الحرب السيبرانية الروسية الأوكرانية

أولاً: التهديدات السيبرانية في مقابل التهديدات المادية: تأثيرات جديدة على أمن الدول

تعرف التهديدات السيبرانية كتهديدات جديدة ضمن السياق التحولي الذي أفرزته فترة ما بعد الحرب الباردة، ففي مقابل التهديدات المادية التي تعتمد على عنصر القوة العسكرية برزت لتضيف بعداً جديداً ومعقداً للأمن الوطني.

أبرز التهديدات السيبرانية كتهديدات جديدة عابرة حدودياً وتفاعلياً

لقد تم طرح مفهوم القوة الناعمة كأحد استراتيجيات التأثير التي تمكن الدولة من توسيع نطاقها الدولي من خلال أدوات غير قسرية كالثقافة مثلاً بدل القوة العسكرية أو الاقتصادية، وقد تطور هذا المفهوم الذي طرحه عالم السياسة الأمريكي "جوزيف ناي" بتقديم مفهوم القوة السيبرانية، الذي يعرفه بأنه "مجموعة من الموارد المرتبطة بإنشاء المعلومات الالكترونية والتحكم بها ونقلها، وتشمل البنية التحتية والشبكات والبرمجيات والخبرات البشرية"، وقد أحدثت القوة السيبرانية خللاً في التوازن الجيوسياسي بإعادة تعريف ديناميكيات القوة العالمية، ويشبه إميل كاتاروزا Amael cataruzza "رئيس اللجنة الوطنية الفرنسية للجغرافيا" هذا التحول بصدمة عميقة كالثورتين الصناعيتين في القرن التاسع عشر والعشرين، والذي أدى إلى إعادة توزيع القوة بين الجهات الفاعلة، والتي قد تشكل فواعل تنافس الدولة التقليدية، فعمالقة التكنولوجيا مثل جوجل وأمازون وفايسبوك وأبل وغيرها تتحدى التسلسلات الهرمية الاجتماعية الراسخة مما يساهم في تآكل النفوذ الحكومي (SIA, 2024)

وعند الحديث عن التهديدات السيبرانية فإنها أضافت بعداً جديداً سواء على مستوى التحليلات النظرية، أو الاستراتيجيات الدولية التي كانت تركز في السابق على الكيفيات التي يتم بها الحفاظ على الأمن الوطني ضمن حماية الحدود القومية، والتي تختلف عن التهديدات المادية سواء من حيث طبيعتها أو أهدافها، كما أن التهديدات السيبرانية فتحت المجال أمام فواعل جديدة، وهو ما يوضحه الجدول رقم-1-

الجدول رقم 1: يوضح الفروق الجوهرية بين التهديدات السيبرانية والمادية

التهديدات المادية	التهديدات السيبرانية	من حيث طبيعتها
صلبة/مرئية	مرنة/غير مرئية	القدرة على إثباتها
قوية: يمكن إثباتها بسبب عنصر المباشرة في الهجوم.	ضعيفة نظرا لعدم مرئيتها كالفيروسات الالكترونية	
دول/تحالفات	دول، أفراد(قراصنة)، جهات غير حكومية	طبيعة الفاعل
على حسب الإمكانيات المسخرة للهجوم.	سريعة وفعالة (عن بعد)	درجة التأثير
البنية التحتية الاقتصاد الأمن	البنية التحتية للدول، المعلومات، الأنظمة، الأفراد	الهدف

المصدر: من إعداد الباحثة.

بتغيير التهديدات السيبرانية لمفاهيم الحدود والسيادة في الأمن الوطني

بروز التهديدات السيبرانية غير من مفاهيم الحدود والسيادة، فقد تم تجاوز الحدود الجغرافية التي كان تأمينها مرادفا لتأمين الدولة، ومع حمايتها لا يمكن حماية الأفراد والمؤسسات داخلها، حيث يمكن تنفيذ أي هجوم دون الحاجة إلى عبورها، وهو ما يجعل الدولة عاجزة عن حماية نفسها بناء على منظور حماية الموقع الجغرافي، كما أنها ستفقد السيطرة على المجال الرقمي حال اعتمادها على المقاربة التقليدية في حماية الأمن الوطني، فالهجمات السيبرانية تنطلق من أي مكان في العالم متجاوزة الحدود الجغرافية والسياسية وهو ما يجعل من الصعب تحديد مصدر الهجوم، أو إيقافه عند الحدود الوطنية لدولة ما. إلى جانب بروز مفهوم السيادة الرقمية الذي يشير إلى قدرة الدولة على ممارسة سلطتها وحماية البنية التحتية الرقمية، أي فرض سيادتها على الفضاء الرقمي، والتي أصبحت أكثر عرضة للاختراق؛ حيث أن البنية التحتية للإنترنت غالبا ماتكون موزعة وعابرة للحدود وتعتمد على شركات لا تخضع للسيطرة الكاملة للدول.

وقد وسعت هاته التهديدات من المستويات التي يمكن أن تتأثر من خلال شن حرب سيبرانية أو هجومات تهدف لضرب الأمن الوطني لدولة ما، أو التي تنفذ

هاته العمليات، حيث يمكن أن يكون المشرف عليها عبارة عن أفراد أو حكومات أو جماعات إرهابية أو قراصنة أو منظمات إجرامية، في حين أن نطاق التأثير لا يشمل دولة بمفردها وإنما يتجاوز حدودها القومية ليحدث تأثيرات على مستوى الفضاء الإقليمي لها، وبالتالي أصبح من غير الممكن تعريف الأمن الوطني من خلال القضايا العسكرية والحدود الداخلية والخارجية، إلى جانب أن تحديد مرتكبيها أمر غير خاضع لضوابط محددة.

ج. منظورات بديلة لفهم طبيعة التهديدات السيبرانية

تجد المنظورات التقليدية نفسها أمام مسألة إعادة تكوين بعض المفاهيم، والانطلاق من مسلمات جديدة بناء على المتغيرات التي تحدثها تحولات ترتبط بفترات زمنية معينة، بالرغم من الاستعانة بفرضياتها والانطلاق من وحداتها التحليلية.

وينطلق منظور الردع السيبراني الذي تم تطبيقه على الفضاء الإلكتروني باعتباره ردعا إلكترونيا، والذي تم استيراده من مفاهيم الردع التي يتم استخدامها في الهجمات النووية في سبيل إسقاطه على المجال السيبراني، ليجد المفهوم قصورا واضحا من حيث القاعدة التطبيقية نظرا لاعتبار الفضاء السيبراني مرنا لا يمكن التعرف على الفواعل المنفذة للاعتداءات ضمنه مقارنة بالفضاءات المادية.

بينما تشرح نظرية تجنب تهديدات التكنولوجيا TTAT كيفية انخراط مستخدمي تكنولوجيا المعلومات في سلوكيات تجنبهم التهديدات السيبرانية، منطلقين من أن طريقة إدراك المستخدمين للتهديد تؤثر على دوافعهم لاستدعاء آلية حماية ضده، وقد اختبر ليانغ وشوي نظريتهما كنموذج لتفسير سلوك تجنب التهديدات التكنولوجية، مركزين على مفاهيم القابلية المتصورة للتأثر (الاعتقاد بتأثير التكنولوجيا الخبيثة على الأجهزة)، ومفهوم الشدة المتصورة (اعتقاد الفرد الشخصي بالضرر الذي قد تلحقه التكنولوجيا الخبيثة بأجهزته وأنظمتها) والتي تخلق تصورا حول حجم التهديدات، وبالتالي سهولة تطبيق إجراءات الحماية و اتخاذ سلوكيات تجنب هاته التهديدات (D.carpenter, 2019, p. 22)

ثانياً: الحرب الروسية الأوكرانية: توظيف الأدوات السيبرانية الروسية واستراتيجيات الدفاع الأوكراني

إن الحرب الروسية على أوكرانيا لم تكن أحادية البعد يمكن فهم معطياتها من خلال التركيز عليه، وإنما قدمت مقاربة معقدة تتحكم فيها العديد من الأبعاد، أهمها البعد السيبراني الذي يحمل مخرجات إستراتيجية وعملية متشابكة، فالاستعانة بمجموعة من الأدوات السيبرانية خلق معادلة صعبة تحمل في عمقها مفهوم الحرب الهجينة ضمن نطاق تقليدي عسكري وآخر معاصر تكنولوجي.

1-التوجه الروسي السيبراني في الحرب مع أوكرانيا: تصور التهديدات السيبرانية وتعزيز الأدوات الهجومية

أ-التصور الروسي للتهديدات السيبرانية وتحولها لعامل هجوم

إن التصور الروسي للتهديدات التي تواجهه منذ نهاية الحرب الباردة إلى اليوم تتبع من عدم الانفصال عن أمجاده السابقة، ورفضه للتواجد الأمريكي على رأس الزعامة العالمية، وسيطرة التفكير ضمن مفهوم "المعضلة الأمنية"، خاصة بعد خروجه من الحرب في حالة ضعف وتفكك، ومنذ ذلك الحين أصبح التصور الروسي مبنيًا على أن توسع الناتو والاتحاد الأوروبي تهديد سياسي واقتصادي وعسكري لأمن روسيا ومصالحها الوطنية، وأنه لا بد من انتهاز إستراتيجية هجومية.

ويبرر انتهاج هاته الإستراتيجية في بعدها المعلوماتي بالتدخل الأجنبي للغرب وتعبئة الشعوب ضده، وهو ما ترجم بالثورات الملونة وصولاً إلى التحالف الأوكراني مع الغرب، حيث جادل إيفغور بانارين" الضابط السابق في جهاز المخابرات السوفيتية"؛ بأن استخدام الغرب لأدوات المعلومات خلال القرن العشرين دفع الروس إلى تدمير بلادهم (سقوط القياصرة الروس عام 1917، ثم انهيار الاتحاد السوفيتي) إلى جانب ادعاءاته بالمحاولات الغربية لإسقاط الأنظمة الصديقة لروسيا باستخدام أدوات معلوماتية (الربيع العربي)، ويبرز هذا التصور للتهديد في عقيدة أمن المعلومات لعام 2016، والتي تنص على أن: "أجهزة الاستخبارات في بعض الدول تستخدم أدوات المعلومات والأساليب النفسية بهدف

زعزعة الوضع السياسي والاجتماعي في مناطق معينة من العالم، وتقويض سيادتها، وانتهاك الأمن على المستوى الإقليمي بمشاركة فواعل مختلفة". (NATO Strategic Communications Centre of, 2021, p. 9)

وبناء على هاته التصورات صنعت روسيا لنفسها ترسانة معلوماتية رصينة وطورت من الجانب التقني لاستخدامه كعنصر قوة لها، وعامل إخضاع للعدو، وأداة لإعادة تشكيل الأوضاع الجيوسياسية لصالحها، بالرغم من إنكارها للاستخدامات السرية لهذا السلاح، عندما تتم مواجهتها بخرق السيادة الرقمية لعدد من الدول خاصة دول حلف الناتو.

بالتوظيف الروسي للأدوات السيبرانية في الحرب ضد أوكرانيا

اعتمدت روسيا على إستراتيجية "السيبرانية الهجومية" كإحدى الطرق للسيطرة على فضاء معلوماتها، وتقويض فضاء معلومات خصومها (Willett, pp. 7-8) مستندة على العقيدة العسكرية التي تقوم على مرحلة تمهيدية قبل الهجوم العسكري المباشر، والتي يتم فيها إرهاب الخصم من خلال تدمير بنية المعلومات ومنع وصوله إليها، واختراق النظام العام لها (المالي، المؤسساتي، نظم الاتصالات) والتأثير على القاعدة الشعبية من خلال نشر معلومات مضللة تؤثر على مسار الحرب وتوجهها، وذلك بناء على محورين أساسيين (المحور المادي الذي يعتمد على الجانب التقني من خلال قرصنة الأجهزة، والمحور المعنوي المرتبط بالجانب النفسي -توجيه الرأي العام -)

-استخدام مجموعات القرصنة لتنفيذ الهجمات السيبرانية:

والتي تقوم على تنفيذ هجمات على حسابات عسكرية ومدنية أوكرانية بهدف الوصول إلى المعلومات وإظهار روسيا بصورة ايجابية، فقد أوضحت شركة ميتا المملوكة لمارك زوكربيرج أن مجموعة تعرف باسم "كتاب الأشباح" نشرت مقاطع فيديو تدعو فيها الجيش الأوكراني للاستسلام، إلى جانب نشر التقارير الكاذبة وبلاغات عن مغادرة القوات الحكومية الأوكرانية وقادتها البلاد، وتنفيذ هجمات حجب الخدمة الموزعة (DDoS) التي تقوم على تعطيل

مواقع الحكومة الأوكرانية. (Khoirunnisa, p. 141)

-الاستعانة بالاستخبارات الروسية لتعزيز مستوى الهجمات:

تقوم روسيا بالاستعانة باستخباراتها لتنفيذ بعض الهجمات، والتي تم رصدتها من خلال شركة "مايكروسوفت" والسيطرة عليها كهجوم "سترونتيوم" (Strontium)-وكالة المخابرات العسكرية لبيئة الأركان العامة الروسية-والتي تستهدف المؤسسات الأوكرانية، ومراكز الفكر في الولايات المتحدة والاتحاد الأوروبي لتحقيق أهداف تكتيكية. (البهي، 2022)

استخدام برمجيات خبيثة لخرق الأنظمة المعلوماتية :

بهدف تعطيل أجزاء من البنية التحتية لأوكرانيا، قامت روسيا في ديسمبر 2015 باستعمال برمجيات خبيثة "ماسحة" على شركات توزيع الكهرباء الأوكرانية لتخريب إمدادات الكهرباء لربع مليون أوكراني، (Willett, p. 9)، كما شمل هذا التعطيل مؤسسات أخرى كالبنوك والسكك الحديدية الوطنية وخدمة البريد ووزارة الصحة، وقدر مسؤول حكومي أوكراني أن 10 من جميع أجهزة الكمبيوتر في البلاد قد تأثرت، بينما قدّرت شركة "Information Systems Security Partners أن 300 شركة أوكرانية قد تأثرت بسبب تسخير دودة الكترونية ذاتية الانتشار وغير خاضعة للرقابة، إلى جانب ثغرة برمجية في أنظمة تكنولوجيا المعلومات تعرف باسم "ثغرة تكنولوجيا المعلومات العالمية"، والتي ألحقت أضرار بالغة لأنظمة 60 دولة أخرى بما في ذلك الولايات المتحدة الأمريكية، ودول أخرى أعضاء في حلف الناتو (Willett, p. 10). وبالتالي تعتبر حرب المعلومات والتضليل عنصرا آخر في الهجوم الروسي على أوكرانيا، فالبرغم من استخدامها لأدوات عسكرية إلا أنها رأتها غير كافية لحسم الصراع لصالحها، وتحقيق أهدافها الجيوسياسية التي لا تقتصر على أوكرانيا كدولة، وإنما على محيطها الإقليمي وداعيمها.

2- إستراتيجية الدفاع الأوكراني لمواجهة الهجمات السيبرانية الروسية

أمام الهجمات السيبرانية الروسية الممنهجة تبنت أوكرانيا معادلة دفاعية صلبة في سبيل صدها، والتي امتدت لدول حلف الناتو، واستندت هاته المعادلة إلى جملة من المحاور الدفاعية .

للتعاون مع مجموعات القرصنة لتنفيذ أنشطة هجومية على أنظمة الكمبيوتر الروسية:

وذلك من خلال تجنيد مجموعات قراصنة مختلفة عملت على تعطيل مواقع بعض المؤسسات الروسية (بنوك، مواقع إعلامية وحكومية، شركات البث التلفزيوني والإذاعي المباشر) (Khoirunnisa, pp. 141-142) والتي تهدف إلى إزالة المتصيدين المؤيدين لروسيا من المواقع الالكترونية الأوكرانية، وحمايتها من القراصنة الروس؛ بمشاركة رسمية وشعبية كخط دفاعي لما تقوم به روسيا من حرب معلومات تستهدف القاعدة الشعبية.

بإنشاء أداة حرب رقمية عسكرية

وتتمثل في أداة دلتا التي تم إنشائها من قبل مجموعة من المتطوعين المدنيين؛ كنظام خدمات آمنة مخصصة للجيش الأوكراني، تعمل على رقمتته وتسهيل إجراءات عمله، ولا سيما بفضل إزالة العديد من مستويات "البيروقراطية"، كما أتاحها تطبيق Diia للمواطنين الأوكرانيين، وأخذت شكل خريطة جغرافية مكونة من عدة طبقات، متاحة من متصفح الويب على أي وسيلة مادية (الهاتف الذكي، الجهاز اللوحي، الكمبيوتر) (Kryvetska, 2025, p. 5)

ج. الاستعانة بأطراف دولية وإقليمية لمواجهة التهديدات السيبرانية الروسية

استجابت بعض الجهات غير الحكومية الفاعلة في المجال السيبراني لدعوة الحكومة الأوكرانية، بما في ذلك القراصنة المتطوعين لتعطيل مواقع الويب الروسية، حيث أعلنت المجموعة التابعة لشركة Anonymous مسؤوليتها عن اختراق RuTube في أوائل ماي، والذي أدى إلى تعطيل منصة الفيديو الروسية لمدة يومين، ومجموعة NB65 التي عملت على اختراق خوادم العديد من شبكات التلفزيون الروسية وتعطيلها (Government of, 2022, p. 5)، وتساعد هاته الفواعل الغير حكومية في تحقيق موازنة مع مجموعات القرصنة الروسية، أي حفظ أمن

المعلومات، وتنفيذ عمليات هجومية تمنع وصول الأخبار المضللة للشعب الأوكراني.

وقامت بعض الدول كالولايات المتحدة الأمريكية والمملكة المتحدة بعمليات استخباراتية ضد روسيا كاستجابة لطلب الحكومة الأوكرانية (Willett, p. 18)، وأرسلت ست دول من الاتحاد الأوروبي خبراء في الأمن السيبراني إلى أوكرانيا، مع خدمة ستار لينك التابعة لإيلون ماسك لدعم عمليات الاسترداد والهجمات الإلكترونية، وتم تخصيص مهمة مواجهة الهجمات الإلكترونية ضمن مهام حلف شمال الأطلسي (الناتو) الرئيسية (Budiman, 2023, p. 1794).

وتثبت استجابة القطاع الخاص، والفواعل الأجنبية لدعوة أوكرانيا مستوى الضرر الذي سببته الهجمات السيبرانية الروسية، ومدى فعالية السلاح المعلوماتي في تحقيق أهداف إستراتيجية، وتجاوزه لخطورة السلاح العسكري سواء من حيث عدم القدرة على التتبع أو الإثبات، كما أن سعي هاته الأطراف لاعتبر أحيانا ردة فعل متعلقة بحماية أوكرانيا، بقدر ما يمثل مواجهة صريحة لروسيا ودحض مساعيها الجيوسياسية في مناطق معينة من العالم، وهو ما يظهر في حجم العقوبات المتباينة المفروضة عليها لشل حركتها الاقتصادية، ومنع تطوير مجالها العسكري والمعلوماتي.

ثالثا: التأثيرات المحتملة للاختراقات السيبرانية ضمن الحرب الروسية الأوكرانية

أحدثت الهجمات السيبرانية المتبادلة تأثيرات متباينة، شملت العديد من الوحدات ضمن فضاءها الإقليمي والدولي، وتجاوزت الطروحات التقليدية القائمة على تعزيز القدرات العسكرية، ضمن مقاربة تحويلية تسعى نحو تطوير الأنظمة الحيوية لمواجهة أساليب الحرب المعاصرة.

1- تأثيرات متباينة على مستوى طرفي الحرب

تبعاً لمساعي الطرفين في حرب سيبرانية، كانت ردود الفعل متباينة من حيث التوقيت والأسلوب، متساوية في الشدة، ونتجت عنها تأثيرات مست البنية التحتية للطرفين على مختلف الأصعدة.

فالنسبة لأوكرانيا على المستوى الاجتماعي انقسمت إلى جزئين جزء شرقي ناطق بالروسية ومعزول تماما؛ مما يجعله غير قادر على الوصول إلى أي معلومات

خارجية عدا الروسية (تلفزيون، راديو) ويمنعه من صياغة آراء مغايرة عن ما تروج له روسيا، بينما يعرف الجزء الغربي محدودية في الوصول إلى وسائل الإعلام الناطقة بالروسية، مما يجعلها تسيطر على الرأي العام وتشكل القرارات لصالحها من خلال الدعاية وتزييف الأخبار (Marie, 2018, p. 14)

وأدت الهجمات المتتالية إلى غلق مواقع الكترونية بما في ذلك وزارة التعليم والعلوم ووزارة الخارجية، وخدمة الطوارئ الحكومية، ومجلس الوزراء ووزارة الطاقة بهدف تعطيل قدرة أوكرانيا من خلال استخدام أساليب هجينة تعتبر الأولى في العالم، حيث كانت الكيانات الحكومية أكثر استهدافا وشكلت 33% من الهجمات الالكترونية، تليها قطاعات البنية التحتية الحيوية مثل الحكومات المحلية والزراعة، والقاعدة الصناعية الدفاعية، والرعاية الصحية والنقل والتمويل (Fyshchuk Iryna, 2024, p. 3)، وقد استهدفت روسيا باستمرار قبل الغزو وأثناءه (باستخدام نسخة مطورة من Indusstroyer/Crash (Stoddart, 2024, p. 9)

وهو ما أشار إليه كل من ديفيد كاتلر: الأمين العام المساعد للاستخبارات والأمن في حلف شمال الأطلسي، ودانيال بلاك: المحلل الرئيسي في فرع تحليل التهديدات الإلكترونية في مجلة الشؤون الخارجية عام 2022 "إن الاعتقاد بأن العمليات السيبرانية لم تلعب أي دور في أوكرانيا لا ينبع من غياب تأثيرها على أرض الواقع، بل على العكس كان حجم العمليات السيبرانية المدمرة التي شنتها موسكو قبل الحرب غير مسبوق، ففي يوم بدء الغزو نجحت وحدات الأمن السيبراني الروسية في نشر برمجيات خبيثة أكثر تدميراً مما تستخدمه عادةً بقية القوى السيبرانية العالمية مجتمعة في عام واحد" (Stoddart, 2024).

وعلى المستوى الاقتصادي تسببت هاته الهجمات في خسارة الإيرادات وانخفاض الإنتاجية، حيث قدر متوسط الضرر الاقتصادي بنحو 22 ألف دولار أمريكي لكل دقيقة من عدم توفر المواقع الالكترونية، مما يعني أنها تكلف الشركات المستهدفة مبالغ طائلة (Marie, 2018)

وبالنسبة لروسيا فإنها هي الأخرى تأثرت بالهجمات السيبرانية الأوكرانية؛ خاصة وأنها لم تتوقع تطوير أوكرانيا لقدراتها السيبرانية بناءً على انكشاف

إستراتيجيتها في الهجوم، وتعرضها لهجمات على مواقع الانترنت والتلفزيون الروسي؛ كهجوم تعطيل الخدمة الذي تناولته الدراسة سابقا. وعلى المستوى الاقتصادي فإن الحرب على أوكرانيا كانت مرهقة للجانب الروسي من خلال تحمل تكاليف العمليات السيبرانية الهجومية، وعملية التطوير المستمر للبنية التحتية السيبرانية من جهة، وتعرضها لعقوبات دولية اقتصادية من جهة أخرى.

بإمتداد التأثيرات خارجيا:

امتدت تأثيرات التهديدات السيبرانية لتشمل بعض الدول التي قدمت الدعم لأوكرانيا في حربها ضد روسيا، أو تلك الواقعة في فضائها الإقليمي، حيث تعرضت لعدد من الهجمات التي استهدفت أنظمة البيانات وعطلت خدمات الانترنت.

وأدت هاته الهجمات الإلكترونية إلى عرقلة الوصول إلى خدمات الاتصالات، تقييد الوصول إلى الأموال، حرمان الوصول إلى الكهرباء والتدفئة والمياه، وتبعاً لتعدد هاته الهجمات وتباينها كانت الآثار التخريبية لها:

-الهجوم على شبكة الأقمار الصناعية Viasat الذي أدى إلى انقطاع خدمة الإنترنت لأكثر من أسبوعين، وحُرم ما يقرب من 9000 مشترك في فرنسا من الإنترنت، وتأثر حوالي ثلث مشتركين آخرين في أوروبا، وفقدت شركة طاقة ألمانية كبرى إمكانية الوصول إلى المراقبة عن بُعد لأكثر من 5800 توربين رياح.

- هجوم ببرمجيات خبيثة على محطة مراقبة حدودية في 25 فبراير 2022؛ الذي أدى إلى إبطاء عملية السماح للاجئين بالعبور إلى رومانيا.

-هجوم على شركة Ukrtelecom؛ تسبب في انهيار الاتصال إلى 13٪ من مستويات ما قبل الحرب. (Duguin, 2023, p. 8)

-شن هجومات مضادة محتملة ضد الولايات المتحدة وكندا، وحلفاء آخرين في حلف شمال الأطلسي؛ كانت ذات تأثيرات على البنية التحتية الحيوية (Government of, 2022, p. 4)

وهو ما أثار مخاوف بشأن "إمتداد الهجمات السيبرانية" إلى دول أخرى غير طرف في الصراع، بناء على تأثير الصلة بين الأمن السيبراني وأمن الفضاء

الخارجي؛ حيث لاحظ بعض المحللين تحولاً نحو استهداف أكبر لحلفاء أوكرانيا من خلال تكتيكات سيبرانية مختلفة أثرت في عام 2023؛ على كل من كندا ونيوزيلندا وبولندا وسويسرا وحلف شمال الأطلسي، مع استمرار درجات التأثير حالياً باستمرار الصراع. (Pytlak, 2024)

ويمكن أن تبدو هذه الهجمات الإلكترونية أيضاً كتحضيرات لهجمات مستقبلية قد تهدف إلى إيذاء الأمريكيين، أو على الأقل ردع الولايات المتحدة ودول أخرى عن حماية مصالحها الحيوية والدفاع عنها، ووفقاً للأدميرال مايك روجرز¹ فإن الهجمات السيبرانية ليست حصرية على أوكرانيا، وإنما تشمل محاولات على شركات الطاقة الأمريكية² (Stoddart, 2024, pp. 14-17) وتحليل مستوى التأثيرات على أطراف الحرب، يثبت مدى فعالية السلاح السيبراني، وإن كانت هاته التأثيرات غير قابلة للمقارنة بتلك العسكرية المباشرة، إلا أنها يمكن أن تكون سبيلاً لتحقيق الضغط على الفاعل محلياً من خلال إفقاده عنصر الثقة الشعبية، وتحقيق السبب لتنفيذ ضربات عسكرية، وكذا الحد من قدرة الدعم الأجنبي؛ من خلال شرعنة التوجهات الهجومية المبنية على الأخبار والمعلومات المضللة.

رابعاً: مآلات الحرب السيبرانية الروسية الأوكرانية

تبعاً لما أفرزته الحرب الروسية الأوكرانية في مختلف أبعادها من تأثيرات مستتة العديد من الأطراف، فإننا قمنا بوضع مجموعة سيناريوهات بناءً على المعطيات السابقة.

1- تصعيد الهجمات السيبرانية على البنى التحتية للطرفين

ستشهد الفترة القادمة تصعيداً لحجم الهجمات السيبرانية من قبل روسيا حسب هذا السيناريو، وذلك بغرض إحداث ضرر أكبر وتقويض دور الحكومة الأوكرانية، في حين أن أوكرانيا ستستمر في تطوير منظومتها الدفاعية السيبرانية، بمساعدة القوى الداعمة لها وهو ماسيؤدي إلى استمرار الحرب وربما يضاعف من حجم التأثيرات؛ نظراً لسعي الطرفين لتطوير التقنيات في حربيهما القادمة، خاصة بعد انكشاف الاستراتيجيات المنتهجة في الحرب الحالية.

2- استخدام الذكاء الاصطناعي في الهجوم والدفاع السيبراني

سيعمل الطرفان على استخدام تقنيات الذكاء الاصطناعي بهدف التجسس والاستطلاع واستغلال الثغرات الموجودة في الأنظمة لكلا الطرفين، خاصة مع تطور التقنيات الحديثة له.

ويمكن للهجمات السيبرانية النفسية الروسية التي تستخدم وسائل التواصل الاجتماعي، مع تطبيق الذكاء الاصطناعي، أن تصبح أكثر استهدافاً وفعالية من ذي قبل، وقد تصبح عمليات التزييف العميق المحسنة بالذكاء الاصطناعي لـ"صناع القرار النخبة" غير قابلة للتمييز عن الشخص "الحقيقي" (Rod Thornton, 2012) وحسب مركز الدراسات الإستراتيجية والدولية ستميز حروب المستقبل بابتكارات تتكيف مع تطور التكنولوجيا، وستمكن برامج الذكاء الاصطناعي أوكرانيا من الحفاظ على تفوقها التكنولوجي، كما استفادت من برمجيات ومنصات بيانات مدعومة بالذكاء الاصطناعي لتعزيز سرعة اتخاذ القرارات في الحرب والحكومة (studies, 2025)

3. سيناريو تصاعد الهجمات الروسية نحو دول حلف الناتو وانكشافيتها كعامل تهديد وحرب جيوسياسية

من المتوقع أن تشهد دول حلف الناتو في السنوات القادمة هجمات سيبرانية نفسية أكثر دقة من الجانب العسكري الروسي، حيث ستتعرض الحكومات الغربية وشعوبها والحملات الانتخابية لمحاولات تلاعب متزايدة بدرجات غير مسبوقة، وقد يؤدي هذا حسب الأدبيات العسكرية الروسية إلى إضعاف طويل الأمد للمؤسسات الغربية (الناتو، الاتحاد الأوروبي.. إلخ) كما قد ينشأ عنه فراغات سياسية قد تسمح للإدارات ذات الميول الروسية بالوصول إلى السلطة (Stoddart، 2024)

وأمام ارتفاع الدعم الغربي لأوكرانيا في حربه ضد روسيا سواء من حيث تزويده بالسلاح أو تطويره تقنيا، أو فرض العقوبات الاقتصادية على روسيا، ستعمل هاته الأخيرة على استهدافه ضمن أحد الفواعل المعيقة لأهدافها الجيوسياسية وسيتحول مفهوم الحرب الباردة إلى معلم نظري.

وقد تم الاعتماد على هاته السيناريوهات ذات النزعة التشاؤمية نظرا للمعطيات التي قدمتها حالة الحرب، الوسائل المستخدمة، والآثار المترتبة وعدم تنازل الطرفين عن أي من مطالبها ضمن الحرب، ما يعني استمرارها في الشق

العسكري والمعلوماتي على حد سواء ضمن مسارات تصاعدية، وتعزيز أساليب جديدة.

خاتمة:

ختاما يمكن القول أن الحرب الروسية الأوكرانية قد جسدت كيف يمكن للعمليات السيبرانية أن تغير من مسار الحرب المعاصرة، وإن كانت هاته التجربة لا تزال غير ناضجة بالمستوى الذي يمكن وضع معطياتها كمعايير عالمية لحروب سيبرانية قادمة على اعتبارها قيد التجريب والتكيف، إلا أنها منحت رؤية لاهتمام العالم بالمتغير المعلوماتي، والسعي نحو تطوير البرامج الحيوية لمواجهة نوع جديد من التهديدات وتطوير التقنيات لحماية الفرد على مستوى أدنى وحماية المصالح الجيوسياسية على مستوى أعلى .

وقد توصلت الدراسة لجملة من النتائج، والمتمثلة فيمايلي:

- لا يمكن التقليل من أهمية ماتوليه روسيا لمحاولة السيطرة على المعلومات عند دراسة الحرب الروسية الأوكرانية، واستخدام التضليل التكتيكي الذي لازم العقيدة الروسية، وامتدادات ذلك على المنظومة الغربية بأكملها، والتي أثبتت فعاليتها؛ كادعاءات حصول أوكرانيا على أسلحة بيولوجية كخطوة لزعزعة المعارضة المحلية والرأي العام العالمي، مما يمنحها القدرة على تنفيذ وشرعنة هجوماتها، وشل حركة الغرب للرد على هاته الهجمات أو تجريمها.
- لعبت التدابير الدفاعية الأوكرانية دورا حاسما في صد الهجوم السيبراني الروسي، وقد شملت هاته التدابير التعلم والتحصين الدفاعي قبل بداية الحرب، إلى جانب التعاون بين القطاع العام والخاص والدولي؛ مما يضعنا أمام احتمال استمرارية الحرب، وتأثير الاعتداءات السيبرانية المستقبلية في الفضاءات الدولية والإقليمية للطرفين.

- بالرغم من ما أحدثته الهجمات السيبرانية الروسية إلا أنها تظل محدودة مقارنة بالأهداف الإستراتيجية الكبرى التي سطرته ضمن عقيدتها العسكرية، وجهودها الواسعة التي كانت ذات تكلفة عالية، ووصولها إلى معادلة صفرية فيما يتعلق بمصالحها الجيوسياسية، وذلك بسبب ارتكابها أخطاء هجومية (الانكشافية) والتي استغلتها أوكرانيا والغرب في تطوير ترسقاتها الدفاعية،

إلى جانب أن تقييم الوضع الأوكراني بناء على معايير الضعف والاستسلام كان خاطئاً.

وبناء على ذلك يمكن اقتراح التوصيات التالية:

❖ ضرورة تعزيز القدرات السيبرانية في الحروب المعاصرة لكل الوحدات الدولية، نظراً لأن التهديدات السيبرانية قد أثبتت قدرتها على إحداث اضطرابات هائلة، والتي يمكن أن تتجاوز التهديدات العسكرية، وبالتالي فإن جميع الدول بدون استثناء بحاجة إلى تطوير استجابات قوية تتجاوز تلك التقليدية والمتمثلة في: - تطوير استراتيجيات شاملة لسد كل الثغرات التي يمكن أن يتم استغلالها من قبل القراصنة لتهديد أمن الأفراد، أو المؤسسات العليا للدول (كوزارة الدفاع، وزارة الخارجية، البنوك، ومختلف المؤسسات المالية والإدارية ذات المهام المركزية).

- بناء القدرات السيبرانية بما يتوافق مع طبيعة هاته التهديدات خاصة بالنسبة لتلك الدول التي لاتزال بعيدة عن التطور التقني العالمي الكبير، مما يجعلها أكثر عرضة لتهديدات سيبرانية بسيطة، وتشمل هاته التقنيات أنظمة حماية عالية الجودة، وإنشاء مراكز استشرافية بناء على المعطيات الجيوسياسية على اعتبارها المحرك لهاته الهجمات.

قائمة المراجع

- البهي، رغبة. (2022). المركز المصري للفكر والدراسات الاستراتيجية، أنظر: 2022/7/3. <https://shorturl.at/zfVyK>
- Antoniuk, D. (2024, 2 8). Ukraine's cyberattacks on Russia aiding ground operations, top Kyiv cyber official says. Récupéré sur The Record: <https://shorturl.at/Rqhdd>
- Azharu, i. (s.d.). the valery gerasimov doctrine. BIPSS Commentary .
- Budiman, I. e. (2023). CYBERSECURITY ANALYSIS IN THE CONTEXT OF THE RUSSIAUKRAINE CONFLICT: CHALLENGES, THREATS, AND DEFENSE STRATEGIES. Jurnal ekonomi , 12 (2).

- D.carpenter, a. o. (2019). Refining Technology the echnology threat Avoidance theor oidance theory. *communications of the ssociation for information ystems* , 44 (22), 22.
- Duguin, S. a. (2023). *The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict*. European Parliament coordinator:policy Department for Externalrelations Directorate General for External policies of the Union.
- Fyshchuk Iryna, e. a. (2024). Managing Cyber attacks in Wartime: the case of Ukraine. *Public Administration Review* .
- Fyshchuk, I. (2024). Managing cyberattacks in wartime: The case of Ukraine,. *Public Administration Review* .
- Government of, c. (2022). *Cyber threatbulletn: Cyber threat Activity Related to the Russian of Ukraine*. Canadian Centre for Cyber Security.
- Khoirunnisa, C. S. Cyber Warfare Strategies in the Russia-Ukraine Conflict(2021-2022): Implications for National Security and Modern Warfare. *Jurnal Public Policy* , 10 (2).
- Kryvetska, A. (2025). cyberguerre et nouvelles technologies : les civils sont-ils un moyen asymétrique redoutable dans la guerre en Ukraine ?., *la revue géopolitique* .
- Marie, B. (2018). *Hotspot Analysis: Cyber and Information warfare in the Ukrainian conflict*. ETH Zurich: center for security studies(css).
- NATO Strategic Communications Centre of, E. (2021). *Russia's Strategy in Cyberspace*. report.
- Pleskach, M. (2020). Standardization in the Field of Cybersecurity and Cyber Protection in Ukraine. *Information& Security* (45).
- Pytlak, A. (2024, February 22). *Flase Alarms:Reflecting on the Role of the Cyber Operations in the Russia-Ukraine War*. Récupéré sur <https://shorturl.at/B8q8o>
- Rod Thornton, M. (2012). The Use of Cyber Tools by the Russian Military: Lessons from the War against Ukraine and a Warning for NATO? *Applied Cybersecurity&internet governance* , Vol3 (No1).

- SIA. (2024, november 6). *Hybrid warfare: how cyber warfare is transforming international relations*. Récupéré sur SIA: <https://shorturl.at/y3OZa>
- Spinu, N. (2020). *Cybersecurity Governance Assessment*. DCAFGeneva center for security sector Governance.
- Stoddart, K. (2024). Russia's Cyber Campaigns and the Ukraine War: From the 'Gray Zone' to the 'Red Zone'. *acig* , 3 (1).
- studies, c. f. (2025). *insights for future conflicts from the russia-ukraine war*. csis.
- Willett, M. The Cyber Dimension of the Russia-Ukraine War. *Survival Global Politics and Strategy* , 64 (5).
- ر. البهي (2022, 7 3). *المركز المصري للفكر والدراسات الاستراتيجية*. Récupéré sur <https://shorturl.at/zfVyK>
- ا. رغبة (2022, 07 3). *المركز المصري للفكر والدراسات الاستراتيجية*. Récupéré sur <https://shorturl.at/ewwtZ>