الترميز الدولي / ISSN (P) :2710-2653 تاريخ استلام البحث : 2026/4/4
ISSN (E) :2960-253X / تاريخ قبول البحث : 2026/5/6
رقم الايداع الوطني / 2375 /2019 تاريخ النشر : 2026/6/30

القدرات السيبرانية الروسية ودورها بالحرب على أوكرانيا بعد عام 2020

Russian cyber capabilities and their role in the war on Ukraine after 2020

م.د. علاء عبد الرزاق عبد القادر

Dr. Alaa Abdul Razzaq Abdul Qader

وزارة التربية/ المديرية العامة لتربية بغداد الكرخ الاولى

Ministry of Education / General Directorate of Education Baghdad Al-Karkh First

alaa1970top@gmail.com

IRAQI
Academic Scientific Journals
https://iasj.rdd.eedu.iq/journals/journal/view/229

القدرات السيبرانية الروسية ودورها بالحرب على أوكرانيا بعد عام 2020

م.د. علاء عبد الرزاق عبد القادر

الملخص

يتناول البحث التحول المتسارع في موقع الفضاء السيبراني ضمن بنية القوة الدولية، من خلال تحليل التجربة الروسية في توظيف الأدوات الرقمية ضمن بيئة صراع مركبة تتداخل فيها الأبعاد العسكرية والمعلوماتية، ويركز على كيفية تحويل القدرات السيبرانية إلى أداة لإدارة الضغط الاستراتيجي عبر استهداف البنى الحيوية وإعادة تشكيل إدراك الخصم لطبيعة التهديد، مع إبراز دور التكامل بين المؤسسات الاستخبارية والتقنية في إنتاج تأثير مستمر داخل بيئة العمليات، ويناقش حدود الفاعلية السيبرانية في تحقيق الحسم، مقابل قدرتها على إطالة أمد الصراع ورفع كلفته، ويبرز أهمية المرونة الدفاعية والتحالفات التقنية في تقليص أثر الهجمات الرقمية، وتقدم الدراسة قراءة تحليلية تفسر التحولات الجارية في طبيعة الصراع المعاصر، وتسلط الضوء على التفاعل بين القوة الرقمية والقدرة المؤسسية، بما يفتح المجال أمام مقاربات جديدة لفهم توازنات الردع في الحروب الحديثة.

الكلمات المفتاحية: القدرات السيبرانية، الحرب الهجينة، الأمن السيبراني

Abstract

This study examines the evolving role of cyberspace in contemporary conflict through an analytical perspective on Russia's use of digital capabilities in complex warfare environments. It highlights how cyber tools are integrated with intelligence and military structures to generate sustained strategic pressure by targeting critical infrastructure and influencing information environments. The study also explores the limits of cyber power in achieving decisive outcomes, emphasizing its role in prolonging conflict and increasing operational costs. Furthermore, it underscores the importance of resilience, defensive capacity, and international technical cooperation in mitigating cyber threats, offering insights into

emerging patterns of deterrence and power in modern hybrid warfare.
Keywords: Cyber capabilities, hybrid warfare, cybersecurity

المقدمة

تعكس القدرات السيبرانية الروسية تطوراً بنيوياً عميقاً في طبيعة القوة المعاصرة من خلال بناء منظومة متكاملة تجمع بين المؤسسات الاستخبارية والعسكرية والتقنية ضمن إطار الحروب الهجينة التي تدمج بين الأدوات الرقمية والعمليات التقليدية في سياق واحد مترابط، حيث تعتمد روسيا على أجهزة رئيسة مثل الاستخبارات العسكرية الروسية (GRU) بوصفها الفاعل الأبرز في تنفيذ العمليات الهجومية، وجهاز الأمن الفيدرالي (FSB) المعني بحماية الأمن الداخلي ومكافحة التهديدات الرقمية، وجهاز الاستخبارات الخارجية (SVR) المختص بعمليات التجسس خارج الحدود، إلى جانب وحدات الحرب الإلكترونية وشبكات الدعم الأكاديمي والتقني التي تسهم في تطوير القدرات الهجومية والدفاعية، وقد أظهرت الحرب على أوكرانيا بعد عام 2020 مستوى متقدماً من توظيف هذه القدرات عبر استهداف البنى التحتية الحيوية مثل الطاقة والاتصالات والنقل والمؤسسات الحكومية والقطاع المالي وفضاء المعلومات، مع استخدام تقنيات متطورة تشمل الهجمات على سلاسل التوريد الرقمية والبرمجيات التخريبية وأنظمة التحكم والإشراف الصناعية (SCADA) التي تدير المرافق الحيوية، فضلاً عن توظيف تقنيات الذكاء الاصطناعي في تحليل البيانات وتنفيذ الهجمات، كما اتسمت العمليات الروسية بدرجة عالية من التكامل مع العمل العسكري والتأثير المعلوماتي بما يعزز الضغط التراكمي على الدولة المستهدفة، وتعتمد فعالية هذه العمليات على مستوى الدمج الاستخباري وتكامل منظومات الاستخبارات والمراقبة والاستطلاع (ISR) في إنتاج تأثير مستمر داخل بيئة الصراع المعقدة.

ينتقل التحليل في هذا البحث إلى تفكيك البنية السيبرانية الروسية من حيث أطرها المؤسسية وأنماط توظيفها العملياتي ضمن سياق الحروب الهجينة، ويُمهّد ذلك لفهم آليات الدمج الاستخباري وتكامل منظومات ISR في إنتاج التأثير العملياتي داخل بيئات الصراع المعاصر.

أهمية البحث: تكمن أهمية البحث في تسليط الضوء على دور القدرات السيبرانية بوصفها أحد مكونات القوة الشاملة في الصراعات المعاصرة، مع بيان تأثيرها في إعادة تشكيل أدوات الحرب الحديثة، يسهم البحث في تقديم فهم تحليلي لتجربة روسيا في توظيف الفضاء السيبراني ضمن الحرب الهجينة، بما يدعم الدراسات الأمنية والاستراتيجية في البيئات المشابهة.

هدف البحث: يهدف البحث إلى تحليل البنية السيبرانية الروسية من حيث أطرها المؤسسية والتقنية وأنماط توظيفها في الصراع مع أوكرانيا بعد عام(2020)، ويركز على تفسير أثر هذه القدرات في مخرجات الحرب وتوازنات الصراع بين روسيا وأوكرانيا والفاعلين الدوليين.

إشكالية البحث: تتمحور إشكالية البحث حول طبيعة الدور الذي تؤديه القدرات السيبرانية في الحروب الحديثة ومدى قدرتها على إحداث تحول في مخرجات الصراع، وتسعى للإجابة عن مدى فاعلية القدرات السيبرانية الروسية في تحقيق تأثير استراتيجي حاسم في الحرب على أوكرانيا.

فرضية البحث: تنطلق فرضية البحث من أن القدرات السيبرانية الروسية تمثل أداة فعالة في إضعاف الخصم وإرباك مؤسساته دون أن تصل إلى مستوى الحسم العسكري، تفترض أن تأثير هذه القدرات يتعزز عند دمجها مع العمليات التقليدية ضمن إطار الحرب الهجينة.

منهج البحث: يعتمد البحث على المنهج الوصفي في عرض المفاهيم المرتبطة بالقدرات السيبرانية والحرب الهجينة وتطورها في السياق الروسي، ويستند إلى المنهج التحليل النظمي في تفسير العلاقة بين توظيف القدرات السيبرانية ومخرجات الصراع في الحالة الأوكرانية.

الحدود الزمانية والمكانية للبحث: تتمثل الحدود الزمانية للبحث في المدة الممتدة من عام (2020) حتى عام (2025) بوصفها مرحلة تصاعد وتوظيف مكثف للقدرات السيبرانية، أما الحدود المكانية فتشمل روسيا وأوكرانيا مع امتداداتها إلى الفضاء الأوروبي والدولي المرتبط بتفاعلات الصراع السيبراني.

هيكلية البحث: تتكون هيكلية هذا البحث من مقدمة وأربعة محاور رئيسة وخاتمة، حيث تعرض المقدمة الإطار العام للموضوع من خلال بيان أهمية القدرات السيبرانية في الصراعات المعاصرة وتحديد مشكلة البحث وأهدافه ومنهجه وحدوده، بينما يتناول المحور الأول البنية المؤسساتية والاستخبارية للقدرات السيبرانية الروسية من خلال تحليل دور الأجهزة الأمنية والعسكرية في بناء هذه المنظومة وتكاملها، ويركز المحور الثاني على التطور التقني والعملياتي لهذه القدرات بعد عام (2020) مع بيان أدوات الهجوم وأساليب التوظيف الحديثة، في حين يعالج المحور الثالث الدور السيبراني الروسي في الحرب على أوكرانيا خلال المدة (2020–2025) من خلال تحليل طبيعة الهجمات وقطاعات الاستهداف، أما المحور الرابع فيتناول أثر هذه القدرات في مخرجات الحرب وتوازنات الصراع على المستويين الإقليمي والدولي، وتختتم الدراسة بخاتمة تتضمن أبرز النتائج والاستنتاجات والتوصيات التي توصل إليها البحث.

اولاً: البنية المؤسساتية والاستخبارية للعمليات السيبرانية الروسية

تمثل البنية المؤسساتية والاستخبارية للعمليات السيبرانية الروسية أحد أهم مكونات القوة الرقمية للدولة الروسية الحديثة، إذ نجحت موسكو خلال العقدين الأخيرين في بناء منظومة سيبرانية متكاملة تعتمد على مؤسسات أمنية وعسكرية واستخبارية تمتلك خبرات تراكمية واسعة وقدرات تقنية متقدمة وتعكس هذه البنية رؤية استراتيجية تعتبر الفضاء الإلكتروني امتدادا طبيعيا لساحات الصراع التقليدي وترى في القدرات الرقمية وسيلة لتعزيز النفوذ الروسي وتعويض جوانب الضعف في القوة التقليدية وتعد هذه المنظومة نتاج عملية إصلاح واسعة أصابت أجهزة الأمن بعد عام 2000 حين بدأت روسيا في إعادة هيكلة مؤسساتها الدفاعية والاستخبارية لمواجهة التهديدات الرقمية المتزايدة.[1]

تعتمد البنية السيبرانية الروسية على ثلاث مؤسسات مركزية تمثل الركيزة الأساسية للعمليات الرقمية وهي الاستخبارات العسكرية الروسية (GRU) وجهاز الأمن الفيدرالي (FSB) وجهاز الاستخبارات الخارجية (SVR) حيث تعمل هذه المؤسسات ضمن هيكلية مترابطة تعكس درجة عالية من التنسيق المؤسسي رغم تباين اختصاصاتها، ويظهر النموذج الروسي تداخلاً وظيفياً بين الأدوار العملياتية بما يعزز القدرة على الدمج الاستخباري ويتيح توظيف الأدوات الدفاعية والهجومية ضمن سياق واحد يخدم الأهداف الاستراتيجية، ويحتل جهاز الاستخبارات العسكرية الروسية (GRU) موقعاً محورياً داخل هذه المنظومة بوصفه الفاعل الأكثر تأثيراً في تنفيذ العمليات السيبرانية الهجومية واسعة النطاق التي تستهدف الأنظمة الحكومية والبنى التحتية الحيوية، إذ تمتلك وحداته قدرات تقنية متقدمة تشمل الوحدة (26165) والوحدة (74455) المرتبطتين بمجموعة (APT28) أو Fancy) (Bearوالتي تضطلع بمهام اختراق الأنظمة الحساسة وجمع المعلومات

الاستخبارية وتعطيل أنظمة القيادة والسيطرة وإحداث تأثيرات مباشرة في شبكات الطاقة والاتصالات خلال مراحل الصراع، ويعتمد هذا الجهاز على مزيج من الكوادر العسكرية المتخصصة في مجالات الهندسة الحاسوبية والاتصالات والإلكترونيات إلى جانب خبرات مدنية يتم استقطابها لتعزيز القدرات البرمجية والهجومية بما يضمن استمرارية التفوق العملياتي ضمن بيئة الصراع الرقمي.[2]

يحظى جهاز الأمن الفيدرالي FSB بدور مركزي في تعزيز أمن المعلومات الداخلي وفي تنفيذ عمليات سيبرانية ذات بعد استخباري ويتركز دوره في اكتشاف التهديدات الرقمية التي تستهدف المؤسسات الحكومية والبنى التحتية الاستراتيجية داخل روسيا ويعمل FSB على رصد شبكات التجسس الإلكتروني ومكافحة الاختراقات التي قد تنفذها جهات أجنبية وتعد الوحدة المركزية للمعلوماتية في FSBمسؤولة عن تطوير أدوات التجسس الداخلية وبرامج التحكم في البيانات التي تتضمن تقنيات متقدمة تتيح مراقبة الإنترنت المحلي ويعمل الجهاز أيضا على تنسيق التعاون بين القطاعين العام والخاص لضمان حماية الشبكات الحيوية ومواجهة التهديدات المتزايدة المرتبطة بالجريمة المنظمة والهجمات المدعومة من دول أجنبية.

يمثل جهاز الاستخبارات الخارجية SVR الذراع الخارجي للمنظومة السيبرانية الروسية ويختص بتنفيذ عمليات التجسس الإلكتروني التي تستهدف الحكومات الأجنبية والمؤسسات الدولية والشركات العالمية الكبرى ويعتمد SVR على وحدات متخصصة في جمع المعلومات الاستراتيجية عبر شبكات سرية في الخارج ويستفيد هذا الجهاز من بيئة العمل الدبلوماسي عبر السفارات والقنصليات الروسية التي توفر غطاء قانونيا لبعض الأنشطة المتعلقة بالاستطلاع الإلكتروني وتلجأ هذه الوحدات إلى استخدام أدوات اختراق متقدمة تستهدف الأجهزة الحساسة

في وزارات الخارجية والدفاع والمؤسسات المالية وتظهر تقارير أمنية غربية أن مجموعات مرتبطة بـ SVR مثل APT29 لعبت دورا فيما عرف بعمليات SolarWindsالتي اخترقت شبكات حكومية أمريكية عام 2020.[3]

يتعزز الدور السيبراني الروسي من خلال وجود وحدات عسكرية متخصصة في الحرب الإلكترونية تابعة لوزارة الدفاع الروسية وتعمل هذه الوحدات على دعم القوات التقليدية أثناء العمليات العسكرية عبر تعطيل وسائل الاتصال التابعة للخصم وإحداث تشويش على شبكات الملاحة والطائرات المسيرة وتحظى هذه الوحدات بإمكانات متقدمة تشمل أجهزة التشويش الإلكتروني ومنظومات السيطرة على الاتصالات والرصد الطيفي وتشير البيانات العسكرية الروسية إلى أن هذه الوحدات شاركت في عمليات واسعة في أوكرانيا وجورجيا وسوريا حيث استخدمت أدوات تشويش متقدمة عطلت قدرات الخصوم على استخدام الطائرات بدون طيار والاتصالات المشفرة.[4]

تعد الأكاديمية العسكرية للاتصالات وأمن المعلومات في سانت بطرسبورغ أحد أهم المؤسسات التعليمية التي تسهم في رفد الأجهزة السيبرانية الروسية بالكوادر المتخصصة وتعمل الأكاديمية على تدريب ضباط وخبراء في الأمن السيبراني والحرب الإلكترونية والهندسة المعلوماتية وتقدم الأكاديمية برامج دراسية متقدمة تشمل تطوير البرمجيات، تحليل البيانات، استخدام الذكاء الاصطناعي في العمليات السيبرانية، وأساليب الهجوم والدفاع الرقمي وتعد هذه المؤسسة أحد الأعمدة العلمية التي تدعم التطور المستمر للبنية السيبرانية الروسية.[5]

ترتبط المنظومة السيبرانية الروسية بشبكة واسعة من المختبرات التقنية وشركات البرمجيات المحلية ويبرز دور شركات مثل "كاسبرسكي لاب" التي رغم كونها شركة مدنية تعمل في مجال الأمن السيبراني إلا أنها تقدم تقارير وأبحاث

تدعم البيئة الأمنية الروسية كما تلعب مؤسسات أكاديمية ومراكز بحثية حكومية دورا في تطوير أدوات سيبرانية يجري استخدامها داخل المؤسسات العسكرية والاستخبارية ويعتمد هذا التعاون على سياسة روسية طويلة الأمد تهدف إلى دمج القدرات المدنية والعسكرية ضمن ما يعرف بـ"العسكرة الرقمية"، تتضمن البنية السيبرانية الروسية أيضا أبعادا قانونية وتنظيمية فقد سنت موسكو تشريعات تهدف إلى تنظيم حركة البيانات ومراقبة الفضاء الرقمي الداخلي عبر قوانين مثل قانون الإنترنت السيادي الذي يعزز قدرة الدولة على التحكم بالشبكات المحلية وضمان استمراريتها في حال قطع الاتصال مع العالم ويمنح هذا القانون الأجهزة الأمنية قدرة مضاعفة على تنظيم النشاط الرقمي داخل الدولة ويسهل تنفيذ عمليات تتعلق بمراقبة التهديدات وحماية البنية التحتية.

يؤثر العامل الاستخباري في تشكيل البنية السيبرانية الروسية تأثيرا مباشرا فالأجهزة الروسية تتعامل مع الفضاء السيبراني باعتباره امتدادا لميدان الجاسوسية التقليدية وتعتمد العمليات التي تنفذها موسكو على مراحل دقيقة تبدأ بالاستطلاع الرقمي عبر زراعة برمجيات مخفية داخل الأنظمة المستهدفة ثم المرحلة التحليلية التي تركز على فهم نقاط الضعف ثم تنفيذ الهجوم المناسب عند الضرورة ويعكس هذا الأسلوب خبرة طويلة في العمل السري وامتلاك آليات متقدمة للتنسيق بين الأجهزة المختلفة.[6]

يمثل التعاون بين الأجهزة الأمنية والعسكرية أبرز مظاهر القوة في البنية السيبرانية الروسية فروسيا تعتمد على مركز موحد للقيادة والسيطرة في الأزمات الكبرى ينسق بين GRU و FSBو SVRإضافة إلى وحدات الحرب الإلكترونية ويسمح هذا التنسيق بتنفيذ عمليات متزامنة ذات طابع هجومي ودفاعي في الوقت نفسه وقد ظهر هذا النموذج بوضوح خلال الحرب على أوكرانيا حيث نفذت موسكو

عمليات سيبرانية معقدة استهدفت بنى تحتية حيوية بينما عملت في الوقت نفسه على حماية شبكاتها الداخلية من الردود المعاكسة، تؤكد البنية المؤسساتية والاستخبارية للعمليات السيبرانية الروسية قدرة موسكو على تنفيذ عمليات رقمية واسعة النطاق تتناسب مع أهدافها الجيوسياسية وتكشف هذه المنظومة عن تطور متسارع في أساليب الهجوم والدفاع الرقمي وتعبر عن رؤية استراتيجية تعتبر الفضاء السيبراني ساحة مركزية من ساحات الصراع الدولي وتظهر التجارب الحديثة أن هذه البنية تمنح روسيا قدرة تنافسية مهمة في مواجهة خصوم يمتلكون تفوقا عسكريا تقليديا وتدل المؤشرات على أن موسكو ستواصل تطوير مؤسساتها السيبرانية وتوسيع نطاق عملها بما يضمن لها موقعا مؤثرا في النظام الدولي خلال العقود المقبلة.[7]

ثانياً: التطور التقني والعملياتي للقدرات السيبرانية الروسية بعد 2020

شهدت القدرات السيبرانية الروسية بعد عام 2020 تطورا متسارعا يعكس تحول الفضاء الإلكتروني إلى عنصر أساسي في العقيدة العسكرية الروسية وفي أدوات القوة التي تعتمد عليها الدولة في صراعاتها الإقليمية والدولية وتزامن هذا التطور مع اشتداد التوتر بين روسيا والغرب وازدياد حجم المواجهات غير التقليدية التي تعتمد على الهجمات الرقمية وحملات التأثير المعلوماتي ويعكس هذا التحول رؤية روسية ترى أن المعارك الحديثة لا تحسم فقط داخل الميدان العسكري التقليدي وإنما تدار بصورة متوازية داخل البنى المعلوماتية للدول والمجتمعات المستهدفة وتقوم هذه الرؤية على استخدام أحدث المنظومات التقنية لتحقيق تفوق عملياتي يلائم بيئة الصراع المعاصر، تمثل الهجمات السيبرانية التي استهدفت البنى التحتية الأوكرانية خلال الفترة 2020–2022 أحد أهم الأدلة التي تؤكد حجم التطور التقني في القدرات الروسية فقد استخدمت موسكو أنواعا متقدمة من البرمجيات

التخريبية التي يصعب اكتشافها والتي تستطيع تعطيل شبكات الطاقة والمصارف والاتصالات وتم تطوير هذه الأدوات داخل مختبرات تابعة لأجهزة الاستخبارات الروسية مثل GRU و SVRوهو ما يشير إلى تناغم بين الجهد التقني والجهد العسكري وتعمل هذه البرمجيات وفق نموذج يعتمد على التسلل التدريجي إلى الأنظمة المستهدفة عبر ثغرات دقيقة في البرامج المستخدمة ويتسم هذا النوع من الهجمات بقدرة عالية على البقاء لفترات طويلة داخل الشبكة دون أن يتم رصدها وهو ما يمنح روسيا إمكانية التحضير لعمليات واسعة قبل تنفيذها.[8]

يتجلى التطور التقني أيضا في استخدام روسيا لأساليب جديدة في الهجوم السيبراني تقوم على ما يعرف بـ"سلاسل التوريد الرقمية" حيث يجري اختراق شركات أو مؤسسات تمتلك برمجيات يستخدمها عدد كبير من المؤسسات الحكومية في العالم وقد برز هذا الأسلوب في حادثة SolarWinds التي كشفت قدرة روسيا على النفاذ إلى شبكات حساسة من دون الحاجة إلى مهاجمتها مباشرة ويعتمد هذا الأسلوب على قدرة عميقة في تحليل البنى البرمجية العالمية وفهم نقاط الضعف المعقدة في التصميم الهندسي للبرمجيات ويعكس هذا الأمر مستوى متقدما من الخبرات التقنية التي صارت تمتلكها المؤسسات الروسية العاملة في المجال السيبراني، يتضمن التطور العملياتي تحولات جوهرية في طريقة تنظيم الهجمات واتساع نطاق التنسيق بين المؤسسات العسكرية والاستخبارية وتعتمد روسيا على نموذج عمليات متكامل يشمل الاستطلاع الرقمي والتحليل والاكتشاف ثم مرحلة الاختراق ثم التدمير أو التعطيل وتقوم هذه المراحل على شبكات اتصال آمنة تسمح للمنفذين بتلقي التوجيهات ومراقبة الأنظمة المستهدفة بشكل متواصل ويظهر هذا التنظيم أن روسيا لم تعد تعتمد على هجمات فردية بل على منظومات عملياتية كاملة تتضمن متابعة

قبل الهجوم وأثناءه وبعده ويكشف هذا المستوى من التنظيم أن الهجمات الروسية جزء من عقيدة عسكرية وليست مجرد عمليات معزولة.[9]

يعد الذكاء الاصطناعي أحد أهم التحولات التقنية التي أثرت في القدرات السيبرانية الروسية بعد عام 2020 فقد بدأت المؤسسات الروسية في توظيف خوارزميات تعتمد على التعلم الآلي لرصد نقاط الضعف في الشبكات وتطوير برمجيات تتفاعل تلقائيا مع بيئة الهجوم وتتيح هذه التقنيات تنفيذ هجمات دقيقة يصعب التنبؤ بها كما تسمح بتطوير برمجيات قادرة على تغيير بنيتها الداخلية للتكيف مع إجراءات الدفاع الرقمي التي يستخدمها الخصم وتشير التقارير إلى أن روسيا تعتمد أيضا على الذكاء الاصطناعي في تحليل المعلومات التي تحصل عليها من عمليات الاختراق مما يسرع عملية استخلاص البيانات المهمة وتوظيفها في صنع القرار.[10]

يبرز التطور التقني كذلك في مجال الحرب الإلكترونية التي أصبحت جزءا مركزيا في العمليات العسكرية الروسية وقد استخدمت موسكو أنظمة تشويش متطورة قادرة على تعطيل الاتصالات اللاسلكية والأقمار الصناعية والطائرات المسيرة وتعد هذه الأنظمة جزءا حيويا من الوجود العسكري الروسي في ساحات الصراع وتعتمد روسيا على منظومات متخصصة مثل Krasukha و Murmansk–BN التي تستخدم لتعطيل الإشارات الإلكترونية ومنع الخصم من استخدام أنظمة الملاحة ويظهر هذا التكامل بين الهجمات السيبرانية والتشويش الإلكتروني قدرة روسيا على تنفيذ عمليات مشتركة تربط بين الفضاء الرقمي والمجال العسكري التقليدي، يتضمن التطور العملياتي أيضا التركيز على ما يعرف بـ"العمليات السيبرانية الهجينة" التي تجمع بين الهجمات الرقمية وحملات التأثير والمعلومات وتستخدم روسيا هذا الأسلوب للتأثير على الرأي العام داخل الدول الغربية من خلال نشر معلومات مضللة عبر وسائل التواصل الاجتماعي وتعتمد

هذه العمليات على شبكات حسابات آلية يتم التحكم فيها من خلال برامج متطورة قادرة على إنتاج محتوى رقمي يحاكي الخطاب المحلي للمجتمعات المستهدفة ويخلق هذا الأسلوب حالة من الارتباك المعلوماتي ويضعف ثقة المواطنين في المؤسسات الرسمية وقد أثبتت هذه العمليات فاعليتها في عدة دول حيث أدت إلى إثارة الانقسامات السياسية والاجتماعية.

تطورت القدرات الروسية أيضا في مجال الهجمات التي تستهدف قطاع الطاقة فقد كشفت الهجمات التي شنت ضد شبكات الكهرباء في أوكرانيا موجة جديدة من البرمجيات التخريبية التي تستطيع التحكم في أنظمة التشغيل الصناعية وتعتمد هذه البرمجيات على فهم دقيق للبنية الهندسية لأنظمة SCADA وهي أنظمة تشرف على تشغيل المحطات الصناعية ويمكن هذا التطور روسيا من ضرب قطاعات حيوية في الدول الخصمة بطريقة تشل قدراتها الاقتصادية والعسكرية ويعد هذا النوع من الهجمات أكثر خطورة لأنه يربط الفضاء السيبراني بالعالم المادي.[11]

يتجلى التطور التقني أيضا في قدرة روسيا على استخدام هجمات حجب الخدمة الموزعة التي تعتمد على شبكات ضخمة من الأجهزة المصابة ويجري استخدام هذه الهجمات لتعطيل المواقع الحكومية والمصرفية في الدول المعادية ويعتمد هذا الأسلوب على بنية تحتية رقمية واسعة تشمل آلاف الأجهزة المصابة التي يمكن توجيهها في وقت واحد لتنفيذ هجوم واحد وتمنح هذه القدرة روسيا إمكانية إحداث تأثيرات سريعة في اللحظات الحساسة من الصراع.

تظهر التجربة الروسية بعد عام 2020 مدى تطور القدرات السيبرانية من حيث التخطيط والتنفيذ والدمج مع العمليات العسكرية التقليدية وتكشف هذه التجربة أن روسيا تعتمد على منظومة رقمية تعتمد على الأساليب التقنية الحديثة والقدرات

الاستخبارية الواسعة وتؤكد المؤشرات أن موسكو ستواصل استثمارها في تطوير هذه القدرات بهدف الحفاظ على قدرتها في مواجهة التحديات المتصاعدة من الولايات المتحدة والاتحاد الأوروبي وتدل هذه التحولات على أن القدرات السيبرانية الروسية أصبحت جزءا من القوة الشاملة للدولة وعنصرا مركزيا في رسم سياستها الخارجية والأمنية خلال الفترة المقبلة.[12]

ثالثاً: الدور السيبراني الروسي في الحرب على أوكرانيا (2020–2025)

يتناول هذا المحور الدور السيبراني الروسي في الحرب على أوكرانيا بوصفه أحد المحاور المركزية في إدارة الصراع الهجين، حيث امتزجت فيه الهجمات الرقمية مع العمليات العسكرية التقليدية، ويسعى المبحث إلى تحليل طبيعة هذه الهجمات، وقطاعات الاستهداف، وأثرها في مسار الحرب وتوازنات الصراع بين روسيا وأوكرانيا والغرب.

1. الهجمات السيبرانية الروسية على البنية التحتية الأوكرانية

يركز هذا الموضوع على دراسة الهجمات السيبرانية الروسية التي استهدفت البنى التحتية الأوكرانية منذ 2020، باعتبارها أدوات لإرباك مؤسسات الدولة وإضعاف قدرتها على الصمود، كما يعالج المطلب أنماط الاستهداف الأكثر حساسية، مثل الطاقة والاتصالات والنقل والقطاع المالي، وتحولها إلى جزء أساسي من استراتيجية الحرب الهجينة.

أ. السياق العام لتصاعد الهجمات السيبرانية الروسية

شهدت المرحلة الممتدة من 2020 إلى ما بعد الغزو الروسي لأوكرانيا في شباط 2022 توسعا نوعيا وكثيفا في طبيعة الهجمات السيبرانية التي استهدفت الدولة الأوكرانية بمؤسساتها الحيوية المختلفة هذه الهجمات لم تكن مجرد نشاط رقمي

عابر، بل شكلت إحدى أهم الأدوات التي اعتمدت عليها موسكو في إدارة صراع طويل الأمد مع كييف، في ظل توتر جيوسياسي متصاعد الهجمات جاءت نتيجة تراكم خبرات روسية في ميدان الحرب السيبرانية منذ عام 2014 حين شهدت أوكرانيا أولى موجات الهجوم الرقمي التي استهدفت شبكات الطاقة والاتصالات ومع اقتراب 2022 اتخذت الهجمات طابعا تحضيريا، حيث تم تنفيذ عمليات تشويه واسعة ضد مواقع حكومية حساسة بما في ذلك مواقع وزارات الخارجية والدفاع والطاقة هذه العمليات حملت رسائل نفسية وسياسية تهدف إلى إضعاف ثقة المواطن الأوكراني بمؤسسات دولته وشل قدرة الأجهزة الحكومية على العمل في لحظات حرجة البيانات التي نشرتها فرق الاستجابة الأوكرانية للحوادث الرقمية تظهر أن عام 2022 وحده شهد أكثر من ألفي حادثة تم التعامل معها، وهي أرقام تعكس المدى الواسع للحرب السيبرانية التي تشنها موسكو.[13]

ب. الهجمات على الاتصالات والأقمار الصناعية وشبكات الإنترنت

استهداف شبكة الاتصالات الأوكرانية كان خطوة مركزية في العمليات السيبرانية الروسية، وهو ما ظهر بوضوح في الهجوم الذي ضرب شبكة KA-SAT التابعة لشركة Viasat في الساعات الأولى من الغزو في 24 شباط 2022 تسبب هذا الهجوم في تعطيل آلاف أجهزة المودم التي تعتمد عليها المؤسسات العسكرية والمدنية في الاتصال بالإنترنت وقد تبين لاحقا أن البرمجية التخريبية المستخدمة وهي من نوع wiper كانت قادرة على مسح الذاكرة الداخلية للأجهزة مما جعل إعادة تشغيلها أمرا مستحيلا من دون استبدال مكوناتها الأساسية هذا الهجوم كشف مدى إدراك موسكو لأهمية الاتصالات في إدارة الأزمات العسكرية إذ إن انقطاع الإنترنت أو ضعف الإشارة ينعكس مباشرة على قدرة القيادة العسكرية الأوكرانية على متابعة التطورات الميدانية تأثير الهجوم تخطى حدود أوكرانيا إذ سجلت عدة

دول أوروبية خللا في شبكات الطاقة وخصوصا في مزارع الرياح التي تعتمد على أجهزة مرتبطة بشبكةKA-SAT ، وهو ما أعطى مؤشرا واضحا على أن الهجمات الروسية ليست محصورة داخل الجغرافيا الأوكرانية بل تمتد إلى شبكات إقليمية ترتبط ببنية تحتية مشتركة.[14]

ج. الهجمات على شبكات الطاقة والبنى التحتية الصناعية

قطاع الطاقة ظل على الدوام أحد أهم الأهداف الاستراتيجية للهجمات السيبرانية الروسية، إذ يمثل شريان الحياة لأي دولة ويعد المساس به وسيلة فعالة لإحداث اضطراب شامل في المجتمع والاقتصاد والمؤسسات الحكومية التجربة التي مرت بها أوكرانيا في عام 2015 مع هجومBlackEnergy ، والذي أدى إلى انقطاع الكهرباء عن ما يقارب مئتي ألف مواطن، شكلت نقطة تحول بارزة في فهم خطورة القدرات الروسية في مجال استهداف أنظمة التحكم الصناعي هذا الهجوم لم يكن مجرد عمل تخريبي عابر، بل كان اختبارا مبكرا لقدرة موسكو على النفاذ إلى أعماق البنية التحتية للطاقة وإرباك منظومات التشغيل والرقابة من داخلها، مما وفر خبرة عملية استندت إليها روسيا في تطوير أدواتها اللاحقة.

بعد عام 2020 انتقل التركيز الروسي إلى مرحلة أكثر تقدما من خلال الاستثمار في تطوير برمجيات تخريبية مصممة خصيصا لاختراق أنظمة SCADA والتحكم بالأجهزة الحيوية داخل محطات الطاقة هذه الأنظمة تشكل العقل الإلكتروني الذي يدير العمليات الصناعية الحساسة مثل توزيع الكهرباء ومراقبة الجهد وتشغيل المحولات، لذلك فإن التحكم فيها أو تعطيلها يمكن أن يقود إلى انهيار جزئي أو كامل في شبكة الطاقة القدرة على اختراق هذه الأنظمة تمكن المهاجم من تنفيذ عمليات دقيقة قد تشمل إيقاف المحولات، أو زيادة الضغط على الشبكة، أو

التلاعب بأجهزة الحماية، ما يجعل الهجوم قادرا على التسبب بأضرار مادية تتجاوز مجرد تعطل رقمي مؤقت.[15]

ومع بدء الغزو الروسي الشامل لأوكرانيا في شباط 2022، أصبح استهداف قطاع الطاقة جزءا لا يتجزأ من استراتيجية هجومية مزدوجة تجمع بين الضربات الجوية والصاروخية التي تستهدف محطات التوليد وخطوط النقل، وبين هجمات سيبرانية تعمل على تعطيل أنظمة التحكم وتشويش عمليات الصيانة والاستجابة الطارئة هذا الدمج بين الهجومين التقليدي والرقمي يعكس الطابع الهجين للحرب الروسية التي لا تفصل بين الساحة الميدانية والفضاء السيبراني، بل تنظر إليهما كساحتين تكمل إحداهما الأخرى بهدف إضعاف قدرة الدولة الأوكرانية على الصمود والاستمرار.

محاولات تعطيل شبكات الكهرباء خلال موجات البرد القارس جاءت ذات تأثير مضاعف، إذ تعتمد نسبة كبيرة من الأسر الأوكرانية على التدفئة الكهربائية، ما يجعل أي خلل في الإمداد تهديدا مباشرا للحياة اليومية النجاح الجزئي لبعض الهجمات أحدث حالة من الضغط الاجتماعي في عدة مدن، وخلق تحديات أمام أجهزة الطوارئ التي اضطرت إلى العمل في ظروف تتسم بانقطاع الاتصالات وضعف القدرة على إعادة تشغيل الأنظمة المتضررة بسرعة هذا الوضع كشف أن الهجمات السيبرانية ليست مجرد وسيلة لإضعاف القدرات العسكرية، بل أداة لإرهاق المجتمع وإضعاف معنويات السكان وإحداث شرخ نفسي ينعكس على قدرة الدولة على إدارة الحرب.[16]

استمرار الهجمات السيبرانية على أنظمة الطاقة بالتزامن مع العمليات العسكرية التقليدية قدم دليلا قاطعا على تمسك روسيا بنموذج الحرب الهجينة، وهو نموذج يقوم على استخدام أدوات متعددة ومتزامنة لتحقيق التأثير الأكبر بأقل التكاليف هذا النموذج يعامل الفضاء السيبراني كامتداد طبيعي للميدان العسكري، ويستفيد من

قدرة الهجمات الرقمية على اختراق الأعماق التقنية للبنى التحتية دون الحاجة إلى تدمير مادي واسع ومن خلال هذا المزج بين القوة الصلبة والقوة الرقمية، سعت روسيا إلى تعظيم أثر عملياتها وإرباك الجهاز الإداري الأوكراني وتقليص قدرة الدولة على الحفاظ على سير الخدمات الأساسية في وقت الحرب.

د. استهداف أنظمة النقل والسكك الحديدية والمطارات

استهداف أنظمة النقل والسكك الحديدية والمطارات مثل أحد المحاور الحيوية في العمليات السيبرانية الروسية، نظرا للأهمية الاستراتيجية التي اكتسبتها شبكات النقل داخل أوكرانيا منذ الأيام الأولى للحرب فقد أصبحت السكك الحديدية شريان الحياة بالنسبة للدولة الأوكرانية، إذ اعتمدت عليها الحكومة في عمليات إجلاء ملايين المدنيين من مناطق الاشتباك، وفي الوقت نفسه اعتمد الجيش عليها في نقل الإمدادات العسكرية والذخائر والوقود والمعدات اللوجستية بين الجبهات المختلفة هذا الدور المزدوج جعل القطاع هدفا ذا قيمة عالية في الحسابات الروسية، لأن أي خلل في حركة القطارات أو منظومات التحكم يمكن أن يؤدي إلى إبطاء العمليات العسكرية وإحداث تكدس بشري يزيد من الضغط على الدولة والمجتمع.

التركيز الروسي انصب على أنظمة الحجز الإلكتروني وأنظمة الإشارات والتحكم المركزية، لأنها تمثل نقاطا حساسة يعتمد عليها المشغلون في إدارة حركة القطارات وضمان سلامة المسارات وكانت هذه الأنظمة عرضة لمحاولات اختراق متكررة هدفت إلى تشويش البيانات وتعطيل لوحات التحكم وإرباك التوجيهات التي تصدر إلى المحطات المنتشرة على طول الشبكة وتركزت الهجمات على نقاط الضعف في التطبيقات المستخدمة لإدارة الرحلات وأنظمة الاتصالات بين المحطات ومراكز القيادة ورغم أن الدفاعات السيبرانية الأوكرانية المدعومة بخبرات غربية نجحت في

إحباط العديد من هذه العمليات، إلا أن استمرار المحاولات أثبت تصميم الجانب الروسي على جعل قطاع النقل أحد ميادين الضغط المتواصلة.[17]

ان الهجمات لم تقتصر على السكك الحديدية، بل طالت أيضا أنظمة المطارات التي تمثل مراكز حساسة للحركة الجوية والمدنية تناولت المحاولات الروسية منصات إدارة الرحلات وبرامج مراقبة الحركة الجوية وبعض الأنظمة التكميلية المستخدمة في تسجيل المسافرين وإدارة البيانات اللوجستية الهدف كان مضاعفا، فمن جهة أرادت موسكو إضعاف القدرات اللوجستية للدولة التي تعتمد على الطيران لنقل المعدات الحساسة والكوادر العسكرية، ومن جهة أخرى سعت إلى خلق حالة من القلق لدى المدنيين عبر إظهار المطارات غير آمنة من الناحية الرقمية وتعطيل هذه الأنظمة ولو لساعات قد يؤدي إلى فوضى واسعة داخل محطات الطيران، ما يفرض ضغوطا اقتصادية ونفسية كبيرة على الدولة في وقت تحتاج فيه إلى تنظيم عملياتها الداخلية بأقصى قدر من الانضباط، وتكشف طبيعة الهجمات عن محاولة روسية لاستهداف العمود الفقري للحياة اليومية في أوكرانيا، إذ إن تعطيل النقل يعني شل الحركة الاقتصادية وتعطيل الإمدادات التجارية، كما يعني زيادة الضغط على مؤسسات الدولة المسؤولة عن إدارة الأزمة ويتجاوز التأثير الجانب اللوجستي ليشمل البعد الاجتماعي، لأن المواطنين الذين يعتمدون على القطارات والمطارات يشعرون بعدم الأمان عندما تتعرض هذه البنية الحيوية لمحاولات اختراق متكررة في ظل الحرب، يؤثر هذا الإحساس في الروح المعنوية العامة ويضعف ثقة المجتمع بقدرة الحكومة على ضمان استمرار الخدمات الأساسية.[18]

وتبين المعطيات الميدانية أن عامي 2023 و2024 شهدا موجة متجددة من الهجمات التي اتسمت بالتكرار والتنوع، ما يعكس وجود استراتيجية روسية تهدف

إلى الضغط على أوكرانيا بوسائل غير مباشرة واستمرار هذا النوع من الاستهداف يكشف أن روسيا تنظر إلى قطاع النقل بوصفه جزءا من المعركة الشاملة، حيث يمكن للهجمات السيبرانية أن تؤدي إلى نتائج عملياتية مؤثرة من دون الحاجة إلى ضربات عسكرية مباشرة كما أن استهداف هذا القطاع يساهم في استنزاف الموارد الأوكرانية عبر إجبارها على تخصيص ميزانيات كبيرة للترميم والتأمين الرقمي والتدريب المستمر للكوادر التقنية.

هـ. الهجمات على المؤسسات الحكومية والقطاع المالي

المؤسسات الحكومية الأوكرانية شكلت محورا ثابتا في الاستهداف السيبراني الروسي، إذ تعرضت خلال السنوات الأخيرة لموجات متلاحقة من الهجمات التي لم تقتصر على التشويه الرقمي أو تعطيل الخوادم، بل امتدت إلى عمليات دقيقة لمسح المحتوى وتخريب قواعد البيانات وحرمان الموظفين من الوصول إلى الأنظمة التشغيلية الأساسية هذه الهجمات كانت تهدف إلى تقويض صورة الدولة من الداخل عبر إظهار هياكلها المؤسسية وكأنها عاجزة عن حماية فضائها المعلوماتي أو تأمين استمرارية خدماتها العامة وتكمن خطورة هذه العمليات في أنها استهدفت صميم عمل الوزارات والهيئات التي تعتمد اعتمادا مباشرا على النظم الرقمية في إدارة الوثائق الرسمية، وتنظيم البيانات المركزية، وتشغيل منظومات المراسلات الإلكترونية التي تعد العمود الفقري للحوكمة الحديثة في أوكرانيا.[19]

تصاعد مستوى التخريب في الأيام الأولى للغزو الروسي حيث وجدت المؤسسات الحكومية نفسها في مواجهة هجمات متزامنة شملت مسح البيانات وإيقاف الخوادم وإرباك حركة الاتصالات الداخلية هذا الواقع خلق تحديا مضاعفا لأن تعطيل الأنظمة الحكومية في اللحظات الحرجة يعني إضعاف القدرة على اتخاذ القرار وإبطاء سرعة الاستجابة وإرباك التنسيق بين السلطات المدنية

والعسكرية كما أن استهداف منصات الخدمات العامة مثل أنظمة الجوازات والضرائب والسجلات الرسمية أثر في ثقة المواطنين بإمكان استمرار الدولة في أداء مهامها خلال الحرب.[20]

القطاع المالي لم يكن بمنأى عن هذا الاستهداف لأنه يمثل أحد الأعمدة الحساسة للاقتصاد الوطني تعرضت البنوك الأوكرانية لهجمات حرمان من الخدمة استهدفت قدراتها التشغيلية وأثرت في أنظمة الدفع الإلكتروني والتحويلات المالية وخدمات الصرافة عبر التطبيقات الرقمية هذه العمليات أحدثت اختناقات واضحة في المعاملات اليومية للمواطنين والشركات وخلقت حالة من الارتباك في السوق المالية بسبب تعطل عمليات الدفع والتحويل، وهي عناصر ترتبط مباشرة بالقدرة الاقتصادية للأفراد والمؤسسات خلال فترات الأزمات، تتضاعف خطورة هذه الهجمات لأنها لا تؤثر فقط في الوظائف التقنية للبنوك بل تمتد إلى البعد النفسي والاجتماعي عبر خلق شعور بعدم اليقين لدى المواطنين الذين يعتمدون على التطبيقات المصرفية للوصول إلى أرصدتهم ودفع التزاماتهم واستلام رواتبهم أي خلل في هذه الأنظمة يفسر فورا على أنه مؤشر على ضعف قدرة الدولة على حماية النظام المالي وقد يمهد لاضطرابات اقتصادية أوسع لذلك استهدف الروس هذا القطاع على نحو ممنهج بهدف إضعاف الاستقرار النقدي والتأثير في معنويات السكان وإرباك المجهود الحربي للدولة من خلال الضغط على محركاتها المالية والاقتصادية.[21]

و. استهداف الإعلام وفضاء المعلومات

الحرب السيبرانية الروسية لم تتوقف عند حدود الهجمات التقنية التقليدية التي تستهدف الخوادم والأنظمة التشغيلية، بل تحولت إلى حرب معلوماتية شاملة تستهدف العقل الجمعي للمجتمع الأوكراني فقد واجهت المؤسسات الإعلامية

الأوكرانية موجات متتابعة من الهجمات التخريبية التي أصابت خوادم البث ومنصات إدارة المحتوى وأوقفت بعض الخدمات الإعلامية لفترات تراوحت بين الساعات والأيام هذه الهجمات لم تكن مجرد محاولة لتعطيل عمليات النشر بل جاءت في إطار استراتيجية تهدف إلى التحكم بمجرى المعلومات وإعادة صياغة البيئة الإعلامية لصالح الرواية الروسية في لحظات حساسة من الصراع،[22] ان العمليات الروسية اعتمدت على مبدأ "السيطرة على السرد" وذلك عبر استهداف وسائل الإعلام المسموعة والمرئية والمنصات الرقمية، بالتزامن مع إطلاق حملات تضليل نشطة على مواقع التواصل الاجتماعي المجموعات المرتبطة بالاستخبارات العسكرية الروسية وظفت شبكات واسعة من الحسابات الآلية التي تعمل على نشر أخبار مزيفة ومحتوى محرف يسعى إلى خلق حالة من القلق والتشويش داخل المجتمع هدف هذه الحملات كان بث مشاعر الخوف والشك وزعزعة ثقة المواطنين بقدرة الحكومة على إدارة العمليات العسكرية وتقديم الحماية اللازمة في أوقات الأزمة.

توسع الحرب المعلوماتية لم يكن منفصلا عن طبيعة العمليات القتالية على الأرض، بل تزامنت حملات التشويه والتضليل مع لحظات التصعيد الميداني، ما منحها تأثيرا مضاعفا التأثير على إدراك الجمهور الأوكراني لطبيعة الحرب ومساراتها أصبح جزءا من معركة الوعي التي تراهن عليها روسيا لإضعاف الروح المعنوية للسكان وإرباك آليات التواصل بين المجتمع والمؤسسات الرسمية كذلك يعد التأثير في الرأي العام الدولي هدفا مركزيا من خلال نشر روايات بديلة تسعى إلى تقليل الدعم السياسي والعسكري الذي تتلقاه أوكرانيا من شركائها الغربيين، هذه الحرب المعلوماتية تشكل امتدادا طبيعيا للعقيدة الروسية في "الحرب الهجينة" التي تدمج بين القوة العسكرية والعمليات النفسية والحملات الدعائية وهي عقيدة تنظر

إلى الوعي كأرض معركة، ترى فيها السيطرة على التدفق المعلوماتي شرطا لنجاح العمليات التقليدية لذلك جاءت الهجمات على وسائل الإعلام الأوكرانية ضمن نهج متكامل يعمل على تشتيت الانتباه العام وتقويض الثقة المؤسسية وإضعاف الحاضنة الاجتماعية للدولة وفي ظل الطبيعة المتسارعة للمعلومات في البيئة الرقمية أصبحت هذه العمليات أحد العناصر التي تسهم في إطالة أمد الصراع وصياغة صورة الحرب لدى المتلقين داخل أوكرانيا وخارجها.[23]

ز. تصاعد ديناميات الهجوم وأهميته الاستراتيجية

تصاعد الهجمات السيبرانية بعد 2022 يعكس تحول الفضاء الرقمي إلى أداة استنزاف مستمرة التقارير الرسمية تشير إلى ارتفاع كبير في عدد الحوادث الموثقة خلال عامي 2023 و2024 هذا التزايد المستمر يوضح أن روسيا تعتمد استراتيجية طويلة المدى للتأثير في بنية الدولة الأوكرانية وتعطيل وظائفها الأساسية كما أن التطور المستمر في الأدوات المستخدمة يظهر قدرة موسكو على تعديل تكتيكاتها بسرعة مع وجود دعم استخباري وتقني منظم الهجمات الروسية تتسم بثلاثة خصائص مهمة هي التكامل مع العمل العسكري، والاستمرارية عبر الزمن، وتنوع الأدوات الرقمية المستخدمة هذه الخصائص تجعل مواجهة هذه الهجمات عملية معقدة تتطلب قدرات دفاعية هائلة وتعاونا دوليا واسعا.[24]

تظهر دراسة الهجمات السيبرانية الروسية على البنية التحتية الأوكرانية أن موسكو نجحت في بناء نموذج متكامل للحرب الرقمية يعتمد على التخريب والاختراق والتشويش والتضليل كما أثبتت الحرب أن الفضاء السيبراني أصبح جزءا جوهريا من إدارة الصراعات وأنه قادر على التأثير في المجتمع والاقتصاد والقدرات العسكرية للدولة المستهدفة التجربة الأوكرانية كشفت في الوقت نفسه أن الدفاع

السيبراني الحديث قادر على امتصاص كثير من هذه الهجمات حين تتوفر القدرة التقنية والدعم الدولي.

رابعاً: أثر القدرات السيبرانية الروسية في مخرجات الحرب وتوازنات الصراع

يمثل أثر القدرات السيبرانية الروسية في مخرجات الحرب وتوازنات الصراع أحد أهم الأبعاد الجديدة في فهم الحرب الروسية الأوكرانية بوصفها حالة نموذجية للحرب الهجينة تطور استخدام موسكو للأدوات السيبرانية جعل الفضاء الرقمي ساحة مكملة لساحة القتال التقليدي، لكنه في الوقت نفسه كشف حدود القوة السيبرانية وعدم قدرتها حتى الآن على حسم الحرب وحدها لذلك يصبح تحليل هذا الأثر بحاجة إلى مقاربة مركبة تربط بين ما حققته روسيا من مكاسب عبر الفضاء السيبراني وبين ما أخفقت فيه، وكيف انعكس ذلك على توازن القوى بين الطرفين وعلى شكل التفاعل بين روسيا والغرب.[25]

تظهر الدراسات التحليلية الكبرى، مثل تقرير مركز الدراسات الاستراتيجية والدولية حول العمليات السيبرانية في الحرب الروسية الأوكرانية، أن الهجمات الروسية لعبت دورا واضحا في إرباك مؤسسات الدولة الأوكرانية وإضعاف بعض قدراتها، لكنها لم تصل إلى مستوى "السلاح الحاسم" الذي يفرض على كييف تقديم تنازلات استراتيجية أو يغير مسار الحرب وحده التقرير يشير إلى أن معظم الهجمات الروسية بقيت في مستوى إعاقة الوظائف وتعطيل الشبكات واستهداف البنية التحتية الحيوية عبر عمليات تخريب من نوعwiper ، دون أن تقترن بنتائج مادية كارثية طويلة الأمد على غرار ما كان متوقعا نظريا من "شل الدولة بالكامل"، في المقابل أظهرت تقارير مايكروسوفت ومركز الأمن السيبراني الكندي أن روسيا استخدمت القدرات السيبرانية كوسيلة متواصلة لـ"الإضعاف التراكمي" أكثر

من كونها أداة لضربة قاضية هذه العمليات استهدفت تعطيل أو تشويه أو تدمير أو النيل من مصداقية المؤسسات الحكومية والعسكرية والاقتصادية الأوكرانية، وتأمين موطئ قدم داخل البنى التحتية الحرجة، إلى جانب حملات تأثير تستهدف الرأي العام في أوكرانيا والغرب، هذا النهج جعل الفضاء السيبراني مجالا لإدامة الضغط وإرباك الخصم بدلا من حسم الصراع بسرعة، ما ينسجم مع تصور روسي أوسع عن الحرب طويلة الأمد وحرب الاستنزاف الشاملة.[26]

أحد أهم التأثيرات المباشرة لهذه القدرات ظهر في الأيام الأولى للغزو عبر الهجوم على شبكة KA-SAT التابعة لشركةViasat ، والذي عطل آلاف أجهزة المودم المستخدمة في الاتصالات الحكومية والعسكرية والمدنية في أوكرانيا وأجزاء من أوروبا الهجوم استخدم برمجية "AcidRain" لمسح مكونات الأجهزة وجعلها غير صالحة للعمل، وهو ما أثر في قدرة أوكرانيا على التواصل في لحظة حرجة جدا من الصراع، كما كشف للأوروبيين حجم التداخل بين أمنهم السيبراني وأمن أوكرانيا، بهذا المعنى أسهمت القدرات السيبرانية الروسية في توسيع نطاق المعركة جغرافيا ونفسيا، لأنها جعلت الدول الأوروبية تدرك أن بنية الاتصالات والطاقة لديها ليست بعيدة عن ميدان الصراع، مع ذلك تكشف تقارير CERT-EU والاتحاد الأوروبي أن هذه الهجمات لم تتمكن من تحطيم قدرة الدولة الأوكرانية على الصمود أوكرانيا، بدعم مباشر من شركات التكنولوجيا الغربية ومراكز الأمن السيبراني في الاتحاد الأوروبي، نجحت في احتواء كثير من الهجمات وتقليل آثارها، كما استفادت من نقل بياناتها الحكومية إلى الحوسبة السحابية في دول حليفة، وهو ما عزز من مرونتها الرقمية وحد من قدرة روسيا على إحداث شلل شامل في المنظومة الإدارية للدولة.[27]

هذا التفاعل يؤشر إلى أن ميزان الصراع السيبراني لا تحدده قدرات المهاجم فقط بل يرتبط أيضا بقدرات الدفاع والتحالفات التقنية العابرة للحدود، وعلى مستوى مخرجات الحرب، يمكن القول إن القدرات السيبرانية الروسية أسهمت في رفع كلفة الصراع على أوكرانيا من خلال استهداف البنى التحتية للطاقة والاتصالات والقطاع المالي، لكنها لم تترجم إلى مكاسب استراتيجية حاسمة لروسيا دراسات مثل تقرير CSISعن "العمليات السيبرانية خلال الحرب الروسية الأوكرانية" وتقرير CNA عن الحرب المعلوماتية تشير إلى أن أي تغيير في خطوط الجبهة أو السيطرة الميدانية كان نتيجة للعوامل التقليدية بشكل أساسي، مثل التفوق المدفعي، والدعم العسكري الغربي، والقدرة على التعبئة، أكثر مما كان نتيجة مباشرة لهجمة سيبرانية محددة بمعنى آخر لعب الفضاء السيبراني دور "مسانِد" يعزز أداء العمليات التقليدية لكنه لم يتحول إلى أداة مستقلة لصناعة النصر.

مع ذلك كان لهذه القدرات أثر مهم في توازنات الصراع الأوسع بين روسيا والغرب الهجمات السيبرانية لم تستهدف أوكرانيا وحدها بل امتدت إلى دول حلف الناتو والاتحاد الأوروبي عبر حملات تجسس وهجمات على أحزاب حاكمة ووزارات دفاع وقطاعات تكنولوجية، كما في حالة الهجوم المنسوب لـ APT28على البنية الرقمية للحزب الحاكم في ألمانيا عام 2023 هذه الوقائع دفعت الدول الغربية إلى اعتبار الأنشطة السيبرانية الروسية جزءا من تهديد شامل للنظام الليبرالي الأوروبي، وعززت من توجهات تعزيز الدفاعات السيبرانية وتعميق التعاون الاستخباري داخل الناتو والاتحاد الأوروبي ، إلى جانب ذلك ساهمت الحرب السيبرانية في إعادة تعريف أدوار الفاعلين غير الحكوميين في الصراع مايكروسوفت وشركات تكنولوجيا أخرى لعبت دورا واضحا في الدفاع عن أوكرانيا عبر توفير بنى سحابية بديلة وتحليلات استخبارية عن أنماط الهجمات الروسية تقارير مايكروسوفت حول

"الدفاع عن أوكرانيا" و"عام من الحرب الهجينة" توضح أن شركات القطاع الخاص أصبحت جزءا عضويا من المعادلة الاستراتيجية، ما أضاف بعدا جديدا إلى توازنات القوة حيث لم يعد الصراع محصورا بين دول بل يشمل شبكات وشركات ومنظمات تعمل في فضاء عابر للحدود .[28]

على مستوى توازنات الردع، أظهرت الحرب أن روسيا رغم امتلاكها ترسانة سيبرانية متقدمة، مقيدة بعدة اعتبارات الاستخدام المفرط أو غير المنضبط لهجمات ذات أثر مدمر على البنى التحتية الغربية يمكن أن يستجلب ردودا قوية ويشرعن هجمات مضادة من دول الناتو لذلك يبدو أن موسكو تعاملت مع القدرات السيبرانية كأداة "تصعيد مضبوط" تهدف إلى الإرباك والضغط دون الوصول إلى عتبة تدفع الحلف إلى رد جماعي واسع هذا السلوك عزز الإطار المفاهيمي الذي يرى في الفضاء السيبراني مجالا تمارس فيه لعبة "العتبات الرمادية" حيث تسعى الدول إلى تحقيق مكاسب دون تجاوز خطوط حمراء استراتيجية، من جهة أخرى، أدت محدودية الأثر الحاسم للهجمات السيبرانية الروسية إلى مراجعة واسعة لدى الخبراء الغربيين لتصور "بيرل هاربور السيبراني" كثير من الدراسات التي حللت مجريات الحرب اعتبرت أن التوقعات السابقة بدولة تنهار رقميا في أول أيام الصراع لم تتحقق، وأن المرونة الرقمية الأوكرانية بدعم غربي شكلت عاملا موازنا، وهذا لا يعني التقليل من خطورة القدرات الروسية بل الإشارة إلى أن الصمود السيبراني والتحالفات التقنية يمكن أن تقلل كثيرا من أثر هذه القدرات في مخرجات الحرب.[29]

في المحصلة يمكن القول إن القدرات السيبرانية الروسية أثرت في مخرجات الحرب على مستويين: الأول مباشر من خلال رفع كلفة الصمود الأوكراني وإرباك مؤسسات الدولة واستهداف البنى التحتية، والثاني غير مباشر من خلال دفع الغرب إلى تعزيز دعمه التقني والعسكري لكييف وتوسيع جبهة الردع السيبراني ضد

موسكو هذه القدرات لم تحدث انقلابا استراتيجيا في ميزان الصراع لكنها أصبحت جزءا لا يتجزأ من منظومة القوة الروسية وأحد العناصر التي ستستمر في تشكيل توازنات الصراع بين روسيا وأوكرانيا وبين موسكو والغرب في الأمد المتوسط والبعيد.

الخاتمة

تُظهر الدراسة أن القدرات السيبرانية لم تعد مجرد ملحق تقني في بنية القوة الوطنية، بل تحولت إلى أحد أعمدتها المركزية في القرن الحادي والعشرين، فالفضاء الإلكتروني بات ميداناً كاملاً للصراع تتقاطع فيه الأبعاد العسكرية والسياسية والاقتصادية والمجتمعية، وأصبح من الصعب فهم ديناميات القوة والردع في النظام الدولي المعاصر من دون إدراك طبيعة هذه القدرات وحدودها وإمكاناتها، وقد بيّن الإطار المفاهيمي أن القدرات السيبرانية ليست مجرد أدوات اختراق وبرمجيات خبيثة، بل هي منظومة متكاملة تشمل البنية التحتية الرقمية، والمؤسسات الاستخبارية والعسكرية، والأطر القانونية والتنظيمية، والموارد البشرية المؤهلة، وأن هذا التعقيد جعل منها أحد أهم مؤشرات القوة الذكية التي تمزج بين الصلبة والناعمة في آن واحد.

أما في الحالة الروسية فقد برهنت الدراسة أن موسكو نجحت في بناء هيكل مؤسسي واستخباري وتقني متقدم للعمليات السيبرانية يقوم على تداخل أدوار أجهزة الاستخبارات العسكرية والأمنية والخارجية مع وحدات الحرب الإلكترونية والبنى البحثية والأكاديمية، هذا الهيكل مكّن روسيا من تنفيذ عمليات هجومية ودفاعية واسعة النطاق ظهرت بوضوح في استهداف البنى التحتية الأوكرانية منذ عام 2020 ولا سيما قطاعات الطاقة والاتصالات والنقل والمؤسسات الحكومية والقطاع المالي وفضاء المعلومات، وقد تميز هذا الدور بطابعه الهجين حيث جرى دمج

الضربات الرقمية مع الضربات العسكرية التقليدية وحملات التأثير المعلوماتي في إطار استراتيجية استنزاف بعيدة المدى تهدف إلى إضعاف قدرة الدولة الأوكرانية على الصمود وإرباك شبكاتها الحيوية والمؤسسية والمجتمعية.

مع ذلك تكشف نتائج البحث أن القدرات السيبرانية الروسية على الرغم من تأثيرها الواضح في رفع كلفة الصراع وتعقيد بيئة عمل الدولة الأوكرانية، لم ترتقِ إلى مستوى الأداة الحاسمة القادرة وحدها على تغيير مخرجات الحرب أو فرض تسوية استراتيجية على كييف وحلفائها، فقد أظهرت التجربة أن فعالية الهجمات السيبرانية تظل مشروطة بمستوى الجاهزية الدفاعية والقدرة على بناء تحالفات تقنية عابرة للحدود وهو ما استفادت منه أوكرانيا عبر الدعم الغربي والسحابة الرقمية والبنى الدفاعية المشتركة، وبذلك تؤكد الحرب الروسية الأوكرانية أن الفضاء السيبراني أصبح ركناً بنيوياً في توازنات الصراع وتشكيل معادلات الردع، لكنه يعمل في الغالب كعنصر مساند ومضاعِف للقوة أكثر من كونه بديلاً كاملاً عن أدوات القوة التقليدية، مع ما يفتحه ذلك من أسئلة نظرية وعملية حول مستقبل الحروب وبُنى الأمن القومي للدول.

الاستنتاجات

1. يتضح من الإطار المفاهيمي والتحليل التطبيقي أن القدرات السيبرانية أصبحت عنصراً مركزياً في قياس القوة الشاملة للدول، إلى جانب القدرات العسكرية والاقتصادية والدبلوماسية، وأنها انتقلت من الهامش الفني إلى قلب الحسابات الاستراتيجية والردعية.
2. أظهرت الدراسة أن روسيا دمجت بين القوة التقليدية والقدرات السيبرانية وحملات المعلومات والعمليات النفسية، ما جعل الفضاء السيبراني جزءاً لا يتجزأ من إدارة

المعركة على المستويين العملياتي والاستراتيجي، خصوصاً في استهداف الطاقة والاتصالات والنقل والمؤسسات الحكومية.

3. البنية المؤسسية والاستخبارية الروسية هي عامل حاسم في فاعلية الهجمات السيبرانية

بيّن تحليل دور GRU و FSBو SVR ووحدات الحرب الإلكترونية والأكاديميات العسكرية أن قوة روسيا السيبرانية لا تقوم على الأدوات التقنية وحدها بل على شبكة مؤسساتية واستخبارية متماسكة قادرة على التخطيط والتنفيذ والتنسيق عبر مستويات متعددة.

4. كشفت الدراسة عن انتقال واضح نحو استخدام أدوات متقدمة مثل استغلال سلاسل التوريد البرمجية، والبرمجيات التخريبية الموجهة ضد أنظمة SCADA، وتوظيف الذكاء الاصطناعي في الهجوم والدفاع، ما عزز قدرة موسكو على إحداث اختراقات عميقة وبعيدة الأثر.

5. الهجمات السيبرانية الروسية رفعت كلفة الصمود الأوكراني دون أن تحسم المعركة

أظهر تحليل استهداف البنى التحتية الحيوية أن هذه الهجمات ساهمت في إرهاق المجتمع الأوكراني وإرباك المؤسسات وخلق ضغط نفسي واقتصادي، لكنها لم تؤد إلى شلل كامل للدولة ولم تستطع تغيير موازين القوى الميدانية بصورة حاسمة.

6. بيّنت التجربة الأوكرانية أن بناء منظومات دفاعية مرنة، ونقل البيانات إلى السحابة، والاستفادة من دعم شركات التكنولوجيا الغربية والمؤسسات الأوروبية، ساهم في امتصاص جانب كبير من الأثر التدميري للهجمات الروسية ما يؤكد أن توازن الصراع السيبراني ليس أحادياً.

7. أظهر البحث أن الهجمات التي طالت دول الناتو والاتحاد الأوروبي، والضغط على البنى التحتية العابرة للحدود، أدت إلى إعادة تعريف التهديد الروسي في الوعي الاستراتيجي الغربي، وعجّلت في بناء أطر دفاع سيبراني جماعي وتعميق التعاون الاستخباري داخل الفضاء الأوروبي الأطلسي.

التوصيات

1. توصي الدراسة بأن تقوم الدول خاصة المنخرطة أو المعرّضة لصراعات إقليمية، بصياغة استراتيجيات سيبرانية واضحة ترتبط مباشرة بمنظومة الأمن القومي والعقيدة العسكرية، بحيث تُحدَّد فيها الأهداف والأدوار والأولويات الدفاعية والهجومية ضمن إطار قانوني وسياسي منضبط.
2. من الضروري إنشاء وحدات وقيادات سيبرانية دائمة داخل الجيوش مع تطوير أجهزة استخبارات إلكترونية محترفة، وبناء قنوات تنسيق بين المؤسسات الأمنية والعسكرية والهيئات المدنية، مع الحفاظ على الرقابة التشريعية لمنع الانزلاق نحو الاستخدام الداخلي التعسفي.
3. توصي الدراسة بإعطاء أولوية قصوى لتأمين قطاعات الطاقة والاتصالات والمصارف والنقل والمؤسسات الحكومية، من خلال تدقيق مستمر للثغرات، وتحديث أنظمة الحماية، واعتماد خطط استمرارية العمل وخطط الطوارئ الرقمية، وربط ذلك بتمارين دورية لمحاكاة الأزمات السيبرانية.
4. تحتاج الدول إلى توسيع برامج إعداد الكوادر في مجالات أمن المعلومات والهندسة الحاسوبية والذكاء الاصطناعي والحرب الإلكترونية، ودعم الجامعات والمراكز البحثية لبناء قاعدة معرفية وطنية قادرة على تطوير أدواتها الخاصة بدلاً من الاعتماد الكامل على الخارج.

5. تبين من التجربة الأوكرانية أن التعاون مع شركات التكنولوجيا العالمية والمؤسسات الأوروبية والأطلسية كان عاملاً حاسماً في تعزيز الصمود السيبراني، لذا تُوصي الدراسة ببناء تحالفات تقنية إقليمية ودولية، وتفعيل آليات تبادل المعلومات الاستخبارية والتحذيرات المبكرة.
6. في ظل تصاعد الهجمات العابرة للحدود، ينبغي الدفع باتجاه وضع قواعد دولية تضبط سلوك الدول في الفضاء السيبراني، وتعرّف الخطوط الحمراء في استهداف البنى المدنية، وتطوّر آليات للمساءلة، بما يحد من مخاطر الانفلات ويقلل احتمالات التصعيد غير المقصود.
7. توصي الدراسة بتوسيع نطاق البحث العلمي ليشمل تحليل قابلية الدول الصغيرة والمتوسطة للتأثر بالحروب السيبرانية بين القوى الكبرى، واستشراف سيناريوهات انتقال العدوى الرقمية إلى بيئات هشة، ووضع سياسات وقائية تساعد هذه الدول على بناء حد أدنى من المناعة السيبرانية في مواجهة صراعات لا تشارك فيها مباشرة.

الهوامش

[11] آية رجب أبواليزيد، العمليات السيبرانية بين روسيا وأوكرانيا: قراءة في الأسباب والنتائج، المركز الديمقراطي العربي، برلين، 2024، ص 12. عبد الله الشامسي، "الانعكاسات الأمنية للحرب الروسية الأوكرانية"، مجلة رؤى استراتيجية، العدد (17)، مركز رؤى استراتيجية، أبوظبي، 2023، ص29.

[2] Mark Galeotti, Putin’s Hydra: Inside the Russian Intelligence Services, London: European Council on Foreign Relations (ECFR), United Kingdom, 2016، ص 10–15.

[3] عبد المنعم علي، *تكتيكات متبادلة: حدود تأثير العمليات السيبرانية في الحرب الروسية الأوكرانية*، مركز المستقبل للأبحاث والدراسات المتقدمة، أبوظبي، 2024، ص 18.

[5] نبيل عودة، *الحرب السيبرانية الركيزة الأولى في بنية الحرب الهجينة الروسية: حرب أوكرانيا نموذجاً*، المركز الأوروبي للدراسات الاستراتيجية والاستخبارات، برلين، 2022، ص 27.

[6] ليونيد سافين، *أوكرانيا والحرب السيبرانية*، مركز الدراسات العربية الأوراسية، إسطنبول، 2022، ص 33.

[7] مسعد نجاح؛ أحمد جلال محمود؛ إيمان نور الدين الشامي، *الحرب السيبرانية الروسية على أوكرانيا: التداعيات والتدابير الوقائية*، مجلة الدراسات السياسية والاقتصادية، كلية الاقتصاد والعلوم السياسية، جامعة القاهرة، المجلد 5، العدد 1، 2025، ص 41.

[8] Canadian Centre for Cyber Security, *Cyber Threat Activity Related to the Russian Invasion of Ukraine*, Government of Canada, Ottawa, 2022, p. 11.

[9] CERT-EU, Russia's War on Ukraine: One Year of Cyber Operations (TLP-CLEAR-CERT-EU-1YUA-CyberOps), European Union CERT, Brussels, 2023, p. 29.

[10] زيد العظم، "أوكرانيا وسياقات الصراع الروسي"، ط1، مركز كارنيغي للشرق الأوسط، بيروت، 2022، ص34.

[11] Institute of Cyber Warfare Research & National Coordination Center for Cybersecurity of Ukraine, Cybersecurity Threat Landscape of Ukraine in 2023, Kyiv, 2024, p. 38.

[12] طارق بن محمد الجهني، واقع استخدام تطبيقات الميتافيرس في تطوير قطاع الفضاء، وقائع المؤتمر العلمي الدولي الرابع عشر "رؤى معاصرة: التطورات الحديثة في العلوم الإنسانية والاجتماعية والطبيعية، شبكة المؤتمرات العربية، إسطنبول، 2024، ص3.

[13] عصام عبد الشافي، الحرب الروسية- الأوكرانية ومستقبل النظام الدولي، العدد 14، مجلة لباب للدراسات الاستراتيجية والإعلامية، مركز الجزيرة للدراسات، الدوحة، 3 أيار 2022، ص113.

[14] حسام إبراهيم واخرون، الحرب الروسية- الأوكرانية عودة الصراعات الكبرى بين القوى الدولية، ط1، مركز المستقبل للأبحاث والدراسات المتقدمة، أبو ظبي، 2023، ص51.

[15] أحمد السيد وآية عبد العزيز، إدارة حرب أوكرانيا بين شخصيتي "بوتين" و "زيلينسكي"، العدد 38، تقديرات مصرية، المركز المصري للفكر والدراسات الاستراتيجية، القاهرة، مصر، اذار 2022، ص23.

[16] العمليات العسكرية الروسية في أوكرانيا (الأسباب والأهداف والنتائج)، مقالة حمورابي، مركز حمورابي للبحوث والدراسات الاستراتيجية، بغداد، 25 شباط 2022، ص123.

[17] الشيماء عرفات، السرديات التاريخية والجغرافية للحرب الروسية في أوكرانيا، العدد 38، تقديرات مصرية، المركز المصري للفكر والدراسات الاستراتيجية، القاهرة، مصر، 2022، ص14.

[18] أحمد دهشان، مواجهة مؤجلة منذ ثلاثة عقود روسيا الولايات المتحدة الامريكية الناتو، أبحاث ودراسات، مركز الدراسات العربية الأوراسية، مصر، 20 كانون الثاني 2022، ص15.

[19] مسيرة الحرب الروسية الأوكرانية منذ انطلاق الحرب 24 فبراير/ شباط حتى 26 إبريل/ نيسان 2022، مقالات، مركز الخطابي للدراسات، سوريا، 2022، ص33.

[20] Pavel Podvig, "Russian Space Systems and the Risk of Weaponizing Space," in Advanced Military Technology in Russia (Chatham House, 2021), https://www.chathamhouse. org/2021/09/advanced-military-technologyrussia/04-russian-space-systems-and-riskweaponizing-space. See also Vasily Dolgov and Yuri Podgornikh, "Space as a Theater of War," [Космос как театр военных действий], Vozdushno-kosmicheskaia Sfera 2 (2013), pp. 7–14.

[21] الشيماء عرفات، السرديات التاريخية والجغرافية للحرب الروسية في أوكرانيا، مصدر سبق ذكره، ص16.

[22] UNHCR, Ukraine Emergency Response Overview, United Nations High Commissioner for Refugees, 2022–2024 ,p61.

[23] A. V. Skrypnik, "On a Possible Approach to Determining the Role and Place of Directed Energy Weapons in the Mechanism of Strategic Deterrence Through the Use of Force," Armaments and Economics 3 (2012)M P.122.

[24] معهد الدوحة للدراسات الاستراتيجية، الأزمة الأوكرانية: قراءة في جذور الصراع، الدوحة، 2023، ص85.

[25] Lawrence Freedman, Command: The Politics of Military Operations in Ukraine, Penguin Books, 2023..p24

[26] راغدة درغام، "انعكاسات الحرب الروسية الأوكرانية على الأمن الأوروبي"، مجلة السياسة الدولية، العدد 230، القاهرة، 2022، ص124.

[27] محمد عبد السلام، "سيناريوهات تطور الحرب الروسية الأوكرانية"، مركز المستقبل للأبحاث والدراسات المتقدمة، أبوظبي، 2022، ص57.

[28] Serhii Plokhy, The Russo-Ukrainian War: The Return of History, W.W. Norton & Company, 2023, p57.

[29] سجاد عبد الجبار الساعدي، "الهجمات السيبرانية في الحروب الحديثة"، مجلة دراسات إقليمية، جامعة الموصل، المجلد 14، العدد 56، 2021، ص 139.