مجلة
الدراسات السياسية والاقتصادية
Journal of Political and Economic Studies
Faculty of Politics and Economics
Suez University

مجلة علمية محكمة
(نصف سنوية)
تصدر عن
كلية السياسة والاقتصاد
جامعة السويس

تأسست المجلة عام 2021

print Issn :2805-3028

ONLINE ISSN :2805-3036

https://psej.journals.ekb.eg/

السنة (٤)

العدد (١)

الأراء الواردة داخل المجلة تعبر عن وجهة نظر أصحابها
وليست مسئولية كلية السياسة و الاقتصاد جامعة السويس

الترقيم الدولى الموحد للطباعة :3028-2805
الترقيم الدولى الموحد الإلكترونى :3036-2805

مجلة الدراسات السياسية والاقتصادية
Journal of Political and Economic Studies

مجلة علمية متخصصة في الشئون السياسية والاقتصادية

مجلة معتمدة من بنك المعرفة المصري

موقع المجلة على بنك المعرفة المصري
https://psej.journals.ekb.eg

تنشر الأعداد تباعًا على موقع دار المنظومة.

العدد (١) - السنة (٤)

تصدر نصف سنويًا

تأسست المجلة عام 2021

الحرب السيبرانية الروسية على أوكرانيا : التداعيات والتدابير الوقائية

أ.د/مسعد نجاح الرفاعي أبو الديار
أستاذ علم النفس، وباحث
دكتوراه في العلوم السياسية
جامعة السويس

أ. د/ إيمان نور الدين الشامي
أستاذ العلوم السياسية
كلية السياسة والاقتصاد
جامعة السويس

أ.م.د/ أحمد جلال محمود
أستاذ العلوم السياسية المساعد
كلية السياسة والاقتصاد
جامعة السويس

ملخص:

تتناول هذه الدراسة الحرب السيبرانية الروسية على أوكرانيا وتداعيات تلك الحرب وانعكاساتها والتدابير الوقائية حيالها. وطبق المنهج الاستقرائي والتاريخي، ومنهج تحليل المضمون، وتتضمَّن هذه الدراسة بالإضافة إلى المقدمة خمسة أجزاء وخاتمة. يناقش الجزء الأول المفاهيم الرئيسة للحرب السيبرانية من خلال إبراز التعريفات الأكثر شمولًا في الموضوع، وذلك جنبًا إلى جنب أبرز التطورات التاريخية للحروب السيبرانية الروسية على أوكرانيا ويناقش الجزء الثاني طبيعة التهديدات السيبرانية بين الروسية على أوكرانيا، ويعرض الجزء الثالث أهداف العمليات السيبرانية الروسية في أوكرانيا وكذلك التعرف على تداعيات الهجمات السيبرانية للحرب الروسية الأوكرانية، وأخيرا تناولت الدراسة تدابير أوكرانيا ضد الهجمات السيبرانية الروسية، وتوصلت الدراسة إلى أنه بالتزامن مع اندلاع الحرب في أوكرانيا حدث أكثر من ٢٠٠ هجمة سيبرانية على أوكرانيا منذ بدء الحرب الروسية على أوكرانيا، واستهداف ما يقرب عن ٧٠ من الكيانات الحكومية الأوكرانية، كما اتسمت الطبيعة المتطورة للتهديدات الروسية السيبرانية بتكتيكات متغيرة باستمرار، ونواقل هجومية جديدة، ودوافع متغيرة. حيث تشمل الهجمات على البنية التحتية الحيوية، والتجسس، وتعطيل الخدمات وحرب المعلومات وحملات التضليل وسرقة الملكية الفكرية. واستهدفت روسيا جراء توظيفها للحرب السيبرانية على أوكرانيا عدة أهداف منها(الحرب النفسية والخداع الاستراتيجي، والإخلال بمعادلة الدعم الغربي لأوكرانيا، وتقويض الثقة في النظام الأوكراني، وحرب السرديات وتآكل الثقة) وعن تداعيات الهجمات السيبرانية في الحرب الروسية الأوكرانية فتمثلت في : (التأثير في الرأي العام وإضعاف الروح المعنوية للسكان الأوكران واستهداف البنية التحتية المدنية وضرب أوكرانيا اقتصادياً، وإضعاف الثقة في الحكومة الأوكرانية،

واتخذت أوكرانيا تدابير ضد الهجمات السيبرانية الروسية من اتباع القاعدة التي تقول الهجوم أفضل وسيلة للدفاع حيث قامت أوكرانيا بعدد من الهجمات السيبرانية على المشآت الروسية.

الكلمات المفتاحية: الحرب السيبرانية ، الهجمات الإلكترونية، الصراع الروسي الأوكراني، التداعيات والتدابير الوقائية

Russian cyber war on Ukraine: repercussions and preventive measures

Abstract

This study deals with the Russian cyber war on Ukraine: the repercussions of that war, its repercussions, and preventive measures against it. The inductive and historical approach and the content analysis approach were applied. In addition to the introduction, this study includes five parts and a conclusion. The first part discusses the main concepts of cyber warfare by highlighting the most comprehensive definitions of the topic, This is side by side with the most prominent historical developments of the Russian cyber wars on Ukraine. The second part discusses the nature of the Russian cyber threats to Ukraine, and the third part presents the goals of Russian cyber operations in Ukraine as well as identifying the repercussions of the cyber attacks of the Russian-Ukrainian war, and finally addressing Ukraine's measures against Russian cyber attacks. The study concluded that, coinciding with the outbreak of war in Ukraine, more than 200 cyber attacks had occurred on Ukraine since the start of the Russian war on Ukraine, targeting approximately 70 Ukrainian government entities. The evolving nature of Russian cyber threats was also characterized by constantly changing tactics and new attack vectors. And variable motives, These include attacks on critical infrastructure, espionage, disruption of services, information warfare, disinformation campaigns, and intellectual property theft. As a result of its use of cyber warfare against Ukraine, Russia targeted several goals, including (psychological warfare, strategic deception, disrupting the equation of Western support for Ukraine, undermining confidence in the Ukrainian regime, war of narratives, and erosion of trust). Regarding the repercussions of cyber attacks in the Russian-Ukrainian war, they were: (influencing public opinion, weakening the morale of the Ukrainian population, targeting civilian infrastructure, hitting Ukraine economically, and weakening confidence in the Ukrainian government. Ukraine took measures against Russian cyber

attacks by following the rule that says the best way is To defend is to attack, as Ukraine has carried out a number of cyber attacks on Russian facilities.

Keywords: Cyber war, cyber attacks, Russian-Ukrainian conflict, repercussions and preventive measures

مقدمة:

إن أحد أخطر التهديدات التي تواجه الأمن القومي في العصر الحديث هي الحروب السيبرانية التي تُعد واحدة من بين أبرز تكتيكات الحروب الحديثة. حيث يمكن للهجمات الإلكترونية أن تهدد الأفراد والشركات والدول على حد سواء. ذلك الخطر الذي يتمثل في الهجمات السيبرانية، التي لا تقل آثارها عن تلك الآثار التي تخلفها النزاعات المسلحة التقليدية، حيث تشكل التهديدات السيبرانية مصدر قلق متزايد بسبب الاعتماد المتزايد على تكنولوجيا المعلومات في العديد من جوانب المجتمع وإمكانية حدوث اضطراب أو ضرر كبير بسبب تلك الهجمات أو التهديدات. وقد كان لها تأثير كبير على مستوى العالم ومن أكبر آثار الهجمات الإلكترونية تدمير البنية التحتية الحيوية، مثل شبكات النقل وشبكات الطاقة والشبكات المصرفية. ويمكن أن يكون للهجمات الموجهة على هذه الأنظمة عواقب واسعة النطاق بما في ذلك انقطاع التيار الكهربائي وتأخير النقل والخسائر المالية .

كما أدى الخوف من التهديدات السيبرانية إلى زيادة الإنفاق على تدابير الأمن السيبراني من قبل الحكومات والشركات الخاصة. حيث تأثر العالم بعدة طرق بفعل الهجمات السيبرانية بما في ذلك الأضرار التي لحقت بالبنية التحتية والأزمة الاقتصادية وانتشار الدعاية أو المعلومات المضللة وفقدان المعلومات الحساسة وانتهاك الخصوصية، فضلاً عن الإضرار بسمعة الدولة واستقرارها الاقتصادي. ونشر الدعاية والتلاعب بالرأي العام، مما قد يؤدي إلى عدم الاستقرار الاجتماعي والسياسي. كما يمكن أن تؤدي

الهجمات الإلكترونية إلى سرقة معلومات حساسة، مثل الملكية الفكرية أو البيانات الشخصية.

ومن أكثر النماذج الحية لتلك الهجمات السيبرانية، هي الحرب الروسية الأوكرانية التي اشتعلت في فبراير ٢٠٢٢. إذ استخدمتها موسكو لشن هجمات إلكترونية على مراكز القيادة والسيطرة الحكومية والعسكرية والخدمات اللوجستية في الداخل الأوكراني بهدف إثارة الفوضى والارتباك داخل أوكرانيا. وتملك روسيا تاريخاً طويلاً في ممارسة العمليات السيبرانية، إذ كانت الحرب الأوكرانية الأخيرة، هي المرة السابعة التي تستخدم فيها موسكو هذه العمليات ضد خصومها في الجوار الإقليمي لذلك كان الداعي لتناول هذا الموضوع والذي يعرض تداعيات التهديدات السيبرانية الروسية على الحرب الروسية الأوكرانية ومسار تلك الحرب والتدابير التي أجرتها أوكرانيا حيال تلك الهجمات..

مشكلة الدراسة:

برز بُعد الأمن السيبراني أو الإلكتروني في الاستراتيجية الأمنية الروسية ٢٠٢٠، واضحًا وأكثر تطورًا، إذ تنص استراتيجية الأمن القومي الروسية الجديدة، على أن الهدف الرئيس لروسيا يتمثل في تحقيق التفوق المعلوماتي في الفضاء السيبراني. ووفقًا لتقرير صادر عن المعهد الدولي للدراسات الاستراتيجية عام ٢٠٢١، احتلت روسيا المركز الثاني مع الصين في ترتيب "مراكز القوة الإلكترونية"، بعد الولايات المتحدة الأمريكية، وهو ما يبرز أهمية بُعد الأمن الإلكتروني في استراتيجية روسيا الأمنية.

وغالبا ما تسفر الهجمات السيبرانية عن إحداث نوع من التوتر والاحتقان في العلاقات الدبلوماسية بين الدول، وهو ما يمكن الاستشهاد عليه من خلال العديد من الهجمات السيبرانية، ولعل آخرها تصاعد ذروة الحرب السيبرانية بين كل من

روسيا وأوكرانيا في ظل أزمة وصراع بين الطرفين. فما هي طبيعة هذه الهجمات السيبرانية، وكيف تشكل في مجملها حربا سيبيرانية تؤجج الصراع بين كييف وموسكو؟

كما تتجسد إشكالية هذا البحث في ماهية التحول الذي يطرأ بشكل مستمر على العالم نتيجة للأثار الكارثية للتهديدات الالكترونية، وما يزيد هذا الأمر صعوبة هو الافتقار إلى دراسات حالات شاملة وواقعية يشكل إحدى الفجوات في الأدبيات والدراسات المتعلقة بالهجمات السيبرانية، والتداعيات التي تنتج عن الحروب والهجمات السيبرانية لا سيما في مواقع التوترات الشديدة مثل ما يحدث في الحرب الروسية الأوكرانية. لذلك جاءت هذه الدراسة للتعرف على تداعيات وطبيعة الحرب السيبرانية الروسية على أوكرانيا: والتدابير الوقائية من أوكرانيا حيالها.

تساؤلات الدراسة:

تسعى هذه الدراسة إلى الإجابة على التساؤل الرئيس الآتي: "ما هو مدى تأثير العمليات السيبرانية لروسيا في أوكرانيا" وينبثق من هذا التساؤل مجموعة من التساؤلات البحثية الفرعية ومنها:

١. **ما** هو مفهوم الحروب السيبرانية ومدى تطورها في النموذج الروسي الأوكراني؟
٢. ما طبيعة التهديدات السيبرانية الروسية في أوكرانيا ومدى تطورها؟
٣. هل استطاعت روسيا من تحقيق أهدافها التي ساعدتها في حربها التقليدية المباشرة وتهديد الأمن الأوكراني.
٤. ما هي تداعيات العمليات السيبرانية الروسية في أوكرانيا والتدابير الوقائية حيالها؟

أهداف الدراسة:

تهدف هذه الدراسة إلى توفير فهم شامل ومتعمق لموضوع الحروب السيبرانية الروسية على أوكرانيا وتداعياته والتدابير المضادة لها، فضلاً عن تحقق الأهداف الفرعية الآتية:

١. التعرف على مفهوم الحروب السيبرانية ومدى تطورها في النموذج الروسي الأوكراني.
٢. الكشف عن طبيعة التهديدات السيبرانية الروسية في أوكرانيا ومدى تطورها
٣. التعرف على الأهداف التي حققتها روسيا نتيجة لعملياتها السيبرانية في أوكرانيا.
٤. تحديد التداعيات للعمليات السيبرانية الروسية في أوكرانيا والتدابير الوقائية حيالها.

أهمية الدراسة:

بات موضوع العمليات السيبرانية يحظى بالمزيد من الاهتمام في الدوائر السياسية والأكاديمية والاستراتيجية بسبب الاعتماد المتزايد على شبكة الإنترنت وانتشارها، فضلًا عن انتشار تطبيقاتها، مثل منصات التواصل الاجتماعي، بحيث باتت البنية الحيوية المدنية والعسكرية وحتى الاجتماعية لأي دولة معتمدةً اعتمادًا كاملًا على شبكة الإنترنت في عمليات التشغيل والتنفيذ والاتصال. وبناءً على هذه الأهمية، باتت كل دولة تحظى بجيش سيبراني أو وحدات سيبرانية تختصُّ بالهجوم والدفاع. وبات الفضاء السيبراني المجال الخامس في الحروب مضافًا إلى المجالات التقليدية الأخرى: البرية والبحرية والجوية والفضائية.

وكذلك تستمد الدراسة أهميتها كونها تسلط الضوء على أحد أبرز الموضوعات الحالية على الساحة الدولية، إذ يعد التهديد الالكتروني من المواضيع الحيوية المهمة، والتي برز دورها وتأثيرها على معظم بلدان العالم، لذلك تكمن أهمية هذه الدراسة في تحديد الاتجاهات والأنماط الرئيسة من حيث أنواع الهجمات السيبرانية التي تم تنفيذها، والقطاعات المستهدفة، وتداعيات هذه الهجمات.

فروض الدراسة:

تنطلق الدراسة من فرضية أساسية وهي " استطاعت روسيا من خلال عملياتها السيبرانية في أوكرانيا من تحقيق أهدافها التي ساعدتها في حربها التقليدية المباشرة وتهديد الأمن الأوكراني".

منهج الدراسة:

اعتمدت هذه الدراسة على المنهج التحليلي والاستقرائي وأداة تحليل المضمون وذلك للتعرف على الحرب السيبرانية الروسية على أوكرانيا وتداعيات تلك الحرب وانعكاساتها والتدابير الوقائية حيالها

تقسم الدراسة:

في ضوء ما سبق وفي اطار سعي الدراسة إلى تحقيق أهدافها والإجابة على تساؤلاتها البحثية واختبار فرضياتها الأساسية والفرعية تم تقسيم الدراسة إلى خمسة محاور كما يلي:

أولاً: مفهوم الحروب السيبرانية ومدى تطورها في النموذج الروسي الأوكراني

أ- مفهوم الحروب السيبرانية:

تُعرف الحروب السيبرانية بأنها "تلك الإجراءات التي تتخذها الدولة من أجل الهجوم على نظم المعلومات للعدو بهدف التأثير و الإضرار بها والدفاع عن نظم المعلومات الخاصة بالدولة ا المهاجمة و إذا سببت الهجومات السيبرانية نزاعا مسلحًا بوصفها عملية إلكترونية سواء هجومية أو دفاعية مما قد يخلق إصابات أو قتل أشخاص أو الإضرار بممتلكات وتدميرها. (١)

وتعرف بأنها حرب غير محدودة المجال، وغامضة الأهداف، وهي حروب أقل تكلفة من الحروب التقليدية ، وكما تعد أكثر ضررًا منها لتشعب أهدافها وتعدد أغراضها، وعادة ما ينتج عنها إصابات ، وقتل للمدنيين والمستهدفين، وتضر بمنشآت الدولة (٢)

ب-الحرب السيبرانيّة الروسيّة الأوكرانية :

الحرب السيبرانيّة الروسيّة الأوكرانية وتُعرَف أيضًا باسمِ الحربِ الإلكترونيّة الروسيّة الأوكرانية هي أحد مُكوِّنات المواجهة بين روسيا وأوكرانيا منذ انهيار الاتحاد السوفيتي في عام ١٩٩١. في حين سُجِّلَت أولى الهجمات السيبرانيّة على أنظمة المعلومات الخاصة بالشركات ومؤسسات الدولة في أوكرانيا خلال الاحتجاجات الجماهيريّة في عام ٢٠١٣، فقد كان السلاح الإلكتروني الروسي تورلا موجودًا ويُستعَمل على فتراتٍ متفرّقة منذ عام ٢٠٠٥. وتصاعدت الحرب السيبرانيّة الروسية مع اختراق شبكة الكهرباء الأوكرانية عام ٢٠١٥ ومرة أخرى عام ٢٠١٦، والهجوم على مواقع حكوميّة أوكرانيا في ديسمبر

(١) نسيب نجيب، الحرب السيبرانية من منظورالقانون الدولي الإنساني ،المجلة النقدية للقانون والعلوم السياسية ، كلية الحقوق والعلوم السياسية جامعة تيزي وزو، المجلد ١٩ ،العدد ٤، ٢٠٢١ص٢.

(٢) الهجمات السيبرانية المدمرة بين روسيا و اوكرانيا : حرب لن ينجو منها أحد ،شبكة النبأ المعلوماتية ، ١٦ آذار ٢٠٢٢ ، تاريخ الدخول، تاريخ الدخول ٢٥ فبراير ٢٠٢٤ https://annabaa.org/arabic/informatics/30480

٢٠١٦، فضلًا عن الهجمات الروسيّة القويّة في يونيو ٢٠١٧، والهجمات على مواقع الحكومة الأوكرانية في يناير ٢٠٢٢ [١]

ج- التطورات التاريخية للحرب السيبرانية بين روسيا وأوكرانيا.

تعد روسيا من أولى الدول التي استغلت الفضاء السيبراني في المجال العسكري، واهتمت بالبحث والتطوير لزيادة قدراتها الهجومية في هذا المجال.

بدأ الاهتمام الروسي بالأبعاد السياسية للأمن الاليكتروني في التسعينيات من القرن الماضي بإنشاء روسيا في عام ١٩٩٢ لمجلس الأمن القومي الروسي وتم إنشاء مؤسسات أخرى تختص فقط بالقضايا السيبرانية وحماية الأمن الاليكتروني الروسي.

لقد تبلور الاهتمام الروسي بقضايا الأمن الاليكتروني في عام ٢٠٠٠ ، وبحلول عام ٢٠٠٥ تم إنشاء أول سلاح اليكتروني روسي " أربوروس" [٢] ومن أهم الهجمات السيبرانية الروسية على أوكرانيا:

١. كانت أول الهجمات السيبرانية المسجلة في أنظمة المعلومات للمؤسسات الخاصة والمؤسسات الحكومية في عام ٢٠١٣ في أوكرانيا نتيجة للاحتجاجات الشعبية في أوكرانيا حيث شهدت البلاد هجوم سيبراني على مواقع التواصل الاجتماعي للتلاعب في وسائل الاعلام وللتأثير على الرأي العام الأوكراني لمنع دخول أوكرانيا في الاتحاد الأوروبي [٣]

(١) عبد المنعم علي، تكتيكات متبادلة:حدود تأثير العمليات السيبرانية في الحرب الروسية الأوكرانية،تاريخ النشر ٢٠٢٤/١/٢ على الرابط
https://futureuae.com/ar/Mainpage/Item/8906
(٢) نسيب نجيب، مرجع سابق ، ص٢.
(٣) نبيل عودة ، العمليات السيبرانية في الحرب الروسية الأوكرانية طبيعتها و أنماطها ، الشرق للأبحاث الاستراتيجية ، 20سبتمبر ٢٠٢٢ ، صفحة ٢٣

٢. استهدفت مجموعة قرصنة روسية تسمى fancy bear أو APT28القوات الصاروخية والمدفعية الأوكرانية وهذه الهجمات دمرت أكثر من ٨٠٪ من مدافع الهاوتزر D-30 الأوكرانية وذلك ما بين ٢٠١٤-٢٠١٦.

٣. ارتبط بروز مجموعة تسمى Cyber berkut في ٢٠١٤ على إثر الصراع داخل أوكرانيا في تلك الفترة الزمنية والتي كانت تتبنى خطاباً معادياً للقوى الغربية وموالياً لموسكو واعترفت تبدلك المجموعة بشنها هجمات إلكترونية أثناء عملية الانتخابات البرلمانية في أوكرانيا حيث اخترقت لجنة الانتخابات المركزية الأوكرانية في انتخابات ٢٠١٤.

٤. كان أول هجوم سيبرانية ناجح على شبكة كهرباء ، حيث في ديسمبر من ٢٠١٥ حيث تم اختراق شبكة الكهرباء في المنطقة الغربية " ايفانو فرانكوفسك " مما أدى إلى الانقطاع التام في التيار الكهربائي على عموم المنطقة و في العام التالي تكرر الاختراق لشبكة الطاقة الأوكرانية من قبل محترفين روس.

٥. قامت أوكرانيا على الصعيد الآخر في ٩ مايو من ٢٠١٦ بشن تسع عمليات اختراق ناجحة لمواقع مجموعة " جمهوريات دونيتسك الشعبية" الانفصالية وأيضاً اخترقت مواقع روسية للدعاية المناهضة لأوكرانيا بالإضافة لشركات عسكرية روسية خاصة.

٦. كانت هجمات نت بتيا (Notpetya) عام ٢٠١٧ واحدة من أشد العمليات السيبرانية تكلفة حيث أصابت الشبكات الخدمية التابعة للقطاعات المصرفية والحكومية لأوكرانيا وعطلت الوصول إليها حيث تسربت تلك الهجمات لتصيب بعد الشبكات الخدمية في العديد من الدول الأخرى مثل

ايطاليا والمملكة المتحدة والولايات المتحدة وأستراليا وقدرت تكلفة تلك الهجمات بعشرات المليارات من الدولارات[١]

٧. وقبل اندلاع الغزو الروسي لأوكرانيا في منتصف يناير ٢٠٢٢ حدث هجوم سيبراني حيث عطلت القراصنة عشرات المواقع التابعة للحكومة الأوكرانية متضمنة وزارة الخارجية الأوكرانية [٢]

٨. أدَّت الهجمات السيبرانيّة الروسية في فبراير ٢٠٢٢، بعد غزو القوات الروسية للمناطق الشرقية من أوكرانيا، إلى إسقاطِ العديد من المواقع الحكومية والمصرفية الأوكرانية الرئيسة. وقد نسَبَت المخابرات الأمريكية تلك الهجمات إلى مهاجمين روس، رغمَ أنَّ الحكومة الروسية نفَت تورّطها[٣]

وبشكل عام وبالتزامن مع اندلاع الحرب في أوكرانيا حدث أكثر من ٢٠٠ هجوم اليكتروني على أوكرانيا منذ بدء غزوها في فبراير حتي إبريل وذلك وفقاً لتحليل أجرته شركة ميكروسوفت ومنهم استهداف ما يقرب عن ٧٠ من الكيانات الحكومية الأوكرانية. [٤]

ثانيا: طبيعة التهديدات السيبرانية الروسية على أوكرانيا

(١) فتحي بولعراس، تداعيات الازمة الاوكرانية على مستقبل اروبا، مجلة السياسة الدولية ، العدد ٢٢٨ ،ابريل ٢٠٢٢ ، المجلد ٥٧

(2)Kaspersky (2023).Kaspersky Cybersecurity threats: what awaits US in 2023? Securelist. 2023. [2 November 2023]. https://www.rfc-editor.org/rfc/rfc4949 https://www.rfc-editor.org/rfc/rfc4949

(3)Pearson, James (27 Feb 2022). "Ukraine launches 'IT army,' takes aim at Russian cyberspace". Reuters (بالإنجليزية). Archived from the original on 2022-03-01. Retrieved 2022-02-27

(٤) شوبير جلالي، مراد فائزة ، مفهوم الحروب السيبرانية والأمن السيبراني، مجلة الحقوق والحريات، جامعة عمار ثليجي الأغواط. كلية الحقوق والعلوم السياسية ، المجلد ١١ ، العدد ١ ، السنة ٢٠٢٣، ص ١٦٤، ١٦٥.

تتسم الطبيعة المتطورة للتهديدات السيبرانية بتكتيكات متغيرة باستمرار، ونواقل هجومية جديدة، ودوافع متغيرة. ويمكن أن تشمل للتهديدات السيبرانية التي ترعاها الدولة هجمات على البنية التحتية الحيوية، والتجسس، وتعطيل الخدمات. كما يتضمن الإرهاب السيبراني بشكل متزايد حرب المعلومات وحملات التضليل وسرقة الملكية الفكرية[١]

لقد شهد العام الأول لحرب أوكرانيا ٤٧ هجوماً سيبرانياً روسياً، بهدف جمع البيانات مباشرة من مصادر الحكومة الأوكرانية، وتزايدت العمليات السيبرانية إذ زادت العمليات السيبرانية الروسية بنسبة ٧٥%. [٢]

وبالنظر إلى أسلوب الهجمات السيبرانية الروسية، فإن الأهداف المفضلة لها ظلت أنشطة التشكيل التخريبية وحملات التجسس خلال الأشهر القليلة الأولى من حرب أوكرانيا عام ٢٠٢٢. إذ شكلت حوادث التعطيل ٥٧.٤% من إجمالي الحوادث، يليها التجسس (٢١.٣%). وتركزت معظم الهجمات السيبرانية الروسية على استهداف جهات فاعلة من القطاع الخاص غير الحكومي بنسبة ٥٩.٦%، تليها الجهات الحكومية والمحلية بنحو ٣١.٩%، وأربعة حوادث فقط، أي نسبة ٨.٥% لاستهداف الجهات العسكرية الحكومية، وهو ما يتوافق مع أهداف روسيا بين عامي ٢٠٠٠ و٢٠٢٠، إذ تركّزت نسبة ٥٧% من العمليات السيبرانية في استهداف جهات فاعلة خاصة غير حكومية، و٣٢% جهات فاعلة حكومية غير عسكرية، و١١% جهات عسكرية حكومية.

(1)Brooks (2023).Brooks C. Cybersecurity trends and statistics; more sophisticated and persistent threats so far in 2023. 2023. [29 October 2023]. Forbes.

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

ويدلل ذلك أن الجهود السيبرانية التي تبذلها روسيا كانت ذات تأثير محدود في الجهود العسكرية الروسية في أوكرانيا في بادئ الأمر ثم زادت حدته مع اشتعال وتيرة الحرب. (١)

واتضحت مؤشرات شدة وخطورة استخدام روسيا للعمليات السيبرانية من خلال تكثيف مهاجمة مواقع أوكرانية وتعطيل القيادة والسيطرة منذ بداية الحرب من خلال نشر روسيا برامج ضارة عطلت نظام الأقمار الاصطناعية وأدت إلى انقطاع أكثر من ٣٠ ألف اتصال بالإنترنت مؤقتاً في جميع أنحاء أوروبا، بما في ذلك ٥ آلاف توربينة رياح، إلى جانب أنه ومنذ بداية الحرب وردت تقارير عن اكتشاف برامج ضارة في البنية التحتية الحيوية في البلدان التي تدعم أوكرانيا بمساعدة عسكرية أجنبية. ففي الولايات المتحدة تم اكتشاف برامج ضارة روسية في البنية التحتية الحيوية المرتبطة بتوليد وتوفير الكهرباء، وفي المملكة المتحدة باتت هناك تخوفات من مساعي موسكو المتزايدة لاستهداف البنية التحتية الحيوية. (٢)

وفي الخامس من يناير ٢٠٢٤ تم اختراق نظام شركة الاتصالات الأوكرانية كييف ستار وهو أحد أكثر الاختراقات دراماتيكية منذ الغزو الروسي الكامل قبل نحو عامين، إلى توقف الخدمات التي تقدمها أكبر شركة اتصالات في أوكرانيا لنحو ٢٤ مليون مستخدم (٣)

(١) عبد المنعم علي، تكتيكات متبادلة:حدود تأثير العمليات السيبرانية في الحرب الروسية الأوكرانية،تاريخ النشر ٢٠٢٤/١/٢ على الرابط
https://futureuae.com/ar/Mainpage/Item/8906

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

(٣) شبكة الشرق الأوسط وشمال أفريقيا للخدمات المالية ،اختراق إلكتروني كبير يستهدف أكبر شركة اتصالات خلوية في أوكرانيا "كييف ستار" تاريخ النشر ٢٠٢٣/١٢/١٣ على الرابط
https://menafn.com/arabic/1107585630/%

في الحادي والعشرين من يناير ٢٠٢٤ تعرض بنك أوكراني للاختراق حيث استهدف قراصنة بنك "مونوبنك"، أكبر بنك في أوكرانيا يعمل عبر الهاتف المحمول ، بموجات من هجمات الحرمان من الخدمة، حسبما أفاد "أوليه هوروكوفسكي"، المؤسس المشارك والرئيس التنفيذي للشركة. وقال "هوروكوفسكي" إن بنك "مونوبنك" تعرض لهجوم بـ ٥٨٠ مليون طلب خدمة في هجوم واحد. وفي الخامس والعشرين من يناير ٢٠٢٤ أفادت العديد من وكالات الدولة الأوكرانية، بما في ذلك شركة الطاقة المملوكة للدولة، بوقوع هجمات إلكترونية أثرت على أنظمة تكنولوجيا المعلومات لديها وقدرتها على التواصل مع الجمهور. وقالت شركة نفتوغاز، أكبر شركة نفط وغاز في أوكرانيا، إن "هجومًا إلكترونيًا واسع النطاق" على أحد مراكز البيانات التابعة لها أدى إلى توقف موقعها على الإنترنت ومراكز الاتصال الخاصة بها عن العمل. (١)

ثالثاً: أهداف العمليات السيبرانية الروسية في أوكرانيا:

على الرغم من استخدام روسيا الضربات الصاروخية وما تبعها من أعمال تخريب وتهجير قسري وتهديدات باستخدام الأسلحة النووية في حرب أوكرانيا، فإنها لم تشن حرباً إلكترونية شاملة ومكلفة ضد أوكرانيا أو مؤيديها في الغرب، فبالرغم من وجود زيادة نسبية في الهجمات السيبرانية خلال الحرب. فإن هذه الهجمات قد أحدثت تأثيراً مادياً نسبيا في ساحة المعركة أو تحّولاً في الأهداف والأساليب، إذ تستهدف روسيا جراء توظيفها النسبي للحرب الإلكترونية والسيبرانية عدة أهداف منها(٢):

(1)Jim Masters ,Russia-Ukraine War: Cyberattack – Kinetic Warfare Timeline, *January 26, 2024*,
https://www.msspalert.com/news/ukraine-russia-cyberattack-timeline-updates-amid-russia-invasion.

(٢)عبد المنعم علي، تكتيكات متبادلة:حدود تأثير العمليات السيبرانية في الحرب الروسية الأوكرانية،تاريخ النشر ٢٠٢٤/١/٢ على الرابط
https://futureuae.com/ar/Mainpage/Item/8906

- استخدام الحرب النفسية والخداع الاستراتيجي حيث سعت العمليات السيبرانية الروسية إلى نشر معلومات مضللة لتقويض الدعم لأوكرانيا، وذلك لتشكيل مواقف دول الجنوب العالمي إزاء الحرب، وإن كان ذلك لا يؤدي دوراً حاسماً حتى أثناء القتال المكثف.
- الإخلال بمعادلة الدعم الغربي لأوكرانيا: تكافح روسيا من أجل دمج التأثيرات السيبرانية والتقليدية في ساحة المعركة وخارجها عبر إحداث موجة من الهجمات الإلكترونية ضد البنية التحتية الأمريكية الحيوية، واستخدام الدعاية الحاسوبية للتقليل من الدعم الأمريكي للحرب في أوكرانيا.
- تقويض الثقة في النظام الأوكراني: تستهدف الاختراقات السيبرانية للمنشآت الحيوية الأوكرانية ما هو أبعد من ساحة المعركة، إذ تسعى إلى تقويض الثقة في كييف وإحداث شعور بنقص السيطرة، بما يؤلب المواطنين الأوكرانيين على الدولة لفشلها في حماية البنية المجتمعية، ومن ثم يزعزع استقرار الحكومة ويؤدي إلى انهيار عام يتيح لموسكو السيطرة على كييف أو الضغط عليها لتقديم تنازلات.
- حرب السرديات وتآكل الثقة: تستخدم روسيا الفضاء الإلكتروني لشن "حرب السرديات" إذ تركز على تآكل الثقة العالمية في أوكرانيا باستخدام الدعاية الحاسوبية. وتتضمن هذه الأساليب إنشاء حسابات وهمية على وسائل التواصل الاجتماعي، واستخدام الروبوتات، واستهداف المحتوى الذي يطالب مجموعات مستخدمين فريدة بتغيير المواقف العامة.

رابعا: تداعيات الهجمات السيبرانية في الحرب الروسية الأوكرانية

نتج عن التهديد السيبراني في الصراع الروسي الأوكراني عن التداعيات الآتية:

أ – التأثير في الرأي العام و إضعاف الروح المعنوية للسكان الأوكران

استهدفت الهجمات السيبرانية الروسية أنظمة اللجان المركزية للانتخابات الأوكرانية في عام ٢٠١٤ من خلال اختراق الحواسيب المسجل عليها نتائج الانتخابات مما أثار حالة من الفوضى و عدم الاستقرار (١)

أثناء الغزو الروسي لأوكرانيا في ٢٤ فبراير عام ٢٠٢٢ كان التأثير على الرأي العام من خلال بث الزعر و الخوف من خلال الأخبار الرائجة حول السيطرة الكاملة لروسيا على كييف ونجاح العمليات البرية القائمة وسقوط الطائرات الأوكرانية مما يسبب في إضعاف الخصم وهزيمته نفسياً وايضاً ما أقدم عليه قراصنة من الجانب الروسي حينما قاموا باختراق شركة الإذاعة الأوكرانية ونشر عن طريقها أخبار تعلن عن استسلام الرئيس الأوكراني زيلنسكي وبثوا رسائل مُضللة (٢)

بالإضافة إلى مجموعة Ghostwriter وهي مجموعة سيبرانية تابعة للقوات الأمنية لدولة بيلاروسيا حليفة روسيا والتي عملت على اختراق منصات التواصل الاجتماعي من خلال بثها لرسائل تريد إيصالها للجمهور، فوفقاً لشركة Meta حاولت المجموعة التسلل إلى حسابات فيسبوك لنشر مقاطع فيديو تظهر فيه القوات الأوكرانية في حالة من الضعف والتهلهل والاستسلام وباستخدام الهجمات السيبرانية المُسماة " DDOS" والتي تسبب في حرمان الخدمة واستخدامها لإشعال الاضطرابات في حركة المرور حيث أنها

(١) ايهاب محمد أبو المجد ،الجيوسيبرانية العالمية والتحولات في أبعاد وخصائص القوة "آليات التوظيف في الاستراتيجية الروسية والصينية "، مجلة البحوث المالية و التجارية ،المجلد ٢٤، العدد الاول، يناير ٢٠٢٣ ، صفحة ١٣١

(2)Sharma (2023).Sharma S. New cyberattack tactics rise up as Ransomware payouts increase, CSO. 2023. [28 October 2023]. https://www.csoonline.com/article/574635/new-cyberattack-tactics-rise-up-as-ransomware-payouts-increase.html https://www.csoonline.com/article/574635/new-cyberattack-tactics-rise-up-as-ransomware-payouts-increase.html.

تملئ موقع الويب بطلبات زائفة بهدف الوصول إلى معلومات مضللة؛ مما يسبب حالة من الإرباك وعدم الاستقرار العام في البلاد. (١)

ب – استهداف البنية التحتية المدنية وضرب أوكرانيا اقتصادياً

نتج عن استخدام روسيا للعمليات السيبرانية المختلفة على أوكرانيا خسائر اقتصادية فادحة لاسيما عند استهداف مقرات أو بنى تحتية تمثل أعمدة رئيسة في الدولة مثل ما حدث في عام ٢٠١٥ فالعمليات السيبرانية التي اتخذتها روسيا ضد أوكرانيا من خلال ضرب شركات الطاقة والكهرباء مما تسبب في حرمان أكثر من ربع مليون أوكراني من الكهرباء في المنطقة الغربية التي تُدعى " فرانو فرانكوفسك " مما أحدث خسائر أضرت بالبلاد وجدير بالذكر بأن هذه العمليات تكررت أيضاً في العام التالي من هذا التاريخ ، وأيضاً استهدفت عمليات سيبرانية أخرى عدداً من البنوك ومؤسسات النقل والخدمات العامة الأوكرانية وكل تلك العوامل تساعد في هز الثقة في الاقتصاد الأوكراني والتأثير على قوة الاستثمارات لعدم الاستقرار في عموم البلاد. (٢)

ج – إضعاف الثقة في الحكومة الأوكرانية

ويعد ذلك من خلال تكرار العمليات السيبرانية المختلفة ضد أوكرانيا مثل تكرار الهجوم السيبراني على شركات الكهرباء في عام ٢٠١٦ ، وما بين عامي ٢٠١٤ حتى ٢٠١٦ استهدفت مجموعة قراصنة روسية تسمى fancy bear القوات الصاروخية والمدفعية الأوكرانية وأحدثت دمار في أكثر من٨٠% من قوات الهاوتزر الأوكرانية-D 30، كما حدث أكبر عملية اختراق سيبراني في تاريخ أوكرانيا في بداية العمليات

(1)Ujang Priyono , Cyber warfare as part of Russia and Ukraine conflict , Jurnal Diplomasi Pertahanan , volume 8 , nomor 2 , 2022 , page 45.

(٢) شوبير جلالي ، مراد فائزة ، مفهوم الحروب السيبرانية والأمن السيبراني ، **مجلة الحقوق والحريات** ، جامعة عمار ثليجي الأغواط.كليةالحقوق والعلوم السياسية ، المجلد ١١ ، العدد ١ ، السنة ٢٠٢٣ ، ص ١٦٤ ، ١٦٥.

العسكرية ضد أوكرانيا في ٢٤ فبراير عام ٢٠٢٢ من خلال هجومwhisper gate ، حيث عطل القراصنة الروس عشرات المواقع الأوكرانية بما فيهم وزارة الخارجية الأوكرانية وفي بداية الحرب استهدفت القوات الروسية تعطيل شبكة اتصالات الأقمار الصناعية مما أدى إلي تعطيل الاتصالات العسكرية الأوكرانية مما تسبب في قطع المعلومات بين أفرع الجيش الأوكراني المختلفة. (١)

خامسا: التدابير الأوكرانية ضد الهجمات السيبرانية الروسية:

من التدابير التي اتبعتها أوكرانيا ضد روسيا هو اتباع القاعدة التي تقول الهجوم أفضل وسيلة للدفاع هو حيث قامت أوكرانيا بعدد من الهجمات السيبرانية على المنشآت الروسية تمثلت في:

١. في ٢٥ فبراير ٢٠٢٢ تم الاعلان عن إنشاء الجيش السيبراني الأوكراني على يدِ ميخايلو فيدوروف، النائب الأول لرئيس الوزراء ووزير التحوّل الرقمي، وذلك تزامنًا مع تزايد الغزو الروسي لأوكرانيا والهدف الأساسي لهذا الجيش السيبراني بحسبِ ميخايلو هو المساهمة وبقوّة في الحرب السيبرانيّة ضد روسيا. وقد طلب فيدوروف المساعدة من خبراء التقنيّة من مختلف بقاعِ العالم، ثمّ نشرَ على حسابٍ رسمي في تيليجرام قائمةً ضمَّت ٣١ موقعًا إلكترونيًا لمنظمات الأعمال والدولة الروسية من أجلِ استهدافها. (٢)

(١) آية رجب أبو اليزيد، العمليات السيبرانية بين روسيا وأوكرانيا : قراءة في الأسباب والنتائج ،المركز الديمقراطي العربي تاريخ النشر ٢٠٢٤/٨/١٢ على الرابط https://democraticac.de/?p=99262

(٢) الجزيرة الاخبارية، بعد عامين من إنشائه.. ما هو حال قراصنة "جيش أوكرانيا الإلكتروني"؟ تاريخ النشر ٢٠٢٤/٣/٢٠ على الرابط https://www.ajnet.me/tech/2024/3/20/%

٢. وفي مايو ٢٠٢٣م انضمت أوكرانيا إلى مركز حلف شمال الأطلسي للدفاع السيبراني، وفق ما أفادت الهيئة التي تتخذ من "تالين" مقرا، فيما اعتبرت كييف أنها «خطوة في الطريق» إلى عضوية الناتو.(١)

٣. في ٢٤ أكتوبر ٢٠٢٣ أنشأت أوكرانيا مركز الدفاع السيبراني كما أعلن المركز الوطني الأوكراني لتنسيق الأمن السيبراني وشركة IP3 International، وهي شركة مطورة لأمن الطاقة، عن إنشاء مركز الدفاع الجماعي للذكاء الاصطناعي (CDAIC) في أوكرانيا يعمل على تعزيز التعاون بين أوكرانيا وحلفائها للحماية من الهجمات السيبرانية.

٤. في يناير ٢٠٢٤م نفذ خبراء إلكترونيون مرتبطون بمديرية الاستخبارات الرئيسة في أوكرانيا هجوم قرصنة على شركة روسية ، مما أدى إلى تدمير البنية التحتية لتكنولوجيا المعلومات بالكامل لشركةIPL Consulting ، وهي شركة متخصصة في تنفيذ أنظمة المعلومات في القطاع الصناعي الروسي، حسبما أفادت HUR في ٢٧ يناير. ووفقًا لمصادر استخباراتية، تسلل المتخصصون إلى الشبكة الداخلية للشركة ودمروا بنيتها التحتية لتكنولوجيا المعلومات، بما مجموعه أكثر من ٦٠ تيرابايت وعشرات الخوادم وقواعد البيانات.

٥. في مطلع عام ٢٠٢٤ :أعلنت الحكومة الدنماركية عن خطط لإرسال مساعدات عسكرية إلى أوكرانيا لتعزيز قدرات الدفاع السيبراني في البلاد

(١) صحيفة الشرق الأوسط ، أوكرانيا تنضم إلى مركز الناتو للدفاع السيبراني، تاريخ النشر ٢٠٢٣/٥/١٧، على الرابط https://aawsat.com/%D8%A7%D9%84

تقدر (١٣ مليون دولار)، لدعم جهود كييف للحفاظ على مرونتها الرقمية ضد الهجمات السيبرانية. (١)

٦. في الأول من فبراير ٢٠٢٤ تمكن متسللو المديرية الرئيسية للاستخبارات بوزارة الدفاع الأوكرانية أيضا من استهداف البرامج العسكرية الروسية المستخدمة لتعديل طائرات دي جيه آي التجارية للتطبيقات العسكرية مما أدى إلى إغلاق الخوادم المسؤولة عن نظام تحديد "الصديق أو العدو" الروسي ومنع القوات من الوصول إلى الخادم لعمليات الطائرات بدون طيار. كما منع الهجوم الإلكتروني القوات من تكوين لوحات التحكم ونقل مقاطع الفيديو إلى مراكز القيادة وتشغيل الطائرات بدون طيار باستخدام واجهات الكمبيوتر مما أدى إلى إيقاف العديد من أساطيل الطائرات بدون طيار وإيقاف العمليات (٢)

٧. في الثاني عشر من يونيو ٢٠٢٤ استهدف قراصنة أوكرانيون الأنظمة الإلكترونية لمطارات روسية متعددة مما تسبب في تعطيل الرحلات الجوية. وشملت المطارات المستهدفة مطار يوجنو ساخالينسك ومطار دوموديدوفو في موسكو ومطار جاجارين في ساراتوف مما أدى إلى تأخير الرحلات الجوية المتجهة بشكل أساسي إلى سوتشي وبودروم وموسكو. كما أجبر الهجوم الطائرات على التحويل إلى سامارا وأوليانوفسك. قبل الهجوم تمكن المتخصصون في مجال الإنترنت من الوصول إلى خادم الموقع الإلكتروني

(1)Jim Masters ,Russia-Ukraine War: Cyberattack – Kinetic Warfare Timeline, *January 26, 2024*,
https://www.msspalert.com/news/ukraine-russia-cyberattack-timeline-updates-amid-russia-invasion.
(2)HUR Initiates Cyberattack on Russian Drone Control Programs". *Kyiv Post (٨ .بالإنجليزية) Feb 2024*. Retrieved 2024-07-28.

الرسمي لمجلس الدوما في منطقة ستافروبول وأضافوا لافتة تحتوي على عبارة "انتظر، سنحررك!" وصوروا الساحة الحمراء وهي تحمل الأعلام الأوكرانية قبل وقت قصير من استهداف المطارات(١)

وبشكل عام ولمساندة حكومة كييف تكاتفت الدول الغربية ضد روسيا، وبدأت بفرض عقوبات عليها وصفت بأنها الأكثر شمولا وتضمنت حظر الرحلات الجوية، والعقوبات الاقتصادية، والطرد من نظام المال الدولي وحظر استيراد النفط الخام الرويس والغاز الطبيعي المسال.

خاتمة الدراسة وتوصياتها:

أولاً: النتائج:

خرجت الدراسة ببعض النتائج الأساسية وهي:

١. أن العمليات السيبرانية في الحرب الروسية الأوكرانية تؤدي دوراً داعماً وليس بالضرورة حاسماً في الحروب الكبرى، إذ ستستمر القوى العظمى في تعزيز قدراتها السيبرانية وضخ الاستثمارات بها لكن هذا الأمر سيؤدي إلى عوائد متناقصة بمجرد اندلاع صراع كبير. وإن كانت للعمليات السيبرانية مزايا متعددة على صعيد الحرب السياسية لكونها عاملاً مساعداً في اندلاع الاشتباك دون أن يرتقي لمستوى الحرب بمفهومها التقليدي، فضلاً عن دورها في العمل السري والمراقبة .

(1)*akharchenko, Kateryna; Dolomanzhy, Karina (12 Jun 2024).* "HUR Hackers Score Cyber-Hit on Russian Airports, Cause Flight Delays". *Kyiv Post (بالإنجليزية)*. Retrieved 2024-07-27.

٢. تتزايد التهديدات السيبرانية واسعة النطاق بمعدلات مثيرة للقلق في أنحاء العالم جميعه. وغالبًا ما يتم ربط هذه الهجمات بالتهديد الذي يتم الترويج له على نطاق واسع والذي يتمثل في الحروب السيبرانية.

٣. العمليات السيبرانية ما هي إلا وجه آخر للصراع الروسي الأوكراني والذي تشعب من صراع أمني واقتصادي وسياسي وتقني وعسكري كما شهدنا في بداية عام ٢٠٢٢ ، فالجانب الروسي لن يتخل أبدًا عن أدواته التقنية في مواجهة الحكومة الأوكرانية لما يسببه من نتائج وخسائر تدب في أركان الجيش الأوكراني ، وعلى الجانب الآخر تحاول أوكرانيا صد الهجمات بالاستعانة بالغرب لمواجهة الهجمات الروسية.

٤. بالتزامن مع اندلاع الحرب في أوكرانيا حدث أكثر من ٢٠٠ هجوم اليكتروني على أوكرانيا منذ بدء الغزو واستهداف ما يقرب عن ٧٠ من الكيانات الحكومية الأوكرانية.

٥. تتسم الطبيعة المتطورة للتهديدات الروسية السيبرانية بتكتيكات متغيرة باستمرار، ونواقل هجومية جديدة، ودوافع متغيرة، حيث تشمل الهجمات على البنية التحتية الحيوية، والتجسس، وتعطيل الخدمات وحرب المعلومات وحملات التضليل وسرقة الملكية الفكرية.

٦. استهدفت روسيا جراء توظيفها النسبي للحرب السيبرانية على أوكرانيا عدة أهداف منها(الحرب النفسية والخداع الاستراتيجي، والإخلال بمعادلة الدعم الغربي لأوكرانيا، وتقويض الثقة في النظام الأوكراني، وحرب السرديات وتآكل الثقة)

٧. وعن تداعيات الهجمات السيبرانية في الحرب الروسية الأوكرانية فتمثلت في : (التأثير في الرأي العام وإضعاف الروح المعنوية للسكان الأوكران واستهداف

البنية التحتية المدنية وضرب أوكرانيا اقتصادياً، وإضعاف الثقة في الحكومة الأوكرانية).

٨. تختلف الآلية التي تدير بها روسيا تفاعلاتها وفقا لطبيعة الظروف الدولية المحيطة .

٩. أن تاريخ الدول في استخدام الحروب السيبرانية إنما تعبر عن قدرتها الفعلية والمتقدمة في استخدامها.

ثانيا: التوصيات:

١. أن التهديدات السيبرانية التي تعطل الخدمات الحيوية مثل شبكات الدفع قد تؤثر بشدة على النشاط الاقتصادي.

٢. أن تعي جميع الدول أن الهدف الأسمى للأمن السيبراني هو القدرة على مقاومة التهديد المستمر في ظل التطورات المتلاحقة لتطبيقات التكنولوجيا.

٣. مواكبة التطور المستمر في إدارة الحرب السيبرانية؛ لأنها المعادلة الناجعة في الحرب الروسية على أوكرانيا.

قائمة المراجـــــع

أولاً: المراجع العربية:

١. آية رجب أبواليزيد، العمليات السيبرانية بين روسيا وأوكرانيا : قراءة في الأسباب والنتائج ،المركز الديمقراطى العربى تاريخ النشر ٢٠٢٤/٨/١٢
على الرابط https://democraticac.de/?p=99262

٢. ايهاب محمد أبو المجد ،الجيوسيبرانية العالمية والتحولات في أبعاد وخصائص القوة "آليات التوظيف في الاستراتيجية الروسية والصينية "، مجلة البحوث المالية و التجارية ،المجلد ٢٤، العدد الاول، يناير ٢٠٢٣ ،ص ١٣١

٣. الجزيرة الاخبارية، بعد عامين من إنشائه.. ما هو حال قراصنة "جيش أوكرانيا الإلكتروني"؟ تاريخ النشر ٢٠٢٤/٣/٢٠ على الرابط https://www.ajnet.me/tech/2024/3/20/%

٤. شبكة الشرق الأوسط وشمال أفريقيا للخدمات المالية ،اختراق إلكتروني كبير يستهدف أكبر شركة اتصالات خلوية في أوكرانيا "كييف ستار" تاريخ النشر ٢٠٢٣/١٢/١٣ على الرابط https://menafn.com/arabic/1107585630/%

٥. شوبير جلالي، مراد فائزة ، مفهوم الحروب السيبرانية والأمن السيبراني، مجلة الحقوق والحريات، جامعة عمار ثليجي الأغواط. كلية الحقوق والعلوم السياسية ، المجلد ١١ ، العدد ١ ، السنة ٢٠٢٣، ص ١٦٤، ١٦٥.

٦. صحيفة الشرق الأوسط ، أوكرانيا تنضم إلى مركز الناتو للدفاع السيبراني، تاريخ النشر ٢٠٢٣/٥/١٧، على الرابط https://aawsat.com/%D8%A7%D9%84

٧. عبد المنعم علي، تكتيكات متبادلة:حدود تأثير العمليات السيبرانية في الحرب الروسية الأوكرانية،تاريخ النشر ٢٠٢٤/١/٢ على الرابط https://futureuae.com/ar/Mainpage/Item/8906

٨. عبد المنعم علي، تكتيكات متبادلة:حدود تأثير العمليات السيبرانية في الحرب الروسية الأوكرانية،تاريخ النشر ٢٠٢٤/١/٢ على الرابط https://futureuae.com/ar/Mainpage/Item/8906

٩. فتحي بولعراس، تداعيات الازمة الأوكرانية على مستقبل اروبا، مجلة السياسة الدولية ، العدد ٢٢٨ ،ابريل ٢٠٢٢ ، المجلد ٥٧

١٠. نبيل عودة ، العمليات السيبرانية في الحرب الروسية الأوكرانية طبيعتها و أنماطها ، الشرق للأبحاث الاستراتيجية، 20 سبتمبر ٢٠٢٢، ص ٢٣.
١١. نسيب نجيب، الحرب السيبرانية من منظور القانون الدولي الإنساني ،المجلة النقدية للقانون والعلوم السياسية، كلية الحقوق والعلوم السياسية جامعة تيزي وزو، المجلد ١٩ ،العدد ٤، ٢٠٢١ص٢.
١٢. الهجمات السيبرانية المدمرة بين روسيا وأوكرانيا: حرب لن ينجو منها أحد ، شبكة النبأ المعلوماتية ، ١٦ آذار ٢٠٢٢، تاريخ الدخول ، تاريخ الدخول ٢٥ فبراير
https://annabaa.org/arabic/informatics/30480٢٠٢٤

ثانياً: المراجع الأجنبية:

1. HUR Initiates Cyberattack on Russian Drone Control Programs". Kyiv Post ,٨ Feb 2024. Retrieved 2024-07-28.
2. Jim Masters ,Russia-Ukraine War: Cyberattack – Kinetic Warfare Timeline, January 26, 2024, https://www.msspalert.com/news/ukraine-russia-cyberattack-timeline-updates-amid-russia-invasion.

3. Sharma ,Sharma S. New cyberattack tactics rise up as Ransomware payouts increase, CSO. 2023. [28 October 2023]. https://www.csoonline.com/article/574635/new-cyberattack-tactics-rise-up-as-ransomware-payouts-increase.html https://www.csoonline.com/article/574635/new-cyberattack-tactics-rise-up-as-ransomware-payouts-increase.html.
4. Ujang Priyono , Cyber warfare as part of Russia and Ukraine conflict , Jurnal Diplomasi Pertahanan , volume 8 , nomor 2 , 2022 , page 45.

5. Kaspersky ,Kaspersky Cybersecurity threats: what awaits US in 2023? Securelist. 2023. [2 November 2023]. https://www.rfc-editor.org/rfc/rfc4949 https://www.rfc-editor.org/rfc/rfc4949
6. Brooks,Brooks C. Cybersecurity trends and statistics; more sophisticated and persistent threats so far in 2023. 2023. [29 October 2023]. Forbes.

7. Jim Masters ,Russia-Ukraine War: Cyberattack – Kinetic Warfare Timeline, January 26, 2024,https://www.msspalert.com/news/ukraine-russia-cyberattack-timeline-updates-amid-russia-invasion

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

9. Pearson, James (27 Feb 2022). "Ukraine launches 'IT army,' takes aim at Russian cyberspace". Reuters (بالإنجليزية). Archived from the original on 2022-03-01. Retrieved 2022-02-27
10. Akharchenko, Kateryna; Dolomanzhy, Karina (12 Jun 2024). "HUR Hackers Score Cyber-Hit on Russian Airports, Cause Flight Delays". Kyiv Post (بالإنجليزية). Retrieved 2024-07-27