الأمن السيبراني في المنشآت الحكومية

Cyber security in government facilities

رحيم محمد *[1]، نبيلة بن يحي[2]

[1] كلية العلوم السياسية والعلاقات الدولية، جامعة الجزائر 03، (الجزائر)، Medsebil83@gmail.com

[2] كلية العلوم السياسية والعلاقات الدولية، جامعة الجزائر 03، (الجزائر)، Nani25@live.com

تاريخ الاستلام: 2023/04/01 تاريخ القبول: 2023/05/05 تاريخ النشر: 2023/06/05

ملخص:

إن تصاعد التوجه نحو الحكومة الإلكترونية التي تعتمد استخدام أنظمة الكمبيوتر وشبكة الإنترنت جعلت من المنشآت الحكومية أكثر عرضة للهجمات السيبرانية التي يمكن أن تستهدفها انطلاقاً من أي مكان في العالم للقيام بعمليات التجسس الإلكتروني أو سرقة المعلومات أو تعطيل الخدمة أو تخريب النظام أو زرع الفيروسات، وعلى ذلك تهدف كافة الحكومات إلى الحفاظ على الأمن السيبراني لتلك المنشآت الحيوية وتحصينها ضد أي هجوم سيبراني من خلال برامج مكافحة الفيروسات وحوائط النيران وتطوير أنظمة الأمان وكافة الإجراءات اللازمة لمنع اختراق أجهزة الحاسوب الخاصة بتلك المنشأت.

كلمات مفتاحية: المنشأت الحكومية؛ الأمن السيبراني؛ الهجمات الإلكترونية؛ الإرهاب السيبراني؛ الأمن القومي.

Abstract:

The escalation of the trend towards e-government that relies on the use of computer systems and the Internet which has become covering all parts of the world, Made it government facilities have become more vulnerable to cyber-attacks that can be targeted from anywhere in the world to carry out electronic espionage, steal information, disrupt service or sabotage system or plant viruses. Accordingly, all governments aim to maintain the cyber security of these vital facilities and immunize them against any cyber-attack, through anti-virus programs, firewalls, the development of security

systems and all necessary measures to prevent hacking of the computers of those facilities.
Keywords: Government facilities; cyber security; cyber-attacks, cyber terrorism; national security.

*المؤلف المرسل: رحيم محمد Medsebil83@gmail.com

1. مقدمة:

لقد جعل الإنترنت العالم أصغر من نواحٍ عديدة، لكنه فتح لنا أيضًا تأثيرات لم تكن من قبل بهذا التنوع والتحدي من قبل. ومع نمو الأمن على نحو متسارع، نما عالم القرصنة بشكل أسرع. والنظر في مسألة الأمن السيبراني يكون بطريقتان (Craigen, D., Diakun-Thibault, N., & Purse, R, 2014, pp. 13-21)؛ الأولى هي أن الشركات التي توفر الحوسبة السحابية تفعل ذلك ولذلك سيتم تأمين هذه الشركات بشكل جيد للغاية باستخدام أحدث تقنيات التشفير المتطورة. أما الطريقة الثانية فتتمثل في حماية المنشأت التي تستخدم هذه البرامج والتقنيات (Daniel, Schatz,; Julie, Wall, 2017, p. 12). وتستخدم المنشأت الحكومية برامج محمية بواسطة أنظمة متصلة بالإنترنت، بما في ذلك الأجهزة والبرامج والبيانات، من الهجمات الإلكترونية. في سياق الحوسبة، يشمل الأمن كلاً من الأمن السيبراني والأمن المادي وكلاهما تستخدمهما المؤسسات للحماية من الوصول غير المصرح به إلى مركز البيانات والأنظمة المحوسبة الأخرى و الأمان المصمم للحفاظ على سرية البيانات وسلامتها وتوافرها، وهو مجموعة فرعية من الأمن السيبراني (Carter, L. and F. Belanger, 2005, pp. 5-25).

وعلى مدى التاريخ، اتخذت المنظمات والحكومات نهج "المنتج النقطي" التفاعلي لمكافحة التهديدات السيبرانية، لإنتاج تقنيات الأمان الفردية واحدة فوق الأخرى لتأمين شبكاتها والبيانات القيمة بداخلها. هذه الطريقة ليست باهظة الثمن ومعقدة فحسب، ولكن أخبار الانتهاكات السيبرانية الضارة لا تزال تهيمن على عناوين الأخبار، مما يجعل هذه الطريقة غير فعالة. بدلاً من ذلك، يمكن للمؤسسات التفكير في نظام أساسي للأمان من الجيل التالي مُتكامل محليًا ومصمم خصيصًا لتوفير حماية متسقة قائمة على الوقاية (Clauberg, Rolf)

يتمثل الهدف الأساسي للأمن السيبراني في تعزيز قدرة الدول على مقاومة التهديدات الكامنة في الفضاء السيبراني، الأمر الذي دفع كثير من دول العالم لوضعه على أجندة عملها، في ظل ظهور الحروب

الإلكترونية التي تتعرض لها، فانتشار القوة السيبرانية بين عدد كبير من الفاعلين على الساحة الدولية أضرت بقدرة الدول على السيطرة والهيمنة، بل ومنحت فاعلين أصغر قدرة للعب دور أكبر من حجمها الفعلي في الفضاء السيبراني؛ مما يعني تغير في توازنات القوى بالنظام الدولي، الأمر الذي غير ماهية بعض التفاعلات بين الوحدات الدولية الفاعلة، من حيث التعاون والنزاع والصراع والهيمنة (جمال الدين، هبه، 2023، صفحة 193).

هذا وتكمن مشكلة الدراسة في التعرف على الأمن السيبراني للمنشآت الحكومية ومدى أهميتها، وكيفية حماية هذه المنشآت من الهجمات السيبرانية، ومدى تأثر الدولة بأي هجوم سيبراني على هذه المنشآت، الأمر الذي يدعونا إلى طرح التساؤلات الآتية: **فيما تتجلى أهمية الأمن السيبراني للمنشآت الحكومية؟ وما هي الإجراءات الواجب اتخاذها لحمايته؟ فيما يتمثل أثر الهجمات السيبرانية على المنشآت الحكومية؟ ما هو أثر انتهاك الأمن السيبراني على الدولة وعلى العلاقات بين الدول؟ وما دور الدولة في الحفاظ على أمنها السيبراني والقومي من الانتهاك؟**

وبغية الإجابة على الإشكالات التي يطرحها موضوع البحث، ارتأينا تقسيم هذه الدراسة إلى ثلاث مباحث؛ حيث تطرقنا في المبحث الأول لنشأة وتطور الأمن السيبراني وارتباطه بالمنشآت الحكومية، في حين سنتطرق في المبحث الثاني إلى بيان أثر التهديدات والمخاطر السيبرانية على المنشآت الحيوية للدولة، بينما خصصنا المبحث الثالث لدراسة انعكاس وتداعيات الأمن السيبراني على الأمن القومي.

2. نشأة وتطور الأمن السيبراني وارتباطه بالمنشآت الحكومية

الأمن السيبراني هو عملية حماية الأنظمة والشبكات والبرامج ضد الهجمات الرقمية. تهدف هذه الهجمات السيبرانية عادةً إلى الوصول للمعلومات الحساسة أو تغييرها أو تدميرها؛ بغرض الاستيلاء على المال من المستخدمين أو مقاطعة عمليات الأعمال العادية. (Happa, Jassim & Glencross, Mashhuda & Steed, Anthony, 2019).

1.2 مدى الحاجة إلى الأمن السيبراني

أصبح لهاجس الأمن أهمية كبرى مع الانتشار الواسع للإنترنت من أجل حماية الكم الهائل من المعلومات الموجود على الشبكة، وخاصة مع اكتشاف وجود العديد من الثغرات ونقاط الضعف في البرامج التي تقوم بتشغيل هذه المنظومة المعقدة والمتشابكة. وأصبحت الهجمات السيبرانية التي ترمي لسرقة البيانات أو تعطيل الخدمة أو تخريب أجهزة الكمبيوتر أمراً شائعاً لاستهداف المنشآت الحكومية التي تمثل

حجر الزاوية في النظام السياسي، والاقتصادي، والعسكري للدولة. تعد التكنولوجيا أمر ضروري لمنح المؤسسات والأفراد أدوات الأمن السيبراني اللازمة لحماية أنفسهم من الهجمات السيبرانية. هذا ويجب حماية ثلاثة كيانات رئيسية: الأجهزة الطرفية مثل أجهزة الكمبيوتر، والأجهزة الذكية، والموجّهات والشبكات والسحابة. وتتضمن أشكال التكنولوجيا الشائعة المستخدمة لحماية هذه الكيانات، الجيل التالي من الجدران النارية والحماية ضد البرامج الضارة وبرامج مكافحة الفيروسات وحلول أمان البريد الإلكتروني (الشريف، أشرف محمد عبدالمحسن، 2007).

والمنشآت الحكومية هي التي تمارس عادة نشاطاً إدارياً أو خدمياً حكومياً، مثل الوزارات والإدارات، على سبيل المثال وزارة الدفاع، والداخلية، والمالية، والمدارس الحكومية، والمراكز الصحية الحكومية، والمستشفيات الحكومية (Happa, Jassim & Glencross, Mashhuda & Steed, Anthony, 2019). ويتمثل الأمن السيبراني لهذه المنشآت في القدرة على حماية البيانات والمعلومات والوثائق الخاصة بها والتصدي لأية هجمات سيبرانية تستهدف تعطيل عملها أو سرقة المعلومات أو زرع أية فيروسات خبيثة تلحق الضرر بالبرامج أو أجهزة الكمبيوتر أو الشبكات (جهاز التخطيط والإحصاء، تعريف المنشأة الحكومية)، ويرتبط الأمن القومي للدول في الوقت الراهن بمدى أمنها وقوة دفاعاتها السيبرانية وطنياً وإقليمياً ودولياً بالقدر الذي يرتكز فيه على مدى امتلاكها لتكنولوجيا المعلومات، وقدرتها على توظيفها لحماية حدود الفضاء السيبراني الاستراتيجي؛ الأمر الذي يتطلب بالتأكيد سياسة تشريعية وأمنية شاملة ترتكز على آليات الاستباق والردع، والدعم المؤسسي واللوجيستي والتنسيق البيني أو متعدد الأطراف من أجل تأسيس منظومة شاملة للأمن السيبراني (Bennett, Louise, 2012).

وعلى ذلك، يجب تأسيس منظومة شاملة للأمن السيبراني في المنشآت الحكومية، من خلال حزمة من الآليات التشريعية والمؤسسية لضمان مواكبة ثورة المعلومات، والإحاطة بكل مستجدات عالم السيبرانية. وقد أصبح الأمن السيبراني يشكل جزءً أساسياً من أي سياسة أمنية وطنية، وسوء الاستغلال المتنامي للشبكات الإلكترونية لأهداف إجرامية يؤثر سلباً على سلامة البنى التحتية للمعلومات الوطنية الحساسة لا سيما على المعلومات الشخصية والبنى التحتية الأمنية الاستراتيجية. (Kumar, Pinosh & Akhilesh, K, 2020, pp. 4-6) ومن الضروري أيضاً وضع منظومة وطنية شاملة لأمن الفضاء السيبراني وحمايته، وتعزيز البيئة القانونية بالأدوات اللازمة بالوقاية من الجريمة السيبرانية إستباقياً، ثم

بعد ذلك اعتماد آليات الردع، كما يجب وضع استراتيجية لنشر الوعي لدى مختلف شرائح المجتمع، سواء من كان منهم من المستخدمين العاديين أو المهنيين أو متخذي القرار والمسؤولين عن سياسات الأمن والسلامة (دلالي، الجيلالي، و بلبشير، يعقوب، 2022، الصفحات 525-576).

هذا وتتم العمليات السيبرانية في وسط يعرف باسم الفضاء السيبراني؛ وهو حيز اجتماعي-مكاني أنتجه الدمج بين التكنولوجيات الوسائطية وشبكة الإنترنت ضمن مصفوفة تشابكية تتيح إنتاج وتبادل مختلف أشكال البيانات والمكونات النصية والسمعية البصرية والتفاعل بين المستخدمين، وهو محكوم بأطر الواقع الاجتماعي وأنظمته الثقافية ورموزه التداولية المحدودية. (محارب, محمود، 2011)، كما أن الفضاء السيبراني يشمل جميع أجهزة الكمبيوتر والمعلومات التي بداخلها والأنظمة والبرامج والشبكات المفتوحة للجمهور، وتلك الشبكات التي صممت لفئة معينة (سيف نصرت الهرمزي، 2019، صفحة 427).

وبسبب هذا الخطر الداهم والمتزايد تم تخصيص المليارات من الدولارات لمكافحة الهجمات السيبرانية؛ فقد بلغت قيمة سوق الأمن السيبراني الدفاعي العالمية 16.22 مليار دولار في عام 2020، ومن المتوقع أن تصل إلى 28.53 مليار دولار بحلول عام 2026، 2027 (Soikkeli, Jukka & Casale, Giuliano & Muñoz-González, Luis & Lupu, Emil, 2022, p. 1)، كما حدث نمو في حجم القوة العاملة في مجال الأمن السيبراني عام 2022 بنحو 11.1% عن العام السابق (Mendel, Jacob, 2019, pp. 24-47).

وبالرجوع إلى مجريات الأحداث، شهد عام 2022 طفرة كبيرة في الهجمات السيبرانية على المنشآت الحكومية. ففيما يخص المنشآت العسكرية، أدى تزايد اعتمادها على شبكة الإنترنت إلى تكرار وتكثيف وزيادة وتعقيد الهجمات الإلكترونية. وتهدف الهجمات السيبرانية إلى تدمير أو تعطيل أنظمة المعلومات أو سرقة البيانات والمعلومات الهامة باستخدام وسائل مختلفة، مثل برامج التجسس، والفيروسات، والبرمجيات الخبيثة، والتصيّد الاحتيالي، والمرفقات الضارة وغيرها من وسائل القرصنة التي أصبحت شائعة ودائمة التجدد (Gavenaite, Julija & Miečinskienė, Algita, 2021, p. 278).

فضلاً عن هذا، فقد ارتفع عدد الهجمات السيبرانية في الشهور الست الأولى من العام 2022 مقارنة بنفس الفترة من عام 2021، فقد حقق نموذج فيروسات الفدية أرباحاً كبيرة بالنسبة

لمطوري فيروسات الفدية والشركات التابعة لهم. ونجحت شركة "تريند مايكرو" في التصدي لتهديدات تقدر قيمتها بنحو 63 مليار في النصف الأول من عام 2022، وهذا يوازي أكثر بنسبة 52% في النصف الأول من 2022 مقارنة بنفس الفترة من عام 2021، وكان القطاع الحكومي والتصنيع والرعاية الصحية من القطاعات التي حظيت بنصيب الأسد بالنسبة للهجمات التي استخدمت فيروسات الفدية شائعة الاستخدام (Sharif, Md Haris & Mohammed, Mehmood, 2022, pp. 138-156). كما شهد عام 2022 تصاعداً كبيراً في عدد الهجمات السيبرانية على برامج العملات المشفرة مثل البيتكوين وغيرها؛ حيث تمت سرقة حوالي 3 مليار دولار من العملات المشفرة، مما أجبر العديد من الدول إلى إنفاق مبالغ طائلة للاستثمار في مجال الأمن والقيام بالعديد من البحوث العلمية في مجال الذكاء الاصطناعي لتطوير تطبيقات جديدة منخفضة التكاليف، لحماية منشآتها (Gavenaite, Julija & Miečinskienė, Algita, 2021).

2.2 مدى خطورة التهديدات السيبرانية

تدرك الحكومات الخطورة التي تشكلها الهجمات السيبرانية على المنشآت الحيوية للدولة من حيث تأثيرها على شبكات المعلومات وأجهزة الحاسب الآلي والبنية التحتية للاتصالات ومراكز دعم اتخاذ القرار، وعلى ذلك قامت بعض الدول بإنشاء مجلس أعلى للأمن السيبراني من أجل منع وصد أية هجمات سيبرانية تستهدف هذه المنشآت الحيوية. ففي مصر على سبيل المثال أعلنت رئاسة الوزراء عن تشكيل المجلس الأعلى للأمن السيبراني الذي يهدف إلى تكوين مظلة شاملة لحماية أمن المعلومات ونظم الحاسب الآلي والشبكات الخاصة بالمنشآت الحكومية لمنع الإضرار بها أو تعطيل خدماتها (3 مخاطر تدفع الحكومة إلى تشكيل المجلس الأعلى للأمن السيبرانى، 2018).

كما يهدف إلى تعزيز الأمن السيبرانى الذي يشمل أمن المعلومات على أجهزة وشبكات الحاسب الآلي، بما في ذلك العمليات والآليات التي يتم من خلالها حماية معدات الحاسب الآلي والمعلومات والخدمات من أي تدخل غير مقصود أو غير مصرح به أو تغيير أو إتلاف للمعلومات والبيانات. وقد تم وضع استراتيجية شاملة لتأمين البنية التحتية للاتصالات والمعلومات لتوفير بيئة آمنة لمختلف القطاعات لتقديم خدمات إلكترونية متكاملة. ويشمل ذلك عدداً من البرامج التي تدعم الأهداف الاستراتيجية للأمن السيبرانى، (Kammouh, Omar & Cimellaro, 2018).

ومع ظهور أنواع جديدة من الهجمات السيبرانية تستهدف إعاقة الخدمات الحيوية، لنشر برمجيات خبيثة وفيروسات لتخريب أو تعطيل البنى التحتية للاتصالات وتكنولوجيا المعلومات وخطورة ذلك على المنشآت الحيوية أصبح من الضروري حماية تلك المنشآت لتجنب الإضرار بالأمن القومي للبلاد (Finkle, J, 2016). أو تلك الهجمات التي تعتمد على تقنيات متقدمة كالحوسبة السحابية، والذكاء الاصطناعي، وإنترنت الأشياء، وأجهزة التنصت على شبكات الاتصال السلكية واللاسلكية، وبرامج فك شفرة واختراق الأنظمة، والبرمجيات الخبيثة التي تمس أمن الشبكات من أجل إحداث فوضى شاملة في منظومة المعلومات الخاصة بالدولة من أجل الابتزاز والتخريب (Choo, K.K.R, 2008, pp. 270-295). كما تم إنتاج فيروسات غاية في التعقيد من أجل تخريب أجهزة المعلومات الخاصة بالمنشآت العسكرية؛ حيث يتطلب ذلك فريق عمل من الخبراء في مجال تكنولوجيا المعلومات وتكاليف باهظة مما يتعين أن تقوم به دول كبرى لاستهداف دول أخرى فيما يعرف باسم الحرب السيبرانية. كما قامت الجماعات الإرهابية باستغلال هذه الأدوات الخطيرة من خلال سرقة أو الاستيلاء على هذه التقنيات وتجنيد الخبراء لشن هجمات إرهابية على الدول التي تستهدفها من أجل التخريب أو جني المال لتمويل أنشطتها الإرهابية (Boughton, Nick, 2019, pp. 18-19).

3. أثر التهديدات والمخاطر السيبرانية على المنشآت الحيوية للدولة

مع تنامي خطر التهديدات والمخاطر السيبرانية يتزايد خطر استهداف المنشآت الحيوية للدولة، ويمكن أن يؤدي الهجوم على تلك المنشآت الحيوية إلى أضرار مادية ومعنوية لا حصر لها تشكل خطورة بالغة على الأمن القومي للدولة (Plėta, Tomas & Tvaronavičiene, Manuela & Casa, Silvia & Agafonov, Konstantin., 2020, pp. 703-715).

فعلى سبيل المثال، في أمريكا مثلاً تقوم الحكومة الفيدرالية يومياً بصد عشرات الآلاف من الهجمات الإلكترونية من جانب الخصوم، بعض هذه الهجمات بسيطة -رسائل بريد إلكتروني تهدف إلى خداع موظف اتحادي متواضع على أمل القيام بهجمات أكثر تعقيداً تستهدف أصول البيانات الأكثر قيمة في البلاد- (The Importance of Cyber Technologies in Government). ومن أجل صد هذه الهجمات، تستخدم الوكالات الحكومية أدوات الأمن السيبراني للقيام بهذه المهمة؛ نظراً لأن المتسللين أصبحوا أكثر تطوراً، وتحتاج الوكالات الحكومية إلى حماية البيانات في كل مرحلة من مراحل حياتها من لحظة جمعها وحتى إرسالها إلى مكان تخزينها وحتى حذفها

(Thakur, Kutub & Liakat, Md & Jiang, Ning & Qiu, Meikang, 2016).

1.3 الجانب المستفاد من الهجمات السيبرانية:

علمت الحكومة الفيدرالية الأمريكية مدى أهمية الأمن السيبراني في مارس من عام 2014 حين تم اختراق مكتب إدارة شؤون الموظفين، الذي يحتوي على المعلومات الشخصية لجميع الموظفين الفيدراليين والأشخاص المتقدمين لشغل الوظائف في الحكومة الفيدرالية (AlZain, Mohammed & Masud, Mehedi & Al-Amri, Jehad & Soh, Ben & Altwairqi, Asalah, 2019, pp. 2131-2139). وعلى الرغم من وجود الكثير من الأسباب المتنوعة لحدوث هذا الانتهاك فقد أدى إلى الاستيلاء على المعلومات الشخصية لما يزيد عن 20 مليون شخص ودفعت الحكومة الفيدرالية مقابل مراقبة ائتمانية مجانية لكل من الضحايا للمساعدة في تصحيح الوضع. وقام الكونجرس ومكتب التحقيقات الفيدرالي بالتحقيق في الأمر واستقال عدد من المسؤولين، وهذا يؤكد أن الهجمات الإلكترونية تحدث بالفعل ويمكن أن تكون مدمرة بشكل لا يصدق، ولمنع مثل هذه الهجمات، تحتاج الوكالات الحكومية إلى الاستثمار باستمرار في تحديات الأمن السيبراني (Prasad, Ramjee & Rohokale, Vandana, 2020).

وطوال العقود القليلة الماضية لم تتوقف الهجمات السيبرانية عن استهداف كبرى المنشآت والوكالات الحكومية والمواقع والوزارات والمؤسسات والجماعات والأفراد مؤدية إلى نتائج كارثية، ويتوقع الخبراء أن تصل تكلفة تلك الهجمات على مستوى العالم بحلول عام 2025 إلى 10.50 تريليون دولار (Choudhary, Atul & Choudhary, Pankaj & Salve, Shrikant., 2018). وعلى سبيل المثال يعد فيروس ميليسا؛ أحد أقدم وأكبر التهديدات الإلكترونية في عام 1999 من قبل المبرمج ديفيد لي سميث، قام بإرسال ملف للمستخدمين يفتح من خلال برنامج ميكروسوفت وورد، وكان يحمل فيروساً. وبمجرد فتح الملف وتنشيط الفيروس تسبب في أضرار جسيمة لمئات الشركات بما في ذلك شركة ميكروسوفت، وقدرت تكلفة إصلاح الأنظمة المتضررة بنحو 80 مليون دولار (Prasad, Ramjee & Rohokale, Vandana, 2020).

هذا وقد أصفر الهجوم على شركة أدوب Adobe عام 2013 إلى انتهاك بيانات 2.9 مليون مستخدم. علاوة على ذلك، فقد أضر بالبيانات الشخصية لما يصل إلى 38 مليون مستخدم،

وزعمت الشركة أنه تم اختراق كلمات المرور ومعلومات بطاقة الائتمان لأول 2.9 مليون مستخدم فقط، ومع ذلك، عانى 35.1 مليون مستخدم من فقدان كلمات المرور وأسماء المستخدمين الخاصة بهم (Saini, Gaganjot & Halgamuge, Malka & Sharma, Pallavi & Purkis, James, 2019, pp. 98-126). وفي عام 2014، تعرضت شركة ياهو لهجمة الكترونية أصفرت عن اختراق 500 مليون حساب، وخلال الهجوم، تمت سرقة المعلومات الأساسية وكلمات المرور، بينما لم تتم سرقة المعلومات المصرفية. وكان الهجوم السيبراني على شبكة كهرباء أوكرانيا في عام 2015 أول هجوم إلكتروني على شبكة كهرباء. (Bendovschi, Andreea, 2015, pp. 24-31).

هذا وكان لبرنامج الفدية تأثيرٌ كبيرٌ على العديد من الصناعات بتكلفة عالمية بلغت حوالي 6 مليارات جنيه إسترليني من أجل إصلاحها؛ على سبيل المثال ما وقع في سنة 2017 والمسمى فقد أثر على حوالي 200 ألف جهاز كمبيوتر في أكثر من 150 دولة (Vander-Pallen, Maame & Addai, Paul & Isteefanos, Stuart & Khan Mohd, Tauheed, 2020). وفي يونيو 2021 حدث أكبر انتهاك لكلمات المرور في التاريخ، رأينا مجموعة من حوالي 8.4 مليار كلمة مرور مسربة في هجوم RockYou2021، في الواقع، كان هذا أكبر اختراق منذ هجوم موقع في RockYou عام 2009 والذي أثر على 32 مليون حساب (Li, Yuchong & Liu, Qinghui, 2021, pp. 8176-8186).

2.3 التعزيزات الأمنية لصد الهجمات السيبرانية

يمكن للمنشآت الحكومية أن يكون لديها مجموعة متنوعة من حلول الأمن السيبراني للاختيار من بينها. وتساهم هذه الحلول الأمنية في حماية البيانات في مراحل مختلفة تتضمن وقت جمع البيانات لأول مرة، ونقلها بين الأنظمة والمستخدمين المختلفين وأثناء التخزين حتى يتم حذفه. وعلى الرغم من وجود العديد من الأنظمة المختلفة، إلاّ أنها جميعاً لديها نفس الهدف وهو تزويد الوكالات الحكومية برؤية واضحة لما يحدث على شبكات الكمبيوتر الخاصة بها وتنبيه المسؤولين إلى أي سلوك مشبوه يشير إلى احتمال حدوث هجمات سيبرانية (Mahfouz, Ahmed & Opara, Emmanuel, 2016). وهناك العديد من الأشكال الشائعة لتقنية الأمن السيبراني التي تتضمن الذكاء الاصطناعي (AI) والتعلم الآلي (ML) حيث تستخدم أحدث الأدوات الإلكترونية تحليلات السلوك للتصدي للجهات التي تقوم

بشن الهجمات في مساراتها ومنع وقوع الملكية الفكرية والبيانات الحساسة في الأيدي الخطأ. وتعمل هذه التحليلات الشاملة عبر بيئات البيانات لتحديد وإيقاف التهديدات لحركة مرور الشبكة والملفات والأجهزة، والاستفادة من تحليلات سلوك المستخدم التي تزداد ذكاءً بمرور الوقت. (Abdalla, Ghazi & Varol, Hacer, 2019, pp. 1-6).

كما يمكن استخدام أنظمة كشف ومنع التسلل التي تعرف باسم أدوات IDS وIPS، لمساعدة موظفي تكنولوجيا المعلومات في تحديد شبكاتهم السلكية واللاسلكية وحمايتها من العديد من أنواع التهديدات الأمنية، وقد أصبحت هذه التقنيات، مثل أدوات أمان الشبكات الأخرى، أكثر شيوعاً مع تزايد تعقيد الشبكات الحكومية. وتكشف كل من حلول IDS و IPS نشاط التهديد على شكل برامج ضارة وبرامج تجسس وفيروسات وديدان وأنواع هجوم أخرى، بالإضافة إلى التهديدات التي تشكلها انتهاكات السياسة. كما تقوم أدوات النظام بكشف التسلل من خلال رصد النشاط المشبوه وكشفه؛ وتؤدي أدوات IPS إلى مراقبة نشطة ومنع الهجمات من قبل مصادر معروفة وغير معروفة (Abdalla, Ghazi & Varol, Hacer, 2019).

ومن جهة أخرى تساهم أدوات مكافحة البرامج الضارة المسؤولين على تحديد البرامج الضارة وحظرها وإزالتها، والغرض الأساسي من البرامج الضارة؛ هو البحث عن نقاط ضعف الشبكة، خاصة في دفاعات الأمان وأنظمة التشغيل والمتصفحات والتطبيقات والأهداف الشائعة مثل Adobe Flash و Acrobat Reader. وتتطلب أفضل الممارسات دفاعًا متعدد الجوانب قد يشمل أيضًا القائمة السوداء لعناوينIP، وأدوات منع فقدان البيانات، وبرامج مكافحة الفيروسات وبرامج التجسس، ومراقبة سياسات تصفح الويب، وكلمات المرور (Dedakia, Priyanka, 2020). فضلاً عن هذا، يمكن استخدام إدارة الأجهزة النقالة والتي تُعرف باسم MDM؛ وهي تسمح للمسؤولين بمراقبة تكوينات الأمان والتحكم فيها عن بُعد عبر الأجهزة المحمولة. ويسمح هذا للموظفين بالعمل عن بُعد على الأجهزة المعتمدة من الوكالة، ولكن يمكن للقيادة أن تعرف أن هذه الأجهزة آمنة حيث يمكنها إدارتها في جميع الأوقات (Suhasini, Sodagudi & Kotha, Sita & Raju, M, 2019).

4. انعكاس وتداعيات الأمن السيبراني على الأمن القومي

يعد الأمن القومي أو الوطني قدرة حكومة الدولة على حماية مواطنيها واقتصادها ومؤسساتها الأخرى، وتشمل بعض المستويات غير العسكرية للأمن القومي الأمن الاقتصادي، والأمن السياسي، وأمن

الطاقة، والأمن الداخلي، والأمن السيبراني، والأمن البشري، والأمن البيئي. لضمان الأمن القومي. ويمكن أن تؤدي الهجمات السيبرانية من خلال الدول أو الأفراد أو التنظيمات الإرهابية إلى الإضرار بالأمن القومي على كافة المستويات على نحو يمكن أن يحرم مدناً بأكملها من الخدمات الحيوية كسرقة المعلومات الشخصية الخاصة بالمواطنين والتي قد تشتمل على أرقام بطاقات الائتمان أو المعلومات الخاصة بالتأمين الصحي أو مذكراتهم الشخصية.

1.4 الصراع السيبراني بين الدول وتهديد الأمن القومي

يمكن القول بأن الصراع العسكري التقليدي بين دول العالم قد تراجع وأفسح المجال للحرب السيبرانية التي تستخدم فيها أسلحة تكنولوجية فتاكة تتفوق في قوتها التدميرية على أسلحة الدمار الشامل ولكن دون أن تسيل قطرة دم واحدة، ويتميز هذا الصراع الإلكتروني بعدم وجود مواجهة مباشرة وعدم معرفة الفاعل على نحو مؤكد وانخفاض التكاليف المادية حيث يمكن لجهاز كمبيوتر متواضع متصل بشبكة الإنترنت أن يشن هجوماً كاسحاً على دولة، ولو من قبل شخص واحد فيقوم بإعداد فيروس مدمر ونشره عبر الشبكة لتدمير العديد من الأجهزة في الكثير من الدول. لقد تحول الفضاء الإلكتروني إلى ساحة جديدة للصراع الدولي متعدد الأطراف، بسبب حالة انعدام الثقة بين الدول المتصارعة بالإضافة إلى التطورات الهائلة في الفضاء الإلكتروني، التي دفعت الدول إلى تبني مناهج جديدة في العقيدة الأمنية لديها وذلك بإضافة القوة السيبرانية أو القدرة على شن أو صد هجمات إلكترونية على خصومها كعنصر رئيسي لمدى قوة الدولة وقدرتها على حسم الصراعات. وعلى إثر ذلك أصبح هناك أمننة لقضية الحروب الإلكترونية، وجعلها قضية هامة تمس الأمن القومي للدول (محمد عاطف إمام إبراهيم، 2022).

لقد أنتجت الحروب الإلكترونية العديد من المخاطر والتهديدات للأمن القومي للدولة؛ سواء من خلال أساليب عملها مثل التجسس الإلكتروني والهجوم الإلكتروني أو من خلال زرع الفيروسات أو تخريب قواعد البيانات وسرقة المعلومات، وعلى المستوى العسكري في شكله الجديد أدت الحروب الإلكترونية إلى تنامي المخاطر السيبرانية خاصة مع قابلية تعرض المنشآت الحيوية في الدولة للهجوم، مما يؤدي إلى التأثير على وظائف تلك المنشآت والحد من كفاءتها على تقديم الخدمات المنوطة بها. والتحكم في شن هذه الهجمات يعتبر أداة استراتيجية وسلاحاً رهيباً في يد الدولة أو الجماعة أو الجهة التي تقوم بهذا الهجوم، وقد لعبت الحروب الإلكترونية دوراً هاماً في عسكرة الفضاء الإلكتروني؛ أي تحويله

إلى ساحة للقتال، وبالتالي تصاعدت وتطورت القدرات الإلكترونية في سباق التسلح السيبراني وتم تبني سياسات دفاعية سيبرانية في مجال تطوير أدوات الحرب الإلكترونية داخل الجيوش الحديثة، ولم يتم الاكتفاء بذلك ولكن تم الاتجاه إلى تطوير قدرات هجومية إلكترونية من أجل القدرة على الردع السيبراني. وقد هدفت الحروب الإلكترونية إلى الهجوم واختراق المخططات العسكرية للدول، مما ساهم في التعرف على طبيعة القوة العسكرية للدولة وتكتيكها العسكري (دحماني، 2017).

أما على المستوى الإقتصادي للدولة، قد تستهدف الهجمات الإلكترونية توقف شبكة الإنترنت كلياً في الدولة المستهدفة، مما يؤدي لتوقف المعاملات البنكية ومعاملات الحكومة الإلكترونية وسرقة أرقام وتفاصيل بطاقات الائتمان التي يتم التسوق بها عبر الإنترنت، مما ينتج عن ذلك تعطل تدفق الأموال في الدولة وبالتالي توقف أهم القطاعات في الدولة مثل الصناعة وغيرها من قطاعات الدولة، كما يمكن أن تستهدف الهجمات أجهزة التحكم في المراقبة الجوية للطائرات مما يؤدي إلى تعطل حركة الملاحة الجوية ويؤدي إلى إغلاق الحدود وعزل الدولة عن العالم الخارجي (Thakur, Kutub & Liakat, Md & Jiang, Ning & Qiu, Meikang, 2016, p. 22).

ومن جانب آخر يمكن أن تؤدي الهجمات السيبرانية على المستوى الخدمي إلى توقف الخدمة في المرافق الحيوية كما يحدث على سبيل المثال عند انقطاع الكهرباء عن المستشفيات أثناء إجراء العمليات الجراحية لمدد طويلة، وكذلك تعطل خطوط السكك الحديدية (Lala, Chandana & Panda, Brajendra, 2001, pp. 300-310).

أما على المستوى الثقافي، يمكن أن تستهدف الهجمات السيبرانية تشويه أو تدمير أو تغيير هوية الدولة من خلال الترويج لأفكار الدولة المهاجمة أو الأفكار المتطرفة بأساليب تستهدف شباب الدولة وتُأثر على أفكاره ومعتقداته (مهدي، 2021، الصفحات 151-174). وهذا ما تستخدمه العديد من الفواعل غير الدولية مثل التنظيمات أو الجماعات الإرهابية التي تستهدف الشباب وتشحنه بأفكار متطرفة تدفعه إلى معاداة دولته أو القيام بأعمال إرهابية تستهدف رموز الدولة أو مواطنيها أو منشآتها الحيوية لإحداث حالة من الاضطراب والقلق وعدم الاستقرار على نحو يضر بالأمن القومي للبلاد (هادي سهيلة، 2020، الصفحات 122-145).

أما على المستوى السياسي، فإن الهجمات السيبرانية يمكن أن تؤدي إلى إثارة الفتن في الدولة وتحريض الشعب ضد حكومته وبث الكراهية من خلال نشر الإشاعات بوجود مخاطر تهدد الدولة وعدم

توفر الاحتياجات الأساسية للشعب وانتشار المحسوبية والفساد ونهب الثروات وحث الشعب على الثورة، ولعب هذا الهدف دوره في ثورات الربيع العربي عام 2011 التي تسببت في سقوط أنظمة حُكم العديد من حُكام الدول العربية بل هناك دول لم تستطيع استرجاع عافيتها بعد هذه الثورات مما جعلها مناطق تنافس بين الدول الكُبرى بل وجعلت التنظيمات الإرهابية من هذه الدول مكاناً لها (دحماني، 2017) .

أضحى امتلاك الدول للقوة الإلكترونية خطراً أكبر على الدول المستهدفة ومن هنا جاء التحول في مفهوم الأمن؛ بحيث لم يعد أمن الدولة القومي مُقتصر على الأمن العسكري بل أصبح هناك الأمن القومي السياسي، والذي يتلخص في المحتوى الأمني للبيانات الرقمية والمعلومات الإلكترونية التي تخص الأحزاب في الدولة، إضافةً للمعلومات التي تتعلق بالبرلمانات وأجهزة الدولة السيادية هي كلها معلومات حساسة قد يؤدي العبث بها لحروب أهلية داخل الدولة، وكذلك الأمن القومي الفكري والثقافي والذي يُمثل ذروة الإنتاج الفكري لأي دولة والتي قد تُساهم في رفع أو خفض مظاهر الأمن القومي للدولة، كالمظهر المادي المتعلق باستقرار المواطنين أو رفع الهواجس الأمنية في الدولة (حمذان، خينش، 2018، الصفحات 19-34).

ونظراً لتعرض المنظومات السياسية، والعسكرية، والاقتصادية، والعلمية، والخدمية، في الدولة لمثل هذه الحروب كان لا بد من وجود أنواع متعددة من الأمن القومي الاقتصادي، والسياسي، والعسكري، والثقافي، والخدمي، من أجل التصدي لمثل هذه الهجمات. ويتم التركيز على الأمن القومي الاقتصادي؛ حيث أنه أكثر القطاعات الأمنية عِرضةً للحروب السيبرانية؛ نظراً لتحول الاقتصاد العالمي لاقتصاد رقمي معتمد على تكنولوجيا المعلومات، وبالتالي تعرض تلك المنظومة لمثل هذه الهجمات قد يتسبب في خسائر اقتصادية وقومية هائلة. كما يتم التركيز أيضاً على الأمن القومي العلمي والبحثي الذي يتعلق بالبيانات والمعلومات الخاصة بالمؤسسات البحثية والعلمية والجامعات والتي تُشكل ثروة قومية مستقبلية تحوي العديد من الاكتشافات وبراءة الاختراع المعرضة للسرقة عن طريق القرصنة الإلكترونية (محمد، شيماء جمال، 2021).

2.4 منظومة وجهود الدولة لمكافحة الهجمات السيبرانية

نظراً لخطورة الهجمات السيبرانية أو الحرب الإلكترونية على الأمن القومي للدولة واستهدافها المنشآت الحيوية للدولة كان يجب على الدولة أن تضع منظومة متكاملة واضحة وشاملة لصد ومجابهة هذه

الهجمات للحفاظ على أمنها القومي بكل أنواعه ومناحيه، وتشمل هذه المنظومة بناء الجيوش السيبرانية التي تتكون من خبراء في الأمن السيبراني، وخبراء في التكنولوجيا، وخبراء في القرصنة وشن الهجمات الإلكترونية، ورصد ميزانيات ضخمة للتطوير في مجال الهجوم والدفاع والحماية. وتعتبر أمريكا الأولى في مجال بناء الجيوش السيبرانية وفي حجم الميزانية الضخمة المخصصة لذلك؛ وتبلغ هذه الميزانية نحو 7 مليارات دولار سنوياً تنفق على الأمن السيبراني، وتخصص كوريا الشمالية حوالي 20% من الميزانية العسكرية للأمن السيبراني.

كما تشمل هذه المنظومة تشكيل هيئات قومية للأمن السيبراني، من أجل المساهمة في رفع مستوى الوعي بالأمن السيبراني وإعداد الاستراتيجية الوطنية لهذا الأخير والإرشادات المتعلقة به ووضع السياسات والمعايير الوطنية للتشفير، بالإضافة إلى سن تشريعات قومية لحماية الأمن السيبراني مثل قانون مكافحة الجرائم السيبرانية (دحماني، 2017). ووجب أن تشمل المنظومة تعزيز الجوانب التقنية ومنها إنشاء حوائط النيران أو الجدران النارية التي تُعد من أهم الوسائل التقنية لصد الهجمات الإلكترونية، وهي تقوم على مبدأ الفصل بين الأنشطة الموثوق بها والأنشطة غير الموثوق بها في شبكات الحاسب الآلي، ومراقبة العمليات التي تمر بالشبكة الإلكترونية من خلال قواعد معينة. كما يشمل ذلك تطبيق تكنولوجيا طبقات التطبيقات؛ الذي يُمكن أن يفهم ويتعامل مع التطبيقات والأنظمة المعقدة ومن ثم يُمكنه اكتشاف إذا كان هناك نظام غير مرغوب فيه يتم تسريبه أو نظام يتم استخدامه بطريقة مؤذية (محمد، شيماء جمال، 2021).

وبالموازاة بإمكان الدولة أن تقوم بإنشاء شركات ومؤسسات متخصصة في أمن المعلومات والمعايير التي تتولى مهمة تشفير المعلومات والبيانات المتداولة إلكترونياً والحفاظ عليها، وتعتبر أمريكا رائدة في إستخدام هذه الآلية؛ حيث يوجد بها المعهد القومي للتكنولوجيا والوكالة الفيدرالية المسؤولة عن أمن المعلومات والتي لها ارتباطات بوكالة الاستخبارات الأمريكية؛ وذلك لأن أمريكا من أكثر الدول المستهدفة في الفضاء الإلكتروني بسبب توجهاتها الداخلية والخارجية (Dorn, Walter & Webb, Stewart, 2019, pp. 19-30). ويجب أيضاً تعزيز الجهود الدولية في مجال الحد من سباق التسلح في الفضاء الإلكتروني؛ حيث يخلق نوعاً من المنافسة بين الدول والتي تتحول لحرب؛ نظراً لامتلاك الطرفين قوة تكنولوجية هائلة تُمكنهم من شن الهجمات الإلكترونية. وقد كانت بداية ظهور سباق التسلح في الصراع الروسي مع استونيا وجورجيا بل والتطور البارز الذي حدث في سباق التسلح تمثل في فيروس

ستاكسنت الموجه ضد البرنامج النووي الإيراني والتي أُتهمت في القيام به كلاً من أمريكا وإسرائيل (Aldlabeeh, 2022).

وتقوم العديد من دول العالم باتخاذ إجراءات وقائية لها صفة تشريعية، بما في ذلك سن تشريعات وقوانين على المستوى القومي لتجريم الدول والجهات والأطراف التي تُقدم على شن الحرب الإلكترونية وتشديد العقوبات على المخالفين. وقد تم إبرام اتفاقية مجلس أوروبا بشأن الجريمة الإلكترونية المعروفة باتفاقية بودابست عام 2001، ألزمت الدول الموقعة بسن القوانين الجنائية ضد أنشطة معينة في الفضاء الإلكتروني، وفي عام 2003 صدر القرار رقم 32 حول موضوع التطور في ميدان المعلومات والاتصالات وأكد على الحاجة إلى تعزيز التنسيق والتعاون الدولي في مكافحة إساءة إستخدام تكنولوجيا المعلومات (Hathaway, Oona & Crootof, Rebecca & Levitz, Philip & Nix, Haley & Nowlan, Aileen & Perdue, William & Spiegel, Julia, 2011, pp. 817-885.)

وصدر دليل يُعرف بدليل تالين بشأن القانون الدولي الإنساني المنطبق على الحرب الإلكترونية وذلك عام 2013 وصدرت نسخة ثانية منه عام 2017، وهو يحدد القواعد يجب على الدول اتباعها عند القيام بشن هجمات في الفضاء الإلكتروني ضدها. وفي عام 2015 صدر تقرير يقر وضع معايير للحد من المواجهة في الفضاء الإلكتروني ووضع معايير لأمن وسلامة البيانات (Vršanský, Peter & Bednár, Daniel, 2017, pp. 38-49)

5. خاتمة:

أضحى الأمن السيبراني مسألة تهم الكثير من الحكومات وذلك بسبب التحولات الجذرية التي حدثت في الصراع الدولي وفي ميزان القوى العالمية؛ حيث تحولت الحرب التقليدية إلى حرب إلكترونية أو سيبرانية تلحق دماراً شاملاً بالعديد من الدول خلال لحظات قصيرة من خلال اقتحام أجهزة الحاسب الآلي المتصلة بشبكة الإنترنت والتي تهيمن على عمل العديد من المنشآت الحيوية للدولة. وأصبح بإمكان الدول والجماعات الإرهابية والأفراد تصنيع فيروسات ضارة يمكن زرعها في المنظومات الإلكترونية الخاصة بالدول أو الشركات أو المنشآت المستهدفة فتؤدي إلى تدمير البيانات أو تعديلها أو تشويهها أو توقف أو تعطل الخدمة في المنشآت الحيوية للدولة المعتمدة على أجهزة الكمبيوتر. كما ألحق أضراراً بأمنها القومي الاقتصادي أو السياسي أو العسكري أو الثقافي على نحو لم يسبق له مثيل. وأدى ذلك إلى تغيّر في ميزان

القوى العالمية؛ حيث أصبحت قوة الدول تقاس بمدى قدرتها على حماية أمنها القومي ومنشآتها الحيوية من الهجمات السيبرانية والحفاظ على أمنها السيبراني وكذلك قدرتها على شن هجمات مضادة أو ما يعرف باسم الردع السيبراني. وبعد الفراغ من هذه الدراسة، توصلنا إلى بعض النتائج وأبدينا بعض التوصيات:

أولاً– نتائج الدراسة:

1) أصبح الأمن السيبراني ضرورة ملحة للدول تفرضها ظروف الصراع العالمي اليوم يجب أن توليه الدول أكبر عناية ممكنة، ومن ثم وجب على الدول حمايته وإلاّ تكبدت خسائر مادية ومعنوية فادحة وتدفع الثمن مضاعفاً.

2) تراجعت الحرب التقليدية والأسلحة التقليدية وأفسحت المجال للحرب السيبرانية التي يمكن أن تضرب مجموعة من الدول في لحظات قصيرة.

3) أصبح الأمن السيبراني جزءً لا يتجزأ من الأمن القومي للدولة والذي يمكن أن يشمل الجوانب العسكرية والاقتصادية والسياسية والثقافية والخدمية، ومن ثم تم بذل العديد من الجهود الدولية في سبيل حمايته من الهجمات السيبرانية وشملت هذه الجهود العديد من القوانين والتشريعات.

ثانيا– توصيات الدراسة:

1) تطوير برمجيات وتقنيات حديثة من أجل حماية المنشآت الحيوية للدولة من أي هجوم سيبراني.

2) سن قوانين وتشريعات حازمة ترفع العقوبة على الجهات أو الأفراد أو التنظيمات التي تقوم بشن هجمات سيبرانية تستهدف الأمن القومي.

3) نشر الوعي بين العاملين في مجال تكنولوجيا المعلومات من أجل عدم الوقوع في براثن الاحتيال الإلكتروني وفتح الملفات المشبوهة.

4) رصد ميزانية ملائمة على مستوى الدولة من أجل تعزيز الأمن السيبراني وتوفير وسائل الأمان لصد الهجمات السيبرانية، وكذا إعداد وتدريب خبراء على مستوى عال في مجال تكنولوجيا المعلومات والأمن السيبراني

6-قائمة المراجع:

1- إنجي محمد مهدي. (04, 2021). الجهاد الإلكتروني: دراسة لتنظيم داعش واستراتيجية الولايات المتحدة لمواجهته. مجلة كلية السياسة والإقتصاد، 22(02).

2- جمال الدين، هبه. (2023). الأمن السيبراني والتحول في النظام الدولي. مجلة كلية الاقتصاد والعلوم السياسية.

3- جهاز التخطيط والإحصاء، تعريف المنشأة الحكومية Récupéré sur (s.d.). .جهاز التخطيط والإحصاء.

4- حمذان، خينش. (05 01, 2018). الحروب الالكترونية وتاثيرها على سيادة الدول. مجلة الدراسات القانونية والسياسية، 04(01).

5- دلالي، الجيلالي، و بلبشير، يعقوب. (2022). رهانات الأمن السيبراني الوطني في ظل التحول الرقمي: قراءة في التأصيل المعرفي واستراتيجية المواجهة التشريعية. مجلة كلية القانون الكويتية العالمية.

6- سليم دحماني. (2017). أثر التهديدات "السيبرانية" على الأمن القومي الولايات المتحدة الأمريكية – أنموذجا – (2001-2017). قسم العلوم السياسية، المسيلة، الجزائر.

7- سيف نصرت الهرمزي. (2019). رصف المقاربات لمنظورات الفاعل الرقمي والانكشاف الاستراتيجي في ظل الفضاء السيبراني، مجلة آداب الفراهيدي،427.

8- الشريف، أشرف محمد عبدالمحسن .(31 10 ,2007) .إدارة الوثائق الإلكترونية في المنظمات الحكومية: المعايير و الإجراءات .الاتحاد العربي للمكتبات والوثائق.

9- محارب, محمود. (2011). إسرائيل والحرب الإلكترونية – قراءة في كتاب حرب في الفضاء الإلكتروني – اتجاهات وتأثيرات على إسرائيل. المركز العربي للأبحاث ودراسة السياسات، 01.

10- محمد، شيماء جمال. (2021). الحرب الإلكترونية واستراتيجية الدول لمواجهتها. مجلة كلية القانون والعلوم القانونية والسياسية، 10(36).

11- محمد محمد عاطف إمام إبراهيم. (23 04, 2022). الفضاء الإلكتروني وأثره على الأمن القومي للدول: الحروب الإلكترونية نموذجاً. من المركز الديمقراطي العربي للدراسات الاستراتيجية، الاقتصادية والسياسية: https://democraticac.de/?p=81775

12– 3 مخاطر تدفع الحكومة إلى تشكيل المجلس الأعلى للأمن السيبراني. (17 12, 2018). ، من جريدة اليوم السابع: https://www.youm7.com/story

13– هادي سهيلة. (2020). الحروب الالكترونية في ظل عصر المعلومات. رؤى استراتيجية، 04(14).

- **باللغة الأجنبية:**

2- Abdalla, Ghazi & Varol, Hacer. (2019). Defending Against Cyber-Attacks on the Internet of Things. 2019 7th International Symposium on Digital Forensics and Security (ISDFS).

3- Aldlabeeh, A. &.-K.-K.-K. (2022). International Efforts in Combating Cyber Security Crimes. Modern Law Review, 86(01).

4- AlZain, Mohammed & Masud, Mehedi & Al-Amri, Jehad & Soh, Ben & Altwairqi, Asalah. (2019, 12). Four Most Famous Cyber Attacks for Financial. International Journal of Engineering and Advanced Technology, 09(02).

5- Bendovschi, Andreea. (2015). Cyber-Attacks – Trends, Patterns and Security Countermeasures. Procedia Economics and Finance, 28.

6- Bennett, Louise. (2012). Cyber Security Strategy. ITNOW, 10-11.

7- Boughton, Nick. (2019). Protecting infrastructure from cyber attack. Network Security(04).

8- Clauberg, Rolf. (s.d.). INTERNATIONAL ASPECTS OF CYBERSECURITY.

9- Carter, L. and F. Belanger. (2005). The utilization of e-government services: citizen trust, innovation and acceptance factors. Journal of Information Systems.

10- Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). difining cyber-security. technology innovation mangement review, 13-21.

11- Choo, K.K.R. (2008). Organised crime groups in cyberspace: a typology. Trends in Organized Crime volume.

12- Choudhary, Atul & Choudhary, Pankaj & Salve, Shrikant. (2018). A Study On Various Cyber Attacks And A Proposed Intelligent System For Monitoring Such Attacks. 3rd International Conference on Inventive Computation Technologies.

13-Daniel, Schatz,; Julie, Wall. (2017). Towards a More Representative Definition of Cyber Security. Journal of Digital Forensics, Security and Law.

14-Dedakia, Priyanka. (2020). Network Security: Cyber-attacks & Strategies to Mitigate Risks and Threads. Priyanka Dedakia Bournemouth University.

15-Dorn, Walter & Webb, Stewart. (s.d.). Cyberpeacekeeping: New Ways to Prevent and Manage Cyberattacks. . International Journal of Cyber Warfare and Terrorism, 09.

16-Finkle, J. (2016). U.S. firm blames Russian 'Sandworm' hackers for Ukraine outage, sur https://www.reuters.com/article/us-ukraine-cybersecurity-sandworm-idUSKBN0UM00N20160108

17-Happa, Jassim & Glencross, Mashhuda & Steed, Anthony. (2019). Cyber Security Threats and Challenges in Collaborative Mixed-Reality. Frontiers in ICT, 1-20.

18-Hathaway, Oona & Crootof, Rebecca & Levitz, Philip & Nix, Haley & Nowlan, Aileen & Perdue, William & Spiegel, Julia. (2011, 08). The Law of Cyber-Attack. California Law Review, 100(04).

19-Gavenaite, Julija & Miečinskienė, Algita. (2021). FORECASTING COSTS OF CYBER ATTACKS USING ESTIMATION THE GLOBAL COST OF CYBER RISK CALCULATOR. Vilnius Gediminas Technical University.

20-Kammouh, Omar & Cimellaro. (2018). Cyber threat on critical infrastructureA growing concern for decision makers. Dans Routledge Handbook of Sustainable and Resilient Infrastructure.

21-Kumar, Pinosh & Akhilesh, K. (2020). Role of Government in Tackling Cyber Security Threat. Springer Singapore, 4-6.

22-Lala, Chandana & Panda, Brajendra. (2001, 07). Evaluating damage from cyber attacks: A model and analysis. IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans, 31(4).

23-Li, Yuchong & Liu, Qinghui. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. Energy Reports, 07.

24-Mahfouz, Ahmed & Opara, Emmanuel. (2016). conquering the cyber-attacks: analysis and protecting the enterprise resources.

International Journal of Business Continuity and Risk Management.

25- Mendel, Jacob. (2019). Cyberattacks on critical infrastructure: An economic perspective. Economics and Business Review CONTENTS.

26- Plėta, Tomas & Tvaronavičiene, Manuela & Casa, Silvia & Agafonov, Konstantin. (2020). Cyber-attacks to critical energy infrastructure and management issues: overview of selected cases. Insights into Regional Development, 02.

27- Prasad, Ramjee & Rohokale, Vandana. (2020). Cyber Threats and Attack Overview. Dans Cyber Security: The Lifeline of Information and Communication Technology (p. 2).

28- Saini, Gaganjot & Halgamuge, Malka & Sharma, Pallavi & Purkis, James. (2019). A Review on Cyberattacks: Security Threats and Solution Techniques for Different Applications. Dans Cyber Warfare and Terrorism.

29- Sharif, Md Haris & Mohammed, Mehmood. (2022). A literature review of financial losses statistics for cyber security and future trend. World Journal of Advanced Research and Reviews.

30- Soikkeli, Jukka & Casale, Giuliano & Muñoz-González, Luis & Lupu, Emil. (2022). Redundancy Planning for Cost Efficient Resilience to Cyber Attacks. IEEE Transactions on Dependable and Secure Computing, 01.

31- Suhasini, Sodagudi & Kotha, Sita & Raju, M. (2019). 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC). Erode, India.

32- Thakur, Kutub & Liakat, Md & Jiang, Ning & Qiu, Meikang. (2016). Impact of Cyber-Attacks on Critical Infrastructure. 2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference.

33- Thakur, Kutub & Liakat, Md & Jiang, Ning & Qiu, Meikang. (2016). Impact Of Cyber-Attacks On Critical Infrastructure. IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference.

34- The Importance of Cyber Technologies in Government. (s.d.), sur nitaac reimagining acquisitions: https://nitaac.nih.gov/resources/articles/importance-cyber-technologies-government

35- Survey on Types of Cyber Attacks on Operating System Vulnerabilities since 2018 onwards. 2022 IEEE World AI IoT Congress (AIIoT).

36- Vršanský, Peter & Bednár, Daniel. (2017, 12 31). Cyber security and the international law. Bratislava Law Review, 01(02).