قضايا سياسية

اسم المقال: التحديات الامنية للدول في الفضاء السيبراني
اسم الكاتب: م.د. سيناء علي محمود
رابط ثابت: https://political-encyclopedia.org/index.php/library/9542
تاريخ الاسترداد: 2026/11/01 14:34 +03

الموسوعة السياسيّة هي مبادرة أكاديمية غير هادفة للربح، تساعد الباحثين والطلاب على الوصول واستخدام وبناء مجموعات أوسع من المحتوى العلمي العربي في مجال علم السياسة واستخدامها في الأرشيف الرقمي الموثوق به لإغناء المحتوى العربي على الإنترنت.
لمزيد من المعلومات حول الموسوعة السياسيّة - Encyclopedia Political، يرجى التواصل على info@political-encyclopedia.org

استخدامكم لأرشيف مكتبة الموسوعة السياسيّة - Encyclopedia Political يعني موافقتك على شروط وأحكام الاستخدام المتاحة على الموقع https://political-encyclopedia.org/terms-of-use

تم الحصول على هذا المقال من موقع مجلة قضايا سياسية الصادرة عن كلية العلوم السياسية في جامعة النهرين ورفده في مكتبة الموسوعة السياسيّة مستوفياً شروط حقوق الملكية الفكريّة ومتطلبات رخصة المشاع الإبداعي التي ينضوي المقال تحتها.

التحديات الامنية للدول في الفضاء السيبراني[▽]

Security challenges facing states in cyberspace

م.د سيناء علي محمود*
Dr. Sinai Ali Mahmoud

المستخلص

أن الفضاء السيبراني قد أصبح ميدانًا رئيسيًا يواجه فيه الأمن القومي للدول تحديات غير مسبوقة وتُبرز الحاجة الملحة لتطوير استراتيجيات فعّالة لمواجهتها، ومع أن هذه التهديدات تُشكل تحديات محلية لكل دولة، إلا أن طبيعتها العابرة للحدود تتطلب تعاونًا دوليًا وأمميًا لتحقيق الأمن السيبراني، تُظهر أهمية هذه الجهود في تعزيز قدرات الدول خاصة تلك التي تفتقر إلى الموارد التقنية والبشرية لمواجهة التهديدات بمفردها، كما تساهم هذه الجهود في صياغة معايير عالمية مشتركة تُساعد في التصدي للجرائم السيبرانية وتوفير حماية شاملة للبنية التحتية الرقمية، ومع ذلك يبقى تعزيز هذه الجهود ضروريًا لمواكبة التطور السريع في أساليب الهجمات الإلكترونية وتوفير حلول مبتكرة تلبي احتياجات العصر.

الكلمات المفتاحية: الامن، الامن السيبراني، الفضاء السيبراني

Abstract

This study addresses the cybersecurity challenges threatening national security, focusing on cyberattacks and digital wars targeting critical infrastructure. It highlights international efforts, including global cooperation and legislative advancements, to mitigate these risks. The research emphasizes the importance of policy development and balancing security with digital rights protection. Recommendations include investing in infrastructure, human resource training, and fostering international collaboration to counter growing cyber threats.

Keywords: security, cybersecurity, cyberspace

▽ تاريخ التقديم : 2025/1/13 تاريخ القبول: 2025/2/9 تاريخ النشر: 2025/3/31

* كلية العلوم السياسية/ جامعة النهرين/ قسم النظم السياسية والسياسات العامة، sinai.ali@nahrainuniv.edu.iq

This is an open access article under the CCBY license CC BY 4.0 Deed | Attribution 4.0 International / | Creative Common" : https://creativecommons.org/licenses/by/4.0

المقدمة

في ظل التطور السريع الذي يشهده العالم الرقمي أصبح الفضاء السيبراني جزءًا لا يتجزأ من حياة الأفراد والمؤسسات والدول، فهو يمثل بنية تحتية حيوية تعتمد عليها الحكومات في إدارة شؤونها الاقتصادية والاجتماعية والسياسية، ومع تزايد الاعتماد على التقنيات الرقمية والشبكات الإلكترونية تزايدت التحديات الأمنية التي تهدد استقرار الدول وسيادتها، في الوقت الحاضر أصبحت الهجمات الإلكترونية أداة فعّالة تستخدمها جهات مختلفة، سواء كانت دولًا أو منظمات غير حكومية أو حتى أفرادًا لاستهداف الأنظمة الحيوية مثل شبكات الطاقة، والمؤسسات المالية، والبنية التحتية الحيوية الأخرى، هذه التهديدات تتطلب استراتيجيات دقيقة ومتطورة للتصدي لها، مما يجعل الأمن السيبراني قضية ذات أولوية قصوى على المستوى العالمي.

أهمية البحث: تبرز أهمية هذا البحث من كونه يسلط الضوء على أحد أكثر التحديات تعقيدًا وتأثيرًا في العصر الحديث، أذ أصبح الفضاء السيبراني ساحة للتنافس والصراع بين الدول، ويُركز البحث على تحليل المخاطر التي تهدد الأمن القومي، مثل الهجمات السيبرانية التي قد تؤدي إلى شلل الأنظمة الحيوية كالاتصالات والطاقة والبنية التحتية المالية، ان هذه القضايا تؤثر بشكل مباشر على استقرار المجتمعات واقتصادات الدول مما يجعل معالجتها ضرورة حتمية.

هدف البحث: يهدف البحث إلى تحليل التحديات الأمنية التي تواجه الدول في الفضاء السيبراني، وتقديم استراتيجيات فعّالة لتعزيز الأمن السيبراني. كما يسعى لتسليط الضوء على الجوانب القانونية والتقنية للتعامل مع التهديدات،

إشكالية البحث: تكمن إشكالية البحث في كيفية قدرة الدول على مواجهة هذه التحديات المتطورة باستمرار في ظل غياب تشريعات دولية واضحة، وضعف التعاون العالمي، وصعوبة مواكبة التطور التكنولوجي السريع، مع الحفاظ على التوازن بين حماية الأمن القومي وضمان حقوق الأفراد في الخصوصية والحرية الرقمية.

فرضية البحث: تفترض الدراسة أن التحديات الأمنية في الفضاء السيبراني الناتجة عن التهديدات السيبرانية المتزايدة تمثل خطرًا متناميًا على الأمن القومي للدول، كما تُرجح أن تحقيق الأمن السيبراني يعتمد على جهود دولية وأممية مشتركة تتضمن تطوير استراتيجيات فعّالة لمكافحة التهديدات، وتعزيز

This is an open access article under the CCBY license CC BY 4.0 Deed | Attribution 4.0 International / | Creative Common" : https://creativecommons.org/licenses/by/4.0

التعاون الدولي، وتحديث التشريعات الوطنية والدولية، بالإضافة إلى بناء بنية تحتية سيبرانية قوية وقدرات تقنية متقدمة قادرة على مواجهة هذه التحديات.

منهج البحث: اعتمد الباحث على منهج التحليل النظمي وكذلك المنهج الوصفي في هذا البحث.

هيكلية البحث: يتناول البحث ثلاث محاور تطرق المحور الأول الى توضيح مفهوم الامن السيبراني والفضاء السيبراني، وكز المحور الثاني على التهديدات السيبرانية التي تواجه الدول، اما المحور الأخير فقد تناول الجهود الدولية والاممية في تحقيق الامن السيبراني، واختتم البحث بخاتمة تنتهي بعدة استنتاجات.

اولاً: مفهوم الامن والفضاء السيبراني

1. مفهوم الامن السيبراني

ظهر مفهوم الأمن السيبراني بعد الحرب الباردة استجابة للمزيد من الابتكارات التكنولوجية والظروف الجيوسياسية المتغيرة، وقد تم استخدامه لأول مرة من قبل علماء الكمبيوتر في أوائل التسعينات للتأكيد على سلسلة من حالات عدم الأمان المرتبطة بأجهزة الكمبيوتر، لكنه تجاوز مفهومه التقني لأمن الكمبيوتر عندما حث المؤيدين على أن التهديدات الناشئة عن التقنيات الرقمية من الممكن أن يكون لها عدة آثار اجتماعية مدمرة [1]، وتطلق كلمة سيبراني (cyber) على كل ما يتعلق بالشبكات الإلكترونية الحاسوبية، وشبكة الإنترنت، والفضاء السيبراني، والفضاء الإلكتروني (Cyber space)، والأخير يعني كل ما يتعلق بشبكات الحاسوب، والإنترنت، والتطبيقات المختلفة وكل الخدمات التي تقوم بتنفيذها كتحويل الأموال عبر النت، أو الشراء أون لاين وغيرها من الخدمات في جميع مجالات الحياة على مستوى العالم[2].

وأن مصطلح الأمن السيبراني شامل يطلق على (أمن المعلومات) شبكة الأنترنت، و(أمن العمليات الإلكترونية)، (وأمن الشبكات)، (وأمن التطبيقات)، والذي هو عبارة عن خطوات دفاع عن البيانات والمعلومات على جميع الأجهزة الإلكترونية المرتبطة بشبكة الأنترنت من الهجمات الضارة، وعمليات القرصنة وسرقة البيانات، والتخريب، والوصول للمعلومات الحساسة، أو الشخصية لتغييرها أو تدميرها، لأغراض متعددة ومنها الاستيلاء على المال من المستخدمين وغيرها، ويطبق الأمن السيبراني في جميع

[1] تغريد معين حسن، الاثر العسكري للأمن السيبراني في الجغرافيا السياسية للدولة، مجلة البحوث الجغرافية، العدد (30)، (العراق: 2019)، ص240.

[2] منى عبد الله السمحان، متطلبات تحقيق الامن السيبراني لأنظمة المعلومات الادارية بجامعة الملك سعود، مجلة كلية التربية، جامعة المنصورة، العدد (111)، (مصر: 2022)، ص9.

This is an open access article under the CCBY license CC BY 4.0 Deed | Attribution 4.0 International / | Creative Common" : https://creativecommons.org/licenses/by/4.0

العلميات والتطبيقات الإلكترونية من المواقع على شبكة الأنترنت التي تخص الأفراد العاديين أو الدولة، الى المصارف والحسابات البنكية، الى عمليات الأقمار الصناعية والعلميات العسكرية [1].

وبحسب (الاتحاد الدولي للاتصالات) في تقريره حول(اتجاهات الإصلاح في الاتصالات للعام2010-2011) فإن الأمن السيبراني هو: "مجموعة من المهمات مثل تجميع وسائل، وسياسات وإجراءات أمنية، ومبادئ يمكن استخدامها لحماية البيئة السيبرانية، وتهدف الحماية إلى جعل المعتدون يعدلون عن خططهم أو منعهم من تنفيذها عبر وضع خطة تتلاءم مع المحيط التقني والبشري والتنظيمي والقانوني للأفراد والمؤسسات"[(2)]، وقدمت (وزارة الدفاع الأمريكية) تعريف دقيق للأمن السيبراني وعدته: بأنه " جميع الاجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكالها الإلكترونية والمادية ومن مختلف الجرائم، الهجمات، التخريب، التجسس، والحوادث"[(3)]، وهناك تعريف للأمن السيبراني للكاتبان (Pekka & Martti): ويشيران بأنه " مجموعة إجراءات اتخذت في الدفاع ضد الهجمات التي تتعرض لها من قراصنة الكمبيوتر وعواقبها، ويتضمن تنفيذ التدابير المضادة المطلوبة"[(4)].

كما وعرفت (المنظمة الدولية للتوحيد القياسي) الأمن السيبراني أو أمن الفضاء الإلكتروني بأنه: " الحفاظ على سرية وسلامة وتوافر المعلومات في الفضاء السيبراني، كما وعرف الفضاء السيبراني على أنه: " البيئة المعقدة الناتجة عن تفاعل الأشخاص والبرامج والخدمات على الإنترنت عن طريق تقنية الأجهزة والشبكات المتصلة به والتي لا وجود لها في أي منها شكل مادي"[5]، وعليه فالأمن السيبراني ما هو إلا آلية دفاع لخلق حماية فعالة من أي تهديدات ناشئة من الأجهزة والأنظمة الإلكترونية المتصلة

---

[1] سالي سعد محمد، الامن السيبراني ودور الجامعات في تعزيزه لدى الطلبة، مركز حمورابي للبحوث والدراسات الاستراتيجية، (العراق: 2022)، ص2.

[2] سليم دحماني، أثر التهديدات السيبرانية على الامن القومي الولايات المتحدة الامريكية أنموذجا (2001-2007)، مذكرة ماجستير مقدمة الى كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف المسيلة، الجزائر، 2018، ص32-33

[3] Syed Rubab- Ahmed Awais - Muhammad Yasin, CyberSecurity: Where Does Pakistan Stand ?, (Sustainable Development Policy Institute, 2019) p2 .on http://www.jstor.org/stable/resrep243, (26/3/2024).

[4] ميار عادل فتحي – تقى حامد معوض، دور القيادة السياسية الروسية في تعزيز الامن السيبراني (2012-2023) ، (المانيا : المركز الديمقراطي العربي، 2023)، في https://democraticac.de/?p=90695

[5] David G. Delaney , Cyber security and the Administrative National Security State:Framing the Issues for Federal Legislation, Maurer School of Law: Indiana University, Vol (40), p 252

This is an open access article under the CCBY license CC BY 4.0 Deed | Attribution 4.0 International / | Creative Common" : https://creativecommons.org/licenses/by/4.0

بالإنترنت، ووضع إجراءات ومعايير لازمة لمواجهة هذه التهديدات، ويعد الأمن السيبراني اليوم شكل من أشكال الأمن القومي.

2. مفهوم الفضاء السيبراني

ان الفضاء السيبراني مصطلح يشير إلى البيئة الافتراضية التي تنشأ من تفاعل شبكات الحواسيب والأنظمة الرقمية، اذ يتم تبادل المعلومات والبيانات بين المستخدمين والأجهزة بشكل غير محدود، ان هذا الفضاء لا يتطلب وجودًا ماديًا حقيقيًا بل يعتمد على البنية التحتية التكنولوجية مثل الإنترنت والشبكات الرقمية والتطبيقات الحديثة، ويتميز الفضاء السيبراني بقدرته على تجاوز الحدود الجغرافية والزمنية مما يجعله وسيلة رئيسية للتواصل بين الناس ولتنفيذ العديد من الأنشطة التجارية والتعليمية والترفيهية، كما أنه يشكل منصة لظهور تقنيات حديثة مثل الذكاء الاصطناعي وإنترنت الأشياء، التي تُعزز من تداخل حياتنا اليومية مع العالم الرقمي.[1]

ان الفضاء السيبراني ليس مجرد منصة للابتكار والتطوير، بل يمثل أيضًا تحديًا كبيرًا يتعلق بأمن المعلومات وخصوصية الأفراد ومع التوسع الهائل في استخدام الإنترنت وتكامل الأنظمة الرقمية، ازدادت التهديدات السيبرانية مثل الهجمات الإلكترونية والبرمجيات الخبيثة وسرقة البيانات لهذا السبب يُعتبر الأمن السيبراني جزءًا لا يتجزأ من مفهوم الفضاء السيبراني، اذ تسعى الحكومات والشركات والأفراد إلى وضع استراتيجيات فعّالة لحماية البيانات وضمان سلامة المعلومات، إضافةً إلى ذلك أثار الفضاء السيبراني العديد من التساؤلات القانونية والأخلاقية حول حقوق الأفراد والرقابة على المحتوى الرقمي، وبالتالي يمكن القول إن الفضاء السيبراني يمثل تطورًا جذريًا في كيفية تفاعل الإنسان مع التكنولوجيا، لكنه يتطلب أيضًا وعيًا أكبر بمخاطره ومسؤولية في التعامل معه لضمان استفادة مجتمعية مستدامة وآمنة. [2]

لقد عرفت الوكالة الفرنسية لأمن أنظمة الإعلام Agence Nationale de Sécurité des Systèmes d'information والتي تعد وكالة قطاعية للدولة مكلفة بالدفاع السيبراني الفرنسي) الفضاء السيبراني على أنه "فضاء التواصل المشكل من خلال الربط البيني لمعدات المعالجة الآلية

[1] محمود محارب، إسرائيل والحرب الالكترونية قراءة في كتاب حرب في الفضاء الالكتروني اتجاهات وتأثيرات على إسرائيل، سلسلة مراجعة كتب صادرة عن المركز العربي للأبحاث ودراسة السياسات، 2011، ص 1.

[2] حمدون توريه، الفضاء السيبراني وتهديد الحرب السيبرانية البحث عن السلام السيبراني، الاتحاد الدولي للاتصالات، جانفي 2011، ص9-12.

This is an open access article under the CCBY license CC BY 4.0 Deed | Attribution 4.0 International / | Creative Common" : https://creativecommons.org/licenses/by/4.0

للمعطيات الرقمية". يمكن القول إن هذا التعريف جاء مركزا على الجانب التقني للفضاء السيبراني، إذ يولي الاعتبار إلى "التجهيزات" و"الأتمتة"، وأن البعد الفضائي ناتج عن الربط البيني العالمي، في حين أن البناء نجده يتمخض عن عاملين: أحدهما تقني ربط بيني وثانيهما (جغرافي)، مما يجعل هذا التعريف مشمول بمأخذ عدم استيعابه من عموم الجمهور.[1]

ثانياً: التهديدات السيبرانية التي تواجه الدول

لقد تحول الفضاء السيبراني إلى ساحة المعركة الخامسة بين القوى الدولية وذلك بعد البر والبحر والجو والفضاء الخارجي، ويعد هذا المجال التكنولوجي المتطور ساحة جديدة للصراعات العالمية، اذ أصبحت الهجمات السيبرانية التي تستهدف البنية التحتية المعلوماتية إحدى أخطر الأدوات المستخدمة في الحروب الحديثة فمثل هذه الهجمات قد تؤدي إلى انهيار اقتصادي كامل لدولة من الدول أو التسبب في أضرار كارثية تمتد إلى كافة القطاعات سواء كانت عسكرية أو مدنية، ان هذا الخطر يتضاعف مع ازدياد الاعتماد العالمي على التكنولوجيا والأنظمة الرقمية في كافة جوانب الحياة اليومية والإستراتيجية، إن الطبيعة الفريدة للفضاء السيبراني بوصفه بعدًا افتراضيًا لا يخضع للسيادة المباشرة للدول تجعله بيئة مثالية للأعمال العدائية، فبينما يمكن للدول فرض سيطرتها على أراضيها أو أجوائها أو مياهها الإقليمية فإنها لا تستطيع بنفس السهولة فرض سيادتها على الفضاء السيبراني، هذا الفضاء المشترك بين الجميع يعتمد على التكنولوجيا التي يستخدمها الأفراد والمؤسسات والشركات والحكومات، مما يجعله عرضة للاستغلال من قبل المهاجمين السيبرانيين.[2]

ان ما يميز الهجمات السيبرانية عن غيرها من أشكال الصراعات التقليدية هو عنصر المفاجأة الذي يصاحبها، اذ يمكن لمثل هذه الهجمات أن تكون سريعة ومدمرة للغاية بحيث لا تتيح للمدافعين الوقت الكافي للرد أو التصدي لها بشكل فعال، ورغم التطور الكبير في أساليب الأمن السيبراني لا تزال الإجراءات الدفاعية سواء كانت سلبية أو إيجابية عاجزة عن التصدي الكامل لهذه الهجمات، وهذا يعود إلى امتلاك

---

[1] بلفرد لطفي أمين، الفضاء السيبراني هندسة وفواعل المجلة الجزائرية للدراسات السياسية 5 جوان 2016، ص ص 145-155.

[2] U.S. Department of Defense, Dictionary of Military and Associated terms, (USA: Joint Publication, 2010), P.201. Also: Julia Creswell, Oxford Dictionary of Word Origins; Cybernetics, (USA: Oxford University Press, 2010), P.31.

This is an open access article under the CCBY license CC BY 4.0 Deed | Attribution 4.0 International / | Creative Common" : https://creativecommons.org/licenses/by/4.0

المهاجمين قدرة متقدمة على التخفي وإخفاء آثارهم، مما يجعل من الصعب تتبعهم أو تحديد مصدر الهجوم بشكل دقيق.

إن مواجهة هذا الواقع تستدعي وضع استراتيجيات مبتكرة وشاملة تجمع بين التدابير الأمنية التقنية والوعي المجتمعي إلى جانب تطوير قوانين دولية تنظم سلوك الدول والجهات الفاعلة في الفضاء السيبراني فمن دون اتخاذ خطوات جادة ومتكاملة، سيظل الفضاء السيبراني ساحة مفتوحة للتهديدات التي لا يمكن التنبؤ بها، مما يعرض الأمن الوطني والدولي لمخاطر غير مسبوقة،[1] لقد ساهمت مجموعة من العوامل في تصاعد التهديدات السيبرانية التي تواجه مصالح الدول، مما أدى إلى احتمالية بروز حروب سيبرانية أصبحت تشكل تهديداً متزايداً على الأمن الوطني والدولي، وتتلخص أبرز هذه العوامل فيما يلي[2]:

1. **تزايد ارتباط العالم بالفضاء الإلكتروني (السيبراني):** لقد أصبح الفضاء الإلكتروني العمود الفقري للتواصل العالمي وإدارة البنى التحتية الكونية مثل شبكات الكهرباء، والمواصلات، والاتصالات، مما يجعلها أكثر عرضة للاستهداف السيبراني، فمع تحول العالم إلى قرية صغيرة مترابطة عبر الإنترنت، أصبح من السهل على المهاجمين اختراق أنظمة واسعة التأثير لتحقيق أهدافهم العدائية.
2. **تراجع دور الدولة في ظل العولمة:** مع ظهور العولمة وانسحاب الدول من بعض القطاعات الاستراتيجية تصاعدت أدوار الشركات متعددة الجنسيات، خاصة تلك العاملة في مجال التكنولوجيا هذه الشركات أصبحت فاعلاً رئيسياً في الفضاء السيبراني، وأحياناً تتحكم بقدرات تفوق تلك التي تمتلكها الدول نفسها، ان هذا التحول قلل من قدرة الحكومات على السيطرة الكاملة على الفضاء السيبراني[3].
3. **الاعتماد المتزايد على الأنظمة الإلكترونية:** لقد باتت الدول تعتمد بشكل كبير على الأنظمة الإلكترونية في جميع منشآتها الحيوية بما في ذلك قطاعات الطاقة، والمياه، والمواصلات، والبنوك،

---

[1] باسكال يونيفاس، الجيوبوليتيك: مقارنة لفهم العالم في 48 مقالا، ترجمة: اياد عيسى، منشورات الهيئة العامة السورية للكتاب، سوريا، 2010، ص81.

[2] جوزيف هيترون وآخرون، حرب واستراتيجية: نهوج ومفاهيم، ج2، ترجمة: ايمن منير، المجلس الوطني للثقافة والفنون، الكويت، 2019، ص71.

[3] محمد سعيد العامري، عادل عبدالله حميد، محمد الأمين البشري، الأمن السيبراني والتحقيقات الرقمية، أبوظبي: المتحدة للطباعة والنشر، 2021، ص ص 23-23,

This is an open access article under the CCBY license CC BY 4.0 Deed | Attribution 4.0 International / | Creative Common" : https://creativecommons.org/licenses/by/4.0

والدفاع، ان هذا الاعتماد جعل هذه المنشآت عرضة للهجمات الإلكترونية التي يمكن أن تُستخدم لإلحاق أضرار جسيمة بمصالح الدول خاصة في أوقات النزاع.

4. **التكلفة المنخفضة للحروب السيبرانية:** بالمقارنة مع الحروب التقليدية التي تتطلب موارد مادية وبشرية ضخمة فإن الحروب السيبرانية تعد منخفضة التكلفة، كما يمكن شن هجوم سيبراني مؤثر بتكاليف قليلة وخلال فترة زمنية قصيرة، مما يجعلها خياراً مغرياً للجهات الفاعلة، سواء الدول أو الجماعات غير الرسمية.
5. **الحروب السيبرانية كأداة للتأثير على المعلومات:** تحولت الحروب السيبرانية إلى وسيلة فعالة للتأثير على المعلومات المستخدمة في مختلف مراحل ومستويات الصراع، سواء على المستوى الاستراتيجي أو التكتيكي، والهدف هنا هو التأثير بشكل سلبي على دقة المعلومات أو تعطيل الأنظمة التي تعتمد عليها مما يربك الخصم ويضعف قدراته[1].
6. **تعظيم القوة الوطنية من خلال الفضاء السيبراني:** تسعى الدول إلى توظيف الفضاء السيبراني لتعزيز قوتها الوطنية من خلال تحقيق تفوق استراتيجي أو تأثير مباشر على البيئات المختلفة، سواء كانت اقتصادية أو عسكرية، وقد أدى ذلك إلى ظهور مفهوم "الاستراتيجية السيبرانية" كعنصر أساسي في بناء القوة الوطنية.
7. **اتساع نطاق الأنشطة العدائية في الحروب السيبرانية:** لم تعد التهديدات السيبرانية مقتصرة على الدول فقط بل أصبح الفضاء السيبراني بيئة مفتوحة للفاعلين غير الحكوميين، مثل الجماعات الإجرامية والقراصنة الإلكترونيين، وتستخدم الدول أحياناً هؤلاء القراصنة كأداة لشن هجمات ضد الخصوم دون ارتباط رسمي، مما يخلق صعوبة في تحديد المسؤولية عن الهجمات.

ولقد أصبحت مختلف دول العالم عرضة للهجمات السيبرانية، التي تشمل عمليات اختراق إلكتروني وتجسس في الفضاء السيبراني بهدف الحصول على معلومات حساسة سواء كانت عسكرية أو مدنية بالإضافة إلى ذلك، تتعرض الدول لتهديدات تتعلق بإتلاف البيانات وتدمير المنشآت الحيوية، ويعود ذلك إلى التفاوت الكبير بين الدول في قدراتها على الحماية والدفاع السيبراني، أذ تمتلك الدول الكبرى تقنيات متقدمة للتحكم في الفضاء السيبراني ما يجعلها تسعى للهيمنة والسيطرة عليه، ان هذا التفاوت إلى جانب

[1] مصطفى ابراهيم سلمان الشمري الأمن السيبراني وأثره في الأمن الوطني العراقي مجلة العلوم القانونية والسياسية المجلد (10)، العدد(1)،كلية القانون والعلوم السياسية، جامعة ديالى،2021،ص156.

This is an open access article under the CCBY license CC BY 4.0 Deed | Attribution 4.0 International / | Creative Common" : https://creativecommons.org/licenses/by/4.0

تصاعد التهديدات أوجد تحديات أمنية معقدة تواجهها الدول دون استثناء،[1] وفيما يلي نستعرض أبرز هذه التحديات: [2]

أ. استهداف البنى التحتية للدولة

تتعرض البنية التحتية للدول سواء المدنية أو العسكرية لهجمات إلكترونية خطيرة تهدف إلى تعطيل أنظمتها وتشغيلها مما يؤدي إلى شلل كامل في الأنشطة الحيوية وتدفق المعلومات، اذ تؤدي هذه الهجمات إلى إرباك العمليات اليومية وتعطيل مرافق الحياة الأساسية، أذ تشمل استهداف محطات الطاقة وشبكات الوقود بالإضافة الى الخدمات المالية والمصرفية وكذلك نظم الاتصالات ووسائل النقل، وفي ظل هذا التحدي باتت الدول تواجه مخاطر غير مسبوقة نتيجة تصاعد وتيرة الهجمات السيبرانية التي تستهدف أمنها واستقرارها ففي يونيو 2017 تعرضت أوكرانيا لهجمات إلكترونية واسعة النطاق استهدفت محطات الطاقة والمؤسسات المالية مما تسبب في تعطيل أنظمة تشغيلية حيوية، وفي حادثة أخرى يُعد فيروس "ستاكسنت " (Stuxnet) الذي ضرب منشأة "ناتانز" الإيرانية لتخصيب اليورانيوم عام 2010 أحد أخطر الأمثلة على الهجمات السيبرانية المتطورة، اذ تسبب في تعطيل حوالي ألف جهاز طرد مركزي. [3]

أما في كوريا الجنوبية، فقد تعرضت شركة الطاقة المائية والنووية لهجوم إلكتروني كبير في ديسمبر 2014 ما أثار قلقًا عالميًا بشأن هشاشة البنية التحتية أمام التهديدات السيبرانية، كما لم تكن الولايات المتحدة بمنأى عن هذه الهجمات، اذ شهدت شبكات الكهرباء فيها هجمات مماثلة عام 2009 تسببت في انقطاعات واسعة النطاق[4]، ان الهجمات السيبرانية لم تقتصر على القطاعات العسكرية أو المالية فقط بل طالت أيضًا قطاع الطاقة بشكل ملحوظ، ففي عام 2008 تعرض خط أنابيب النفط التركي لهجوم سيبراني غامض أدى إلى اشتعال النيران فيه دون إطلاق أي إنذارات أو مستشعرات، فيما اعتبرت التقارير الأمريكية أن روسيا كانت وراء الهجوم بسبب اعتراضها على إنشاء خط الأنابيب "باكو – تبليسي – جيهان"، وكذلك في البرازيل، تعرضت مرافق الطاقة لهجمات سيبرانية عام 2008 أدت إلى انقطاع الكهرباء على نطاق واسع، اذ توقفت قطارات الأنفاق وإشارات المرور، وتعطل سد "إيتايبو"، ثاني أكبر محطة لتوليد الطاقة في

---

[1] إيهاب خليفة، تنامي التهديدات السيبرانية للمؤسسات العسكرية، مجلة اتجاهات الاحداث، العدد (22)، 2017، ص56.

[2] صلاح مهدي هادي الشمري وزيد محمد علي إسماعيل، الأمن السيبراني كمُرتكز جديد في الاستراتيجية العِراقية، مجلة قضايا سياسية، السنة الثانية عشر، العدد62، (بغداد: جامِعة النهرين، كُلية العلوم السياسية،2020)، ص278–281.

[3] ميرة عبد العظيم محمد عبد الجواد، مصدر سبق ذكره، ص432.

[4] إيهاب خليفة، مصدر سبق ذكره، ص57.

This is an open access article under the CCBY license CC BY 4.0 Deed | Attribution 4.0 International / | Creative Common" : https://creativecommons.org/licenses/by/4.0

البلاد، مما أثر على حياة أكثر من 60 مليون شخص، هذه الحادثة أبرزت مدى خطورة الهجمات السيبرانية على البنية التحتية للطاقة [1].

وشهدت السعودية عام 2017 هجومًا سيبرانيًا خطيرًا باستخدام فيروس *"الصخرة الدوارة Stone) (Drill الذي استهدف قطاعات الطيران والبتروكيماويات، مما تسبب في خسائر كبيرة للشركات العاملة في هذه القطاعات، وفي عام 2019 شنت مجموعات قرصنة إيرانية سلسلة من الهجمات السيبرانية المتقدمة (APT) التي استهدفت شبكات المعلومات والبنية التحتية في السعودية، الإمارات، قطر، الكويت، والبحرين واستمرت هذه الهجمات لفترات طويلة بهدف تعميق تأثيرها وضمان تحقيق أهداف استراتيجية. [2]

تشير هذه الهجمات إلى وجود ثغرات كبيرة في أنظمة الدفاع السيبراني حتى لدى الدول المتقدمة ما يجعل البنية التحتية عرضة للاختراق، كما أن تطور تقنيات القرصنة وتعدد الجهات الفاعلة سواء دول أو جماعات غير رسمية زاد من صعوبة التصدي لهذه التهديدات، بالإضافة الى غياب إطار قانوني دولي واضح لتنظيم الفضاء السيبراني يترك المجال مفتوحًا للفوضى، اذ تُستخدم الهجمات كأدوات للابتزاز أو لتحقيق مكاسب سياسية ومع تزايد الاعتماد على التكنولوجيا أصبحت تداعيات الهجمات السيبرانية أكثر خطورة مما يستوجب استجابة عالمية أكثر فعالية.[3]

ب. اختراق الأنظمة العسكرية وتدميرها

ان الهجمات السيبرانية التي تستهدف الأنظمة العسكرية تعد من أخطر التهديدات في العصر الحديث، أذ تتجاوز مجرد التخريب أو التعطيل لتصل إلى مرحلة السيطرة الكاملة على نظم القيادة والتحكم، اذ تقوم فرق من القراصنة المحترفين أو الجيوش الإلكترونية التابعة لدول معينة بشن هجمات تستهدف اختراق نظم القيادة والسيطرة عن بعد مما يمكنهم من الاستيلاء على منظومات عسكرية حساسة مثل الطائرات بدون طيار والغواصات النووية وحتى الأقمار الصناعية العسكرية، إذا نجحت هذه الهجمات فإن

---

[1] حمدون إ. توريه وآخرون، البحث على السلام السيبراني، الاتحاد الدولي للاتصالات، جنيف، 2011، ص7.

* هو برمجية خبيثة (Malware) متطورة تستخدم في الهجمات السيبرانية الموجهة (Targeted Attacks) يُعتقد أنها طُورت من قِبل جهات متخصصة لشن هجمات تجسس أو تخريب إلكتروني على أهداف حساسة مثل المؤسسات الحكومية أو الشركات الكبرى.

[2] مصطفى إبراهيم سلمان الشمري، مصدر سبق ذكره، ص165.

[3] حسين باسم عبد الأمير، تحديات الامن السيبراني، مركز الدراسات الاستراتيجية، جامعة كربلاء، شبكة المعلومات الدولية (الانترنت)، على الرابط:

/http://kerbalacss.uokerbala.edu.iq/wp/blog/2018/05/17/%DD9%8A

This is an open access article under the CCBY license CC BY 4.0 Deed | Attribution 4.0 International / | Creative Common" : https://creativecommons.org/licenses/by/4.0

العواقب قد تكون وخيمة، اذ يمكن إعادة توجيه الأسلحة نحو أهداف غير مقصودة، سواء كانت داخلية أو ضد دول صديقة وحليفة[1]، على سبيل المثال، يمكن اختراق طائرة بدون طيار وإعادة توجيهها لتنفيذ هجوم داخل أراضي الدولة المالكة لها أو استغلالها لتهديد أمن دولة أخرى، وبالمثل إذا تعرضت غواصة نووية للاختراق فإن القراصنة قد يتمكنون من تعطيلها أو استخدامها بطريقة تهدد الأمن البحري.[2]

أما بالنسبة للأقمار الصناعية العسكرية فتعد من أهم الأدوات المستخدمة في المراقبة وتحديد المواقع ونقل البيانات الحساسة واختراقها يعني إمكانية تعطيل شبكات الاتصالات العسكرية أو حتى توجيه ضربات استباقية عبر تعطيل أنظمة الإنذار المبكر[3]، ومع ازدياد الاعتماد على التكنولوجيا في إدارة العمليات العسكرية تتزايد احتمالية تعرض هذه الأنظمة للاختراق، فالتطور التكنولوجي على الرغم من فوائده في تحسين الأداء العسكري، جعل أنظمة القيادة والتحكم تعتمد بشكل شبه كامل على شبكات الكمبيوتر وبرامج الاتصال، ما يجعلها عرضة للهجمات السيبرانية وإذا استمر هذا الاتجاه دون تعزيز تدابير الحماية فقد نجد أنفسنا أمام سباق سيبراني يهدد الاستقرار الأمني العالمي[4].

ان إحدى الأهداف الأساسية للهجمات السيبرانية هي تعطيل وتدمير الأنظمة الإلكترونية الخاصة بالمنشآت العسكرية الحيوية، اذ تتضمن هذه الهجمات استهداف شبكات الدفاع عن بُعد التي تُعد العمود الفقري للأنظمة الدفاعية للدول اذ يمكن تعطيلها بالكامل أو إتلافها جزئيًا مما يترك الدول عرضة للهجمات العسكرية التقليدية دون قدرة على التصدي لها، بالإضافة إلى ذلك تُستخدم الهجمات السيبرانية لإتلاف شبكات الاتصال الخاصة بالقطاع العسكري ما يعطل تدفق الأوامر بين القيادات الميدانية والمقرات المركزية وهو ما يؤدي إلى خلق حالة من الإرباك داخل المنظومة العسكرية، كما تشمل هذه الهجمات تدمير الأنظمة التي تعمل على تخزين وتشغيل البيانات العسكرية الحساسة، ان اختراق هذه البيانات يؤدي إلى تسريب

---

[1] ياسمين بلعسل بنت نبي والحسين عمروش، التهديدات الالكترونية والامن السيبراني في الوطن العربي، مجلة نوميروس الاكاديمية، العدد(2)، 2021، ص171.

[2] مروان سالم العلي، التحديات الاستراتيجية للأمن الوطني العِراقي في ضوء المُتغيرات الدولية، مجلة تكريت للعلوم السياسية، العدد20، (تكريت: جامِعة تكريت، كُلية العلوم السياسية،2020)، ص58-61.

[3] إيهاب خليفة، مصدر سبق ذكره، ص57.

[4] مروان سالم العلي، مصدر سبق ذكره، ص62.

This is an open access article under the CCBY license CC BY 4.0 Deed | Attribution 4.0 International / | Creative Common" : https://creativecommons.org/licenses/by/4.0

معلومات استراتيجية قد تشمل تفاصيل العمليات العسكرية ومواقع القوات أو حتى نقاط الضعف في أنظمة الدفاع[1].

ان الهجمات السيبرانية لا تتوقف عند هذا الحد، بل تمتد إلى التدخل المباشر في البيانات العسكرية اذ يمكن للمهاجمين التلاعب بالبيانات أو حذفها بالكامل مما يجعل اتخاذ القرارات العسكرية أمرًا بالغ الصعوبة، علاوة على ذلك قد يتم استخدام هذه الهجمات كوسيلة للتشويش والإرباك خلال الأوقات الحرجة مثل أوقات النزاع المسلح أو العمليات العسكرية الجارية مما يضعف موقف الدولة المستهدفة، ان هذه الهجمات تبرز لنا الحاجة الملحة لتعزيز الدفاعات الإلكترونية ووضع أنظمة حماية قوية قادرة على التصدي لهذه التهديدات المستمرة فالتهاون في هذا المجال قد يؤدي إلى عواقب كارثية تُهدد الأمن الوطني للدول.

ان الهجمات السيبرانية ليست موجهة فقط نحو التخريب بل أصبحت أداة فعالة في سرقة التصميمات العسكرية والتقنيات التكنولوجية الحديثة، وتسعى العديد من الدول أو الجماعات إلى استهداف شركات الدفاع والمؤسسات العسكرية من أجل سرقة بيانات حساسة حول تصنيع وتطوير الأسلحة، أحد أبرز الأمثلة على ذلك هو الهجوم الذي شنه قراصنة صينيون على شركة "لوكهيد مارتين" الأمريكية والذي أسفر عن سرقة معلومات حساسة حول تكنولوجيا تصنيع المقاتلة "إف-35". لاحقًا، استخدمت الصين هذه البيانات لتطوير مقاتلة "جي-20" مما أثار قلقًا عالميًا حول حماية الملكية الفكرية في المجال العسكري، ان سرقة تصميمات الأسلحة لا تقتصر على المقاتلات فقط بل تمتد إلى تقنيات أخرى مثل الطائرات بدون طيار، فقد تعرضت شركات أمريكية تعمل على تطوير هذا النوع من الطائرات إلى هجمات سيبرانية استهدفت سرقة تصميماتها وآليات تصنيعها، ان هذه المعلومات يمكن أن تُستخدم لتطوير أسلحة مشابهة أو حتى لتحسين الأسلحة القائمة لدى الدول المنافسة.

إضافة إلى ذلك تتيح هذه الهجمات للمهاجمين فهم نقاط الضعف في الأسلحة والتقنيات المستهدفة، مما يُمكنهم من تطوير استراتيجيات هجومية مضادة، على سبيل المثال يمكن لمعلومات حول نظام الدفاع الصاروخي لدولة معينة أن تساعد خصومها في تصميم أسلحة قادرة على اختراقه أو تعطيله، الهجمات السيبرانية في هذا السياق تُظهر الجانب الخفي للحروب الحديثة، اذ أصبح الفضاء السيبراني ساحة مفتوحة

[1] كرار عباس متعب، الحرب السيبرانية: دراسة في استراتيجية الهجمات السيبرانية بين الولايات المتحدة الامريكية وايران، مجلة حمورابي للدراسات، العدد (40)، مركز حمورابي للدراسات، 2021، ص198.

This is an open access article under the CCBY license CC BY 4.0 Deed | Attribution 4.0 International / | Creative Common" : https://creativecommons.org/licenses/by/4.0

للتجسس وسرقة الابتكارات الدفاعية الأمر الذي يتطلب استثمارات كبيرة في تقنيات الحماية الإلكترونية، بالإضافة إلى تعزيز التعاون الدولي للحد من انتشار هذه الأنشطة التي تهدد التوازن العسكري بين الدول[1].

ت. سرقة المعلومات العسكرية والتلاعب بها

تُعد الهجمات السيبرانية على قواعد البيانات العسكرية من أخطر التهديدات، اذ يتم استهداف هذه القواعد لسرقتها أو تزييفها أو حتى تدميرها إلكترونيًا، تسعى هذه الهجمات لاختراق الشبكات الخاصة بالمؤسسات العسكرية بهدف الحصول على خرائط أنظمة التسليح أو التصميمات الخاصة بالمعدات العسكرية. على سبيل المثال، انطلقت واحدة من أخطر الهجمات ضد أنظمة حواسب الجيش الأمريكي في عام 2008، عندما تم استخدام وصلة (USB) متصلة بجهاز كمبيوتر محمول تابع للجيش الأمريكي في قاعدة عسكرية بالشرق الأوسط، هذه الوصلة سمحت بنشر برامج تجسس في الأنظمة السرية وغير السرية دون اكتشافها في الوقت المناسب، مما خلق "جسرًا رقميًا" تم من خلاله نقل آلاف الملفات إلى خوادم خارجية.[2]

بالإضافة إلى ذلك، استهدفت هجمات سيبرانية أخرى أكثر من 72 شركة، من بينها 22 مكتبًا حكوميًا و13 شركة تعمل كمقاولين لقوات الدفاع، بهدف سرقة معلومات حساسة حول الخطط والمباني العسكرية، وفي 26 و27 سبتمبر 2019، تعرض العراق لهجوم سيبراني واسع النطاق استهدف حوالي 30 موقعًا حكوميًا من بين هذه المواقع كانت مواقع وزارات الدفاع والداخلية والخارجية والأمن الوطني والصحة، واستغل القراصنة ثغرات أمنية في هذه المواقع، وقاموا بتطبيق تغييرات على بيانات البحث لتوجيه المستخدمين إلى صفحات مختلفة، ورغم أن بعض المواقع قد تمت استعادتها سريعًا إلا أن استعادة مواقع أخرى استغرقت وقتًا أطول اذ تمكن المهاجمون من اختراق قواعد بيانات حساسة وأخذ كميات كبيرة من المعلومات المفترض أن تكون محمية بشكل جيد.[3]

ان الهجمات السيبرانية تُظهر تعددية خطورتها، اذ تشمل التجسس، إغلاق الأنظمة المعلوماتية، استهداف أنظمة المعلومات المدنية والعسكرية، والتلاعب بأنظمة توجيه الأسلحة، ويمكن لهذه الهجمات أن

---

[1] Richard Kassel, Glossary of key information security terms, (USA: National Institute of Standards and Technology, Department of Commerce, 2013), P.57.

[2] إيهاب خليفة، تنامي التهديدات السيبرانية للمؤسسات العسكرية، مصدر سبق ذكره، ص57.

[3] Rex Hugh, Towards a Global Regime For Cyber Warfare (London: Cyber Security project Chatham House, 2009), P.P.12-13.

This is an open access article under the CCBY license CC BY 4.0 Deed | Attribution 4.0 International / | Creative Common" : https://creativecommons.org/licenses/by/4.0

تسبب إطلاق الأسلحة نحو أهداف غير مقصودة، مثل البنية التحتية الحيوية المدنية التي تشمل شبكات الكهرباء، أسواق الأوراق المالية، قواعد البيانات المالية، وخطوط تنقية المياه.[1]

مثل هذه التهديدات تمثل خطرًا شديدًا على الدول القومية، اذ تؤثر سلبًا على اقتصاداتها وبنيتها التحتية وأنظمتها السرية، إضافة إلى ذلك تؤدي الهجمات إلى إضعاف القدرات العسكرية من خلال جمع وتحليل معلومات استخبارية دقيقة، لذلك أصبح ردع هذه الهجمات أحد أهم أولويات الردع السيبراني.

ثالثاً: الجهود الدولية والاممية في تحقيق الامن السيبراني

على الرغم من غياب سلطة عليا تُنظم التفاعلات في الفضاء السيبراني، إلا أن هناك جهودًا دولية تهدف إلى ضبط سلوك الوحدات الفاعلة في هذا المجال تشمل هذه الجهود اتفاقات دولية على المستويين الإقليمي والثنائي بين الدول، والتي تسعى إلى وضع خطط واستراتيجيات وطنية، تعمل على تقديم الدعم التقني والفني، وتدريب الكوادر البشرية، وتفعيل آليات المحاسبة والعقاب، على سبيل المثال تُعد المنظمة الدولية للشرطة الجنائية (الإنتربول) إحدى الجهات الفاعلة في مواجهة الجرائم السيبرانية من خلال تقديم الدعم في تعقب ومحاسبة الجناة، ويمكن تصنيف هذه الجهود على مستويات أممية وإقليمية وثنائية، اذ يتم السعي إلى مأسسة التعاون الدولي داخل التنظيمات القائمة لمواجهة هذه التهديدات المتزايدة، [2] ويمكن تصنيف أبرز تلك الجهود على مستويات أممية، وإقليمية وثنائية تم خلالها محاولات لمأسسة الجهود الدولية بداخل التنظيمات الدولية القائمة، ويمكن طرح أبرزها في الآتي:

1. الجهود الأممية:

عملت الأمم المتحدة على بذل جهود كبيرة لمأسسة وتنظيم التصدي للهجمات والجرائم السيبرانية، اذ شملت هذه الجهود وضع قواعد موضوعية وإجرائية، وتنظيم مؤتمرات وقمم دولية، إلى جانب مبادرات قامت بها بعض الهيئات والأجهزة التابعة لها، ومن أبرز هذه الجهود ما يلي:[3]

---

[1] إيهاب خليفة، مجتمع ما بعد المعلومات: تأثير الثورة الصناعية الرابعة على الامن القومي، العربي للنشر والتوزيع، القاهرة، 2019، ص114.

[2] مراد مشوش، الجهود الدولية لمكافحة الإجرام السيبراني، مجلة الواحات للبحوث والدراسات، العدد 2، 2019، شبكة المعلومات الدولية (الانترنت)، على الرابط: https://www.asjp.cerist.dz/en/PresentationRevue

[3] عباس بدران، الحرب الإلكترونية: الاشتباك في عالم مُتغير، ط1، (بيروت: مركز دِراسات الوحدة العربية،2010)، ص27 وما بعدها.

This is an open access article under the CCBY license CC BY 4.0 Deed | Attribution 4.0 International / | Creative Common" : https://creativecommons.org/licenses/by/4.0

أ. وضعت الأمم المتحدة مجموعة من القواعد الموضوعية والإجرائية لمواجهة الجرائم السيبرانية فتتضمن القواعد الموضوعية: النص على قائمة الحد الادنى للأفعال المتعين تجريمها واعتبارها من قبيل الإجرام السيبراني وتحديثها دورياً والمتضمنة: جريمة الاحتيال أو الغش المرتبط بالكمبيوتر، وجريمة التزوير التي تطال برامج الكمبيوتر أو التزوير المعلوماتي وجريمة تخريب واتلاف الكمبيوتر، وجريمة الدخول غير المصرح به، وجريمة الاعتراض غير المصرح به.

ب. أما القواعد الإجرائية فتتضمن بعض الأسس الواجب أخذها في الاعتبار من أبرزها، كوجوب تحديد السلطة المعنية بإجراء التفتيش والضبط في بيئة تكنولوجيا المعلومات، ووجوب التعاون الفعال بما يتيح التنسيق والتعاون للأغراض القضائية في حل الجرائم، والسماح للسلطات العامة باعتراض الاتصالات داخل البيئة المعلوماتية مع استخدام الأدلة التي يمكن ان يتحصل عليها، وكذلك وادخال بعض التعديلات التشريعية في حالة الضرورة بما يتماشى مع طبيعة الإجرام السيبراني داخل القانون الوطني وكذلك القواعد القائمة في مجال الإثبات الالكتروني من حيث مصداقية الأدلة و ما يمكن أن تثيره من مشاكل عند تطبيقها[1].

2. مؤتمرات وقمم دولية:

ساهمت الأمم المتحدة من خلال تنظيم مؤتمرات وقمم دولية في تعزيز الجهود العالمية لمواجهة التهديدات السيبرانية المتزايدة، وسعت إلى بناء تعاون دولي فعال لمكافحة الجرائم الإلكترونية، ومن أبرز هذه الجهود:

أ. مؤتمر هافانا 1990:

خلال المؤتمر الثامن لمنظمة الأمم المتحدة حول منع الجريمة ومعاملة المجرمين، الذي عُقد في هافانا عام 1990، أُقر قانون خاص بالجرائم المرتبطة بالحاسوب، وشكل هذا القانون خطوة رائدة في توجيه الجهود الدولية لتنظيم التعامل مع الجرائم السيبرانية ووضع إطار قانوني لها.

ب. لجنة منع الجريمة والعدالة الجنائية (أبريل 2010):

في الدورة الثانية عشرة للجنة الأمم المتحدة لمنع الجريمة والعدالة الجنائية، تم الإعلان عن إنشاء فريق خبراء حكومي دولي متخصص لدراسة الجريمة السيبرانية، الهدف من هذا الفريق هو تحليل

[1] nternational Multilateral Partnership Against Cyber Threats (IMPACT): https://en.wikipedia.org/wiki/International_Multilateral_Partnership_Against_Cyber_Threats

This is an open access article under the CCBY license CC BY 4.0 Deed | Attribution 4.0 International / | Creative Common" : https://creativecommons.org/licenses/by/4.0

أبعاد المشكلة السيبرانية على الصعيد الدولي، وتقديم توصيات حول كيفية صياغة استجابات فعالة وشاملة لمكافحة هذا النوع من الجرائم.

ت. جلسة المجلس الاقتصادي والاجتماعي للأمم المتحدة(2010)

خصص المجلس الاقتصادي والاجتماعي جلسة إعلامية لمناقشة التحديات التي يفرضها الأمن السيبراني، والفرص والتهديدات الناجمة عن التوسع الكبير في استخدام الإنترنت، وقد شدد المشاركون على ضرورة تنسيق الجهود الدولية لمواجهة الحروب السيبرانية المحتملة، محذرين من أن النطاق الدولي لهذه الهجمات وعواقبها الوخيمة يتطلب استجابات منسقة، وأكدوا أن الحلول الجزئية أو الدفاعات الفردية لم تعد كافية، داعين إلى بناء استراتيجيات جماعية شاملة.[1]

ث. إنشاء الشراكة التعددية ضد التهديدات السيبرانية

في إطار البناء المؤسسي أطلقت الأمم المتحدة مبادرة "الشراكة التعددية ضد التهديدات السيبرانية " (IMPACT)عام 2009، تُعد هذه المنظمة أول كيان مدعوم من الأمم المتحدة يعمل على دعم الأمن السيبراني من خلال توفير منصات للتعاون الدولي، وتقديم المساعدة التقنية للدول الأعضاء لمواجهة الهجمات السيبرانية.

ج. قرار مجلس الأمن رقم 2341:(2017)

في فبراير 2017، أصدر مجلس الأمن الدولي القرار رقم 2341 الذي ركز على حماية البنية التحتية الحيوية من الهجمات السيبرانية، دعا القرار الدول الأعضاء إلى تطوير استراتيجيات وطنية لحماية البنية التحتية الحرجة من التهديدات الإلكترونية، وتعزيز التعاون الإقليمي والدولي في هذا المجال.[2]

ح. اعتماد قرار الأمم المتحدة رقم 247/74:(2019)

في ديسمبر 2019 اعتمدت الجمعية العامة للأمم المتحدة القرار رقم 247/74 الذي دعا إلى تشكيل لجنة خبراء حكومية دولية مفتوحة العضوية لبحث وضع اتفاقية دولية شاملة بشأن مكافحة

[1] مراد مشوش، مصدر سبق ذكره، ص (انترنت).

[2] أحمد عبد الكريم عبد الوهاب، ومحمود عبد الرحمن خلف، إشكالية الأَمن السيبراني العِراقي بين التهديدات السيبرانية والتقنين المُقيد للحُريات، مجلة قضايا سياسية، السنة الثانية عشر، العدد60، (بغداد: جامِعة النهرين، كُلية العلوم السياسية،2020)، ص142.

This is an open access article under the CCBY license CC BY 4.0 Deed | Attribution 4.0 International / | Creative Common" : https://creativecommons.org/licenses/by/4.0

استخدام تكنولوجيا المعلومات والاتصالات لأغراض إجرامية، تهدف هذه اللجنة إلى تعزيز التعاون الدولي وتطوير إطار قانوني دولي يواجه التحديات الناشئة عن الجرائم السيبرانية.

خ. اعتماد اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية:(2024)

في 24 ديسمبر 2024 اعتمدت الجمعية العامة للأمم المتحدة اتفاقية جديدة ملزمة قانونيًا تهدف إلى منع ومكافحة الجريمة السيبرانية، جاء هذا الاعتماد بعد مفاوضات استمرت خمس سنوات، وتهدف الاتفاقية إلى تعزيز التعاون الدولي وتوفير الدعم الفني وبناء القدرات، خاصة للدول النامية.[1]

3. الجهود على المستوى الاقليمي

تعكس هذه الجهود التزام الأمم المتحدة بتعزيز التعاون الدولي لمواجهة التحديات السيبرانية المتزايدة، من خلال المؤتمرات والقمم، وأطلقت الأمم المتحدة مبادرات نوعية ووضعت أسسًا مؤسسية لاستجابة عالمية شاملة تهدف إلى الحد من تأثير الجرائم السيبرانية على الأمن والسلم الدوليين، وتتعدد الجهود الإقليمية التي تبذلها المنظمات والدول للتصدي للهجمات السيبرانية، اذ أسفرت هذه الجهود عن إنشاء لجان وإدارات متخصصة، بالإضافة إلى توقيع اتفاقيات قانونية لمكافحة الجرائم السيبرانية، فيما يلي أبرز تلك الجهود:

أ. **منظمة حلف شمال الأطلسي (الناتو): محاولات مأسسة الجهود الإقليمية:** أنشأ حلف الناتو هيئة خاصة بإدارة الدفاع السيبراني، بالإضافة إلى فريق للاستجابة للحوادث الحاسوبية بهدف تقديم دعم سريع للبلدان الأعضاء التي تتعرض لهجمات سيبرانية، كما أسس الحلف مركزًا للتميز في مجال الدفاع السيبراني التعاوني، مقره في إستونيا، يضم هذا المركز خبراء متخصصين في البحث والتدريب في مجال الأمن السيبراني، وتشمل البلدان الداعمة لهذا المركز: إستونيا، لاتفيا، ليتوانيا، ألمانيا، إيطاليا، الجمهورية السلوفاكية، وإسبانيا، ان هذه الجهود تهدف إلى تعزيز القدرات الدفاعية للبلدان الأعضاء وتنسيق الردود السريعة على الهجمات السيبرانية.[2]

ب. **المجلس الأوروبي واتفاقية بودابست بشأن الجرائم السيبرانية:** اعتمد المجلس الأوروبي اتفاقية بودابست بشأن الجرائم السيبرانية كإطار قانوني لمكافحة بعض الجرائم السيبرانية، توفر الاتفاقية أحكامًا

---

[1] الأمم المتحدة، الجمعية العامة للأمم المتحدة تعتمد اتفاقية تاريخية لمكافحة الجريمة السيبرانية، شبكة المعلومات الدولية (الانترنيت)، تمت زيارة الموقع بتاريخ 2025/1/2، يمكن الحصول عليه من خلال الرابط التالي:
https://www.unodc.org

[2] الموقع الرسمي للمنظمة الدولية للشرطة الجنائية "الأنتربول"، خدمات التعاون في مجال مكافحة الجريمة السيبرية، شبكة المعلومات الدولية (الانترنت)، على الرابط: https://www.interpol.int/ar/4/6/6

This is an open access article under the CCBY license CC BY 4.0 Deed | Attribution 4.0 International / | Creative Common" : https://creativecommons.org/licenses/by/4.0

قانونية نموذجية يمكن للدول تكييفها لتناسب احتياجاتها الوطنية، وتركز الاتفاقية على جرائم مثل النفاذ غير القانوني (القرصنة) واعتراض الاتصالات، ومع ذلك، فإنها لا تشمل بعض التهديدات السيبرانية الأكثر تطورًا، مثل التجسس الإلكتروني والتخريب، وعلى الرغم من أنها تُشجع التعاون الدولي من خلال تجريم الجرائم السيبرانية الأساسية، إلا أن قوتها الإلزامية محدودة نظرًا لتجنبها مخالفة التشريعات الوطنية لبعض الدول، جدير بالذكر أن الاتفاقية، التي فُتح باب التوقيع عليها في نوفمبر 2001، صُدق عليها من قبل ثلاثين دولة فقط، بما في ذلك دولة واحدة فقط من خارج أوروبا.[1]

ج. **الاتحاد الدولي للاتصالات: تعزيز الأمن السيبراني عبر الشبكات الذكية:** قام الاتحاد الدولي للاتصالات بإنشاء فريق متخصص بالشبكات الذكية بهدف جمع وتوثيق المعلومات والمفاهيم المتعلقة بالأمن السيبراني، يعمل الفريق على إعداد توصيات لدعم الشبكات الذكية وزيادة فعاليتها في مواجهة التهديدات السيبرانية، ان هذه المبادرة تساهم في تعزيز التعاون بين الدول لتطوير استراتيجيات أكثر كفاءة للتصدي للهجمات الإلكترونية.[2]

د. **التعاون الثنائي: نماذج من الشراكات الدولية:** سعت بعض الدول إلى تعزيز التعاون الثنائي مع دول أخرى لمواجهة التحديات السيبرانية، ومن أبرز هذه المبادرات، إنشاء صندوق الصين–إسرائيل بين شنغهاي وهونج كونج وتل أبيب ((GEOCعام 2013، يهدف الصندوق إلى الاستثمار في شركات التكنولوجيا المتقدمة، بما في ذلك علوم الحياة، الطابعات ثلاثية الأبعاد، والأمن السيبراني. [3]

وانطلاقاً مما سبق، وعلى الرغم من الجهود الدولية المبذولة في هذا المجال، إلا أنه يتوجب على المجتمع الدولي تكثيف جهوده لوضع القواعد والإجراءات الرسمية التي تنظم سلوك الفاعلين الدوليين ضمن الإطار والنسق الدولي، وبعد استعراض الجهود الأممية والدولية الرامية إلى الحد من الهجمات السيبرانية وتنظيم الأمن السيبراني في المجتمع الدولي، فإنه من الضروري الانتقال إلى استعراض الدفاع في الفضاء السيبراني، يهدف الدفاع الإلكتروني إلى حماية القدرات التكنولوجية للأمن الوطني في الدول، والتي تشمل خطوط الاتصالات، وشبكات الكمبيوتر، والبنية التحتية سواء المدنية أو العسكرية، إضافةً إلى ذلك يسعى

---

[1] هبة جمال الدين، الأمن السيبراني والتحول في النظام الدولي، مجلة كلية الاقتصاد والعلوم السياسية، العدد (94)، جامعة القاهرة، 2023، ص199.

[2] Telecommunication Standardization Sector (ITU–T)، Focus Group on Smart Grid (FG Smart)، www.itu.int/ITU–T/focusgroups/smart

[3] GEOC: GoCapital & Eoc official website، What is GEOC، www.gocapitalgp.com/strategy

This is an open access article under the CCBY license CC BY 4.0 Deed | Attribution 4.0 International / | Creative Common" : https://creativecommons.org/licenses/by/4.0

إلى تأمين البيانات الحيوية ذات الأهمية البالغة مما يساهم في نهاية المطاف في تعزيز وتحقيق الأمن السيبراني للدول وفيما يلي يمكن استعراض وتحديد أهداف الدفاع الإلكتروني بشكل شامل وكالتالي[1]:

- **حماية الأهداف العسكرية:** تشمل حماية الأهداف العسكرية تأمين جميع النظم الحيوية المرتبطة بالعمليات العسكرية، بدءًا من نظم الإدارة والمراقبة ونظم التحكم والسيطرة إلى نظم توجيه الأسلحة وقطاع الاتصالات الحربية، كما يشمل ذلك تأمين الأسلحة آلية القيادة مثل الطائرات من دون طيار، التي تعتمد بشكل كبير على التكنولوجيا الرقمية، بالإضافة إلى ذلك، يمتد دور الحماية ليشمل المنشآت العسكرية والحيوية، مثل محطات الطاقة النووية، التي تمثل هدفًا استراتيجيًا قد يتعرض لمحاولات اختراق إلكتروني، ومن ضمن هذه الحماية، هناك أهمية قصوى لتأمين البيانات العسكرية الحساسة، والتي تشمل معلومات تفصيلية حول أفراد القوات المسلحة مثل الأسماء، والرتب، والمرتبات، والوظائف داخل الجيش، إلى جانب أماكن الإقامة الشخصية، علاوةً على ذلك، تسعى هذه الحماية إلى منع أي وصول غير مصرح به إلى معلومات شديدة الحساسية مثل مخطوطات التسليح، وتصميمات الأسلحة، وخرائط انتشار القوات، وتوزيع الأسلحة، إن تأمين هذه العناصر الحيوية يضمن سلامة العمليات العسكرية وحماية الدول من الهجمات السيبرانية التي تستهدف الإضرار بقدراتها الدفاعية والأمنية.
- **حماية البنية التحتية الحرجة:** تعد البنية التحتية الحرجة من الركائز الأساسية لأي دولة، وهي تشمل مجموعة من القطاعات الحيوية التي يعتمد عليها سير الحياة اليومية واستقرار الاقتصاد والأمن الوطني، لذلك فإن حماية هذه البنية من الهجمات السيبرانية أو الاختراقات الإلكترونية يُعد أمرًا في غاية الأهمية.
- تشمل الحماية **قطاع الاتصالات**، اذ يتم تأمين شبكات الاتصال والبنية التحتية المرتبطة بها لضمان استمرارية التواصل بين الأفراد والمؤسسات، ومنع أي تعطيل قد يؤثر على سير العمل كما يمتد ذلك إلى قطاع المواصلات، والذي يشمل شبكات النقل العام والأنظمة التقنية المستخدمة لإدارة حركة المرور والطيران والموانئ، مما يضمن استمرارية التنقل بشكل آمن[2].

[1] إيهاب خليفة، تنامي التهديدات السيبرانية للمؤسسات العسكرية، مصدر سبق ذكره، ص55-56.

[2] أحمد عبد الكريم عبد الوهاب، ومحمود عبد الرحمن خلف، مصدر سبق ذكره، ص146.

This is an open access article under the CCBY license CC BY 4.0 Deed | Attribution 4.0 International / | Creative Common" : https://creativecommons.org/licenses/by/4.0

- من بين الأهداف الرئيسية أيضًا، **محطات الطاقة**، التي تعد أساس إمداد البلاد بالكهرباء والطاقة اللازمة لتشغيل جميع القطاعات، حمايتها من الهجمات الإلكترونية يضمن عدم انقطاع الطاقة أو استخدامها كوسيلة ضغط على الدولة، بالإضافة إلى ذلك، تشمل الحماية **قواعد البيانات الحكومية** التي تحتوي على معلومات حساسة تخص المواطنين والدولة، مما يحول دون تسريب أو استغلال هذه البيانات.
- أما في مجال الاقتصاد، فالحماية تمتد إلى **البنوك والمؤسسات المالية**، التي تعتمد على نظم رقمية معقدة لإدارة العمليات المالية، ان تأمين هذه الأنظمة يمنع اختراق الحسابات المصرفية، وسرقة الأموال، أو تعطيل الأنظمة التي تعتمد عليها الأسواق المالية، كذلك يتم تأمين **خدمات الحكومات الذاتية** التي أصبحت جزءًا أساسيًا من تقديم الخدمات الرقمية للمواطنين، مثل أنظمة الدفع الإلكتروني واستخراج الوثائق الرسمية[1].

بالتالي، فإن حماية البنية التحتية الحرجة ليست مجرد مسألة تقنية، بل هي عنصر أساسي للحفاظ على الأمن القومي، وضمان استمرارية الخدمات الأساسية، وحماية رفاهية المواطن واستقرار الدولة.

- **دعم وحدات الحرب الإلكترونية:** وهي الوحدات المتخصصة في إدارة الحروب السيبرانية للدول، اذ تتمثل مهمة الدفاع الإلكتروني في تأمين الخطوط الخلفية لهذه الوحدات، مما يساهم في حماية الأهداف الاستراتيجية للدولة عند تعرضها لهجوم إلكتروني مضاد، بالإضافة إلى توفير غطاء إلكتروني للوحدات المقاتلة لتحقيق التسوية والخداع وصعوبة تحديد مصدر الهجوم.
- **تحقيق الردع الإلكتروني:** يتم ذلك من خلال زيادة تكلفة الهجوم الإلكتروني على الدولة المعتدية عبر تطوير أنظمة دفاع إلكترونية شديدة التعقيد يصعب اختراقها، اذ تتطلب وقتًا وجهدًا كبيرين للتغلب عليها، كما يشمل ذلك تعزيز قدرات تتبع الهجمات الإلكترونية وتحديد مصادرها، مما يساهم في التأثير على قرارات الخصم وردعه عن شن هجمات مستقبلية على الدولة، ورغم الجهود التي تبذلها الدول لاعتماد سياسات تأمين فعالة ضد الهجمات السيبرانية، إلا أن التطور التقني في السنوات الأخيرة كشف عن تزايد الهجمات الإلكترونية المتنوعة، بدءًا من عمليات ينفذها مهاجمون

[1] مروان سالم العلي، مصدر سبق ذكره، ص166.

This is an open access article under the CCBY license CC BY 4.0 Deed | Attribution 4.0 International / | Creative Common" : https://creativecommons.org/licenses/by/4.0

ذوو خبرة فردية وصولًا إلى حملات إلكترونية مدعومة من الدول، هذا الوضع أدى إلى بروز أهمية الردع السيبراني كنهج مكمل للدفاع السيبراني، بدلاً من الاكتفاء به فقط.[1]

في ظل التحديات الراهنة، أصبح من الضروري دعم الدفاع الإلكتروني باستراتيجية ردع فعّالة، اذ يهدف الردع إلى خلق عوائق تجعل أحد أطراف الصراع يتجنب القيام باعتداءات أو هجمات مستقبلية، وعلى الرغم من تشابه مفهوم الردع في الفضاء السيبراني مع الردع التقليدي في التفاعلات الدولية، إلا أنه يختلف جزئيًا، اذ لا يمكن لأحد الأطراف القضاء التام على الطرف الآخر كما هو الحال في الردع النووي، علاوة على ذلك يصعب تحقيق الردع الإلكتروني نظرًا لخاصية التخفي التي تميز الهجمات السيبرانية، والتي تجعل من الصعب تحديد هوية المهاجم أو التنبؤ بمصدر الهجوم، ما يؤدي إلى تعقيد الصراعات، بالإضافة إلى ذلك، فإن تعدد الفاعلين، سواء من الدول أو الجهات غير الحكومية، الذين يستخدمون الفضاء السيبراني في صراعاتهم الدولية، يزيد من احتمالات النزاع مع التقدم التقني المتسارع.[2]

ومع تنامي التوترات والصراعات بين الدول على المستويين الإقليمي والدولي، يُتوقع أن تعتمد الدول بشكل متزايد على الحروب الإلكترونية كأداة في إدارة صراعاتها، خاصة مع تزايد أدوار الجهات المسلحة غير الحكومية، ان هذا التصاعد في التهديدات الناشئة عن الفضاء السيبراني يستدعي من الدول اتخاذ تدابير لضبط سلوكها في هذا المجال، مع التركيز على تطوير قدرات دفاعية قوية لحماية نفسها من هذه التهديدات، ومن هذا المنطلق يمكن الإشارة إلى أن الدفاع السيبراني الوقائي يعتمد على ثلاثة أساليب رئيسية سيتم تفصيلها من خلال التالي[3]:

- **الكشف المبكر عن الهجمات:** يتم ذلك من خلال استخدام أجهزة استشعار (Sensors) متقدمة على الشبكات والبرامج والتطبيقات، بالإضافة إلى توظيف المعلومات الاستخباراتية لرصد أي نشاط غير طبيعي قد يُعتبر مؤشرًا على هجمات سيبرانية محتملة، يتيح هذا الكشف المبكر البدء بمواجهة تلك الهجمات واحتوائها قبل أن تنشط على الشبكة أو الأنظمة المستهدفة.
- **الهجوم السيبراني الاستباقي:** يعتمد هذا النهج على نشر "الديدان البيضاء(White Worms) "، وهي برامج متطورة مصممة لاكتشاف التطبيقات الضارة وتدميرها قبل أن تُستخدم في شن هجمات

[1] محمد أكرم محسن، التهديد السيبراني للأمن الاقليمي في القرن الحادي والعشرين: إسرائيل أنموذجاً، (رسالة ماجستير غير منشورة، الموصل: جامِعة الموصل، كُلية العلوم السياسية،2022)، ص197-202.

[2] المصدر نفسه.

[3] إيهاب خليفة، تنامي التهديدات السيرانية للمؤسسات العسكرية، مصدر سبق ذكره، ص100.

This is an open access article under the CCBY license CC BY 4.0 Deed | Attribution 4.0 International / | Creative Common" : https://creativecommons.org/licenses/by/4.0

سيبرانية محتملة، كما تقوم هذه البرامج بتدمير أدوات وبرمجيات القراصنة، مما يساهم في إحباط مخططات الهجمات وتحديد مصدرها وهوية منفذيها، بما يتيح تنفيذ هجمة إلكترونية مضادة تُعرف باسم "الاختراق العكسي.(Hack-back) "

- **التضليل والإخفاء والخداع:** يتضمن هذا الأسلوب إخفاء هويات الأهداف الاستراتيجية للدولة على الإنترنت، وتضليل الخصم أثناء محاولته الوصول إليها أو اختراقها، يتم ذلك باستخدام أدوات التمويه والخداع التي تغيّر ملامح الأهداف وتجعل من الصعب التعرف عليها، مما يساعد على تشتيت الانتباه عن الهدف الحقيقي وتضليل المهاجم.

وفي ختام هذا البحث، يتضح أن حروب المستقبل ستعتمد بشكل كبير على الذكاء الاصطناعي في مجالات التسلح العسكري، بما في ذلك أنظمة الأسلحة التقليدية في البر والبحر والجو والفضاء، هذا التوجه سيحول ساحة المعركة إلى بيئة افتراضية تعتمد على قوة الحوسبة لتحديد الأهداف وطرق التعامل معها، بالإضافة إلى نظم تحليل العمليات ونتائجها والتقنيات المصاحبة، وستكون البرمجة العامل الحاسم في تحديد نتائج حروب المستقبل وتحقيق التفوق العسكري، كما برز الدور المحوري للثورة المعلوماتية والاتصالية في صياغة النظرية العسكرية الحديثة، نتيجة لعاملين رئيسيين: الأول يتمثل في ربط أنظمة الأسلحة إلكترونيًا، سواء عبر نظم تحكم آلية مباشرة أو من خلال وسائل الاتصال الحديثة التي تتيح لمراكز القيادة التحكم عن بعد، أما العامل الثاني، فيتجلى في تقليص الفارق الجغرافي والزمني بين العمليات العسكرية، وذلك نتيجة زيادة مدى أنظمة الأسلحة وسرعتها ودقة إصابتها للأهداف.

الخاتمة

في ختام هذا البحث، يتضح أن الفضاء السيبراني قد أصبح ميدانًا رئيسيًا يواجه فيه الأمن القومي للدول تحديات غير مسبوقة وتُبرز الحاجة الملحة لتطوير استراتيجيات فعّالة لمواجهتها، ومع أن هذه التهديدات تُشكل تحديات محلية لكل دولة، إلا أن طبيعتها العابرة للحدود تتطلب تعاونًا دوليًا وأمميًا لتحقيق الأمن السيبراني، تُظهر أهمية هذه الجهود في تعزيز قدرات الدول خاصة تلك التي تفتقر إلى الموارد التقنية والبشرية لمواجهة التهديدات بمفردها، كما تساهم هذه الجهود في صياغة معايير عالمية مشتركة تُساعد في التصدي للجرائم السيبرانية وتوفير حماية شاملة للبنية التحتية الرقمية، ومع ذلك يبقى تعزيز هذه الجهود ضروريًا لمواكبة التطور السريع في أساليب الهجمات الإلكترونية وتوفير حلول مبتكرة تلبي احتياجات

This is an open access article under the CCBY license CC BY 4.0 Deed | Attribution 4.0 International / | Creative Common" : https://creativecommons.org/licenses/by/4.0

العصر، يُبرز هذا البحث ضرورة تكاتف الدول لتحقيق توازن بين الحفاظ على سيادتها الوطنية والعمل الجماعي لمواجهة التحديات السيبرانية، ان الأمن السيبراني لم يعد خيارًا، بل أصبح شرطًا أساسيًا لاستقرار الدول وحمايتها في عصر رقمي متسارع، ويتطلب ذلك استثمارًا مستمرًا في التكنولوجيا، التعليم، والتشريعات، إلى جانب تعزيز التعاون الدولي كركيزة لضمان مستقبل آمن ومستدام في الفضاء السيبراني.

References:

1 .Tagreed Moein Hassan, The Military Impact of Cybersecurity on the Political Geography of the State, Journal of Geographical Research, Issue (30), (Iraq: 2019), p. 240.

2 .Mona Abdullah Al-Samhan, Requirements for Achieving Cybersecurity for Administrative Information Systems at King Saud University, Journal of the College of Education, Mansoura University, Issue (111), (Egypt: 2022), p. 9.

3 .Sally Saad Muhammad, Cybersecurity and the Role of Universities in Promoting It among Students, Hammurabi Center for Research and Strategic Studies, (Iraq: 2022), p. 2.

4 .Salim Dahmani, The Impact of Cyber Threats on National Security: The United States as a Model (2001-2007), Master's Thesis submitted to the Faculty of Law and Political Science, Mohamed Boudiaf University, M'sila, Algeria, 2018, pp. 32-33.

5 .Mayar Adel Fathi - Taqi Hamid Moawad, The Role of the Russian Political Leadership in Promoting Cybersecurity (2012-2023), (Germany: Arab Democratic Center, 2023), at https://democraticac.de/?p=90695.

6 .Mahmoud Muharab, Israel and Cyberwarfare: A Reading of the Book "War in Cyberspace: Trends and Impacts on Israel," a book review series published by the Arab Center for Research and Policy Studies, 2011, p. 1.

7 .Hamdoun Touré, Cyberspace and the Threat of Cyberwar: The Search for Cyber Peace, International Telecommunication Union, January 2011, pp. 9-12.

8 .Belfred Lotfi Amin, Cyberspace: Engineering and Actors, Algerian Journal of Political Studies, June 5, 2016, pp. 145-155.

9 .Pascal Yunivas, Geopolitics: A Comparison to Understand the World in 48 Articles, translated by Ayad Issa, Syrian General Book Authority Publications, Syria, 2010, p. 81.

10 .Joseph Hetron et al., War and Strategy: Approaches and Concepts, Vol. 2, translated by Ayman Mounir, National Council for Culture and Arts, Kuwait, 2019, p. 71.

11 .Muhammad Saeed Al-Amri, Adel Abdullah Hamid, Muhammad Al-Amin Al-Bishri, Cybersecurity and Digital Investigations, Abu Dhabi: United Printing and Publishing, 2021, pp. 23-23.

12 .Mustafa Ibrahim Salman Al-Shammari, Cybersecurity and Its Impact on Iraqi National Security, Journal of Legal and Political Sciences, Volume (10), Issue (1), College of Law and Political Science, University of Diyala, 2021, p. 156.

13 .Ihab Khalifa, The Growing Cyber Threats to Military Institutions, Events Trends Journal, Issue (22), 2017, p. 56.

This is an open access article under the CCBY license CC BY 4.0 Deed | Attribution 4.0 International / | Creative Common" : https://creativecommons.org/licenses/by/4.0

14 .Salah Mahdi Hadi Al-Shammari and Zaid Muhammad Ali Ismail, Cybersecurity as a New Pillar of Iraqi Strategy, Political Issues Journal, Twelfth Year, Issue 62, (Baghdad: Al-Nahrain University, College of Political Science, 2020), pp. 278-281.

15 .Hamdoun I. Touré et al., Research on Cyber Peace, International Telecommunication Union, Geneva, 2011, p. 7.

16 .It is advanced malware used in targeted cyber attacks. It is believed to have been developed by specialized entities to launch espionage or sabotage attacks against sensitive targets such as government institutions or large corporations.

17 .Hussein Bassem Abdul Amir, Cybersecurity Challenges, Center for Strategic Studies, University of Karbala, International Information Network (Internet), at the link: http://kerbalacss.uokerbala.edu.iq/wp/blog/2018/05/17/%DD9%8A/

18 .Yasmine Balasal Bint Nabi and Al-Hussein Amroush, Electronic Threats and Cybersecurity in the Arab World, Numerus Academic Journal, Issue (2), 2021, p. 171.

19 .Marwan Salem Al-Ali, "Strategic Challenges to Iraqi National Security in Light of International Changes," Tikrit Journal of Political Science, Issue 20, (Tikrit: Tikrit University, College of Political Science, 2020), pp. 58-61.

20 .Karar Abbas Mutab, "Cyberwar: A Study of the Strategy of Cyberattacks between the United States and Iran," Hammurabi Journal of Studies, Issue (40), Hammurabi Center for Studies, 2021, p. 198.

21 .Ihab Khalifa, "The Rise of Cyber Threats to Military Institutions," op. cit., p. 57.

22 .Ihab Khalifa, "Post-Information Society: The Impact of the Fourth Industrial Revolution on National Security," Al-Arabi for Publishing and Distribution, Cairo, 2019, p. 114.

23 .Murad Mashwash, "International Efforts to Combat Cybercrime," Al-Wahat Journal for Research and Studies, Issue 2, 2019, available online at: https://www.asjp.cerist.dz/en/PresentationRevue

24 .Abbas Badran, "Cyber Warfare: Engagement in a Changing World," 1st ed. (Beirut: Center for Arab Unity Studies, 2010), pp. 27 ff.

25 .Ahmed Abdel Karim Abdel Wahab and Mahmoud Abdel Rahman Khalaf, "The Problem of Iraqi Cybersecurity Between Cyber Threats and Restrictive Regulation of Freedoms," Political Issues Journal, 12th Year, Issue 60, (Baghdad: Al-Nahrain University, College of Political Science, 2020), p. 142.

26 .United Nations, UN General Assembly adopts historic convention to combat cybercrime, Internet, accessed on January 2, 2025, available at: https://www.unodc.org

27 .The official website of the International Criminal Police Organization (INTERPOL), Cooperation Services in Combating Cybercrime, Internet, available at: https://www.interpol.int/ar/4/6/6

28 .Heba Gamal El-Din, Cybersecurity and the Transformation of the International System, Journal of the Faculty of Economics and Political Science, Issue (94), Cairo University, 2023, p. 199.

29 .Muhammad Akram Mohsen, The Cyber Threat to Regional Security in the Twenty-First Century: Israel as a Model (unpublished master's thesis, Mosul: University of Mosul, College of Political Science, 2022), pp. 197-202.

30. Ihab Khalifa, The Growing Cyber Threats to Military Institutions, previously cited source, p. 100.

This is an open access article under the CCBY license CC BY 4.0 Deed | Attribution 4.0 International / | Creative Common" : https://creativecommons.org/licenses/by/4.0