



أثر تهديدات الأمن السيبراني على العلاقات الدولية: رؤيا معاصرة للصراع الدولي

علي عبد الخضر محمد المعموري^(*)

(*) أستاذ مساعد دكتور - الجامعة العراقية - كلية القانون والعلوم السياسية drali2864@gmail.com

المستخلص

تعد تهديدات الأمن السيبراني عاملاً أساسياً في تشكيل موازين القوى الدولية، إذ انتقل الصراع من الميادين المادية إلى الفضاء الرقمي، الذي أصبح مجالاً جديداً للحروب. ولم تعد الهجمات السيبرانية مجرد أدوات تخريبية، بل تحولت إلى استراتيجيات سياسية تستهدف سيادة الدول واستقرارها الداخلي والبنى التحتية الحيوية، مما جعل الأمن القومي مرتبطاً بحماية الأنظمة المعلوماتية. وأسهمت هذه التهديدات في ظهور «المنطقة الرمادية» التي يقع فيها الصراع بين السلم والحرب الشاملة، حيث يصعب تحديد مصدر الهجمات وإثبات المسؤولية عنها، الأمر الذي يحد من فاعلية الردع التقليدي و يتيح للمهاجمين الإنكار. كما أدى ذلك إلى تصاعد سباق التسلح السيبراني بين القوى الكبرى، ودفع الدول الصغيرة والمتوسطة إلى تطوير قدراتها الرقمية لتعويض ضعفها العسكري التقليدي، مما أعاد تشكيل التحالفات والخصومات الدولية وفقاً للقدرات التكنولوجية، إلى جانب العوامل الجغرافية والاقتصادية.

الكلمات المفتاحية

الأمن السيبراني، الهجمات الإلكترونية، العلاقات الدولية، الصراع الدولي

للاستشهاد بهذا البحث:

المعموري ع. ع. ا. م. (٢٠٢٣). أثر تهديدات الأمن السيبراني على العلاقات الدولية: رؤيا معاصرة للصراع الدولي.

مجلة كلية القانون والعلوم السياسية، ٣٤، ٣٣٣-٤٥٦. <https://doi.org/10.61279/bggx2a88>

تاريخ الاستلام: ١٢ اذار ٢٠٢٦ تاريخ القبول: ٢٠ حزيران ٢٠٢٦ تاريخ النشر ورقيا: ٢٥ تشرين الثاني ٢٠٢٦

متوفر على الموقع الإلكتروني: ٢٥ تشرين الثاني ٢٠٢٦

متوفر على: <https://jlps.edu.iq/index.php/jlps/ar/article/view/670>

متوفر على: <https://iasj.mohesr.gov.iq/journals/journal/view/253>

ترميز رقمي: <https://doi.org/10.61279/bggx2a88>

مفهرسة على: <https://doaj.org/toc/2664-4088>

المجلة تعمل بنظام التحكم المجهول لكل من الباحث والمحكمين

هذا البحث مفتوح الوصول ويعمل وفق (نسب المشاع الإبداعي) (نسب المصنف - غير تجاري - منع الاشتقاق ٤.٠ دولي)

يحتفظ المؤلفون بحقوق النشر (Copyright) لأعمالهم المنشورة في المجلة، مع منح المجلة حق النشر الأول وذلك حسب سياسات المجلة

نسخة المجلة المنشورة هي النسخة الرسمية المعتمدة لأغراض التوثيق والاستشهاد العلمي

المجلة مؤرشفة في مستوعب المجلات العراقية المفتوحة

للزيد من المعلومات مراجعة الروابط من خلال الضغط على الشعارات ادناه



The Impact of Cybersecurity Threats on International Relations: A Contemporary Vision of International Conflict

Ali AB. Mohammed Alma'amouri(*)

(*)Assistant Professor Dr. - Iraqi University – College of Law & Political Science drali2864@gmail.com

Abstract

Cybersecurity threats have become a fundamental factor in shaping the international balance of power, as conflict has shifted from physical battlefields to cyberspace, now considered a new domain of warfare. Cyberattacks are no longer merely destructive tools but political strategies targeting state sovereignty, domestic stability, and critical infrastructure, making national security dependent on protecting information systems. These threats have contributed to the emergence of the “gray zone,” where conflict occurs between peace and full-scale war. In this context, identifying the sources of attacks and proving responsibility are difficult, weakening traditional deterrence and allowing attackers to deny their involvement. This situation has intensified the cyber arms race among major powers and encouraged small and medium-sized states to develop digital capabilities to compensate for their conventional military weaknesses. Consequently, international alliances and rivalries have increasingly been shaped by technological capabilities, alongside geographical and economic factors.

Key Words

cybersecurity, cybersecurity mechanisms, international relations, international conflict

Recommended citation

المعموري ع. ا. م. (٢٠٢٣). أثر تهديدات الأمن السيبراني على العلاقات الدولية: رؤيا معاصرة للصراع الدولي. *مجلة كلية القانون والعلوم السياسية*، ٣٤، ٤٣٣-٤٥٦. <https://doi.org/10.61279/bggx2a88>

Received 12 Mar. 2026; accepted 20 June 2026

published 25 Oct. 2026 ; published online: 25 Oct. 2026

Available online at: <https://jlps.edu.iq/index.php/jlps/ar/article/view/670>

Online archived copy can be found at: <https://iasj.mohesr.gov.iq/journals/journal/view/253>

Indexed by: <https://doaj.org/toc/2664-4088>

Crossref DOI: <https://doi.org/10.61279/bggx2a88>

This article has been reviewed under the journal's double-blind peer review policy.

This article is open access and licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License (CC BY-NC-ND 4.0).

Authors retain the copyright to their works published in the journal, while granting the journal the right of first publication according to the journal's [policies](#).

The published version of the journal is the official version authorized for documentation and scholarly citation purposes.

The journal is archived in the Iraqi Open Access Journals database.

For more information, please refer to the links by clicking on the logos below.



المقدمة

شهد العقدان الأخيران تحولاً جذرياً في طبيعة التفاعلات الدولية، حيث لم يعد الفضاء الجغرافي التقليدي (البري، والبحري، والجوي، والفضائي) هو الساحة الوحيدة لممارسة السيادة أو خوض النزاعات. فقد برز "الفضاء السيبراني" كبيئة استراتيجية خامسة، تتداخل فيها المصالح السياسية والاقتصادية والأمنية للدول بشكل غير مسبوق. إن هذا الفضاء، الذي بدأ كأداة عالمية للتواصل والتبادل المعرفي، استحال تدريجياً إلى ميدان جديد للتنافس الجيوسياسي، حيث أصبحت القدرة التكنولوجية تضاهي، بل وتتفوق أحياناً، على القوة العسكرية التقليدية في قدرتها على تحقيق الأهداف السياسية.

وتأتي أهمية دراسة أثر تهديدات الأمن السيبراني في سياق رؤية معاصرة للصراع الدولي، بالنظر إلى أن الهجمات الرقمية أتاحت للدول، ولجهات فاعلة غير رسمية، القدرة على استهداف العمق الاستراتيجي للخصوم بتكلفة منخفضة ومخاطر سياسية محسوبة. إن الانتقال من الحروب الحركية إلى ما يُعرف بـ "الحروب الصامتة" أدى إلى إعادة تعريف مفاهيم استقرت لعقود في أدبيات العلاقات الدولية، مثل السيادة الوطنية، والردع، وتوازن القوى. ففي ظل عالم مترابط شبكياً، أصبح تعطيل شبكة كهرباء أو اختراق منظومة مالية وطنية لا يقل خطورة عن هجوم عسكري كلاسيكي، مما يضع المجتمع الدولي أمام معضلة أمنية وقانونية

معقدة، حيث تتلاشى الحدود الفاصلة بين حالة السلم وحالة الحرب في ظل تهديدات عابرة للحدود الوطنية.

مشكلة البحث:

تتمثل إشكالية البحث في استقصاء مدى التأثيرات التي تفرضها تهديدات الأمن السيبراني على التفاعلات الدولية المعاصرة، لا سيما في ظل تصاعد وتيرة الهجمات الإلكترونية العابرة للحدود، وما تفرزه من تحديات أمنية معقدة على المستوى العالمي. كما تتناول المشكلة البحثية طبيعة الاستراتيجيات التي ينبغي على الدول تبنيها للتعامل مع هذا النمط الجديد من الحروب الإلكترونية، في ضوء التطورات التكنولوجية المتسارعة التي أعادت صياغة مفاهيم الأمن الوطني والدولي.

أهمية البحث:

تكمن أهمية البحث في مدى الآثار المترتبة التي يسببها الأمن السيبراني في العلاقات الدولية بعدها كحالة صراع من نوع جديد.

أهداف البحث:

١. يهدف البحث الى معرفة الامن السيبراني والمفاهيم المرتبطة به ، وكذلك حول ماهية التهديدات السيبرانية.
٢. البحث في استراتيجيات المتخذة لمكافحة التهديدات السيبرانية على المستوى الدولي.

المعتمدة في الدراسة، ثم تنقسم المتن إلى ثلاثة محاور رئيسية. يتناول المحور الأول البُعد النظري لمفهوم الأمن السيبراني والتهديدات المرتبطة به، في حين يستعرض المحور الثاني أبرز الاستراتيجيات الدولية المعتمدة في مواجهة التهديدات السيبرانية. أما المحور الثالث، فيركّز على الإشكاليات المعقدة والمخاطر المتنامية التي تهدد أمن الفضاء السيبراني. ويختتم البحث بخاتمة تتضمن أبرز النتائج والتوصيات، بالإضافة إلى قائمة المصادر المعتمدة.

المحور الأول

الامن والتهديدات السيبرانية: دراسة نظرية

أولاً: مفهوم الامن السيبراني

يُعد مفهوم الأمن السيبراني (Cybersecurity) من الركائز الأساسية في العصر الرقمي الحديث، حيث تداخلت التكنولوجيا في أدق تفاصيل الحياة اليومية، مما استوجب بناء منظومة حماية تضمن استمرارية الأعمال وخصوصية البيانات. فيما يلي استعراض مفصل لهذا المفهوم من حيث اللغة والاصطلاح.

١ - مفهوم الأمن السيبراني لغوياً

تألف العبارة من شقين: "الأمن" و "السيبراني".

- الأمن: (Security) في اللغة العربية، مشتق من الجذر (أمن)، وهو نقيض الخوف، ويدل على

٣. يهدف البحث الى تحديد الإشكالية المهددة للأمن السيبراني والكيفية التي يتم التعاطي معها.

فرضية البحث:

ينطلق البحث من فرضية مفادها:

١. ان هناك علاقة طردية بين زيادة الاعتماد على الفضاء الرقمي والسيبراني وبين تصاعد وتيرة الصراع الدولي.

٢. القدرات السيبرانية أصبحت كأداة لتعويض النقص الحاصل في القوة العسكرية التقليدية والاستراتيجيات المتبعة بشأن ذلك.

٣. التعامل الدولي فيما يخص بإشكالية مهددات الأمن السيبراني وانعكاس ذلك على تلك الدول لا سيما وانها ممكن ان تؤدي الى تآكل مفهوم السيادة الوطنية التقليدي.

منهج البحث:

اعتمد هذا البحث على مجموعة من المناهج العلمية، من أبرزها المنهج التحليلي والمنهج المقارن، بالإضافة إلى المنهج التحليلي النظامي، وذلك بهدف دراسة الظاهرة محل البحث بصورة شاملة ومتكاملة.

هيكلية البحث:

يتكوّن هيكل البحث من مجموعة من العناصر الأساسية التي تبدأ بالملخص والمقدمة، يليهما عرض للمنهجية

هذا المفهوم تقنياً على ثلاثة أعمدة رئيسية تُعرف بـ (CIA Triad)^٤:

- السرية (Confidentiality): ضمان عدم اطلاع الأشخاص غير المصرح لهم على البيانات الحساسة.
- السلامة (Integrity): ضمان عدم تعديل البيانات أو العبث بها أثناء تخزينها أو نقلها.
- التوافر (Availability): ضمان قدرة المستخدمين المصرح لهم على الوصول إلى الأنظمة والخدمات في أي وقت يحتاجون إليه. كما يشمل المصطلح حماية البنية التحتية للمعلوماتية الوطنية، ومنع الهجمات الإلكترونية التي قد تستهدف الأنظمة الحيوية مثل شبكات الكهرباء، البنوك، والمؤسسات العسكرية.

٣- الفرق بين أمن المعلومات والأمن السيبراني

غالباً ما يتم الخلط بينهما، إلا أن أمن المعلومات هو المظلة الأشمل التي تهتم بحماية المعلومات سواء كانت ورقية أو رقمية، بينما يركز الأمن السيبراني حصراً على حماية "الفضاء السيبراني" (الأجهزة، الشبكات،

السكينة والطمأنينة^١. أما في القواميس الأجنبية، فكلمة Security تعني التحرر من الخطر أو التهديد^٢.

- السيبراني: (Cyber) هي كلمة معربة من السابقة الإنجليزية (Cyber)، والتي تعود جذورها إلى الكلمة اليونانية (Kybernetes) وتعني "ربان السفينة" أو "المتحكم". استُخدمت لأول مرة في سياق "السيبرنيطيقا" (Cybernetics) "من قبل العالم "نوربرت فاينر" لوصف نظم التحكم والاتصال في الآلة والحيوان. بدمج المصطلحين، يشير المعنى اللغوي إلى "توفير الطمأنينة والحماية لكل ما يتعلق بنظم التحكم والاتصال الرقمي"^٣.

٢- مفهوم الأمن السيبراني اصطلاحاً

يُعرف الأمن السيبراني بأنه "مجموعة الوسائل التقنية والإدارية والتعليمية التي يتم استخدامها للحفاظ على المعلومات والأجهزة والشبكات والبرامج من الاختراق أو التلف أو التغيير أو الوصول غير المصرح به". ويقوم

١ ابن منظور. لسان العرب. بيروت: دار صادر، المجلد ١٣، ص ٢١.

2 International Telecommunication Union. ITU-T Recommendation X.1205: Overview of Cybersecurity. Geneva: ITU, 2008, Section 3.2.1.

3 Norbert Wiener. Cybernetics: Or Control and Communication in the Animal and the Machine. Cambridge, MA: MIT Press, 1948, p. 11.

4 National Institute of Standards and Technology. (2017). An Introduction to Information Security (NIST Special Publication 800-12 Rev. 1, p. 7). U.S. Department of Commerce.

منشأ خارجي أو داخلي، مما أدى إلى تعدد مستوياتها (محلي، إقليمي، دولي) وتنوع مصادرها وأطرافها الفاعلة، الأمر الذي ساهم في بروز نمط جديد من التهديدات المركبة والمعقدة^٥.

ويُعرف الباحث "باري بوزان" التهديد بأنه فعل موجه ضد مؤسسات الدولة، يتم من خلاله توظيف عناصر القوة أو الأيديولوجيا لإلحاق الضرر بدولة أخرى، ويشمل ذلك التهديد بغزو، أو احتلال، أو إلحاق أذى جسيم. ويرى بوزان أن الدول ذات القوة الكبيرة غالباً ما تواجه تهديدات خارجية، بينما تتعرض الدول الضعيفة لمزيج من التهديدات الداخلية والخارجية.

وفي ظل التحولات التكنولوجية المتسارعة، يواجه العالم اليوم أشكالاً متعددة من التهديدات الأمنية الحديثة، التي تسم بالتعقيد والديناميكية وسرعة الانتشار، إلى الحد الذي باتت فيه لا تؤثر على دولة بعينها فحسب، بل تمس الأمن العالمي برمّته. وتُعد التهديدات السيبرانية (Cyber Threats) من أبرز هذه التهديدات المستحدثة، لما تنطوي عليه من خطورة وتعقيد. فهذه التهديدات تتطور بشكل مستمر، وتتخذ صوراً متعددة،

والبيانات الرقمية) والوقوف في وجه الهجمات التي تأتي عبر الشبكة^٥.

ثانياً: التهديدات السيبرانية

تُشير كلمة "تهديد" من حيث الأصل اللغوي إلى نية مسبقة لإلحاق الضرر أو الأذى، بقصد زعزعة حالة من الاستقرار أو الأمن^٦. ويُفهم التهديد بوصفه مؤشراً على وجود توجه عدائي قد يؤدي إلى معاقبة أو إيذاء طرفٍ معين. وقد عرف قاموس أوكسفورد مصطلح "التهديد" بأنه سلوك أو فعل يمثل خطراً على حياة الكائنات الحية، مثل التلوث الذي يهدد حياة البشر والحيوانات^٧.

أما من الناحية الاصطلاحية، فقد اكتسب مفهوم "التهديد" معانٍ أوسع في السياق الأكاديمي المعاصر، إذ لم يعد مقتصرًا على التحديات العسكرية التقليدية ذات المصدر الخارجي فحسب، بل أصبح يشمل طيفاً متنوعاً من التحديات المرتبطة بالتحولات العميقة في بنية النظام الدولي بعد انتهاء الحرب الباردة. وتبعاً لذلك، توسعت دائرة التهديدات لتشمل الجوانب الاقتصادية والاجتماعية، والثقافية، والبيئية، سواء كانت ذات

5 National Institute of Standards and Technology. (2017). An Introduction to Information Security (NIST Special Publication 800-12 Rev. 1, p. 7). U.S. Department of Commerce.

٦ جودة ابو ألياس، الامن البشري وسيادة الدول، المؤسسة الجامعية للدراسات والنشر والتوزيع، بيروت، ٢٠١١، ص ٤٧.

٧ قاسم حجاج، التدخل الانساني للجيش الوطني الشعبي في مواجهة الكوارث الطبيعية، مداخلة مقدمة في الملتقى الدولي حول الدفاع الوطني بين الالتزامات والتحديات الاقليمية، ٢٠١٤.

٨ شهرزاد ادمام، طبيعة التهديدات الامنية الجديدة، مجلة الندوة للدراسات القانونية، ٢٠١٣، ص ٣٣.

الذي استهدف منشآت إيران النووية، وهجمات على شبكات الطاقة في أوكرانيا.

-الحرب السيبرانية (Cyber Warfare):

وهي تعد من أهم أدوات التهديدات السيبرانية وذلك لأنسامها بالتأثير الكبير والاستراتيجي ، حيث تمثل استخدام الدول للفضاء السيبراني كأداة في الصراعات العسكرية، تشمل الهجمات على شبكات الاتصالات، الأقمار الصناعية، ونظم التحكم العسكرية ومن أمثلة ذلك الهجمات الإلكترونية بين الولايات المتحدة والصين أو كوريا الشمالية⁹.

-التجسس السيبراني (Cyber Espionage):

تستخدمه الدول للحصول على معلومات حساسة من الحكومات أو الشركات الكبرى ، ومن أمثلة ذلك عمليات اختراق استهدفت الكثير من وزارات الدفاع، السفارات، والشركات العاملة في الصناعات الحساسة¹⁰.

يصعب التنبؤ بها أو وضع أطر ثابتة لاحتوائها، مما يجعل من مواجهتها تحدياً أمنياً عالمياً بالغ الأهمية.

كما يوجد هناك أنواع مختلفة من التهديدات السيبرانية على المستوى الدولي وأهم هذه الأنواع التهديدات المباشرة والتهديدات غير المباشرة وكالتالي:

١ - التهديدات المباشرة:

التهديدات السيبرانية المباشرة على المستوى الدولي أصبحت تمثل تحدياً كبيراً للدول والحكومات، نظراً لاعتماد العالم بشكل متزايد على التكنولوجيا الرقمية والبنية التحتية المتصلة بالشبكة. هذه التهديدات تُنفذ غالباً من قبل جهات مدعومة من الدول أو مجموعات منظمة وتستهدف مصالح سياسية، اقتصادية، وعسكرية، أما أبرز التهديدات السيبرانية المباشرة على المستوى الدولي:

-الهجمات على البنية التحتية الحيوية (Critical Infrastructure Attacks):

تستهدف القطاعات الحساسة مثل محطات الطاقة، شبكات المياه، المستشفيات، وأنظمة النقل ، ومن أمثلة ذلك هجوم (Stuxnet)

9 Schmitt, Michael N., ed. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge: Cambridge University Press, 2017, p25

10 Rid, Thomas. Active Measures: The Secret History of Disinformation and Strategic Warfare. New York: Farrar, Straus and Giroux, 2020, p314.

• الهجمات عبر سلاسل التوريد (Supply Chain Attacks):

تُهاجم الشركات الوسيطة أو الموردين للوصول إلى بيانات أو أنظمة حساسة، ومن أمثلة ذلك الهجوم على شركة (SolarWinds) الذي أثر على العديد من الجهات الحكومية الأمريكية^{١٤}.

التهديدات غير المباشرة: تشير التهديدات غير المباشرة إلى تلك التي تُصيب كيانات أو مؤسسات لم تكن مستهدفة بشكل مباشر، مما يستدعي تجاوز التقييم التقليدي للتهديدات نحو تبني إطار تحليلي أكثر شمولاً، يُعنى بفهم ديناميكيات التهديدات وتطورها. ولا يقتصر ذلك على التعرف على مصادر التهديد، بل يتطلب تحليل الأنماط والتوجهات التي تكشف عن مسارات التصعيد السيبراني المحتمل.

ومن ناحية أخرى، فقد أصبحت التهديدات الأمنية تسم بالامتداد الزمني الذي يعقد عملية رصدها، والاتساع الجغرافي الذي يجعل من الصعب تحديد

-الهجمات على الأنظمة الاقتصادية والمالية:

تستهدف الأنظمة المصرفية وأسواق المال لتعطيلها أو سرقة الأموال، ومن أمثلة ذلك هجمات برمجيات الفدية التي أثرت على أنظمة مالية دولية^{١١}.

• الابتزاز السيبراني (Cyber Extortion):

تستهدف مجموعات إجرامية الشركات الكبرى والمؤسسات الحكومية، حيث تُسَفَّر البيانات وتُطلب فدية مالية ضخمة للإفراج عنها، من أمثلة ذلك هجمات (NotPetya) و (WannaCry) التي أثرت على دول عديدة^{١٢}.

• الحملات الدعائية والتلاعب بالرأي العام (Disinformation Campaigns):

تُستخدم وسائل التواصل الاجتماعي لنشر الشائعات، تضليل الرأي العام، أو التأثير على الانتخابات، ومن أمثلة ذلك التدخل الروسي المزعوم في الانتخابات الأمريكية عام ٢٠١٦^{١٣}.

¹¹ Mazarr, Michael J., et al. The Character of Manipulation: The Use of Information as a Tool of Statecraft. Santa Monica, CA: RAND Corporation, 2019. P25

¹² Verizon Business. 2024 Data Breach Investigations Report (DBIR). New York: Verizon, 2024, p15.

¹³ The Brookings Institution. Cyber Campaigns and the Future of Political Warfare. Washington, D.C.: Brookings Press, 2022, p57.

¹⁴ National Institute of Standards and Technology (NIST). Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations. NIST Special Publication 800-161 Rev. 1. Gaithersburg, MD: U.S. Department of Commerce, 2022.

نطاقها بدقة^{١٥}، وإذا ما تم اعتبار الأمن مفهوماً يتجاوز الحدود الوطنية بفعل فواعل متعددة الجنسيات، فإن نتائج هذا المفهوم تعزز من طبيعة الأمن بوصفه قضية "عبر وطنية" (Transnational). وهذا يفرض إعادة النظر في المنظومات المعرفية والإيديولوجية التي يتم من خلالها تصنيف التهديدات الأمنية، وصياغة أولوياتها وفقاً لتساؤلات جوهرية من قبيل: "لن يُضمن الأمن؟"، "ضد من؟"، و"بأي وسيلة؟"^{١٦}.

المحور الثاني

استراتيجيات مكافحة التهديدات السيبرانية على

المستوى الدولي

أولاً: استراتيجيات الخاصة بالدول

تواجه أجهزة الأمن والمخابرات في مختلف دول العالم تحديات متزايدة ومعقدة، إذ لم تعد التهديدات الأمنية تقتصر على الأطر التقليدية، بل اتخذت في السنوات الأخيرة أشكالاً جديدة ترتبط ارتباطاً مباشراً بالفضاء السيبراني. وتعد الجرائم الإلكترونية واحدة من أسرع أنواع الجرائم انتشاراً وتطوراً، وتسم بخطورتها العابرة للحدود، ما يجعلها من أبرز مصادر التهديد للأمن القومي في العصر الرقمي.

إن تزايد الاعتماد على الإنترنت وشبكات المعلومات أدى إلى خلق بيئة خصبة لانتشار الهجمات السيبرانية التي تستهدف الأنظمة الحساسة في الدول، وفي مقدمتها البنية التحتية الحيوية، مثل: شبكات الطاقة، والاتصالات، والقطاع المالي. وقد أصبح من الواضح أن الوسائل التقليدية لمكافحة الجريمة لم تعد كافية لمواجهة التهديدات السيبرانية المعاصرة، ما دفع العديد من الدول إلى إعادة النظر في سياساتها الأمنية. وتتنوع أشكال الجريمة السيبرانية لتشمل طيفاً واسعاً من الأنشطة غير القانونية، مثل الاحتيال المالي، وغسل الأموال، واستغلال الأطفال عبر الإنترنت، والتصيد الاحتيالي، والاختراق، وسرقة البيانات الحساسة. وتشير التقديرات إلى أن الخسائر الاقتصادية العالمية الناجمة عن هذه الأنشطة بلغت حوالي ٣ تريليونات دولار في عام ٢٠١٥، ويتوقع أن ترتفع بمعدل سنوي يصل إلى ١٥٪ لتصل إلى نحو ١٠,٥ تريليون دولار بحلول عام ٢٠٢٥. وتعد هذه الأرقام دليلاً واضحاً على أن الجريمة السيبرانية تمثل أحد أكبر تحولات الثروة الاقتصادية في التاريخ الحديث، متجاوزة حتى الأضرار الناتجة عن الكوارث الطبيعية، بل وتدر أرباحاً تفوق عوائد تجارة المخدرات غير المشروعة عالمياً^{١٧}.

١٥ احمد فريجة والدمية فريجة، الامن والتهديدات الامنية في عالم ما بعد الحرب الباردة، مجلة دفاتر السياسة والقانون، ٢٠١٦، ص 116.

١٦ محمد حشعي، مدرسة باريس للدراسات الامنية واشكالية مستوى التحليل في العلاقات الدولية، مجلة السياسة الدولية، ٢٠١٨، ص 17.

17 NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), 20th Century Redux: Cyber Power, Tallinn, NATO CCDCOE Publications, 2016.

وبناءً على ذلك، أصبح التعاون الدولي في مجال مكافحة التهديدات السيبرانية ضرورة ملحة، وقد أخذت العديد من المؤسسات الأمنية الدولية، وعلى رأسها الشرطة الجنائية الدولية (الإنتربول)، على عاتقها مسؤولية دعم الدول الأعضاء بتقنيات متقدمة لتعزيز قدراتها في التصدي لهذا النوع من الجرائم. وتقوم الإنتربول بتشغيل قواعد بيانات متقدمة تساعد الدول على تتبع النشاطات الإجرامية، من بينها قاعدة بيانات الاستغلال الجنسي للأطفال عبر الإنترنت (ICSE)، والتي أسهمت حتى الآن في تحديد أكثر من ٣٠ ألف ضحية حول العالم^{١٨}.

وفيما يخص دول الشرق الأوسط، فقد كانت بعض الدول مثل الإمارات العربية المتحدة والمملكة العربية السعودية من أكثر الدول تعرضاً للهجمات السيبرانية خلال الفترة الممتدة من منتصف عام ٢٠٢١ إلى منتصف عام ٢٠٢٢، بحسب تقارير صادرة عن شركات متخصصة في الأمن السيبراني، مثل شركة Group-IB. كما تُعد هجمات الفدية الرقمية من أخطر التهديدات التي واجهت المؤسسات في المنطقة خلال تلك الفترة^{١٩}. وقد بادرت حكومات المنطقة إلى اتخاذ

إجراءات فعالة لتعزيز بنيتها السيبرانية، من خلال إصدار تشريعات متقدمة وتنفيذ استراتيجيات وطنية لمكافحة الجريمة الرقمية. فعلى سبيل المثال، أطلقت الإمارات العربية المتحدة العديد من المبادرات في هذا المجال، حيث أنشأت مجلس الأمن السيبراني في عام ٢٠٢٠ لوضع استراتيجية شاملة للأمن السيبراني، إضافةً إلى تأسيس مركز دبي للأمن الإلكتروني الذي يُعنى بوضع سياسات ومعايير تضمن أمن المعلومات في الجهات الحكومية والتصدي للأخطار الرقمية^{٢٠}.

أما المملكة العربية السعودية، فقد خطت خطوات نوعية في هذا المجال من خلال تأسيس الهيئة الوطنية للأمن السيبراني عام ٢٠١٧، والتي تهدف إلى وضع الأطر القانونية والتنظيمية للأمن السيبراني، وتنفيذ حملات توعية وطنية. كما أطلقت المملكة المنتدى الدولي للأمن السيبراني كبادرة تسعى إلى تعزيز التعاون الدولي في هذا المجال، وتنسيق الجهود العالمية لمواجهة التهديدات السيبرانية^{٢١}.

١٨ زينب عباس راضي، فاعلية الأمن السيبراني في السياسة العالمية (المفهوم والتدابير الأمنية للدول)، مجلة آشور للعلوم القانونية والسياسية، المجلد ٢، العدد ١، ٢٠٢٥، ص 551.

١٩ الهيئة الوطنية للأمن السيبراني، الاستراتيجية الوطنية للأمن السيبراني، الرياض، المملكة العربية السعودية، ٢٠٢٣.

<https://nca.gov.sa/ar/pages/national-strategy>، تاريخ الوصول ١٣ يناير ٢٠٢٦.

٢٠ البوابة الرسمية لحكومة دولة الإمارات العربية المتحدة، 'السلامة السيبرانية والأمن الرقمي'، استراتيجيات ومبادرات، 2024.

<https://u.ae/ar/information-and-services/justice-safety-and-the-law/cyber-safety-and-digital-security>، (تاريخ الوصول 13 يناير 2026).

٢١ الهيئة الوطنية للأمن السيبراني السعودي، الاستراتيجية الوطنية للأمن السيبراني، مصدر سبق ذكره.

يجب ان تتجلى دور الشركات التقنية الكبرى في حماية الفضاء السيبراني ورفع مستوى التعاون بين القطاعين، وقد أدى التعاون بين الحكومات مع شركات مثل مايكروسوفت وغوغل في مواجهة التهديدات السيبرانية الى الحد من الكثير من الهجمات السيبرانية^{٢٢}.

ثانياً: استراتيجيات الخاصة بالمنظمات الدولية المتخصصة

يتعين على المنظمات التركيز على تحسين عملياتها السيبرانية لأنها تشكل عنصراً أساسياً في تحديد الفيروسات ومراقبة التنبيهات وتحديد التهديدات في الوقت الفعلي. ومن المعتقدات الخاطئة أن العمليات السيبرانية تتعلق فقط بمنع التهديدات السيبرانية، إنه مفهوم أوسع يمزج بين استراتيجيات مختلفة لإدارة التهديدات بشكل فعال. وتضمن هذه النظرة الشاملة حماية واسعة النطاق ضد المخاطر السيبرانية المتطورة. وتستخدم العمليات السيبرانية لمراقبة وتحليل أمن المؤسسة للكشف عن الحوادث السيبرانية والاستجابة لها. وهي تعمل على المستوى التشغيلي، وليس على الاستراتيجية أو البنية التحتية. يمكن للعمليات السيبرانية أن تحدث فرقاً كبيراً في وضع المؤسسة من خلال تقديم المراقبة في الوقت الفعلي وتحديد التهديدات لتحسين استعداد المؤسسة ضد التهديدات السيبرانية^{٢٣}.

بالنتيجة ، يمكن ان تتخذ الدول دوراً استراتيجياً مهماً في الدفاع السيبراني وحماية الفضاء السيبراني ، حيث من الممكن ان يعطي ذلك دافعاً الى دول أخرى ان تلحق بركب الدول التي بدأت باتخاذ استراتيجيات الامن السيبراني، حيث يتم كل ذلك من خلال:

- ١- التحالفات السيبرانية: تشكيل تحالفات دولية لمواجهة التهديدات السيبرانية كما هو الحال مع "الناتو السيبراني" ، وكذلك دور التعاون الدولي في تعزيز الأمن السيبراني وتطوره.
- ٢- القوانين والتشريعات الدولية: الحاجة إلى إطار قانوني دولي ينظم الهجمات السيبرانية. تحديات صياغة هذه القوانين بسبب تباين المصالح.
- ٣- تطوير استراتيجيات دفاعية وطنية: من اهم تلك الإستراتيجيات الدفاعية لتلك الدول من اجل تعزيز أمنها السيبراني، هو زيادة الإنفاق على الأمن السيبراني ضمن الموازنات الوطنية، وهذا في الأساس سيزيد من عملية تفاعل تلك الدول من اجل رفع مستوى التعاون الدولي فيما يخص التهديدات السيبرانية.
- ٤- الشراكات بين القطاعين العام والخاص: ويعد هذا الامر مهم وعلى مستوى عالي من الحساسية لأن اصل الهجمات السيبرانية جاءت في الأصل من افراد ومجموعات خارج اطر المؤسساتية وهنا

٢٢ المصدر نفسه.

٢٣ منى عبد الله، متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود، مجلة كلية التربية، جامعة المنصورة، ٢٠٢٠، ص ٨.

وهناك ثلاث مكونات رئيسية تدعم استراتيجية مكافحة الهجمات السيبرانية، وأهمها:

١. استخبارات التهديدات السيبرانية:

تعتبر مهمة في فهم ومنع الهجمات السيبرانية المتقدمة الخفية التي يصعب اكتشافها ومنعها، وذلك لحماية موارد المنظمة وتقليل المخاطر المحتملة. كآلية للكشف المبكر عن التهديدات الخفية في الفضاء الإلكتروني. وبالتالي، تكون تقنية CTI الفنية مفيدة عند تحديد مؤشرات الهجوم وطرق منعه، في حين تعمل تقنية CTI الشاملة على تمكين تدابير الأمن الاستباقية وإدارة المخاطر بشكل أفضل^{٢٤}.

٢. البنية التحتية السيبرانية:

تعمل البنية الأساسية السيبرانية على تعزيز شبكات العلماء من مختلف التخصصات، مما يعزز قدرات حل المشكلات. إن القدرة على تحليل البيانات الضخمة التي يتم جمعها من مصادر متنوعة تؤدي إلى اختراقات كبيرة، مما يبرز أهمية البنية الأساسية السيبرانية في البحث الحديث. وهي تشمل مجموعة واسعة من التقنيات، من أنظمة الحوسبة عالية الأداء إلى الخوادم،

وتسلط الضوء على التعقيد والتخصص المطلوب في بيئات البحث^{٢٥}.

٣. القوى العاملة السيبرانية:

تصنف القوى العاملة السيبرانية أدوار العمليات السيبرانية إلى سبع فئات رئيسية، ولكل منها مجالات متخصصة لضمان أمن تكنولوجيا المعلومات والأداء، وكالتالي^{٢٦}:

الفئة الأولى: (التشغيل والصيانة): التركيز على دعم نظام تكنولوجيا المعلومات والإدارة والصيانة.

الفئة الثانية: (الحماية والدفاع): يتضمن تحديد التهديدات التي تتعرض لها أنظمة تكنولوجيا المعلومات والتخفيف منها.

الفئة الثالثة: (التحقيق): يشمل التحقيق في الأحداث والجرائم الإلكترونية التي تنطوي على موارد تكنولوجيا المعلومات.

الفئة الرابعة: (التجميع والتشغيل): متخصص في عمليات الإنكار والخداع وجمع المعلومات.

24 National Science Foundation (NSF), Cyberinfrastructure Vision for 21st Century Discovery, Washington, D.C., NSF Press, 2007, p8.

25 Ibid, p9.

26 National Institute of Standards and Technology (NIST), NICE Cybersecurity Workforce Framework (NIST Special Publication 800-181), Gaithersburg, U.S. Department of Commerce, 2020, p18.

الفئة الخامسة: (التحليل): مراجعة المعلومات وتقييمها لأغراض استخباراتية.

الفئة السادسة: (إدارة القيادة): توفير التوجيه للعمل الفعال في مجال الأمن السيبراني.

الفئة السابعة: (التوفير الآمن): يركز على تصميم وبناء أنظمة تكنولوجيا المعلومات الآمنة.

في الحقيقة ، إن الحماية المناسبة لأنظمة المعلومات تشكل قضية نوعية رئيسية لإدارة المخاطر التنظيمية. إن إدارة المخاطر هي عملية يتم من خلالها تحديد عوامل الخطر ثم القضاء عليها فعليا. إن تحليل هو منهجية (FMEA) أوضاع فشل وتأثيراتها لإدارة المخاطر لتحديد أوضاع فشل النظام وتأثيراتها وأسبابها. يحدد تحليل أوضاع فشل وتأثيراتها نقاط الضعف المحتملة في النظام. يسمح هذا النهج للشركات بتصحيح المناطق التي تم تحديدها من خلال العملية قبل فشل النظام. في هذه الورقة، نحدد العديد من عوامل فشل الحرجة التي قد تعرض أمن أنظمة المعلومات للخطر. من خلال القيام بذلك نقوم بشكل منهجي بتحديد وتحليل وتوثيق أوضاع فشل المحتملة والآثار المحتملة لكل فشل على النظام. تؤدي (FMEA) عملية تحليل أوضاع فشل وتأثيراتها المقترحة للأمن السيبراني إلى وصف مفصل لكيفية تأثير الفشل على أداء النظام وكيف يمكن تجنبها. يتم

توضيح مدى قابلية تطبيق تحليل أوضاع الفشل وتأثيراتها المقترح بمثال من مطار إقليمي^{٢٧}.

المحور الثالث

اشكالية ومهددات الامن السيبراني

أولاً: الموازنات الوطنية المحدودة مع مستوى التهديدات السيبرانية

تعد الهجمات السيبرانية من أكبر التهديدات التي تواجه الحكومات والمؤسسات الوطنية في العصر الحديث. فمع تزايد استخدام التكنولوجيا والانترنت في جميع جوانب الحياة، أصبحت البيانات الحساسة والمعلومات الحكومية عرضة للاختراق والسرقة من قبل القراصنة الإلكترونيين.

في واقع الامر ان تحديد الموازنة الوطنية المناسبة لمواجهة التهديدات السيبرانية يعتبر تحدياً كبيراً، حيث تتطلب استراتيجيات الأمن السيبراني استثمارات كبيرة في التكنولوجيا والتدريب والتحديث المستمر. ومن الضروري أن تكون الموازنة الوطنية متوازنة بين الاستثمار في الأمن السيبراني وبين الاحتياجات الأخرى للدولة. يمكن تحقيق هذا من خلال تخصيص ميزانية كافية لتحسين قدرات الدولة في مجال الأمن السيبراني، وضمان تحديث التقنيات والأدوات المستخدمة لمواجهة التهديدات الجديدة. كما يجب أيضاً

27 Ibid, p19.

كيفية التعامل مع الهجمات الإلكترونية والحفاظ على سرية المعلومات.

٢- تبادل المعلومات: يمكن للحكومات تعزيز التعاون مع بلدان أخرى والمنظمات الدولية لتبادل المعلومات والخبرات في مجال الأمن السيبراني.

٣- الاستفادة من التكنولوجيا المتاحة: يجب على الحكومات استخدام التكنولوجيا المتاحة بشكل فعال لتعزيز أمنها السيبراني، مثل استخدام برامج مكافحة الفيروسات وتحديث الأنظمة الأمنية بانتظام.

٤- الاستثمار في البحث والتطوير: يجب على الحكومات الاستثمار في البحث والتطوير لتطوير تقنيات جديدة في مجال الأمن السيبراني والتصدي للتهديدات الجديدة.

باختصار، تواجه الحكومات تحديا كبيرا في مجال تأمين مواردها المالية لمكافحة التهديدات السيبرانية، ولكن من خلال اتباع استراتيجيات فعالة وتعاون مع الجهات المعنية، يمكنها تعزيز أمنها السيبراني وحماية بياناتها بشكل أفضل.

توجيه الاستثمارات نحو تدريب وتأهيل الكوادر البشرية لتعزيز القدرات الوطنية في هذا المجال^{٢٨}.

بالإضافة إلى ذلك، يجب أن تكون هناك استراتيجية واضحة لتحقيق التوازن بين الموازنة الوطنية ومستوى التهديدات السيبرانية، مع مراعاة الأولويات الأمنية والاقتصادية للدولة. ويجب أن تكون هناك آليات لمراقبة وتقييم كفاءة استخدام الموارد المالية وضمان تحقيق الأهداف المحددة في مجال الأمن السيبراني. ومع ذلك، تواجه الحكومات تحديا كبيرا في مجال تخصيص الموارد المالية لمكافحة هذه الهجمات السيبرانية، خاصة مع وجود موازنات وطنية محدودة. فعلى الرغم من أهمية حماية البيانات والمعلومات الحكومية، إلا أن الاستثمار في تكنولوجيا الأمن السيبراني يتطلب تكاليف مرتفعة ومستمرة^{٢٩}.

وبالتالي، يجب على الحكومات أن تبحث عن سبل بديلة لتعزيز أمنها السيبراني بموارد محدودة. من بعض الخطوات التي يمكن اتخاذها^{٣٠}:

١- توعية الموظفين: يجب على الحكومات توعية موظفيها بأهمية الأمن السيبراني وتدريبهم على

28 Lawrence A. Gordon and Martin P. Loeb, The Economics of Information Security: A Framework for Making Decisions, 1st edn, New York, Springer-Verlag, 2006, p47.

29 OECD, Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies, Paris, OECD Publishing, 2012, p68.

30 S. Furnell, Cyber Security: Everything You Need to Know About Computer and Cyber Safety, 2nd edn, London, BCS Learning & Development Ltd, 2021, p113.

ثانياً: التزايد المستمر لمستوى التهديد السيبراني

وتشمل هذه الهجمات سرقة البيانات الشخصية والمالية، وتعطيل خدمات الإنترنت، واختراق الأنظمة الحيوية، والتجسس الصناعي، والكثير من الأنشطة الضارة الأخرى. يعود التزايد في مستوى التهديد السيبراني إلى عدة عوامل، منها النمو السريع للتكنولوجيا والانترنت، وزيادة استخدام الأجهزة الذكية والتطبيقات الرقمية، وتطور أساليب القرصنة والاحتيال الإلكتروني. بالإضافة إلى ذلك، تزايدت الاعتمادية على البيانات والمعلومات الرقمية في مجالات مختلفة، مما يجعلها هدفاً سهلاً للهجمات السيبرانية. للتصدي لهذا التهديد المتزايد، يجب على الأفراد والشركات والحكومات اتخاذ تدابير أمنية فعالة وتحسين استراتيجيات الأمن السيبراني. يجب توعية الأفراد بأهمية حماية بياناتهم الشخصية وتجنب الوقوع في فخ الاحتيال الإلكتروني. كما يجب على الشركات تعزيز أنظمة الأمان والحماية لحماية بيانات العملاء والمعلومات الحساسة^{٣١}.

بالنظر إلى التحديات السيبرانية المستمرة، يجب على الجميع أن يكونوا يقظين ومستعدين لمواجهة هذا التهديد بكل فعالية وحزم. إن عدم التصدي للهجمات

السيبرانية يمكن أن يؤدي إلى خسائر كبيرة، سواء من ناحية المال أو السمعة أو الأمان. لذا، يجب على الجميع الاستثمار في الأمان السيبراني وتطوير القدرات الضرورية للتصدي لهذا التهديد المتزايد. التزايد المستمر لمستوى التهديد السيبراني هو من الموضوعات الحيوية في عالم الأمن السيبراني اليوم، ويعكس تطور التهديدات التي تواجه الأفراد والمنظمات والحكومات على حد سواء. نعدد التقارير والدراسات التي تناول هذا الموضوع^{٣٢}، واهم تلك التقارير التي تناولت التزايد المستمر لمستوى التهديدات السيبرانية هي:

١- تقرير "التوجهات العالمية في الأمن السيبراني" (Global Cybersecurity Trends Report):

يعد هذا التقرير مرجعاً رئيسياً لفهم التهديدات السيبرانية العالمية، حيث يستعرض الاتجاهات الحالية في الهجمات السيبرانية والتقنيات المستخدمة، بالإضافة إلى التحديات التي تواجهها الشركات في التصدي لهذه التهديدات^{٣٣}.

31 P.W. Singer and Allan Friedman, Cybersecurity and Cyberwar: What Everyone Needs to Know, Oxford, Oxford University Press, 2014, p69.

٣٢ حسن محمد حسن، 'الأمن السيبراني وتحديات الأمن القومي في العصر الرقمي'، المجلة العربية للدراسات الأمنية، المجلد 37، العدد 2، 2021، ص 145.

33 World Economic Forum (WEF), Global Cybersecurity Outlook 2024, (Geneva: WEF, 2024), p. 12.

٢- تقرير "الأمن السيبراني في الشركات" من قبل "مجموعة بوسطن الاستشارية (BCG)":"

يقدم التقرير تحليلاً عميقاً حول كيفية تأثير التهديدات السيبرانية على الشركات وسبل مواجهتها، ويشمل إحصائيات عن الأضرار المالية والسمعية الناجمة عن الهجمات السيبرانية.^{٣٤}

٣- تقرير "أداء الأمن السيبراني ٢٠٢٣" من قبل "شركة مايكروسوفت"

يناقش التقرير التهديدات الإلكترونية الأكثر شيوعاً، مثل البرمجيات الخبيثة، الهجمات عبر البريد الإلكتروني، والهجمات على سلاسل التوريد. كما يسلط الضوء على دور الذكاء الاصطناعي في تعزيز الهجمات والهجمات المستهدفة.^{٣٥}

٤- تقرير "التهديدات المتقدمة المستمرة" (APT) : (Threat Report)

يتعامل هذا التقرير مع الهجمات السيبرانية المتقدمة التي تنفذها مجموعات قرصنة موجهة، والتي تستهدف المؤسسات الكبرى مثل الحكومات والشركات متعددة

الجنسيات. ويقدم تفاصيل عن أساليب الهجوم وتقنيات الحماية.^{٣٦}

٥- تقرير "التهديدات في الحوسبة السحابية" (Cloud Security Threat Report):

مع تزايد استخدام الحلول السحابية، يتم التركيز على التهديدات الأمنية المتعلقة بهذه البيئة. يعرض التقرير التحديات المتعلقة بحماية البيانات عبر السحابة.^{٣٧}

٦- تقرير "الأمن السيبراني والتطورات المستقبلية" من قبل المنتدى الاقتصادي العالمي (WEF):

يستعرض هذا التقرير التوجهات المستقبلية في الأمن السيبراني ويحدد المخاطر التي قد تنشأ في المستقبل، مثل الهجمات المعتمدة على الذكاء الاصطناعي وحروب المعلومات.^{٣٨}

٧- تقرير "التهديدات السيبرانية في قطاع الرعاية الصحية" (Healthcare Cyber Threat Report):

يركز على التهديدات الموجهة ضد أنظمة الرعاية الصحية، والتي قد تؤدي إلى تسريب بيانات حساسة أو تعطيل العمليات الحيوية.^{٣٩}

34 Boston Consulting Group (BCG), What Leaders in Cybersecurity Get Right: Annual Cybersecurity Survey 2024, (Boston: BCG, 2024), p. 8.

35 Microsoft, Microsoft Digital Defense Report 2023, (Redmond: Microsoft Corporation, 2023), pp. 24-30.

36 Mandiant (Google Cloud), M-Trends 2024, (Milpitas: Mandiant, 2024), p. 15.

37 Check Point Software Technologies, 2024 Cloud Security Report, (San Carlos: Check Point, 2024), p. 19.

38 World Economic Forum (WEF), Cybersecurity and Future Developments: Insight Report, (Geneva: WEF, 2024), p. 22.

39 Health-ISAC, Healthcare Cybersecurity Benchmarking Study 2024, (Florida: Health-ISAC, 2024), p. 11.

خلال الاستثمار المنظم في التقنيات الحديثة، وتبني استراتيجيات وطنية شاملة للأمن السيبراني. ويُعد إشراك المنظمات الدولية المتخصصة في هذا المجال، كمنظمة الشرطة الجنائية الدولية (الإنتربول)، خياراً استراتيجياً مهماً لتعزيز قدرات الدول في التصدي للمخاطر الرقمية. إذ تعتمد العديد من دول العالم اليوم على شراكات متقدمة مع الإنتربول في سبيل مكافحة الجريمة الإلكترونية، وهو ما يتطلب من الدول الأعضاء في المنظمة - وعددها ١٩٥ - أن تكون مهيأة بشكل فعال للتعامل مع هذا النوع من التهديدات بأساليب وقائية واستباقية.

فالجرائم السيبرانية لم تعد تمثل تهديداً مستقبلياً فقط، بل أصبحت من أبرز التحديات الراهنة التي تواجه الأمن الوطني والدولي على حد سواء. ورغم عدم وجود نموذج واحد يصلح لجميع حالات التصدي لتلك التهديدات، إلا أن التعاون الدولي وتبادل البيانات والخبرات العابرة للحدود يمثلان ركيزة أساسية لبناء منظومة فعالة للتصدي للجريمة السيبرانية بمختلف أشكالها.

رغم أن التهديدات السيبرانية قد تؤدي إلى نزاعات، فإنها أيضاً تمثل فرصة للتعاون الدولي. فقد دفعت خطورة التهديدات بعض الدول إلى العمل سوياً لمواجهةها ويتم ذلك من خلال:

١ - اتفاقيات دولية للأمن السيبراني:

ظهرت العديد من الاتفاقيات مثل "اتفاقية بودابست لمكافحة الجرائم الإلكترونية" لتعزيز

إجمالاً، تركز التقارير على التحليل الاستراتيجي والتقني لتهديدات الأمن السيبراني، كما تسلط الضوء على أهمية الابتكار في أنظمة الدفاع لمواجهة هذه التهديدات.

الخاتمة والاستنتاجات

في ختام هذا البحث، يمكن القول إن تهديدات الأمن السيبراني أصبحت من القضايا الحيوية التي تؤثر بشكل كبير على العلاقات الدولية والصراعات العالمية في الوقت الحاضر. فقد أدى تطور التكنولوجيا الرقمية إلى تحول الأنشطة العسكرية والسياسية إلى الفضاء السيبراني، ما جعل الدول في مواجهة تحديات جديدة تتطلب استراتيجيات أكثر تعقيداً ومرونة. وبات من الواضح أن الهجمات السيبرانية تمثل وسيلة جديدة للتأثير على الأمن القومي والاقتصاد والاستقرار السياسي، ما يخلق بيئة من التوترات والصراعات بين القوى الدولية.

إن هذه التهديدات قد تعيد تشكيل موازين القوى العالمية، حيث أصبح كل طرف يسعى لتعزيز قدراته السيبرانية في مواجهة الخصوم المحتملين. لذا، تتطلب هذه الظاهرة الدولية التعاون المشترك بين الدول لوضع أطر قانونية وأمنية تحكم استخدام الفضاء السيبراني، فضلاً عن تعزيز الاستعدادات الدفاعية لمواجهة هذا النوع من الصراع.

نظراً لطبيعة العصر الرقمي الراهن وسرعة التحولات التكنولوجية المتلاحقة، أصبحت الحاجة ملحة لاعتماد مقاربة جادة في مواجهة الجرائم السيبرانية، وذلك من

مستوى دولي شامل لضمان استقرار العلاقات الدولية وحماية المصالح الوطنية في هذا المجال الحيوي.

إقرار تضارب المصالح

يُقر المؤلف بعدم وجود أي تضارب محتمل في المصالح فيما يتعلق بالبحث أو التأليف أو نشر هذا المقال.

التمويل

لم يتلقَ المؤلف أي دعم مالي لإجراء هذا البحث أو تأليفه أو نشره.

البيان الأخلاقي

هذا البحث يتوافق مع المعايير الأخلاقية لإجراء الدراسات العلمية. وقد تم الحصول على موافقة خطية من جميع المشاركين الأفراد المشمولين في الدراسة.

بيان توفر البيانات

البيانات متاحة عند الطلب من المؤلف المراسل.

الشكر والتقدير

لا يوجد شكر وتقدير أفصح به الباحث

التعاون القانوني والتقني بين الدول وغيرها الكثير من الاتفاقيات.

٢- مشاركة المعلومات:

إنشاء منصات دولية لتبادل المعلومات حول التهديدات السيبرانية والهجمات المحتملة يساعد في تعزيز الاستجابة العالمية، والتعامل بشكل مباشر مع كافة مستويات التهديدات السيبرانية.

٣- التدريب وبناء القدرات:

تسعى الدول المتقدمة إلى دعم الدول الأقل تطوراً في بناء قدراتها السيبرانية لمواجهة التحديات، مما يقلل التهديدات السيبرانية القادمة من تلك الدول ويسهم بالتالي مشاركة فعالة وحقيقية لتلك الدول في الدفاع السيبراني.

وفي النهاية، فإن الأمن السيبراني لم يعد مجرد مسألة فنية أو تكنولوجية، بل أصبح جزءاً من الاستراتيجيات السياسية والاقتصادية، ويجب أن يتم التعامل معه على

المصادر

أولاً: المصادر العربية

١- الكتب

ابن منظور. لسان العرب. بيروت: دار صادر، المجلد 13.

جودة أبو ألياس. (2011). الأمن البشري وسيادة الدول. بيروت: المؤسسة الجامعية للدراسات والنشر والتوزيع.

٢- البحوث المنشورة في المجلات العلمية

أحمد فريجة، والدمية فريجة. (2016). الأمن والتحديات الأمنية في عالم ما بعد الحرب الباردة. مجلة دفاثر السياسة والقانون.

شهرزاد آدمام. (2013). طبيعة التهديدات الأمنية الجديدة. مجلة الندوة للدراسات القانونية.

محمد حشمي. (2018). مدرسة باريس للدراسات الأمنية وإشكالية مستوى التحليل في العلاقات الدولية. مجلة السياسة الدولية.

زينب عباس راضي. (2025). فاعلية الأمن السيبراني في السياسة العالمية (المفهوم والتدابير الأمنية للدول). مجلة آشور للعلوم القانونية والسياسية، 2 (1).

منى عبد الله. (2020). متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود. مجلة كلية التربية، جامعة المنصورة.

حسن محمد حسن. (2021). الأمن السيبراني وتحديات الأمن القومي في العصر الرقمي. المجلة العربية للدراسات الأمنية، 37 (2).

٣- المداخلات وأعمال المؤتمرات

قاسم حجاج. (2014). التدخل الإنساني للجيش الوطني الشعبي في مواجهة الكوارث الطبيعية. مداخلات مقدمة في الملتقى الدولي حول الدفاع الوطني بين الالتزامات والتحديات الإقليمية.

٤- التقارير والاستراتيجيات الحكومية والمصادر الإلكترونية

الهيئة الوطنية للأمن السيبراني. (2023). الاستراتيجية الوطنية للأمن السيبراني. الرياض، المملكة العربية السعودية. <https://nca.gov.sa/ar/pages/national-strategy> تاريخ الوصول: 13 يناير (2026).

البوابة الرسمية لحكومة دولة الإمارات العربية المتحدة. (2024). السلامة السيبرانية والأمن الرقمي. استراتيجيات ومبادرات. <https://u.ae/ar/information-and-services/justice-safety-and-the-law/cyber-safety-and-digital-security> تاريخ الوصول: 13 يناير (2026).

ثانياً: المصادر الأجنبية

١- الكتب

- Furnell, S. (2021). *Cyber Security: Everything You Need to Know About Computer and Cyber Safety* (2nd ed.). BCS Learning & Development Ltd.
- Gordon, L. A., & Loeb, M. P. (2006). *The Economics of Information Security: A Framework for Making Decisions* (1st ed.). Springer-Verlag.
- Rid, T. (2020). *Active Measures: The Secret History of Disinformation and Strategic Warfare*. Farrar, Straus and Giroux.
- Schmitt, M. N. (Ed.). (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press.
- Singer, P. W., & Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press.
- Wiener, N. (1948). *Cybernetics or Control and Communication in the Animal and the Machine*. MIT Press.

٢- المعايير والأطر والأدلة الفنية

- International Organization for Standardization. (2012). *Information Technology—Security Techniques—Guidelines for Cybersecurity (ISO/IEC 27032:2012, Clause 4)*.
- International Telecommunication Union. (2008). *ITU-T Recommendation X.1205: Overview of Cybersecurity (Section 3.2.1)*. ITU.
- National Institute of Standards and Technology. (2017). *An Introduction to Information Security (NIST Special Publication 800-12 Rev. 1, p. 7)*. U.S. Department of Commerce.
- National Institute of Standards and Technology. (2020). *NICE Cybersecurity Workforce Framework (NIST Special Publication 800-181)*. U.S. Department of Commerce.
- National Institute of Standards and Technology. (2022). *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (SP 800-161 Rev. 1)*. U.S. Department of Commerce.

٣- الكتب والتقارير المتعلقة بالأمن الدولي والسياسات الأمنية

Mazarr, M. J., et al. (2019). *The Character of Manipulation: The Use of Information as a Tool of Statecraft*. RAND Corporation.

NATO Cooperative Cyber Defense Centre of Excellence. (2016). *20th Century Redux: Cyber Power*. NATO CCDCOE Publications.

OECD. (2012). *Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies*. OECD Publishing.

National Science Foundation. (2007). *Cyberinfrastructure Vision for 21st Century Discovery*. NSF Press.

The Brookings Institution. (2022). *Cyber Campaigns and the Future of Political Warfare*. Brookings Press.

٤- التقارير الدولية وتقارير الشركات والمؤسسات

Boston Consulting Group. (2024). *What Leaders in Cybersecurity Get Right: Annual Cybersecurity Survey 2024*.

Check Point Software Technologies. (2024). *2024 Cloud Security Report*.

Health-ISAC. (2024). *Healthcare Cybersecurity Benchmarking Study 2024*.

Mandiant (Google Cloud). (2024). *M-Trends 2024*.

Microsoft. (2023). *Microsoft Digital Defense Report 2023*. Microsoft Corporation.

Verizon Business. (2024). *2024 Data Breach Investigations Report (DBIR)*.

World Economic Forum. (2024). *Cybersecurity and Future Developments: Insight Report*.

World Economic Forum. (2024). *The Global Cybersecurity Outlook 2024*.

References

- Abdullah, M. (2020). *Cybersecurity requirements for management information systems at King Saud University*. *Journal of the College of Education, Mansoura University*.
- Adamam, S. (2013). *The nature of new security threats*. *Al-Nadwa Journal for Legal Studies*.
- Boston Consulting Group. (2024). *What leaders in cybersecurity get right: Annual cybersecurity survey 2024*.
- Check Point Software Technologies. (2024). *2024 cloud security report*.
- Furnell, S. (2021). *Cyber security: Everything you need to know about computer and cyber safety (2nd ed.)*. BCS Learning & Development Ltd.
- Freija, A., & Freija, A. (2016). *Security and security threats in the post-Cold War world*. *Dafatir al-Siyasa wa al-Qanun Journal*.
- Gordon, L. A., & Loeb, M. P. (2006). *The economics of information security: A framework for making decisions (1st ed.)*. Springer-Verlag.
- Hajjaj, Q. (2014). *The humanitarian intervention of the People's National Army in the face of natural disasters*. Paper presented at the International Conference on National Defense between Commitments and Regional Challenges.
- Hassan, H. M. (2021). *Cybersecurity and national security challenges in the digital age*. *Arab Journal of Security Studies*, 37(2).
- Health-ISAC. (2024). *Healthcare cybersecurity benchmarking study 2024*.
- Ibn Manzur. (n.d.). *Lisan al-Arab (Vol. 13)*. Dar Sader.
- International Organization for Standardization. (2012). *Information technology—Security techniques—Guidelines for cybersecurity (ISO/IEC 27032:2012, Clause 4)*.

- International Telecommunication Union. (2008). ITU-T Recommendation X.1205: Overview of cybersecurity (Section 3.2.1). ITU.*
- Jawdat Abu Elias. (2011). Human security and state sovereignty. University Foundation for Studies, Publishing and Distribution.*
- Mandiant (Google Cloud). (2024). M-Trends 2024.*
- Mazarr, M. J., et al. (2019). The character of manipulation: The use of information as a tool of statecraft. RAND Corporation.*
- Microsoft. (2023). Microsoft digital defense report 2023. Microsoft Corporation.*
- National Cybersecurity Authority. (2023). National cybersecurity strategy. Riyadh, Saudi Arabia. <https://nca.gov.sa/ar/pages/national-strategy>*
- National Institute of Standards and Technology. (2017). An introduction to information security (NIST Special Publication 800-12 Rev. 1, p. 7). U.S. Department of Commerce.*
- National Institute of Standards and Technology. (2020). NICE cybersecurity workforce framework (NIST Special Publication 800-181). U.S. Department of Commerce.*
- National Institute of Standards and Technology. (2022). Cybersecurity supply chain risk management practices for systems and organizations (SP 800-161 Rev. 1). U.S. Department of Commerce.*
- National Science Foundation. (2007). Cyberinfrastructure vision for 21st century discovery. NSF Press.*
- NATO Cooperative Cyber Defence Centre of Excellence. (2016). 20th century redux: Cyber power. NATO CCDCOE Publications.*
- OECD. (2012). Cybersecurity policy making at a turning point: Analysing a new generation of national cybersecurity strategies. OECD Publishing.*
- Qabain, S. (2012). The history of the Romanovs. Hindawi Foundation.*

- Rid, T. (2020). *Active measures: The secret history of disinformation and strategic warfare*. Farrar, Straus and Giroux.
- Schmitt, M. N. (Ed.). (2017). *Tallinn manual 2.0 on the international law applicable to cyber operations*. Cambridge University Press.
- Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press.
- The Brookings Institution. (2022). *Cyber campaigns and the future of political warfare*. Brookings Press.
- UAE Government Official Portal. (2024). *Cyber safety and digital security. Strategies and Initiatives*. <https://u.ae/ar/information-and-services/justice-safety-and-the-law/cyber-safety-and-digital-security>
- Verizon Business. (2024). *2024 data breach investigations report (DBIR)*.
- Wiener, N. (1948). *Cybernetics or control and communication in the animal and the machine*. MIT Press.
- World Economic Forum. (2024). *Cybersecurity and future developments: Insight report*.
- World Economic Forum. (2024). *Global cybersecurity outlook 2024*.
- Hashmi, M. (2018). *The Paris School of Security Studies and the problem of the level of analysis in international relations*. *International Politics Journal*.
- Radhi, Z. A. (2025). *The effectiveness of cybersecurity in global politics: Concept and security measures for states*. *Ashur Journal of Legal and Political Sciences*, 2(1).