# الحروب الحديثة: الهجمات السيبرانية واستهداف البنى التحتية للدول

# Modern Warfare: Cyber Operations and the Targeting of National Critical Infrastructure

**محمد الحرماوي طالب باحث بسلك الدكتوراه،**
**مختبر القانون العام والعلوم السياسية**
**كلية العلوم القانونية والاقتصادية والاجتماعية بوجدة**
**جامعة محمد الأول، المغرب**

**الملخص**

الهجمات السيبرانية على البنية التحتية الحيوية للدول / Critical National Infrastructure أصبحت من أخطر التهديدات للأمن القومي والاستقرار. مع التحول الرقمي السريع، تعتمد قطاعات حيوية مثل الكهرباء، المياه، الاتصالات، النقل، الصحة، والمالية على أنظمة معلوماتية متصلة، مما يجعلها أهدافًا مباشرة لهجمات الدول، الجماعات المنظمة، والمجرمين السيبرانيين. تشمل هذه الهجمات برامج الفدية التي تعطل الخدمات بتشفير البيانات، وهجمات الحرمان من الخدمة (DDoS) التي تغمر الأنظمة بحركة زائدة، والهجمات على أنظمة التحكم الصناعي (ICS/SCADA) التي قد تتسبب بأضرار مادية، إضافة إلى هجمات سلاسل التوريد البرمجية التي تتيح الوصول إلى مؤسسات متعددة عبر ثغرة واحدة.

**الكلمات المفتاحية** : الذكاء الاصطناعي، الهجمات السيبرانية، الأمن السيبراني، السيادة الرقمية، البنية التحتية الحيوية.

**Abstract**

Cyberattacks are increasingly used as geopolitical tools, for espionage or destabilization, as seen in the Ukraine power grid attack and the Stuxnet malware targeting nuclear facilities. Consequences include service disruption, economic losses, threats to public safety, and erosion of trust in state institutions, while exposing weaknesses in legislation and inter-agency coordination.

To address these risks, states must adopt comprehensive national cybersecurity strategies, including legal updates, public-private cooperation, and building capabilities for threat detection and incident

response. Investments in research, training, international standards compliance, and information sharing are essential to enhance national cyber resilience. In sum, cyberattacks on critical infrastructure are no longer just technical threats but multidimensional security challenges requiring proactive, coordinated defense to safeguard essential services and national stability.
Keywords: Artificial Intellegence, Cyberattaks, Cybersecurity, Digital Sovereinty, Critical Infrastructure

**المقدمة**

لم يسلم العالم من ويلات الحرب التقليدية والتدمير العسكري حتى برز للوجود سلاح الهجمات السيبرانية الذي يشكل اليوم تحديا كبيرا للأمن القومي والعديد من الباحثين يعتبرون الفضاء السيبراني بمثابة المجال الخامس في الحروب بعد البر والبحر والجو والفضاء، ففي ظل التطور الرقمي الذي يشهده العالم زادت بشكل ملحوظ حجم التهديدات السيبرانية والاختراقات المتتالية، فأصبح أمن الفضاء السيبراني إحدى المهام ذات الأولوية في الشؤون الداخلية لكل دولة، فتبلور في ظهور الأمن السيبراني وبروز القوة السيبرانية التي توزعت وانتشرت بين عدد كبير من الفاعلين على مستوى الدولي والمحلي ما جعل الفضاء السيبراني مجالا جديدا للصراع والحرب.

تختلف مصطلحات الحرب والصراع والهجوم في الفضاء السيبراني تبعا لتوظيف الدول سياسيا ودعائيا للهجمات المضادة إلكترونيا، فقاموس كامبردج عرف الحرب السيبرانية على أنها نشاط استخدام الإنترنت لمهاجمة أجهزة الكمبيوتر في بلد من أجل إتلاف أشياء مثل أنظمة الاتصالات والنقل أو إمدادات المياه والكهرباء، ويمكن أن يؤدي استخدام الحرب الإلكترونية إلى زعزعة استقرار الأنظمة المالية أو نظام الهاتف أو شبكة الإنترنت.

عرفه المفكر جوزيف ناي الحرب السيبرانية بأنها الأعمال العدائية في الفضاء السيبراني التي لها آثار تعادل أو تفوق العنف الحركي التقليدي.[428]

أما كينيت جيرس يعرفها بأنها القدرة على الدفاع والهجوم على المعلومات، من خلال شبكات الحاسب الالي عبر الفضاء السيبراني بالإضافة إلى شل قدرة الخصم على القيام بنفس الهجمات، وتشمل هذه الحرب خمسة عناصر حسب جيرس وهي التجسس، الدعاية والحرمان من خدمة الإنترنت، تعديل البيانات والتلاعب بها، والتلاعب بالبيانات التحتية.[429]

عرف ماركو روسيني الحرب السيبرانية بأنها تطويع الإمكانيات الإلكترونية العسكرية لأجل التأثير في مواقع إلكترونية أخرى وتعطيلها أو تدميرها سواء أكانت تقدم خدمة مدنية أو عسكرية.[430]

وفي تعريف أخر لمايكل شميت نجد أنها مجموعة من الإجراءات التي تتخذها الدول للهجوم على نظم المعلومات المعادية بهدف التأثير والإضرار بها وفي الوقت ذاته للدفاع عن نظم المعلومات الخاصة بالدولة المهاجمة.[431]

---

428- Nye Josephs, Nuclear Lessons for Cyber Security?, Strategic studies Quarterly, vol 5, No 4, winter 2011, pp 18-38.

429- Kenneth Geers, Cyberspace and the changing Nature of ware, the NATO cooperative Cyber Defence, Center of Excellence, Tallinn, Estonia, 2008, PP.2-4.

430- Marco Roscini, World Wide Warfare - jus ad bellum and the use of cyber Force, Max Planck yearbook of United Nations Law, vol 14, 2010, p91.

431- Michael Schmitt, Computer Network Attack and the Use off Force in International Law through on a Normative, the Colombia journal of transitional law, vol 27, No 885-937, 1999, p7.

عرفه الأستاذ نلس ميلتسر الحرب السيبرانية بأنها الحرب التي تتم في الفضاء السيبراني من خلال الوسائل والأساليب السيبرانية،[432] وعرفها ماركو جريك بأنها استخدام المعلومات والاتصالات في إدارة الحرب باستخدام الإنترنت.[433]

إن عدم الاتفاق دوليا على معنى قانوني أو تعريف للحرب السيبرانية يجعل وضع تعريف مانع جامع لها في غاية الصعوبة خصوصا إذا علمنا أنها تستخدم في عبارات وصيغ وسياقات مختلفة ولا تقتصر على النزاعات المسلحة دائما.

عرف الفضاء السيبراني العديد من الحروب والهجمات السيبرانية مثل ما وقع بين روسيا وأستونيا عام 2007، وبين روسيا وجورجيا 2008، والولايات المتحدة الأمريكية وإيران منذ عام 2009 وحتى عام 2013، وكوريا الشمالية وكوريا الجنوبية في عامي 2011 و2013، وكوريا الشمالية والولايات المتحدة الأمريكية عام 2016 عقب الانتخابات الرئاسية الأمريكية وإيران والمملكة العربية السعودية عام 2016 و 2017 بالإضافة إلى هجمات الفدية الخبيثة التي اجتاحت العالم عامي 2017 و 2018 وهجمات أخرى بعد هذا التاريخ.

*** أهمية الدراسة:**

تكمن أهمية الدراسة في أنها تحلل وتستعرض قدرات الهجمات السيبرانية وتفاعلاتها في الفضاء السيبراني وتكشف عن خطورتها ومدى تأثيرها على الأمن القومي للدول.

*** أهداف الدراسة:**

– تهدف الدراسة إلى بيان أهمية الأمن السيبراني للدول.

– تسلط الضوء على خطورة الهجمات السيبرانية وإمكانية تدميرها للبنايات التحتية للدول، وتحقيق خسائر بشرية واقتصادية مالية وسياسية.

*** إشكالية الدراسة:**

---

[432]- Nils Melzer, Cyberwarfar and International Law, UNIDIR, 2011, p4.

[433]- د ماركو جريك ، فهم الجريمة السيبرانية دليل للبلدان النامية ، منشورات الاتحاد الدولي للاتصالات،2009، ص 54.

تتمحور إشكاليات الدراسة حول مدى تأثير الهجمات السيبرانية على أمن البنية التحتية الحرجة والأمن القومي للدول؟

*** أسئلة الدراسة:**

– إلى أي حد تأثر تهديدات الأمن السيبراني على البنية التحتية الحيوية للدول ؟

– مدى تأثير الهجمات السيبرانية على القطاع الاقتصادي والسياسي والاجتماعي للدول؟

– كيف يمكن تجاوز أو الحد من خطورة الهجمات السيبرانية وتحقيق سيادة رقمية؟

*** حدود الدراسة:**

الحدود الزمنية لهذه الدراسة هي بداية أخطر الهجمات أما الحدود المكانية فهي الفضاء السيبراني وبالخصوص الدول التي تتوفر على قوة سيبرانية.

*** منهج الدراسة:**

نعتمد في هذه الدراسة على المنهج الوصفي لوصف ظاهرة الهجمات السيبرانية وحروبها والمنهج التحليلي لتحديد انعكاساتها على الأمن السيبراني والبيانات التحتية والأمن القومي للدول.

*** هيكلة الدراسة:**

سعيا منا لمعالجة الإشكالية والأسئلة المتفرعة عنها سنبحث موضوعنا في محورين:

**المحور الأول: الهجمات السيبرانية على البنية التحتية الحيوية**

**المحور الثاني: سبل تحقيق الأمن السيبراني**

**المحور الأول: الهجمات السيبرانية على البنية التحتية الحيوية**

أصبحت الهجمات السيبرانية خلال العقدين الأخيرين أحد أبرز التهديدات التي تواجه الدول والمؤسسات، خصوصا مع التحولات المتسارعة نحو الرقمنة والاعتماد المتزايد على التكنولوجيا في تشغيل مختلف القطاعات الحيوية. فالبنية التحتية الحيوية مثل الطاقة، والمياه، والاتصالات، والنقل، والرعاية الصحية تشكل العمود الفقري لاستمرارية حياة المجتمعات

الحديثة، وانقطاعها أو تعطيلها قد يخلق آثارا واسعة تتجاوز الخسائر الاقتصادية لتصل إلى تهديد الأمن القومي والاستقرار الاجتماعي.

تتسم الهجمات السيبرانية الموجهة نحو البنى الحيوية بطابعها المعقد والمتعدد الأبعاد، إذ تجمع بين المعرفة التقنية العالية والدوافع الاستراتيجية والسياسية والاقتصادية. فبعض الفاعلين يسعون لإحداث خلل مباشر يؤثر في الخدمات الأساسية، بينما يستهدف آخرون جمع بيانات حساسة أو اختبار نقاط الضعف ضمن منظومات الدول. ويزداد هذا التحدي صعوبة مع انتشار إنترنت الأشياء، وتزايد الترابط بين الأنظمة التشغيلية، مما يخلق مساحات جديدة للهجوم قد يستغلها المخترقون بسهولة أكبر.

إضافة إلى ذلك، فإن الطابع غير المرئي للهجمات السيبرانية وسرعتها وقدرتها على تجاوز الحدود الجغرافية يجعل من الصعب اكتشافها مبكرا أو تحديد مصادرها بدقة، وهو ما يعقد ردود الفعل ويحد من فعالية الأطر القانونية التقليدية. كما أن تزايد الاعتماد على الشبكات الرقمية في إدارة محطات الطاقة، وأنظمة التحكم الصناعي، والمستشفيات، والمطارات، جعل أي اختراق محتمل قادرا على إحداث شلل كامل في الدولة خلال دقائق قليلة.

- **الهجمات السيبرانية على منشآت الطاقة النووية للمحطات الكهربائية والمائية:**

أدى التطور التكنولوجي الذي عرفته البيئة الاستراتيجية العالمية نحو صياغة جيل جديد من التفاعلات الاستراتيجية التي بنيت على أساس افتراضي يعتمد على الاتصالات بوصفه مرتكزا استراتيجيا لديمومتها.

فتزايد الاعتماد على ربط البنى التحتية بالفضاء السيبراني أنتج ما يسمى البنية التحتية الاستراتيجية، كقطاع الطاقة والاتصالات، النقل، والخدمات الحكومية والمالية والتجارة الإلكترونية وغيرها، فظهر معها شكل جديد من التهديدات يمكن أن تسببه دولة أخرى دون

الحاجة لدخول أراضيها عن طريق الهجمات السيبرانية الموجهة ضد الأنظمة السيبرانية للمنشآت الحيوية لما لها من سمات مدنية وعسكرية متداخلة.[434]

من أبرز الهجمات وأخطرها كانت الهجمة على حواسب الجيش الأمريكي في عام 2008[435]. من خلال خازن إلكتروني (USB) متصل بكمبيوتر محمول تابع للجيش في قاعدة عسكرية موجودة في الشرق الأوسط، ولم يكتشف برنامج التجسس في الأنظمة السرية إلا بعد نقل آلاف الملفات من البيانات على خوادم خارجية (serveurs)[436].

كما تم استهداف أكثر من 72 شركة من بينها 22 مكتب حكومي و 13 من مقاولي قوات الدفاع بهدف سرقة معلومات حول الخطط والمباني العسكرية[437] .

خلال يونيو 2017 تعرضت أوكرانيا لهجمة سيبرانية شلت محطة الطاقة بالإضافة إلى المؤسسات وأحد أكبر مطاراتها.[438]

---

[434] بتر سنجر، دروس الحروب الماضية والاتجاهات التكنولوجية المستقبلية، بحث في كتاب الحروب المستقبلية في القرن 21، مركز الإمارات للدراسات والبحوث الاستراتيجية، أبو ظبي، الطبعة الأولى، 2014، ص 143.

[435] ينظر مرجع فرح يحيى زعاترة للمزيد حول التهديدات السيبرانية على الأمن القومي الأمريكي، العربي للنشر والتوزيع، مصر، الطبعة الاولى،2024، ص 151.

[436] د. أولاف تايلر، التهديدات الجديدة: الأبعاد الإلكترونية، مجلة حلف الناتو،11/11/2011، تاريخ الولوج 25/02/2025 متوفر على الرابط التالي:
http://www.nato.int/docu/review/2011/11-september/Cyber-Threads/AR/index.htm

[437] المرجع نفسه.

[438] Lizzie Dearden, Ukraine Cyber attack : chaos as national bank, State power provider and airport hit by Hackers, Independent , Jun 27/2017, last accessed 5/8/2024, accessible at :
https://www.independent.co.uk/news/world/europe/ukraine-cyber-attack-hackers-national-bank-state-power-company-airport-rozenko-pavlo-cabinet-computers-wannacry-ransomware-a7810471.html

ومثلها إيران تعرضت عام 2010 إلى هجمات فيروس" ستاكسنت" التي عطلت حوالي ألف من أجهزة الطرد المركزي في منشأة لتخصيب اليورانيوم في ناتانز وسط إيران.[439]

وقد تعرضت كوريا الجنوبية في ديسمبر 2014 لهجمات على أنظمة كمبيوتر شركة الطاقة المائية والنووية بحيث عثرت الشركة على دودة برمجية في بعض نظم التحكم بمحطة توليد الكهرباء من الطاقة النووية وأعلنت حالة تأهب مشيرة إلى ضلوع كوريا الشمالية في الهجوم دون ما يؤكد ذلك.[440]

وحول نفس الهجمات نشرت أمريكا تقريرا تتهم به روسيا أنها شنت هجمات سيبرانية على منشآت نووية ومحطات للكهرباء والمياه في الولايات المتحدة الأمريكية وأوروبا خلال الفترة الممتدة من 2015 إلى 2017[441].

أما في ألمانيا تم اكتشاف فيروسات خبيثة خلال أبريل من عام 2016، داخل كمبيوتر في مفاعل Gundermmingeen غوندرمينغ بحيث أصاب حواسيب ووسائط معلوماتية غير أنه لم يأثر على المفاعل لأن العمليات الصناعية مفصولة عن الإنترنيت.[442] وفي يونيو 2017 تعرضت محطة تشرنوبل النووية لهجمة سيبرانية ما أدى إلى انقطاع مؤقت بأنظمة

---

[439] صلاح عبد الرحمان الحديثي، مرجع سابق، ص ص 145-148.
ينظر: زهير حمداني، "ستاكسنت" حصان طروادة الذي أدخله عميل هولندي لمحطة نطنز النووية الإيرانية، الجزيرة، 2024/01/10، تاريخ الولوج 2024/9/27، متوفر على الرابط التالي :
https://tinyurl.com/2xqm5hpd

[440] سكاي نيوز عربية، طوارئ بكوريا الجنوبية لحماية محطاتها النووي، سكاي نيوز، أبو ظبي، 2014/12/26 تاريخ الولوج 2024/09/27، متوفر على الرابط التالي:
https://tinyurl.com/2cwon929

[441] إيهاب خليفة، مرجع سابق، ص 93.

[442] مركز المستقبل، تهديدات غير تقليدية: آليات حماية البنية التحتية الحرجة من الاختراق الإلكتروني، المستقبل للأبحاث والدراسات المتقدمة، 10 أكتوبر 2016، تاريخ الولوج 05/03/2025 متوفر على الرابط التالي:
https://tinyurl.com/27nnuycf

تشغيل "ويندوز" أوقف العمل على المراقبة الآلية للإشعاعات المتسربة في المنطقة الصناعية وتم تنفيذها يدويا.[443]

اتهمت روسيا كذلك الولايات المتحدة الأمريكية بشنها هجوم سيبراني بواسطة هاكرز عسكريين على الأنظمة الإلكترونية الخاصة بشبكات الطاقة الكهربائية وباتصالات سلكية روسية، إضافة إلى منظومة القيادة في الكرملين والتي جعلوها مهيأة للتعرض لهجمات إلكترونية أمريكية.[444]

في 23 يونيو 2018 أعلنت وزارة الأمن الداخلي الأمريكية عن اختراق هاكرز روسي غرفة التحكم في المرافق الكهربائية، الأمر الذي أتاح لهم إمكانية قطع التيار في الولايات المتحدة، بما يرتبه ذلك من إشاعة الفوضى والاضطرابات وذلك لاعتماد كافة الخدمات الحيوية على الكهرباء.[445]

---

[443] إيهاب خليفة، تهديدات سيبرانية: هل يستطيع القراصنة اختراق المنشآت النووية؟ المستقبل للأبحاث والدراسات المتقدمة، 7 يناير 2020، تاريخ الولوج 05/03/2025 متوفر على الرابط التالي:
https://tinyurl.com/2boularkhttps://tinyurl.com/2boulark

[444] ألكسندرتوميلين، روسيا تؤكد اتخاذ كل ما يلزم لحماية أمن المعلومات بعد أنباء عن اختراق أنظمتها الإلكترونية، روسيا اليوم 5 نونبر 2016، تاريخ الولوج 07/03/2025 متوفر على الرابط التالي:
https://tinyurl.com/27mmww8k

[445] البوابة التقنية، وزارة الأمن الداخلي الأمريكية: القراصنة الروس قادرين على التحكم بالمرافق الكهربائية الأمريكية، البوابة التقنية 24/07/2018 تاريخ الولوج 07/03/25 متوفر على الرابط التالي:
https://tinyurl.com/jhbzmu6

- **الهجمات السيبرانية على القطاع المالي:**

أثار البنك الدولي في عدة تقارير أصدرها على أن القطاع المالي يتعرض لهجمات سيبرانية تكلفتها تقدر بحوالي 9% من صافي دخل البنوك على مستوى العالم.[446]

في عام 2016 استهدف البنك المركزي لبنغلاديش بما يعرف بعملية لازاروس في محاولة لسرقة مليار دولار، ووجهت الاتهامات إلى كوريا الشمالية، واعتبرت هذه العملية ناقوس الخطر وإنذار حقيقي لأسواق المال وبأن الهجمات السيبرانية تهديد حقيقي للاستقرار المالي.[447]

- **الهجمات السيبرانية على قطاع الاتصالات وحركة الملاحة البحرية والبرية والجوية:**

يعرف قطاع الاتصالات والملاحة البرية والبحرية والجوية هجمات سيبرانية تهدف تعطيل الرادارات والملاحة وتعطيل برامج هبوط الطائرات وإقلاعها، إضافة إلى اختراق شبكات الهاتف وتعطيل محطات توزيع الخدمة وتجميد التواصل بين الأفراد واستهداف حسابات شبكة التواصل الاجتماعي.[448]

ومن أمثلة الهجومات نجد الهجوم الذي سبق المواجهة الروسية الأوكرانية عام 2015 وهجوم إستنيا في ماي 2007 الذي شل كل القطاعات الحيوية بالبلاد والمواقع الرسمية لرئاسة الوزراء والبرلمان.

- **الهجمات السيبرانية على القطاع الصحي:**

الهجمات السيبرانية ضد مرافق الرعاية الصحية حديث نسبيا ورغم التحول الرقمي الذي عرفته وتحقيقه لخدمات عالية ويوفر بيانات هامة، يلاحظ بعض القصور في تدابير الأمن السيبراني،

---

[446] تيم مور، أرثر نيلسون، التهديد السيبراني العالمي، تقرير التمويل والتنمية، صندوق النقد الدولي، مارس 2021، ص 25.
محمد إسماعيل، الأمن السيبراني في القطاع المصري، صندوق النقد العربي، موجز سياسات، العدد الرابع، يونيو 2019، ص 1.

[447] تيم مور، أرثر نيلسون، مرجع سابق.

[448] أميرة عبد العظيم، محمد عبد الواحد، المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام، مجلة القانون والشريعة، عدد 35، الجزء3، 2020، ص 433.

وهو ما يجعلها هدفا رئيسيا لمرتكبي الجرائم السيبرانية وتشكل خطرا على حياة المرضى والأطقم الطبية الصحية.[449]

تعطل هجمات برامج الفدية الضارة شبكات الرعاية الصحية بغرض الحصول على مبالغ مالية مثل هجمات واناكراي على المملكة المتحدة لعام 2017، الذي أطاح بالخدمة الصحية، وسبب خسائر قدرت ب 92 مليون جنيه إسترليني، بسبب فقدان خدمات وتكاليف تكنولوجيا المعلومات عقب الهجوم الذي قام به قراصنة كوريا الشمالية والذي عطل 80 مؤسسة وألغى 19000 موعد خلال أسبوع واحد وهدد الأمن الصحي.[450]

وتبقى أول وفاة لامرأة ألمانية بسبب هجوم سيبراني على مستشفى في مدينة دوسلدوف الواقعة غرب البلاد بعد نقلها إلى مستشفى آخر بسبب تعطل الخدمة.[451]

ويتعرض قطاع الصحة كذلك إلى حملات التضليل التي استعرت في مرحلة تفشي وباء كورونا، حيث تعرضت مخابر البحث واللقاحات إلى هجمات حدرت منها الأمم المتحدة، سواء

---

[449] فريق منظمة الصحة العالمية، الهجمات السيبرانية على البنيات التحتية الصحية والحيوية، 6 فبراير 2024، على الرابط التالي:
https://www.who.int/ar/news-room/questions-and-answers/item/cyber-attacks-on-critical-health-infrastructure

[450] National Health Executive, WannaCry cyber-attack cost the NHS £92m after 19,000 appointments were cancelled,12/1/2018 , available from : https://www.nationalhealthexecutive.com/articles/wannacry-cyber-attack-cost-nhs-ps92m-after-19000-appointments-were-cancelled

[451] السيدة شارلوت ميتشل هي أول وفاة بسبب هجوم إلكتروني على الرعاية الصحية. انظر: الجزيرة، أخطأ القراصنة فماتت المريضة..أول حادثة قتل بسبب هجوم إلكتروني، 2020/09/20، على الرابط التالي:
https://tinyurl.com/22wyousq

من خلال بيع علاجات على الأنترنيت أو الهجوم على أنظمة المعلومات الحيوية في المستشفيات، وانتشار المعلومات الكاذبة حول الفيروس.[452]

وقد دعت كل من اللجنة الدولية للصليب الأحمر ومنظمة الصحة العالمية لوقف الهجمات السيبرانية على قطاع الصحة، خصوصا العاملة في مواجهة جائحة كوفيد 19 في تلك الفترة، ومن أمثلة على الهجمات نجد هجوم كوريا الشمالية عل أنظمة كمبيوتر مختبرات فايزر الأمريكية.[453]

**المحور الثاني– سبل تحقيق الأمن السيبراني**

سببت الحروب السيبرانية جملة من المخاطر والتداعيات على تفاعلات السياسة الدولية والأمن القومي، فقد أصبحت المعضلة الأمنية تتجاوز المفهوم التقليدي ولم تعد المخاطر عسكرية بل أصبحت متنوعة، فالعلاقة بين الأمن السيبراني والأمن القومي تزداد كلما زاد نقل المحتوى المعلوماتي والعسكري والسياسي والاقتصادي والعلمي إلى الفضاء السيبراني، خاصة مع التحول

[452] الأمم المتحدة، كوفيد 19 والمعلومات المضللة،15/04/2020 على الرابط التالي:
https://tinyurl.com/2c7xpag9

[453] Philippe lemaire, Vaccins contre le covid-19 : la corèe du Nord suspectée d'avoir voulu pirater Fizer, 16 février 2021. Disponible sur le lien :
https://tinyurl.com/23egr33d

- اللجنة الدولية للصليب الأحمر، نداء إلى الحكومات، ضعوا أيديكم معا لإيقاف الهجمات السيبرانية على قطاع الرعاية الصحية، 18 ماي 2000 متاح على الرابط:
- منظمة الصحة العالمية، منظمة الصحة العالمية تعلن تزايد الهجمات الإلكترونية بمقدار خمسة أضعاف وتحث على اليقظة، بيان 23 أبريل 2020 ، متاح على الرابط:
https://www.who.int/ar/news/item/30-08-1441-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance

الرقمي، حيث تصبح قواعد البيانات القومية في حالة انكشاف خارجي وعرضة للهجمات السيبرانية.

إن الأمن السيبراني هو بعد جديد ضمن أبعاد الأمن القومي، أحدث تغييرات جوهرية في مفاهيم العلاقات الدولية كالصراع والقوة والتهديد، حيث حتم على فواعل المجتمع الدولي الانتقال من عالم مادي لعالم افتراضي، وبالتالي أصبح مفهوم الأمن السيبراني ضرورة حتمية في عالم اليوم، خاصة في ظل ارتباط كافة التفاعلات الدولية بالجانب الرقمي التكنولوجي، مما يستدعي إيجاد ميكانزمات ووسائل تواجهه التهديدات السيبرانية وتحقق الأمن السيبراني القومي.[454]

- **السيادة الرقمية**

إن السيادة الرقمية تعني قدرة الدولة أو المؤسسة على التحكم في بياناتها الرقمية، والبنية التحتية لتكنولوجيا المعلومات الخاصة بها، دون تدخل خارجي، وهي امتداد للسيادة الوطنية في المجال الرقمي، حيث تمكن الدول من فرض قوانينها ومعاييرها على البيانات والخدمات الرقمية ضمن حدودها، فأهداف السيادة الرقمية الأساسية تتلخص في حماية البيانات الوطنية من التجسس والاستغلال وتقليل الاعتماد على الشركات والتقنيات الأجنبية ودعم الاقتصاد الرقمي المحلي وتعزيز الابتكار وضمان خصوصية الأفراد والمؤسسات.[455]

ويشكل الأمن السيبراني الدرع الواقي للفضاء الرقمي لكل دولة ويشمل مجموعة من الاجراءات الفنية والادارية لحماية الأنظمة والشبكات والبيانات من التهديدات والهجمات السيبرانية، فالأمن السيبراني ضرورة لا غنى عنها للحفاظ على الاستقرار الرقمي، حيث ترتكز أهم عناصره، على الوقاية من خلال أنظمة الحماية والتشفير وعلى الرصد لاكتشاف الهجمات مبكرا والاستجابة

[454] محمود علي: الحروب السيبرانية وتطور الاستراتيجية العسكرية للدول، دار النشر العربية، 2022، ص 22

[455] Milton Muller, Digital Sovereignty : what does it mean?, Georgia Institute of Technology, Internet governance project, USA, 2021 , p 1-4.

بخطط طوارئ للتعامل مع الحوادث، والتعافي لاسترجاع الأنظمة والبيانات بعد التعرض للهجمات.[456]

إن تحقيق السيادة الرقمية لا يمكن أن يتحقق إلا عبر أمن سيبراني قوي، فغياب الحماية الرقمية يعرض البيانات الوطنية للاختراق، ويقوض استقلالية القرار الرقمي، وبالمقابل فإن وجود سيادة رقمية يعزز القدرة على تطوير منظومة أمنية مستقلة بعيدة على التجسس والتبعية[457]. حيث تبقى أبرز تحديات السيادة الرقمية والأمن السيبراني هو اعتماد العديد من الدول على الشركات الأجنبية مثل ميكروسوفت وغوغل، وضعف البنية التحتية الرقمية ونقص الكفاءات البشرية المؤهلة في مجال الأمن السيبراني وتشريعات غير مواكبة للتحولات الرقمية.[458]

إن بناء سيادة رقمية قوية وتحقيق أمن سيبراني متكامل لم يعد خيارا بل ضرورة ملحة في العصر الرقمي، فالدول التي تسعى لحماية مصالحها واستقلالها الرقمي عليها أن تستثمر في التقنيات الوطنية وتطوير استراتيجيات أمنية متقدمة، وتشرك القطاعين العام والخاص في بناء قطاع رقمي آمن.

بدأ ازدياد اهتمام الدول بتنمية قدرتها السيبرانية لما تكبدها الهجمات من خسائر وتهديد الأمن الاقتصادي المحلي والدولي، إذ ساعد مؤشر الأمن السيبراني العالمي"GCI" التابع للاتحاد الدولي للاتصالات على قياس مدى التزام الدولة بالأمن السيبراني ومستوى التطور الذي وصلت إليه، ويقدم توضيحا للتدابير القانونية والتقنية والتنظيمية التي تلزم الدولة لبناء قدراتها والتعاون مع الدول الأخرى على النحو الآتي:[459]

---

[456] William Stalling, lawrie Brown, Computer Security Principles and Pratice, 5th Edition, Published by Pearson, July 28, 2023, USA, P 1-25.

[457] Lauras Demardis, the Globale war For Internet Governance, Yale University Press, New Haven and London, 2014, p86.

[458] الخطيب عبد الله، الأمن السيبراني والتحول الرقمي في الوطن العربي: التحديات والاستراتيجيات، المجلة العربية لتكنولوجيا المعلومات، 18(2)، ص 45-60.

[459] قوادرة حسين، التداعيات الاقتصادية لحرب المعلومات السيبرانية، مجلة الناقد للدراسات السياسية، مجلد5، العدد1، ص 213.

- محور الأطر القانونية: يقيس مدى توافر مؤسسات وأطر فنية للتعامل مع الأمن السيبراني.
- محور القدرة الفنية: يقيس مدى توافر مؤسسات وأطر فنية للتعامل مع الأمن السيبراني
- محور تنظيمي: يقيس مدى توافر سياسات واستراتيجيات على المستوى الوطني لتنمية وتطوير الأمن السيبراني.
- محور بناء القدرات: يقيس مدى توافر برنامج للبحث والتطوير والتعليم والتدريب المرتبط بالأمن السيبراني وتأهيل معتمد لمتخصصين من مؤسسات عامة.
- محور بناء التعاون: يقيس مدى توافر شركات فعالة وأطر للتعاون وشبكات لتبادل المعلومات والخبرات ذات الصلة بالأمن السيبراني.

يقدم مؤشر الأمن السيبراني العالمي تصنيف لجميع الدول كل دولة على حدة، وفي غالب الأمر يظهر تشارك بعض الدول في الترتيب بما يوضح توازن في مستوى الاستعداد لديهم، إلا أنه أثبت وجود فجوة في قدرة الأمن السيبراني بين الدول الأقل نموا والدول النامية.[460]

إلى جانب هذا المؤشر يوجد مؤشر القوة السيبرانية الوطنية (NCBI) التابع لمركز بلفر للعلوم والشؤون الدولية والذي نشر في عام 2020 القدرات الإلكترونية للدول في سياق سبعة أهداف وطنية تسعى الدول لتحقيقها وهي كالآتي:[461]

- مسح ومراقبة المجموعات المحلية؛
- التحكم في بيئة المعلومات ومعالتها؛
- العمل على جمع الملعومات الاستخباراتية الأجنبية التي تدعم الأمن القومي؛
- تقوية وتعزيز الدفاعات السيبرانية الوطنية؛
- القدرة على تدمير أو تعطيل الخصم؛
- الحصول على مكاسب تجارية أو تعزيز نمو الصناعة المحلية؛

[460] المرجع نفسه.
[461] فرح يحي زعاترة، مرجع سابق، ص 69.

- المشاركة في تحديد القواعد والمعايير التقنية الإلكترونية الدولية وبناء على منهجية هذا المقياس التي ترتكز على التمييز بين النية والقدرة في التعامل مع الأمن السيبراني الوطني بناء على الأهداف السابقة، فإن الحكومات يمكن أن تملك القدرة من دون وجود النية لاستخدام أي وسائل سيبرانية ويمكن حدوث العكس تماما.

- **الدفاع والردع السيبراني**

يشكل الدفاع السيبراني مجموعة من القدرات النظامية التي تمتلكها القوات المسلحة للحماية من تأثيرات الهجمات السيبرانية، والتخفيف من حدتها والتعافي منها بسرعة.[462]

وتضمن مجموعة الإجراءات التقنية للدفاع السيبراني على الجدران النارية وأنظمة كشف التسلل، إدارة الهوية، وتشفير البيانات، إضافة إلى السياسات الأمنية والتدريب المستمر.463

تتمحور أهداف الدفاع السيبراني حول الحفاظ على مقدرات الأمن القومي التكنولوجي للدولة، من خطوط اتصالات وشبكات كمبيوتر وبنية تحتية سواء مدنية أو عسكرية، فضلا عن تأمين البيانات الحيوية، بما يساهم في تحقيق الأمن السيبراني.464

أما الردع السيبراني فهو القدرة على منع الخصم من تنفيذ هجوم عبر إقناعه بعدم جدوى الهجوم أو خوفا من العواقب ويقسم إلى:

- الردع بالعقوبة: التهديد بالرد على الهجوم عبر هجوم مضاد أو عقوبات اقتصادية أو سياسية.
- الردع بالحرمان: تقوية الدفاعات لدرجة تجعل الهجوم غير مثمر.

---

[462] James B .Godwin III, Andrey kulpin, karl Fredrick Rauscher and valery yachenko, Critical Terminology Foundations 2 : Russia-U.S. Bilateral on cybersecurity, East-west Institute, Policy Report, No 2, 2014, p51.

[463] Huan Zhang, Kangfeng Zheny, Strategy Selection For Moving Target Defense in Incomplete Information Game, Computers, Materials & continua, CMC,Vol 62, N2, 2020, pp763-786.

[464] إيهاب خليفة، مرجع سابق، ص193.

- الردع بالغموض: خلق حالة من عدم اليقين لدى الخصم حول قدرات الرد.[465]

كما يمكن أن نميز بين نوعين من الردع السيبراني ردع بالمنع أو الردع السلبي، وردع بالانتقام أو الردع الإيجابي، ويحدث الردع بالمنع من خلال تقوية النظم الدفاعية بصورة ترفع تكلفة هجمات الخصم عن مكاسبه، وغالبا لا يكون الهدف الرئيسي هنا هو الردع بقدر ما يكون هو الدفاع والتأمين ضد أي عدو محتمل وليس عدوا محددا بعينه، وهنا تكون حسابات الخصم بالسالب، أي أن يدرك ارتفاع تكلفة الهجوم عن المكاسب التي يمكن أن تتحقق، أما الردع بالانتقام فهو ردع إيجابي يقوم على فكرة العقاب وفيه يدرك الخصم أن أي هجوم سيتبعه هجوم أخر انتقامي لا يستطيع تفاديه أو تحمله ويشمل ذلك الإعلان عن المصالح الحيوية واستعراض القوة والتهديد باستخدامها في حالة المساس.[466]

الردع السيبراني يمثل قدرة الدولة على تطوير قدرات عسكرية موثوقة ومتبادلة ومتماثلة على الفضاء السيبراني، تكون قادرة على التأثير في قرارات الخصم وتمنعه من شن هجمات عسكرية عبر الفضاء السيبراني.[467]

يشكل الدفاع والردع السيبراني علاقة تكامل، فرغم أن الدفاع يركز على الحماية، والردع يهدف إلى المنع، إلا أن الاستراتيجيتين متكاملتين، فنجاح الردع يعتمد إلى حد كبير على قوة الدفاع، حيث تعزز الأخيرة مصداقية التهديد، بالمقابل يخفف الردع الفعال من حجم الهجمات، مما يقلل من الضغط على الدفاعات السيبرانية.[468]

---

[465] Nye.J.S, Detterrence and Dissuasion in cyberspace, Internationale Security, 1/1/2017, 41(3) : pp 44-71.

[466] إيهاب خليفة، مرجع سابق، ص 199.

[467] Jason Rivera, Achieving cyberdetterence and the ability of small states to hold large states at risk, Architectures in cyberspace, Cycon 2015, Nato Cooperative Cyber Defense Centere of Excellence, May 2015, p 7.

[468] Lindsay.J.R, Tippring the scales : the attribution problem and the feasibility of deterrence against cyberattack, journal of cybersecurity, 1(1), p 53-67.

في ظل تعقيدات البيئة الرقمية المعاصرة، يصبح من الضروري اعتماد مقاربة مزدوجة تشمل كلا من الدفاع والردع السيبراني، فالدفاع يوفر الحماية والتقليل من الضرر، في حين أن الردع يمنع الهجمات من الأصل، إن بناء منظومة متكاملة تشمل الجانب التقني والسياسي والقانونين هو السبيل لتعزيز الأمن السيبراني وضمان استقرار الدول في العصر الرقمي.

**الخاتمة**

نخلص من خلال هذه الدراسة، أن حرب الهجمات السيبرانية لم تعد مجرد ظاهرة رقمية، بل أصبحت تشكل تهديدا جوهريا للأمن القومي في مختلف أبعاده. إذ أتاح تطور الفضاء الرقمي فرصا غير مسبوقة للجهات الفاعلة سواء الحكومية أو غير الحكومية لتنفيذ هجمات ذات طابع استخباراتي أو تخريبي، غالبا دون قدرة الدول المستهدفة على الرد بالمثل أو حتى التعرف الفوري على مصدر الهجوم. هذا الواقع يكشف هشاشة النظام الدولي أمام هذا النمط من الحروب، ويفرض تحديات قانونية وتشغيلية غير مسبوقة، في ظل غياب اتفاقيات ملزمة تنظم استخدام القوة في المجال السيبراني.

وقد بينت الدراسة أن بناء منظومة أمنية سيبرانية متكاملة هو ضرورة استراتيجية، خاصة مع تصاعد الهجمات الموجهة ضد البنية التحتية، والمؤسسات الحيوية، ووسائل الإعلام، والمؤسسات العسكرية. كما أظهرت أن الرد الفعال على هذه التهديدات لا يمكن أن يكون تقنيا فقط، بل يجب أن يدمج ضمن سياسات وطنية شاملة، تشريعية، تعليمية، ودبلوماسية.

**لائحة المراجع**

**مراجع باللغة العربية**

**الكتب:**

– فرح يحيى زعاترة التهديدات الســـيبرانية على الأمن القومي الأمريكي، العربي للنشـــر والتوزيع، مصر ،الطبعة الأولى،2024.

– صـلاح عبد الرحمان الحديثي و كاميران عزيز حسـن، التفصـيل الشـامل لتطور القواعد القانونية الخاصـة بالحرب السـيبرانية، المجموعة العلمية للنشـر والتوزيع، القاهرة، مصـر، الطبعة الأولى، 2021.

**الدوريات:**

– أميرة عبد العظيم، محمد عبد الواحد، المخاطر السـيبرانية وسـبل مواجهتها في القانون الدولي العام، مجلة القانون والشريعة، عدد 35، الجزء3، 2020.

– بتر سنجر، دروس الحروب الماضية والاتجاهات التكنولوجية المستقبلية، بحث في كتاب الحروب المستقبلية في القرن 21، مركز الإمارات للدراسات والبحوث الاستراتيجية، أبو ظبي، الطبعة الأولى، 2014.

– محمود علي، الحروب السيبرانية وتطور الاستراتيجية العسكرية للدول، دار النشر العربية، 2022.

الخطيب عبد الله، الأمن السـيبراني والتحول الرقمي في الوطن العربي: التحديات والاسـتراتيجيات، المجلة العربية لتكنولوجيا المعلومات، 18(2).

– محمد إسـماعيل، الأمن السـيبراني في القطاع المصـري، صـندوق النقد العربي، موجز سياسات، العدد الرابع، يونيو 2019.

– قوادرة حسين، التداعيات الاقتصـادية لحرب المعلومات السـيبرانية، مجلة الناقد للدراسـات السياسية، مجلد5، العدد1.

**المقالات:**

– ألكسندر توميلين، روسيا تؤكد اتخاذ كل ما يلزم لحماية أمن المعلومات بعد أنباء عن اختراق أنظمتها الإلكترونية، روسيا اليوم، 5 نونبر 2016، تاريخ الولوج 07/03/2025 متوفر على الرابط التالي:

https://tinyurl.com/27mmww8k

– إيهاب خليفة، تهديدات سيبرانية: هل يستطيع القراصنة اختراق المنشآت النووية؟ المستقبل للأبحاث والدراسات المتقدمة، 7 يناير 2020، تاريخ الولوج 05/03/2025 متوفر على الرابط التالي:

https://tinyurl.com/2boulark

– الأمم المتحدة، كوفيد 19 والمعلومات المضللة،15/04/2020 على الرابط التالي:

https://tinyurl.com/2c7xpag9

– اللجنة الدولية للصليب الأحمر، نداء إلى الحكومات، ضعوا أيديكم معا لإيقاف الهجمات السيبرانية على قطاع الرعاية الصحية، 18 ماي 2000 متاح على الرابط:

https://tinyurl.com/27jn9ul2

– الجزيرة، أخطأ القراصنة فماتت المريضة..أول حادثة قتل بسبب هجوم إلكتروني، 20/09/2020، على الرابط التالي:

https://tinyurl.com/22wyousq

– البوابة التقنية، وزارة الأمن الداخلي الأمريكية: القراصنة الروس قادرين على التحكم بالمرافق الكهربائية الأمريكية، البوابة التقنية 24/07/2018 تاريخ الولوج 07/03/25 متوفر على الرابط التالي:

https://tinyurl.com/jhbzmu6

– د.أولاف تايلر، التهديدات الجديدة: الأبعاد الإلكترونية، مجلة حلف الناتو،11/11/2011، تاريخ الولوج 25/02/2025 متوفر على الرابط التالي:

http://www.nato.int/docu/review/2011/11-september/Cyber-Threads/AR/index.htm

– زهير حمداني، "ستاكسنت" حصان طروادة الذي أدخله عميل هولندي لمحطة نطنز النووية الإيرانية، الجزيرة، 2024/01/10، تاريخ الولوج 2024/9/27، متوفر على الرابط التالي :

https://tinyurl.com/2xqm5hpd

– مركز المستقبل، تهديدات غير تقليدية: آليات حماية البنية التحتية الحرجة من الاختراق الإلكتروني، المستقبل للأبحاث والدراسات المتقدمة، 10 أكتوبر 2016، تاريخ الولوج 05/03/2025 متوفر على الرابط التالي:

https://tinyurl.com/27nnuycf

– منظمة الصحة العالمية، منظمة الصحة العالمية تعلن تزايد الهجمات الإلكترونية بمقدار خمسة أضعاف وتحث على اليقظة، بيان 23 أبريل 2020، متاح على الرابط:

https://www.who.int/ar/news/item/30-08-1441-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance.

– سكاي نيوز عربية، طوارئ بكوريا الجنوبية لحماية محطاتها النووي، سكاي نيوز، أبو ظبي، 2014/12/26 تاريخ الولوج 2024/09/27، متوفر على الرابط التالي:

https://tinyurl.com/2cwon929

– فريق منظمة الصحة العالمية، الهجمات السيبرانية على البنيات التحتية الصحية والحيوية، 6 فبراير 2024، على الرابط التالي:

https://www.who.int/ar/news-room/questions-and-answers/item/cyber-attacks-on-critical-health-infrastructure

**التقارير:**

– د ماركو جريك ، فهم الجريمة السيبرانية دليل للبلدان النامية ، منشورات الاتحاد الدولي للاتصالات، 2009.

– تيم مور، أرثر نيلسون، التهديد السيبراني العالمي، تقرير التمويل والتنمية، صندوق النقد الدولي، مارس 2021.

**مراجع باللغة الإنجليزية:**

**ouvrages:**

-James B .Godwin III, Andrey kulpin, karl Fredrick Rauscher and valery yachenko, Critical Terminology Foundations 2 : Russia-U.S. Bilateral on cybersecurity, East-west Institute, Policy Report, No 2, 2014.

-Jason Rivera, Achieving cyberdetterence and the ability of small states to hold large states at risk, Architectures in cyberspace, Cycon 2015, Nato Cooperative Cyber Defense Centere of Excellence, May 2015.

- Kenneth Geers, Cyberspace and the changing Nature of ware, the NATO cooperative Cyber Defence, Center of Excellence, Tallinn, Estonia, 2008.

- Lauras Demardis, the Globale war For Internet Governance, Yale University Press, New Haven and London, 2014.

- Milton Muller, Digital Sovereignty : what does it mean?, Georgia Institute of Technology, Internet governance project, USA, 2021.

- Nils Melzer, Cyberwarfar and International Law, UNIDIR, 2011.

- William Stalling, lawrie Brown, Computer Security Principles and Pratice, 5th Edition, Published by Pearson, USA, July 28, 2023.

**Les articles :**

-Huan Zhang, Kangfeng Zheny, Strategy Selection For Moving Target Defense in Incomplete Information Game, Computers, Materials & continua, CMC,Vol 62, N2, 2020.

Lindsay.J.R, Tippring the scales : the attribution problem and the feasibility of deterrence against cyberattack, journal of cybersecurity, 1(1).

- Marco Roscini, World Wide Warfare - jus ad bellum and the use of cyber Force, Max Planck yearbook of United Nations Law, vol 14, 2010.

- Michael Schmitt, Computer Network Attack and the Use off Force in International Law through on a Normative, the Colombia journal of transitional law, vol 27, No 885-937, 1999.

-Nye.J.S, Detterrence and Dissuasion in cyberspace, Internationale Security, 1/1/2017, 41(3) .

- Nye Josephs, Nuclear Lessons for Cyber Security?, Strategic studies Quarterly, vol 5, No 4, winter 2011.

- Lizzie Dearden, Ukraine Cyber attack : chaos as national bank, State power provider and airport hit by Hackers, Independent , Jun 27/2017, last accessed 5/8/2024, accessible at :
https://www.independent.co.uk/news/world/europe/ukraine-cyber-attack-hackers-national-bank-state-power-company-airport-rozenko-pavlo-cabinet-computers-wannacry-ransomware-a7810471.html

- National Health Executive, WannaCry cyber-attack cost the NHS £92m after 19,000 appointments were cancelled,12/1/2018 , available from :
https://www.nationalhealthexecutive.com/articles/wannacry-cyber-attack-cost-nhs-ps92m-after-19000-appointments-were-cancelled

- Philippe lemaire, Vaccins contre le covid-19 : la corèe du Nord suspectée d'avoir voulu pirater Fizer, 16 février 2021. Disponible sur le lien :
https://tinyurl.com/23egr33d