Afro-Asian Journal of Scientific Research (AAJSR)
المجلة الأفروآسيوية للبحث العلمي
E-ISSN: 2959-6505
Volume 3, Issue 3, 2025
Page No: 280-288
Website: https://aajsr.com/index.php/aajsr/index
SJIFactor 2024: 5.028 ISI 2024: 0.580 معامل التأثير العربي (AIF) 2024: 0.74

الحرب السيبرانية والأمن القومي: تهديدات وتحديات مستقبلية

فتحي الطيب التريكي*
قسم العلوم السياسية، كلية الاقتصاد والتجارة القربوللي، جامعة المرقب، الخمس، ليبيا

Cyber Warfare and National Security: Future Threats and Challenges

Fathi Al-Tayeb Muhammad Al-Turaiki *
Political Science Department, Faculty of Economics and Commerce, Al Qarbouli, Elmergib University, Libya

*Corresponding author faaltreeki@elmergib.edu.ly *المؤلف المراسل
تاريخ الاستلام: 2025-07-09 تاريخ القبول: 2025-09-01 تاريخ النشر: 2025-09-07

الملخص

اصبحت اليوم اكثر من اي وقت مضى الهجمات السيبرانية من الاسلحة التي يتم استخدامها من قبل العديد من القوى المختلفة سعيا منها لتحقيق غايات محددة، مما جعل تلك الاسلحة اليوم أكثر خطورة لتهديدها أمن و سرية و خصوصية البيانات، فقد مست بأمن العديد من الدول و أسرارها حيث تعرضت العديد من الدول إلى اختراقات و قرصنة الكترونية خطيرة تم الفضح من خلالها على أهم البيانات و الخصوصيات التي تهدد أمنها، فالأمر أصبح أكثر صعوبة مما كان عليه سابقا، وعليه تهدف هذه الورقة العلمية إلى التعرف على ماهية هذه الحرب السيبرانية، وما تأثيرها على الامن، كما تسعى الدراسة إلى تقديم الصورة المستقبلية لهذه الحرب .

الكلمات المفتاحية: الحرب السيبرانية، الهجمات السيبرانية، الأمن السيبراني، الأمن.

Abstract

Today, more than ever, cyber-attacks have become a lethal weapon used by various forces in pursuit of specific goals. This has made this weapon even more dangerous, threatening the security, confidentiality, and privacy of data. It has affected the security and secrets of many countries, with many countries being subjected to serious cyber breaches and hacking, exposing their most important data and privacy, threatening their security. The matter has become more difficult than it was in the past. Therefore, this scientific paper aims to identify the nature of this cyber war and its impact on national security. The study also seeks to present a future picture of this war.

Keywords: Cyber Warfare, Cyber-Attacks, Cyber Security, National Security.

المقدمة

إن دول العالم اليوم تواجه تحديات متزايدة بسبب ما يُعرف بالأمن السيبراني والحرب السيبرانية، لما لهما من مخاطر على مختلف جوانب الحياة. على الرغم من ذلك، لا يزال هناك نقص في الإطار المفاهيمي المحدد الذي يصف هذه المخاطر بدقة، مما يجعل مهمة مكافحتها أكثر صعوبة. لذا، يسعى هذا البحث إلى تحليل هذا الموضوع وفهم أبعاد الحرب السيبرانية والأمن السيبراني، وتأثيرهما على الأمن القومي. ولتحقيق فهم دقيق وشامل، سيتم استعراض المفاهيم وثيقة الصلة بالموضوع، بهدف تقديم صورة واضحة وتحليل استشرافي لمستقبل الحرب السيبرانية وما يمكن أن تؤول إليه.

مشكلة البحث

يُعَدّ الفضاء السيبراني أحد الأبعاد الجديدة للقوة، التي تتيح للدول القوية استخدامه لتعزيز أمنها القومي. ومع تحول الإنترنت إلى ساحة عالمية للنشاطات المدنية، أصبح أيضًا أداة للضغط السياسي والتجسس، مما جعل الأمن السيبراني يتصدر أجندة الأمن القومي والاستراتيجيات الدفاعية للدول.

ومن هذا المنطلق، تنطلق مشكلة البحث من محاولة الإجابة عن التساؤل الرئيسي :ما هو المقصود بالحرب السيبرانية، وما مدى تأثيرها على أمن الدول؟

ويتفرع من هذا التساؤل عدة أسئلة فرعية يسعى هذا البحث للإجابة عنها:

- ما هو الأمن السيبراني وما هي أبعاده؟
- ما هو واقع الأمن في ظل التطور التكنولوجي واستخدام تقنية المعلومات في الحروب الحديثة؟
- ما هي السيناريوهات المستقبلية للحرب السيبرانية؟

فرضية البحث

يفترض هذا البحث وجود **علاقة قوية ومباشرة** بين الحرب السيبرانية والأمن السيبراني والأمن القومي للدول، وهو ما سيتم التحقق منه من خلال التحليل والدراسة.

منهج البحث

يفرض موضوع الأمن السيبراني على الباحث استخدام المنهج الوصفي التحليلي، وذلك لتحليل المعطيات المتاحة حول الموضوع وتتبع أبعاده ومضامينه من خلال المصادر العلمية المتاحة، بالرغم من شحها في هذا المجال.

أهمية البحث

تنبع أهمية هذا البحث من كونه يسلط الضوء على موضوع حيوي وحديث على الساحتين العلمية والأكاديمية، وهو الحرب السيبرانية .وتزداد الأهمية في ظل التهديد الذي تشكله هذه الحرب الإلكترونية الجديدة على الأمن القومي لأي دولة، وما لها من مخاطر على جميع نواحي حياة المجتمعات.

أهداف البحث

1. تقديم **صورة واضحة** للحرب السيبرانية ومدى خطورتها على أمن الدول.
2. تقديم **إضافة علمية** متواضعة إلى الأدبيات المتخصصة في هذا المجال، لتكون مرجعًا للمهتمين والباحثين الجدد.

تقسيمات البحث

لقد تناولت هذ الموضوع من خلال ثلاثة مباحث، حيث المبحث الأول يتناول الحرب السيبرانية من حيث المفهوم والابعاد والتأثيرات، والمبحث الثاني يتناول مفهوم الأمن السيبراني ومفهوم الأمن من حيث العلاقة والتأثير. والمبحث الثالث يتناول رؤية مستقبلية للباحث تحت عنوان السيناريوهات المستقبلية للحرب السيبرانية.

- النتائج.
- الخاتمة.
- قائمة الصادر.

المبحث الأول: الحرب السيبرانية

يكثر الحديث عن الحرب العالمية الثالثة وتزاد المخاوف لدى دول العالم من مخاطرها وأبعادها ومن الاعتداءات واحتمالات وقوعها، وكانت لدى القادة سواء القيادات العسكرية أو السياسية العديد من الشكوك والتوقعات لحصول حاثة مشابهة لحادثة بيرلهاربل 1941[1]، مع أنه إلى يومنا هذا لم يوجد تعريف محدد وجامع يوصف هذه الحالة (الحرب السيبرانية) ويعترف به دولياً، فهي تبدوا عمليًا امتداد للحرب الاستخباراتية التي أخذت مكان ما عرف سابقًا بالحرب الباردة، فهي لاتزال سرية وخفية ويحيطها الكثير من الغموض.

للتعرف إلى ماهية الحرب السيبرانية (War Cyber) يجب أن نشير إلى معنى الحرب وأهدافها وأن نفرق بين أنواع الحروب وأجيالها المتعددة. إن جوهر الحرب يدور حول إكراه الخصم على تنفيذ إرادتنا، وذلك عبر أعمال القوة والعنف[2].

الهجمات السيبرانية هي: تلك الاجراءات التي تتخذها الدولة من أجل الهجوم على نظم المعلومات للعدو وبهدف التأثير والاضرار فيها، والدفاع عن نظم المعلومات الخاصة بالدولة المهاجمة وإذا شكلت الهجمات السيبرانية وتبعاً للظروف نزاعاً مسلحاً، فنكون أمام مصطلح الحرب السيبرانية أو ما يعرف بالهجوم السيبراني وفقاً لقواعد القانون الدولي الانساني، بوصفه عملية الكترونية سواء هجومية أو دفاعية يتوقع أن تتسبب في اصابة أو قتل أشخاص أو الاضرار بأعيان أو تدميرها[3].

وبالتالي فإن الهجمات السيبرانية يمكن أن تكون أوسع نطاقاً من الحرب السيبرانية وقد تحدث خارج اطار الحروب وقد تكون سبباً لبدء الحرب، وتتميز الحرب السيبرانية عن الحرب التقليدية، في أن المفهوم التقليدي للحرب، ينطوي على استخدام الجيوش النظامية ويسبقها اعلان واضح لحالة الحرب وميدان قتال محدد، بينما تبدو هجمات الفضاء الإلكتروني غير محددة المجال وغامضة الأهداف، كونها تتحرك عبر شبكات المعلومات والاتصالات الا لعابرة للحدود الدولية، إضافة إلى اعتمادها ما يمكن وصفه بأسلحة الكترونية جديدة تلائم طبيعة السباق الالكتروني لعصر المعلومات، حيث يتم توجيهها ضد المنشئات الحيوية أو دسها عن طريق عملاء أجهزة الاستخبارات، وعليه فأن احد معايير

([1]) –Amy lee, ''CIA chief leon panetta :Cyberattaek coud Be'Next Pearl Harbor, Huff post,13/6/2011, accessed on 20/5/2025, at:https://bit.3ILFR TV.

([2])- كارل فون كالوزفيتز، الوجيز في الحرب، ترجمة أكرم ديري والهيثم الأيوبي، ط 2(المؤسسة العربية للدراسات والنشر، بيوت 1988) ص 74 وما بعدها.

([3]) -أحمد عيسى نعمة الفتلاوي ، الهجمات السيبرانية: مفهوما والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر،< مجلة المحقق المحلي للعلوم القانونية والسياسية ، جامعة بابل ، كلية القانون ، العدد 4 ، السنة الثامنة 2016 ،ص 614.

التمييز بين الحرب السيبرانية والحرب التقليدية يمكن أن يكون وفقا لطبيعة السلاح المستخدم [4]. وبالتالي يمكن القول إن الحرب السيبرانية، هي الحرب التي تستخدم فيها الاسلحة غير التقليدية ووفقًا للآثار المترتبة على استخدام هكذا نوع من الاسلحة والمتمثلة بالتدمير واسع النطاق.

وبالتالي تعرف الأسلحة غير التقليدية وفقاً للجنة الاسلحة التقليدية للأمم المتحدة والصادر عام 1968 بأنها: "اسلحة الانفجارات الذرية والأسلحة المصنوعة من مادة ذات نشاط اشعاعي وأسلحة الفتك الكيميائية والبيولوجية، وأي نوع من الأسلحة الأخرى التي يتم تصنيعها في المستقبل والتي تتشابه خصائصها في الأثر التدميري مع القنبلة الذرية أو الأسلحة الاخرى"[5] .

وبفضل الثورة المعلوماتية، ظهرت لدينا بيئة جديدة وهي الفضاء الالكتروني، وهو يختلف عن البيئات الأخرى، (الاقليم البري - البحري الجوي - الفضاء الخارجي) وظهور الفضاء الالكتروني جعل الدول تدخله ضمن حساباتها الاستراتيجية وأمنيا، حيث ظهر بعد جديد في الصراعات الدولية، هو" صراع الفضاء الالكتروني" يستطيع من خلاله اي أحد من اطراف الصراع إيقاع خسائر فادحة بالطرف الآخر، بحيث يتسبب بخسائر عسكرية واقتصادية كبيرة من خلال: قطع أنظمة الاتصال بين الوحدات العسكرية، أو تضليل المعلومات، أو سرقة معلومات سرية عنها، أو من خلال التلاعب بالبيانات الاقتصادية والمالية ومسحها، أو تزييفها من أجهزة الحواسيب و من الصعب تخيل صراع عسكري اليوم دون أن يشتمل على أبعاد إلكترونية، والتي أصبحت في صميم اهتمامات الأنظمة الدفاعية لأي مواجهات محتمل حدوثيا في المستقبل [6].

وفي ظل الصراع المستمر في الشرق الأوسط، شهد عام 2024 مشهدًا جيوسياسيًا تغذيه الهجمات السيبرانية التي تنفذها مجموعات القرصنة الناشطة (هاكتيفيست) ومجموعات التهديدات المتقدمة المستمرة (APT)، والتي تستهدف الحكومات والبنية التحتية الحيوية وأقسام أمن المعلومات في المنظمات الدولية. وفيما يلي أبرز الملاحظات: الدول الأكثر استهدافًا في الشرق الأوسط: هي إسرائيل (68.2%)، تليها الإمارات العربية المتحدة (8.5%) والمملكة العربية السعودية (6.6%)[7].

وبالتالي تشكل هجمات الحرمان من الخدمة الموزعة (DDoS) نسبة 73.2% من إجمالي الهجمات في عام 2024، حيث كانت مجموعات الهاكتيفيست هي الجهات الرئيسية المنفذة لهذه الهجمات تعتبر المؤسسات الحكومية والقطاع العام أكثر القطاعات تضررًا في الشرق الأوسط، ومن المتوقع أن يصل سوق استخبارات التهديدات الإلكترونية (CTI) في الشرق الأوسط إلى أكثر من 31 مليار دولار بحلول عام 2030 (وفقًا لشركة Frost & Sullivan [8]، وهذا يُظهر حاجة واضحة ونية لمكافحة الزيادة الكبيرة في الهجمات الإلكترونية المستهدفة عبر المنطقة، وقد برزت صناعات النفط والغاز في المنطقة كأهداف بارزة للعديد من مجموعات التهديدات المتقدمة المستمرة (APTs) والمجموعات الخبيثة الأخرى حول العالم، حيث أصبحت في دائرة الضوء كأهداف رئيسية بسبب اقتصاداتها المزدهرة وزيادة الاعتماد على الرقمنة، كما أوضحته دراسة IBM لعام 2023، فقد ارتفعت حوادث الأمن السيبراني في الشرق الأوسط إلى مستوى قياسي بلغ متوسط تكلفة خرق البيانات 8.07 مليون دولار لكل حادثة، مقارنة بعام 2022 الذي بلغت فيه التكلفة 7.46 مليون دولار، ناهيك عن زيادة ملحوظة مقارنة بالمعدل العالمي البالغ 4.45 مليون دولار لكل حادثة. وهذا يضع الشرق الأوسط في المرتبة الثانية بعد الولايات المتحدة الأمريكية كأكثر المناطق التي تشهد أعلى متوسط تكلفة لخرق البيانات (وفقًا لتقرير IBM عن تكلفة خرق البيانات 2023) [9].

كما سبق ذلك الهجمات السيبرانية على (استونيا وجورجيا وإيران)، حيث الهجمات التي وقعت على استونيا 2007، حيث كان السبب هو عملية نقل تمثال يخلد الجنود الروس في الحرب العالمية الثانية، الذي جعل روسيا تشن هجمات سيبرانية على أستونيا، تنوعت من حجب الخدمة الموزعة، والتي استهدفت العديد من المصالح الحكومية والاعلامية، مما أدى إلى شلل الخدمة في البنية التحتية الرقمية لأستونيا، وتم ذلك على مرحلتين:

- الأولى استهدفت المواقع الحكومية والاعلامية التي بثت اعتذار مزور لرئيس الوزراء الاستوني حول عملية النقل للتمثال 27-29 ابريل 2007.
- الثانية استهدفت البنوك والبنية التحتية والانترنت حيث كانت أكثر خطورة وتعقيدًا وأوقفت عدد من الطلبات للدخول الى هذه المواقع 400 ضعف المستوى الطبيعي.

([4]) - عمر رضا بيومي، مخاطر اسلحة الدمار الشامل الاسرائيلية على الأمن العربي، ط1 (القاهرة: ، دار النهضة العربية 2002) ، ص 25.

([5]) -عمر بن عبدالله سعيد البلوشي، مشروعية اسلحة الدمار الشامل وفقا لقواعد القانون الدولي، (بيروت ، دار الحلبي الحقوقية 2007) ، ص ص15-17.

([6])- محمود محمد علي، الحروب السيبرانية وتطور الاستراتيجية العسكرية للدول (bdf جامعة اسيوط، 2022) ص7، تاريخ المشاهدة 3\8\2025 www.noor-book.com

([7])-Orlaith Traynor. “An Overview of Cyber Attacks in the Middle East 2024”. CybelAngel. Online: https://cybelangel.com/cyber-attacks-middle-east-2024.

([8])-الجزيرة. “الأمن السيبراني يستحوذ على 3.3 مليارات دولار من إنفاق الشرق الأوسط عام 2024.” الجزيرة نت. https://www.ajnet2024 . شوهد في 12\8\2025.

([9])- المصدر نفسه.

في عام 2010، كشف العالم عن واحدة من أكثر الهجمات السيبرانية تعقيدًا وأثرًا على الساحة الجيوسياسية، والمعروفة باسم (ستكسنيت). هذه البرمجية الخبيثة التي استهدفت برنامج إيران النووي كانت أول هجوم سيبراني مسجل يهدف بشكل محدد إلى تعطيل بنية تحتية صناعية عبر الإنترنت وفي دراسة متعمقة حول هذا الهجوم تم تحليل تأثير (ستكسنيت) على التوازن الجيوسياسي في منطقة الشرق الأوسط، وكيف أنه لم يكن مجرد حادثة تقنية، بل تحركًا استراتيجيًا ذو أبعاد سياسية واقتصادية بعيدة المدى، الهجوم لم يستهدف فقط المنشآت النووية الإيرانية، بل جاء كجزء من حرب سيبرانية خفية تهدف إلى إبطاء تقدم إيران في مجال الطاقة النووية وتقويض نفوذها الإقليمي، تأثيرات (ستكسنيت) لم تقتصر على إيران فحسب، بل غيرت بشكل جذري مفهوم الحرب السيبرانية على الصعيد العالمي. لأول مرة، أدركت الدول والقوى الكبرى أن الصراعات لم تعد مقتصرة على الحروب التقليدية بل امتدت لتشمل الفضاء السيبراني، حيث يمكن لأية دولة أو جهة فاعلة أن تشن هجمات مدمرة عبر الإنترنت تستهدف بنى تحتية حيوية. هذه الحادثة دفعت دول العالم إلى إعادة تقييم استراتيجياتها الأمنية وتطوير قدراتها الدفاعية والهجومية في الفضاء السيبراني، إيران، التي وجدت نفسها في مواجهة هجوم غير تقليدي، اتخذت خطوات لتعزيز قدراتها السيبرانية الدفاعية والهجومية، مما أدى إلى تصاعد سباق التسلح السيبراني في المنطقة. في الوقت نفسه، أظهرت الهجمات كيف يمكن للتكنولوجيا أن تستخدم كسلاح في الصراعات الجيوسياسية، ما دفع العديد من الدول إلى إعادة النظر في استراتيجياتها الأمنية الوطنية [10].

وتعد الصراعات السيبرانية فيمن أبرز التحديات الأمنية التي تواجه الدول في العصر الحديث، حيث تحولت الحروب الإلكترونية إلى أداة رئيسية تستخدمها الدول والجهات الفاعلة غير الحكومية لتحقيق أهدافها الجيوسياسية [11].

وبالتالي نلاحظ أن هذه الهجمات كما يراها الكثيرون بأنها لم تصل الى الحرب السيبرانية انما يمكن وصفها بنزاع او صراع يخلق توتر بين دولتين، فهي لم تسبب اضرارًا بشرية خطيرة على المدنيين، ولكنها مثلت خطرًا على السلام، ولو اعتبرناها حربا لأنها استهدفت التخريب للعديد من المصالح الحيوية، وخاصة التي لها علاقة بالقوات المسلحة، حيث تم اعتبارها هجمات سيبرانية لجيش سيبراني معين استخداما للقوة.

وبالنظر الى طبيعة الفضاء الالكتروني وما يلحق به تعقيد وتطور سريع في التقنية، وامكانية التمويه للاعتداءات، وصعوبة التنبؤ به، وصعوبة ما يمكن اعتباره حربا عسكرية او اعتداء أو حرب سيبرانية، فالسرقات التي تتعرض لها المصارف وعمليات التجسس الصناعي ليست الا اعمالا حربية على الرغم من ابعادها الخطيرة على الأمن، وذلك لتأثيرها على الاقتصاد وحياة المواطنين ورفاهيتهم في بلدانهم [12].

ومن خلال الدراسة للعلاقات الدولية وخاصة مبدأ "الامتناع عن استخدام القوة " من عليه ميثاق الامم المتحدة على انه "يمتنع اعضاء الهيئة جميعا في علاقاتهم الدولية عن التهديد باستعمال القوة وباستخدامها ضد سلامة الاراضي او الاستقلال السياسي لأي دولة او على وجه لا يتفق ومقاصد الامم المتحدة"، نلاحظ ان هناك من يذهب الى اعتبار الحرب السيبرانية هي الحرب التي لا حدود لها ولا ضوابط فالمعلومات واسعة الانتشار وساحة المعركة في كل مكان، وامكانات الجمع بين التقنيات المختلفة متوافرة، والحدود بين الحرب واللاحرب لم تعد موجودة ولذلك نجد ان الدول التي تعي خطورة ذلك يزداد لديها مستوى الخوف والقلق على سيادتها في هذا الفضاء السيبراني من جهة، واستشعارها صعوبة الحركة فيه لحركته غير الرسمية من جهة أخرى، وهنا تجدر الاشارة الى صعوبة معرفة الجهة التي تقف وراء أي هجوم بالإضافة صعوبة الرد عليه في حينه، والدول العربية نجدها في وسط هذه الهجمات السيبرانية، نتيجة تمتعها بوفرة عناصر الطاقة بالإضافة الى المشاكل والصراعات التي تمر بها من وقت لآخر [13] .

وكذلك نلاحظ ان استخدام الهجمات السيبرانية كوسيلة ضغط سياسية من أجل اتخاذ قرار او موقف معين، فمثلا تصريح قائد سلاح الجو الاماراتي "اللواء خالد أبو العينين" (ان البنية التحتية الإلكترونية المتقدمة في بلاده جعلتها هدفا للمتسللين عبر الانترنت) [14].

وكذلك ما حدث من تعطيل لشركة آرامكو في السعودية، وهددت بإعاقة قدرات انتاج حوالي تسعة ملايين برميل يوميا للسوق الدولية وحدث ذلك نتيجة فيروس الكتروني يحمل اسم "شامون", حيث يعتبر هذا الفيروس جزء من الحرب [15] الإلكترونية الحاصلة في الشرق الاوسط والتي وجهت الاتهامات الى إيران[16].

([10]) - تحسين الشيخلي ، دور الحرب السيبرانية في تشكيل ملامح الشرق الاوسط (وكالة الحدث الاخبارية في 27\اكتوبر 2024) https://www.alhadathcenter.net/ 2024\7\29 شوهد في

([11]) - أحمد فتحي محمود. "الحروب السيبرانية: روسيا وأوكرانيا نموذجا." (القاهرة: مركز آتون للدراسات، 2023)، https://www.atoonra.com/ شوهد في 30\7\2025.

([12])- ''la guerre Cyberntique,n ouveaupretxte des pressions ant-iraniennes!''Iran French Radio,21/10/2012,accessed on 10/6/2025,at.https://bit.hgjdly/3pVkdbj.

([13]) -Ibid,p.93.

([14])- "تصاعد الهجمات الالكترونية على البنية التحتية في الخليج", الوطن: 12\12\2022 ، شوهد في 15\7\2025 في https://ly/3gDFUOQ.

([15]) -Ibid,p.93.

([16])- Bruce Riedel,''In Saudi Arabia and Israel, signals that Iran has Retaliation in Works, The Daily Beast,14\7\2017, accessed on 20\6\2025, at :https:bit.ly/35NWJME.

المبحث الثاني: مفهوم الأمن السيبراني والامن

أولا: مفهوم الأمن السيبراني:

للوهلة الأولى نجد من يرى الأمن السيبراني بأنه المجال الذي نتج عن ثورة التكنولوجيا والمعلومات والاتصالات الحديثة، وهي شديدة الصلة بالعالم المادي، وذلك عبر العديد من بنى الاتصالات، وأنظمة المعلومات، واتصال كل ذلك بالأنترنت، حيث يمكن ان نحدد بعض تعريفات الأمن السيبراني فيما يلي:

1- حسب رؤية "دلين تاليه "فقد عرفه بأنه (المجال الذي يتألف من مكونات مادية وغير مادية، ويتسم بالاستخدام للكمبيوتر، والمجال الكهرومغناطيسي لتخزين المعلومات وتعديلها وتبادلها عبر شبكات الكمبيوتر) [17].

2- الاتحاد الأوروبي للاتصالات يعرفه بأنه: (مجموعة من المهمات الأمنية مثل تجميع وسائل وسياسات واجراءات أمنية، ومبادئ توجيهية ومقاربات لإدارة المخاطر وتدريبات وممارسات فضلى وتقنيات يمكن استخدامها لحماية البيئة السيبرانية وموجودات المؤسسات والمستخدمين) [18].

3- وتعرفه وكالة الأمن السيبراني وأمن البنية التحتية الأميركية (سي آي إس إيه) بأنه "فن حماية الشبكات والأجهزة والبيانات من الوصول غير المصرح به أو الاستخدام الإجرامي، ويمثل ممارسة ضمان سرية المعلومات وسلامتها وتوافرها".

4- وتعرفه الموسوعة البريطانية بأنه "حماية نظم الحوسبة والمعلومات من الأضرار والسرقة والاستخدام غير المصرح به".

5- وتعرفه شركة "كاسبر سكاي" الدولية الخاصة للأمن السيبراني بأنه "أشكال الدفاع عن الحواسيب والخوادم والأجهزة المحمولة والأنظمة الإلكترونية والشبكات والبيانات من الهجمات الخبيثة، ويعرف أيضا بأمن تكنولوجيا المعلومات أو الأمن الإلكتروني للمعلومات"[19].

ولكي نفهم كل هذا أكثر لابد من التطرق إلى التهديد المرتبط حيث نلاحظ أن هذا التهديد هو احتمال نجاح اعتداء سيبراني على ما يمكن اعتباره مصلحة حيوية أو أفراد أو دول أو منظمات، وذلك من خلال الاختراق أو الوصول إلى شبكات المعلومات حيث يتم اتلافها أو تعطيلها أو سرقتها، أما ما يُقصد بـنقاط الضعف فهو مدى انكشافها على ذلك التهديد في اتجاه معين، مثل الثغرات الجانبية في البرامج والمشغلات. وبالتالي يمكن أن نحدد هذه الهجمات السيبرانية وفقا للأضرار التي تخلفها، ومدى خطورة ذلك في المجتمعات [20]، وهذه التهديدات تكون متنوعة منها ما يستهدف السلامة العامة عندما يتم اختراق انظمة النقل والطاقة وادارة الكوارث او انظمة الدفاع.

ثانياً: مفهوم الأمن

على الرغم من استخدامه على نطاق واسع، فإن مفهوم" الأمن "يعني أشياء مختلفة لأشخاص مختلفين. تقليدياً، كان يُعرَّف الأمن على أنه الحماية من الهجوم الخارجي، وبالتالي كان يُنظر إليه بشكل أساسي على أنه يعادل الدفاعات العسكرية في مواجهة التهديدات العسكرية. وقد ثبت أن هذه الرؤية ضيقة للغاية، فالأمن يتضمن ما هو أكثر من تجهيز القوات المسلحة واستخدامها.

الأكثر من ذلك، فإن هذه الرؤية قد تدفع المرء إلى الاعتقاد بأن أفضل طريقة لزيادة الأمن هي زيادة القوة العسكرية. وعلى الرغم من أن القوة العسكرية تُعدُّ مكونًا مهمًا جدًا في الأمن، فإنها جانب واحد فقط منه. فالتاريخ مليء بالأمثلة على سباقات التسلح التي أدت إلى إضعاف الأمن بدلًا من تقويته.

أدى ذلك إلى بروز الحاجة إلى صياغة تعريف أوسع للأمن يتضمن الأبعاد الاقتصادية والدبلوماسية والاجتماعية، بالإضافة إلى البعد العسكري. وقد قدم أرنولد ولفرز مثل هذا التعريف عندما قال: (يقيس الأمن بمعناه الموضوعي مدى غياب التهديدات الموجهة للقيم المكتسبة، ويشير بمعناه الذاتي إلى غياب الخوف من أن تتعرض تلك القيم إلى هجوم) [21].

يوضح هذا التعريف أنه على الرغم من أن الأمن مرتبط مباشرة بالقيم، فإنه ليس قيمة في حد ذاته، وإنما موقف يسمح لدولة ما بالحفاظ على قيمها، وبالتالي فإن الأفعال التي تجعل أمة ما أكثر أمناً ولكنها تحط من قيمها لا نفع لها. ومن الصعب قياس الأمن بأي طريقة موضوعية، ولذلك فإن الأمن يصبح تقييماً مبنياً على مفاهيم لا تتعلق بالقوة والضعف، وإنما أيضاً بالقدرات والنوايا الخاصة بالتهديدات المدركة.

ويعرف تريجر وكرننبرج الأمن بأنه "ذلك الجزء من سياسة الحكومة الذي يستهدف خلق الظروف المواتية لحماية القيم الحيوية"[22].

([17]) - Michael N.Schmitt(ed.), Tallinn Manualon the Inter-International Law Applicable To cyher Warfare (Cambridge: Cambridge University Prwss,2013).p.258

([18])- حسن الحاج علي احمد وآخرون، تحرير مروان قبلان، الامن العربي وتحديات الامن الاقليمي ، ط1 (لبنان، بيروت، المركز العربي لدراسة السياست2023) ،ص389.

([19])-https://www.aljazeera.net/ ، شوهد في 12\7\2025، 12:30 .

([20])-Solange Ghernaouti-Helie,Cyber Power:Crime, confliet and Security in Cyberspace(Paris:EPFL PRESS,2013).

([21])-https://www.aljazeera.net/ ، شوهد في 12\7\2025، 12:30 .

([22])-https://www.aljazeera.net/ ، شوهد في 12\7\2025، 12:30 .

ويعرفه هنري كيسنجر بأنه يعني "أية تصرفات يسعى المجتمع – عن طريقها – إلى حفظ حقه في البقاء[23].
أما روبرت ماكنمارا فيرى أن "الأمن هو التنمية، وبدون تنمية لا يمكن أن يوجد أمن، والدول التي لا تنمو في الواقع، لا يمكن ببساطة أن تظل آمنة[24].
ويوضح تنوع تعريفات مفهوم الأمن أن هناك قدراً من التخلف النظري للمفهوم، ويذكر باري بوزان عدة أسباب لذلك التخلف، وهي[25]:

أ- صعوبة المفهوم

يُعَد مفهوم **الأمن** معقدًا ومركبًا لدرجة تجعل من الصعب على الدارسين الانجذاب إليه، مما يدفعهم غالبًا إلى دراسة مفاهيم أكثر وضوحًا ومرونة. هذا التعقيد يجعل مفهوم الأمن مثيرًا للجدل والخلاف بين الباحثين.

ب- الأمن والقوة

هناك تشابك كبير بين مفهومي **الأمن** و**القوة**، خصوصًا بعد ظهور المدرسة الواقعية في العلاقات الدولية. هذه المدرسة ترتكز على فكرة التنافس من أجل القوة، وتنظر إلى الأمن على أنه مشتق من القوة ووسيلة لتعظيمها.

ج- التوجه المثالي

ظهرت موجة من المفكرين **المثاليين** الذين يرفضون أفكار المدرسة الواقعية، ويقدمون هدفًا بديلًا للأمن وهو **السلام** . يسعى هؤلاء المثاليون إلى تحقيق الأمن من خلال التعاون والحلول السلمية، لا من خلال التنافس العسكري.

د- هيمنة الدراسات الاستراتيجية

تسيطر الدراسات الاستراتيجية على مجال الأمن، حيث تركز بشكل أساسي على الجوانب العسكرية والدفاعية. هذا التركيز يهدف إلى خدمة المتطلبات الدفاعية والحفاظ على الوضع الراهن، مما أسهم في تضييق الأفق التحليلي للمفهوم والحد من أبعاده النظرية.

هـ- دور رجال السياسة

يلعب رجال السياسة دورًا في زيادة غموض مفهوم الأمن، وذلك بهدف توفير مساحة أكبر للمناورة. يستخدمون هذا الغموض لتحقيق أهدافهم سواء في أغراض الاستهلاك السياسي الداخلي أو في سياق الصراع الخارجي.

استناداً إلى التحليل السابق، يمكن القول إن هناك عدة خصائص تميز مفهوم الأمن تتمثل في:

1- الأمن هو خلاصة التفاعل بين عوامل داخلية وإقليمية ودولية:

تتعلق العوامل الداخلية بحماية المجتمع من التهديدات الداخلية المدعومة بقوى خارجية وبشرط أن تكون أهداف النظام السياسي معبرة عن القيم الحقيقية للشعب، وأن تسمح المؤسسات السياسية بتوفير قنوات المشاركة. والعوامل الإقليمية هي الخاصة بعلاقات الدولة مع الدول المجاورة لها في الإقليم أو المنطقة الجغرافية. والعوامل الدولية بمعنى أبعاد علاقات الدولة في المحيط الدولي وطبيعة تحالفاتها الدولية وطبيعة علاقاتها بالقوى العظمى[26].

2- الأمن له جانبان:

- جانب موضوعي يمكن تحديد مكوناته وعناصره والتعبير عنها كمياً.
- جانب معنوي يتعلق بالروح المعنوية ومدى ارتباط الشعب بالنظام السياسي، وأي دراسة متكاملة لابد وأن تأخذ كلا الجانبين في الاعتبار.

3- الأمن ظاهرة ديناميكية حركية:

يتسم الأمن كظاهرة بالحركة والتغيير، فهو ليس مرحلة تصلها الدولة وتستقر عندها، فلا يمكن اعتبار الأمن حقيقة ثابتة تحققها الدولة مرة واحدة وإلى الأبد، فلا يمكن لأي دولة أن تتوقف عند مجموعة من الإجراءات والأعمال ترى أنها حققت من خلالها أمنها، بل هي تتابع باستمرار ما يدور فيها وبينها وحولها إقليمياً ودولياً لتعدل من أوضاعها وتحركاتها، وتطور من قوتها لتحافظ على درجة الأمن التي ترغب في تحقيقها، أي أنه إذا كان الأمن يعرف مجموعة من الثوابت فإن هناك أيضاً العديد من المتغيرات التي تكسب الأمن خاصية الديناميكية[27].

4- الأمن حقيقة نسبية وليست مطلقة:

لم يذكر التاريخ دولة تمكنت من السيطرة على مقدرات العالم، وأحكمت سيطرتها عليه، ومن ثم حققت لنفسها الأمن المطلق، وهذا يعود لسبب واحد وهو أن الأمن المطلق لدولة ما يعني التهديد المطلق لأمن كل الدول المجاورة، بل حتى الدول التي اختارت طريق الحياد لا تعيش في أمن مطلق، بل يمكن تهديد أمنها بفعل القوى ذاتها التي حافظت على حياد تلك الدول. ويكون سعي الدول لزيادة هامش أمنها دافعاً للأطراف الأخرى لسد الفجوة، أو تعويض النقص، وبالتالي تدخل كل الأطراف في تسابق أمني هائل ليس له سوى نتيجة واحدة وهي الإخلال بالأمن. ومن ثم فإن ما تسعى إليه كل الدول عادة هو تحقيق الأمن النسبي لها آخذة في الاعتبار أمن الدول المجاورة، أو تلك التي تدخل معها في علاقات وثيقة، كما أن

---

(23)- https://www.aljazeera.net/ ، شوهد في 12\7\2025، 12:30 .
(24)- https://www.aljazeera.net/ ، شوهد في 12\7\2025، 12:30 .
(25)- https://www.aljazeera.net/ ، شوهد في 12\7\2025، 12:30 .
(26)- https://www.aljazeera.net/ ، شوهد في 12\7\2025، 12:30 .
(27)- https://www.aljazeera.net/ ، شوهد في 12\7\2025، 12:30 .

مفهوم الأمن نسبي من الناحية الإيديولوجية، فتغير نظام الحكم في دولة ما بشكل أساسي، أو تغير الإيديولوجية التي تأخذ بها النخبة الحاكمة، كلها تطرح تأثيراتها على مفهوم الأمن.

وخلاصة كل ذلك نرى ان الأمن السيبراني والأمن يشكلان اليوم حجر الزاوية في حماية الدول والأفراد، لا سيما في هذه الفترة التي تشهد تصاعدًا غير مسبوق في التهديدات السيبرانية، هذه التهديدات التي تستهدف البنية التحتية الحيوية للدول مثل أنظمة الطاقة، البنوك، المؤسسات الحكومية وحتى الأفراد، لا تأتي فقط من جهات معادية للدول بل تشمل أيضًا جهات منظمة قادرة على إحداث ضرر كبير عبر الإنترنت، في ظل هذا الوضع المتوتر، أصبح الأمن السيبراني والأمن جزءًا لا يتجزأ من استراتيجيات الدفاع الوطني، حيث يسعى الجميع لحماية مصالحهم من الهجمات التي قد تزعزع استقرارهم.

المبحث الثالث: السيناريوهات المستقبلية للحرب السيبرانية

لقد اصبحت الصراعات السيبرانية في العالم اليوم جزءًا لا يتجزأ من الديناميكيات الجيوسياسية الإقليمية والعالمية، حيث مهد التطور السريع للتكنولوجيا وغياب خطوط الاشتباك التقليدية الطريق أمام تحولات استراتيجية في طبيعة النزاع، وبالتالي الاعتماد المتزايد على الفضاء السيبراني كأداة للردع والضغط السياسي وجعل من الضروري أن تتبنّى الدول مقاربات شاملة تطوّر من قدراتها الدفاعية والهجومية وتدمج البعدين التقني والتشريعي والبشري، وعلى مستوى التوجه المستقبلي للصراع السيبراني يمكن التنبؤ بعدة اتجاهات رئيسية:

- توظيف العمليات السيبرانية مع العمليات التقليدية: سيزداد توظيف الهجمات الإلكترونية في المواجهات عسكرية وسياسية تقليدية؛ حيث تُستخدم لتهيئة الظروف أو تهدئة الخطوط الأمامية قبل أي تصعيدٍ مفتوح، أو لتعطيل سلاسل الإمداد الحيوية للمنافسين.
- زيادة درجة الصراع غير المتكافئ: هما ممكن تظهر أدوات وتقنيات أكثر تخصصًا تمكن الجهات الفاعلة الصغيرة من التمترس خلف حواجز السياسات الدولية، مع زيادة الاعتماد على الذكاء الاصطناعي في الهجمات والاستطلاع السيبراني، وتوظيف شبكات «الديب ويب» لتسهيل تبادل القدرات الخبيثة.
- قيام تحالفات سيبرانية إقليمية: في مواجهة التهديدات المشتركة، ستسعى دولٌ مثل مصر والإمارات والسعودية إلى تأسيس أطر تعاون ثنائية وثلاثية لتعزيز تبادل المعلومات وتطوير بنى تحتية مشتركة لمراقبة الحوادث والاستجابة لها، مستفيدةً من الخبرات المتراكمة والمراكز الوطنية للأمن السيبراني.
- التحديات التشريعية والقانونية: سيزداد الضغط على المجتمعات الدولية لاعتماد معايير قانونية واضحة تصنف الهجمات السيبرانية وتحدد ممارسات الردع، بما يقترب من الإطار الذي تنظمه الأعراف الدولية للحروب التقليدية؛ غير أن السرية وصعوبة التمييز بين المقاتل والمدني تزيد من تعقيد هذه العملية.
- اهتمام متزايد على القدرات الذاتية: وسط تصاعد التوترات، ستتكثف الاستثمارات في بناء الكفاءات المحلية وتطوير البرامج الأكاديمية والتدريبية، مما يعزز استقلالية الدول عن المزودين الأجانب ويحدّ من نقاط الضعف في سلاسل التوريد التقني.

إن التحدي الأبرز للمستقبل هو القدرة على تحقيق توازنٍ مرن بين رفع مستوى الجاهزية السيبرانية والتوافق مع المساحات المفتوحة للتعاون الدولي، بحيث لا تتحول الساحة السيبرانية إلى سباق تسلح لا ينتهي، ويمتص موارد الدول دون جدوى حقيقية. في هذا السياق، تبقى رؤية الاستراتيجية الوطنية للأمن السيبراني 2023–2027 في مصر نموذجًا واعدًا، إذ ربطت بين الأبعاد التقنية والتشريعية والثقافية، ووضعت أسسًا لتعزيز الوعي وتطوير القدرات والابتكار.

سيظل الفضاء السيبراني والحرب السيبرانية مجالًا حيويًا لصياغة التوازنات الاستراتيجية في العالم، ليس فقط كأداة للنزاع بل أيضًا فرصة للتكامل والتعاون عبر خطوط التماس الرقمية. ومن خلال الاستثمار المستمر في القدرات البشرية والتكنولوجية، وتعزيز الأطر التشريعية وضبط آليات الردع والسيطرة على التصعيد، يمكن للدول الإقليمية أن تطوّع هذه البيئة لتعزيز أمنها وترسيخ دورها الفاعل في المشهد الدولي القائم على التحول.

النتائج

إنّ موضوع الحرب السيبرانية مهم وجديد على الساحة الاكاديمية والبحثية لحاجته الى الخبرة والدراية بعلوم التقنية الالكترونية الحديثة التي يستطيع الباحث من خلالها البحث والتحليل كلك المعلومات المتوفرة، حيث من المفيد ان نذكر بعض النتائج التي توصلت اليها في هذا البحث المتواضع:

1- إنّ الحرب السيبرانية اليوم واسعة الانتشار ولها القوة الكبيرة في التأثير على البنية الحيوية وهي في ازدياد مستمر.
2- وجود العلاقة الوثيقة بين الأمن وأمن المعلومات "الأمن السيبراني" حيث أصبح من الضروري إدراج تقنية المعلومات في قواعد التدريب والدراسة للمجتمعات.
3- إن الحرب السيبرانية تشكل تهديد للمستقبل في كل النواحي الحيوية، وعملية مواجهتها لا تقل أهمية عن مواجهة اي تهديد تقليدي.
4- الحرب اليوم أصحت هجينة تجمع بين العمليات العسكرية التقليدية والهجمات السيبرانية وحملات التضليل الخفية والسرية.

الخاتمة

لم تعد الحرب السيبرانية تهديدًا مستقبليًا بعيد الأفق، بل أصبحت واقعًا يوميًّا يتسارع مع كل تطور تكنولوجي. فحتى عام 2050، تشير السيناريوهات إلى تحولات كبرى قد تمس بعمق البنى التحتية الحيوية حول العالم، من الاقتصاد إلى الطاقة والصحة والتعليم، خاصة في العالم العربي، نواجه لحظة فارقة إما أن نغتنم الفرصة لبناء قدرات رقمية متينة وتحصين أمننا السيبراني، أو نترك أنفسنا عرضة لهجمات قد تشل مؤسساتنا، وتعطل حياة مواطنينا، وتهدد مستقبل أجيالنا، التحرك اليوم ليس رفاهية بل ضرورة وطنية، فبالاستثمار في التكنولوجيا، وتدريب الكوادر، وتفعيل الشراكات الدولية، يمكننا أن نحول هذا التحدي إلى فرصة استراتيجية، ونرسم لأنفسنا موقعًا فاعلًا ومؤثرًا في خريطة الأمن السيبراني العالمي.

قائمة المصادر

المراجع العربية

الكتب

1. البلوشي، ع. ب. ع. س .(2007) .مشروعية أسلحة الدمار الشامل وفقًا لقواعد القانون الدولي .دار الحلبي الحقوقية.
2. بيومي، ع. ر .(2002) .مخاطر أسلحة الدمار الشامل الإسرائيلية على الأمن العربي (ط. 1). دار النهضة العربية.
3. كالوزفيتز، ك. ف .(1988) .الوجيز في الحرب)أ. ديري &ه. الأيوبي، المترجمون، ط. 2). المؤسسة العربية للدراسات والنشر.
4. محمود، أ. ف .(2023) .الحروب السيبرانية: روسيا وأوكرانيا نموذجًا .مركز آتون للدراسات.
5. محمد علي، م .(2022) .الحروب السيبرانية وتطور الاستراتيجية العسكرية للدول (رسالة ماجستير غير منشورة). جامعة أسيوط.
6. الحاج علي أحمد، ح .(2023) .الأمن العربي وتحديات الأمن الإقليمي (م. قبلان، محرر، ط. 1). المركز العربي لدراسة السياسات.

الدوريات

7. الفتلاوي، أ. ع. ن. (2016). الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر .مجلة المحقق المحلي للعلوم القانونية والسياسية، 8(4).
8. الوطن. (تاريخ غير متوفر) .تصاعد الهجمات الإلكترونية على البنية التحتية في الخليج.
9. الشيخلي، ت. (27 أكتوبر 2024) .دور الحرب السيبرانية في تشكيل ملامح الشرق الأوسط .وكالة الحدث الإخبارية.

المواقع الإلكترونية

10. الجزيرة نت .(2024) .الأمن السيبراني يستحوذ على 3.3 مليارات دولار من إنفاق الشرق الأوسط عام 2024 . الجزيرة. تم الاسترداد في 12 أغسطس 2025، من https://www.ajnet
11. الجزيرة نت. (تاريخ غير متوفر) .الصفحة الرئيسية .تم الاسترداد في 12 يوليو 2025، من https://www.aljazeera.net/

المراجع الأجنبية

الكتب

1. Buzan, B. (1983). People, states and fear. Wheatsheaf Books.
2. Ghernaouti-Helie, S. (2013). Cyber power: Crime, conflict and security in cyberspace. EPFL Press.
3. Kissinger, H. (1969). Nuclear weapons and foreign policy. Wild Field and Nicholson.
4. McNamara, R. S. (1966). The essence of security. Harper Press.
5. Schmitt, M. N. (Ed.). (2013). Tallinn manual on the international law applicable to cyber warfare. Cambridge University Press.
6. Trager, F. N., & Kronenberg, P. S. (Eds.). (1973). National security and American society. Kansas University Press.
7. Wolfers, A. (1962). Discord and collaboration: Essays on international politics. John Hopkins University Press.

الدوريات والمواقع الإلكترونية

8. Lee, A. (2011, June 13). CIA chief Leon Panetta: Cyberattack could be 'next Pearl Harbor'. HuffPost. Retrieved May 20, 2025, from https://bit.ly/3ILFRTV
9. Riedel, B. (2017, July 14). In Saudi Arabia and Israel, signals that Iran has retaliation in works. The Daily Beast. Retrieved June 20, 2025, from https://bit.ly/35NWJME

10. Traynor, O. (2024). An overview of cyber attacks in the Middle East 2024. CybelAngel. https://cybelangel.com/cyber-attacks-middle-east-2024.
11. Iran French Radio. (2012, October 21). La guerre cybernétique, nouveau prétexte des pressions anti-iraniennes!. Retrieved June 10, 2025, from https://bit.ly/3pVkdbj