

الجريمة الإلكترونية وتحديات الأمن السيبراني - دراسة في آلية الردع السيبراني

Cybercrime and Cybersecurity Challenges: A Study on Cyber Deterrence Mechanisms

<https://doi.org/10.65384/2565-005-001-002>

حسين عبدالقادر

جامعة أبي بكر بلقايد تلمسان / الجزائر

تاريخ النشر: 2026/06/30	تاريخ المراجعة: 2026/04/13	تاريخ الإستلام: 2026/04/08
-------------------------	----------------------------	----------------------------

الملخص:

ركزت المدرسة النقدية كثيرا على الانتقال من المفهوم الكلاسيكي للأمن الذي يتخذ من الدولة وحدة للتحليل الى اعتماد الفرد كأساس للتحليل أين برز مفهوم الأمن الإنساني وأمن الفرد. أمام ما نعيشه من تطور تكنولوجي أصبح الفضاء السيبراني مهددا ويشكل أيضا مصدرا للتهديد الوطني للدول، وعليه تأتي هذه الدراسة للتركيز على موضوع الأمن السيبراني وتحديات الاختراق الإلكتروني. بالمقابل ظهرت الجريمة الإلكترونية بشكل لافت للانتباه أمام غياب بعض التعزيزات الأمنية ووجود ثغرات قانونية لدى وجب الانتقال الى آلية الردع السيبراني لضمان وتحقيق الأمن الوطني، إضافة الى ضرورة امتلاك القوة السيبرانية والتكنولوجيا المتقدمة والتفرد بها لتحقيق السيطرة في الفضاء السيبراني وتحقيق الأمن السيبراني ما يدعم مسألة السيادة الوطنية الكاملة للدولة. الكلمات المفتاحية: الجريمة الإلكترونية، الفضاء السيبراني، الردع الإلكتروني، الاختراقات الإلكترونية، حروب الجيل الخامس، الأمن الوطني.

Abstract;

The Critical Security Studies (CSS) perspective has significantly contributed to shifting the focus of security analysis from the traditional state-centric approach, which regards the state as the primary referent object of security, to a human-centered perspective that emphasizes the individual as the core unit of analysis. This intellectual transformation has led to the emergence of concepts such as human security and individual security as central dimensions of contemporary security discourse.

In the context of rapid technological advancements, cyberspace has evolved into a highly contested domain that is increasingly vulnerable to a wide range of threats while simultaneously posing substantial risks to national security. Consequently, this study examines the growing importance of cybersecurity and the challenges associated with cyber intrusions and malicious cyber activities.

Moreover, the proliferation of cybercrime has accelerated due to persistent security vulnerabilities, inadequate protective measures, and gaps in existing legal and regulatory frameworks. In response to these challenges, the adoption of effective cyber deterrence strategies has become essential for safeguarding national security and protecting critical information infrastructures. Furthermore, the development, control, and strategic deployment of cyber capabilities and advanced technologies are crucial for enhancing a state's position in cyberspace, strengthening cybersecurity resilience, and preserving national sovereignty in the digital age.

Keywords: Cybercrime, Cyberspace, Cyber Deterrence, Cyber Intrusions, Fifth-Generation Warfare, National Security.

مقدمة

أصبح الأمن السيبراني أحد المكونات الجوهرية للأمن الوطني في ظل التحول الرقمي المتسارع الذي يشهده العالم، حيث باتت البنى المعلوماتية للدول - بما فيها الأنظمة الحكومية والعسكرية والقضائية والاقتصادية تمثل ركائز حيوية تستوجب حماية مستمرة، ومع تنامي الاعتماد على الفضاء الإلكتروني في مختلف مجالات الحياة، برزت تهديدات جديدة تستهدف البنى التحتية المعلوماتية، وتعرض الأمن القومي لأخطار مباشرة وقد دفع هذا التطور الدول الى تأسيس هيئات وطنية متخصصة في الأمن السيبراني، ما جعل هذا المجال معياراً لمدى جاهزية الدول وقدرتها على حماية مصالحها الحيوية.

من هذا المنطلق تزداد الحاجة الى بناء قدرات وطنية في مجال الردع السيبراني، باعتباره الآلية الأكثر فعالية للحد من الهجمات الإلكترونية، وتنطلق هذه الدراسة من الاشكالية التالية:

كيف يمكن لسياسة الردع الإلكتروني الحد من التهديدات الأمنية في الفضاء السيبراني وتعزيز الأمن السيبراني للدول؟

تنطلق الدراسة من فرضية مفادها أن تعزيز القدرات التكنولوجية والردعية للدول في الفضاء السيبراني يساهم في الحد من الجريمة الإلكترونية وتقوية منظومات الأمن الوطني، ولتحليل الاشكالية سنحاول التطرق للنقاط التالية:

- مقدمة عامة (حروب الجيل الخامس والتطور التكنولوجي في الفضاء الرقمي)
- الاطار المفاهيمي لكل من الفضاء السيبراني، الأمن السيبراني، الجرائم الإلكترونية، الردع الإلكتروني...الخ

- طبيعة التهديدات الأمنية، التحديات الأمنية
- الردع الإلكتروني كآلية لتحقيق الأمن السيبراني وتعزيز الأمن الوطني.
- خاتمة تتضمن أبرز النتائج والتوصيات)

1- تحديد الإطار المفاهيمي:

- مفهوم الفضاء السيبراني:



يعد الفضاء السيبراني بيئة تفاعلية معقدة تتداخل فيها العناصر المادية وغير المادية، و تشمل الأجهزة الرقمية والشبكات والبرمجيات والمستخدمين بمختلف فئاتهم، ووفقا للوكالة الفرنسية لأمن أنظمة المعلومات ANSSI، وهي وكالة حكومية مكلفة بالدفاع السيبراني الفرنسي، بأنه: "فضاء التواصل الناتج عن الربط البيئي العالمي لمعدات معالجة البيانات الرقمية" (شلوش، 2018، صفحة 190)، اذن هو عبارة عن بيئة تفاعلية حديثة، تشتمل على عناصر مادية وغير مادية، مكوّن من مجموعة من الأجهزة الرقمية، وأنظمة الشبكات والبرمجيات، والمستخدمين سواء مشغلين أو مستعملين. كما أن هناك مَن عرّف الفضاء السيبراني بوصفه الذراع الرابعة للجيش الحديثة بعد البر والبحر والجو والفضاء الخارجي. (جبو، 2012)

• الأمن السيبراني:

يمثل الأمن السيبراني مجموعة الممارسات واتخاذ الاجراءات الرامية الى حماية الأنظمة المعلوماتية من الاختراق أو التعطيل أو الاتلاف أو الوصول غير المصرح به، ويشتمل عموما على حماية البيانات، الشبكات، البرمجيات وأمن الاتصالات ، وقد قدمت وزارة الدفاع الأمريكية تعريفا له بأنه " مجموعة الاجراءات التنظيمية الرامية الى حماية المعلومات من الجرائم والهجمات والتجسس والحوادث المختلفة. يمكن القول بأن الأمن السيبراني يتأسس على ثلاث ركائز أساسية هي : السرية، السلامة وديمومة الخدمة.

كما يشتمل الأمن في الفضاء السيبراني على دعائم وقواعد ضبط الاتصال ونقل وانتقال المعلومات، كما يشير الى أمن الاتصالات وما يتعلق بالحفظ والتخزين اضافة الى أمن المواقع الالكترونية (مصطفى و الشمري، 2021، صفحة 164).

أما من الناحية اللغوية فان المفهوم مكون من لفظين هما الأمن والسيبراني .

الأمن: عكس الخوف أو بمعنى السلامة والأمن مصدر الفعل أمنا وأمانا في النفس وسكون القلب وزوال الخوف .

أما التعريف الاصطلاحي فالأمن السيبراني مأخوذة من كلمة (سيبر Cyber) وتعني صفة لأي شيء مرتبط بثقافة الحواسيب أو تقنية المعلومات أو الواقع الافتراضي.

الأمن السيبراني (التعريف الاجرائي): يمكن حصره في كل ما يتعلق بأمن المعلومات لشبكات الحاسب الآلي، كما يشير الى العمليات والآليات التي تهدف لحماية معدات الحاسوب والمعلومات والخدمات من أي اختراق غير مقصود أو غير مصرح به وهذا من خلال استخدام مجموعة من الامكانيات الفنية، الإدارية، التقنية والتنظيمية لمنع الاستخدام غير المصرح به، والحد من سوء الاستغلال واستعادة المعلومات الإلكترونية ونظم الاتصالات والمعلومات التي تحتويه بشكل دقيق ومحمي. (عادل، 2012، صفحة 188) بالمقابل قدّمت وزارة الدفاع الأمريكية تعريفا لمصطلح الأمن السيبراني جاء فيه: " كل الاحترازمات والاجراءات التنظيمية من أجل ضمان أمن المعلومات بجميع أشكالها الإلكترونية والمادية من مختلف الهجمات، الجرائم، التخريب، والتجسس، والحوادث المختلفة.

يمكن أن تطلق كذلك كلمة سيبراني على الشبكات الإلكترونية الحاسوبية، وشبكة الإنترنت، وهو يعني كل ما يتعلق بشبكات الحاسوب والإنترنت والتطبيقات المختلفة (كالواتر والفيس بوك والمليجرام وتويتر وغيرها من 100 تطبيق) وكل الخدمات التي تقوم بتنفيذها (تحويل الأموال والشراء التسوق عبر الإنترنت) وغيرها من الآلات والخدمات في جميع مجالات الحياة على مستوى العالم.

وعليه فان الأمن السيبراني يقصد به جميع الإجراءات والتدابير والتقنيات والأدوات المستخدمة لحماية سلامه الشبكات والبرامج والبيانات من التخريب أو العبث أو الوصول غير المصرح به ويشمل ذلك حماية الأجهزة والبيانات على حد سواء.

وقد عرفه (البار والمرحبي) بأنه مصطلح مركب أتى من كلمتي (Cyber_ security) وكلمة سير لاتينية الأصل ومعناها الفضاء المعلوماتي فيصبح المقصود بالأمن السيبراني أمن الفضاء المعلوماتي وهو تعبير أوسع وأعم من أمن المعلومات فقط. (عبد العظيم و عبد الجواد، 2020، الصفحات 415-416)

مفهوم الردع السيبراني:

هو مجموعة آليات تهدف الى منع الخصم من شن هجوم الكتروني من خلال خلق تكلفة عالية تفوق المكاسب المحتملة، ويستند الى ثلاث ركائز

- مصداقية الدفاع: بناء أنظمة مقاومة للهجمات وقابلة للاستعادة



- القدرة على الانتقام: امتلاك وسائل الرد السيبراني المؤثر
- الرغبة في الانتقام: اعلان الاستعداد لاتخاذ اجراءات مضادة

يمثل الردع السيبراني اطارا معقدا بسبب صعوبة تحديد منفذ الهجوم، وانتشار الفواعل غير الحكومية وتعدد أساليب الاخفاء والتخفي في الفضاء الرقمي (Orji, 2014, pp. 31 - 46)

1- القدرة على الردع بالمثل:

يشترط تحقيق الردع أن يتكبد الطرف المهاجم خسائر تفوق تلك التي لحقت بالطرف المدافع، وهو ما يستدعي امتلاك القدرة على تنفيذ هجمات سيبرانية مضادة بعد تحديد هوية المهاجم الأصلي، وهو أمر غالبا ما يكون معقدا وصعب التحقيق في الواقع العملي.

2- مصداقية الدفاع:

يقتضي تأمين أنظمة المعلومات وتعزيز قدرتها على الصمود أمام محاولات الاختراق بما يضمن أن أي هجوم ناجح لا يؤدي الى تدمير الآليات Backup Systems ، من أبرزها أنظمة النسخ الاحتياطي الكلي للأنظمة أو فقدان شامل للبيانات ، وعلى الرغم من ارتفاع التكلفة المرتبطة بهذا الخيار الا أنه يعدّ من أكثر الحلول العملية فعالية في مجال الحماية السيبرانية.

3- اظهار نية الردع :

لا يكف امتلاك القدرة على الردع بالمثل، بل يتعين على الجهة المتضررة أن تعلن صراحة عن استعدادها للردّ على أي هجوم، اذ أن الافصاح عن هذه النية يشكل عنصرا أساسيا في تحقيق الردع الفعال (تيرتري، 2011).

رغم امكانية ضبط مفهوم الأمن السيبراني وتحديد مرتكزاته نظريا، فان هذا المفهوم لا يحظى باجماع دولي على المستوى التطبيقي ، ويتجلى ذلك في التباين بين الولايات المتحدة الأمريكية والصين، اذ تميل الولايات المتحدة الأمريكية الى استخدام مصطلح "الأمن السيبراني" Cyber Security للتركيز على حماية التكنولوجيات والشبكات والأنظمة الرقمية، في حين تفضل دول مثل الصين وروسيا اعتماد مصطلح أشمل هو "أمن المعلومات" Information Security ليشمل حماية المعلومات المتداولة

عبر الشبكات وكذا التقنيات المرتبطة بها، وفي ظل غياب معجم مفاهيمي موحد يستمر الخلاف حول كيفية استخدام الفضاء الرقمي وسياسات الردع وطبيعة التهديدات التي ينبغي التصدي لها. يعرف الأمن السيبراني بأنه جهد مستمر يهدف الى حماية شبكات المعلومات وبيانات الأفراد والمؤسسات من الوصول غير المصرح به ومن مختلف أشكال الاختراق أو الأضرار التي قد تمس سلامة الأنظمة الرقمية.

تعدّ مسألة أمن المعلومات من أبرز قضايا الثورة الصناعية الرابعة، حيث أصبح نجاح المؤسسات مرتبطا بدرجة كبيرة بقدرتها على حماية ما تمتلكه من بيانات ومعطيات، ومع ذلك فإن الأنظمة المعلوماتية والبنى التحتية المتصلة بالشبكات تظل عرضة لمختلف التهديدات والهجمات السيبرانية التي تتسم بالتنوع والتطور المستمر من حيث الأدوات والآليات المستخدمة، فضلا عن اختلافها باختلاف الفاعلين والسياقات الزمنية والمكانية وغالبا ما تؤدي هذه الهجمات الى تعطيل الخدمات والحاق خسائر مادية ومعنوية بالمؤسسات المستهدفة، وعليه يتضح أن للأمن السيبراني أهمية بالغة في مختلف مجالات الحياة المعاصرة خاصة في ظل تسارع وتيرة التحول الرقمي وثورة المعلومات، وقد أسهم تنوع أساليب الاختراق في تعميق التحديات المرتبطة بحماية البيانات الشخصية، الأمر الذي يبرز بوضوح اشكالية ضعف الوعي بأهمية الأمن السيبراني كأحد العوامل الرئيسية في تفاقم هذه المخاطر.

الهجمات السيبرانية: تعرّف بأنها سلوك أو نشاط عدائي يستهدف إضعاف أو تعطيل قدرات ووظائف أنظمة وشبكات الحاسوب لتحقيق أهداف ذات طابع سياسي أو استراتيجي، وذلك عبر استغلال ثغرات أمنية تمكّن الفاعل من التأثير في سير عمل النظام أو التلاعب بمكوناته.

الجريمة السيبرانية: هي أي فعل غير قانوني يرتكب باستخدام أجهزة إلكترونية أو شبكات معلوماتية، ويشمل القرصنة، السرقة الرقمية، الابتزاز الإلكتروني، التخريب، وانتحال الهوية وتمثل هذه الجرائم تحديا كبيرا للأمن الوطني نظرا لحدودها العابرة للدول وسرعة تنفيذها وتطور أدواتها، وهي ذلك النوع من الجرائم التي تتطلب الإلمام الخاص بتقنيات الحاسب الآلي ونظم المعلومات لارتكابها أو التحقيق فيها ومقاضاة فاعليها". اذن هي كل جريمة متصلة باستخدام جهاز الاعلام الآلي، وهو تصرف غير شرعي، يرتكب باستخدام تقنيات المعلومات والاتصالات. (البهي، 2022)

القوة السيبرانية: يعتبر جوزيف.س ناي Nye.S Joseph من أهم الدارسين للقوة السيبرانية، وقد عرّفها بأنها "امكانية الحصول على النتائج المرجوة من خلال استخدام مصادر المعلومات المرتبطة بالفضاء السيبراني، وهي القدرة على استخدام الفضاء السيبراني لإيجاد مزايا للدولة، والتأثير على الأحداث المتعلقة بالبيئات التشغيلية الأخرى وذلك عبر أدوات سيبرانية".

2- طبيعة التحديات الأمنية للدول في الفضاء السيبراني:

يمثل الفضاء السيبراني ميدانا رئيسيا من ميادين الصراعات الحديثة، وقد أصبح عنصرا أساسيا في حروب الجيل الخامس، حيث يمكن للهجمات السيبرانية أحداث شلل كامل للبنية التحتية الحيوية، وتعطيل القطاعات الاقتصادية والعسكرية والخدماتية، فاستهداف الهجوم للبنية المعلوماتية يمكن أن يشكل ضربة قاضية لاقتصاد بلد من البلدان، (بونيفاس، 2020، صفحة 81).

من أبرز العوامل التي ساعدت على تنامي التهديدات السيبرانية ما يلي:

يمكنه الحاق الضرر الفادح في كل القطاعات التي يمكن التسلل لها الكترونيا سواء كانت عسكرية أو مدنية، ومن خلال الاعتبارات السابقة الذكر حول طبيعة الفضاء السيبراني، يمكن أن تظهر توابع أخرى قابلة للنقاش، فلا تستطيع الدول أن تعبر عن سيادتها في الفضاء السيبراني، لأن اعتماد الناس على هذا البعد التكنولوجي يجعله عرضة بشكل خاص للأعمال العدائية، فلا يزال المهاجمون السيبرانيون يتمتعون بمميزات تفوق إمكانيات المدافعين بسبب التأثير المفاجئ الذي لا يمكن أن يقلل من قوته أي أسلوب أمني أو دفاعي سلبي أو حتى إيجابي بشكل تام، كما أن هؤلاء المهاجمين يمتلكون القدرة على إخفاء آثارهم، ولا تسمح الحالة المعرفية بوضع توصيف دقيق للعمليات الهجومية التي تحدث في الفضاء السيبراني، الأمر الذي يجعلنا في مواجهة جميع الاحتمالات. (هينروتين ، 2019، صفحة 71)

يمكن حصر أبرز العوامل التي أسهمت في تصاعد التهديدات السيبرانية في مجموعة من المحددات البنيوية والتحوليات الدولية المعاصرة وفي مقدمتها التوسع المتسارع في الاعتماد على الفضاء السيبراني، الأمر الذي زاد من هشاشة البنية التحتية المعلوماتية العالمية وجعلها أكثر عرضة للهجمات الإلكترونية.

كما أسهمت العولمة في إعادة تشكيل دور الدولة، من خلال تراجع حضورها في بعض القطاعات الاستراتيجية مقابل تنامي نفوذ الشركات متعددة الجنسيات، لاسيما العاملة في المجال التكنولوجي، باعتبارها فاعلاً مؤثراً في البيئة السيبرانية.

إلى جانب ذلك، أدى الاعتماد المتزايد للدول على الأنظمة الرقمية في إدارة مرافقها الحيوية إلى رفع مستوى المخاطر، حيث أصبحت هذه المنشآت أهدافاً محتملة للهجمات الإلكترونية، خاصة في سياقات الصراع كما تتميز الحروب السيبرانية بانخفاض تكلفتها مقارنة بالحروب التقليدية، فضلاً عن مرونتها الزمنية وسرعة تنفيذها، مما يعزز جاذبيتها كأداة صراعية.

من جهة أخرى، برزت الحروب السيبرانية كوسيلة فعالة للتأثير في المعلومات والأنظمة المرتبطة بها، سواء على المستوى الاستراتيجي أو العملي، بهدف إضعاف الخصم والتأثير على قدراته الوظيفية. وفي السياق ذاته، أصبح الفضاء السيبراني مجالاً لتعظيم القوة الوطنية، من خلال تحقيق التفوق الرقمي وبناء استراتيجيات سيبرانية متكاملة.

أخيراً، اتسع نطاق الفاعلين المنخرطين في الأنشطة السيبرانية العدائية، ليشمل ليس فقط الدول، بل أيضاً فاعلين من غير الدول، مثل الجماعات المنظمة والقرصنة، الذين قد يتم توظيفهم بشكل غير مباشر لتنفيذ هجمات سيبرانية، دون وجود ارتباط رسمي واضح، مما يزيد من تعقيد بيئة التهديدات السيبرانية (العلي، 2020، ص 78-79).

3- أهمية الأمن السيبراني :

تتجلى أهمية الأمن السيبراني بوصفه أحد القضايا الناشئة في حقل العلاقات الدولية من خلال حداثة هذا المجال وتنامي تأثيره في الدراسات الأمنية المعاصرة. فقد ارتبطت البدايات النظرية لهذا الحقل بمحاولات مبكرة لتحليل دور التكنولوجيا الرقمية في الأمن، كما في أعمال Arquilla و Ronfeldt (1993) حول مفهوم "حرب الشبكات" (Netwar) و "الحرب السيبرانية" (Cyberwar)، والتي فتحت المجال أمام نقاشات نظرية وأخلاقية واسعة حول طبيعة التهديدات السيبرانية.

مع نهاية الحرب الباردة، شهدت الدراسات الأمنية تحولات عميقة، تمثلت في الانتقال من المقاربة التقليدية الضيقة المتمركزة حول الدولة إلى مقاربات أكثر شمولاً وديناميكية، تأخذ بعين الاعتبار فاعلين جدد وتهديدات غير تقليدية. وفي هذا السياق، برزت إسهامات مدرسة كوبنهاغن، لاسيما أعمال باري بوزان (Barry Buzan) وأولي ويفر (Ole Wæver)، التي قدّمت مفهوم “الأمننة (Securitization)”， والذي يركّز على الكيفية التي يتم من خلالها بناء القضايا وطرحها كتهديدات أمنية من قبل فاعلين محددين، بدلاً من اعتبارها تهديدات موضوعية ثابتة.

في إطار تطور مفاهيم القوة في العلاقات الدولية، لم تعد القوة مقتصرة على أبعادها الصلبة المرتبطة بالقدرات العسكرية والاقتصادية، بل امتدت لتشمل القوة الناعمة القائمة على الجاذبية والتأثير، ومع ثورة المعلومات ظهر مفهوم “القوة السيبرانية (Cyber Power)” كأحد أبرز تجليات التحول في بنية القوة. وقد أسهم الفضاء السيبراني في إعادة توزيع القوة بين عدد أكبر من الفاعلين، بما في ذلك الفاعلون من غير الدول، مما أضعف احتكار الدولة التقليدي لمصادر القوة، ومنح الجهات الأصغر قدرة أكبر على التأثير في البيئة الدولية، سواء عبر أدوات صلبة أو ناعمة.

انطلاقاً من ذلك، ازداد اهتمام الباحثين في العلاقات الدولية والدراسات الأمنية والاستراتيجية بدراسة تأثير التكنولوجيا الرقمية على مفاهيم أساسية مثل السيادة، والقوة، والحوكمة العالمية، والأمننة (Idris & Shanmugam, 2007)، في ظل التحولات التي فرضها الفضاء السيبراني على طبيعة التفاعلات الدولية.

أما على المستوى التطبيقي، فقد ارتبط بروز الأمن السيبراني بتنامي الهجمات السيبرانية، وهو ما يعود إلى عاملين رئيسيين: أولهما، التطور التكنولوجي المرتبط بظهور الحواسيب منذ منتصف القرن العشرين، وتطور قدراتها في معالجة وتخزين البيانات الرقمية، مما أدى إلى اعتماد واسع عليها في مختلف القطاعات الحيوية. وثانيهما، ظهور شبكة الإنترنت التي أحدثت تحولاً جذرياً في أنماط التواصل وتبادل المعلومات، وساهمت في تسريع وتيرة الاعتماد على التكنولوجيا في المجالات الأمنية والعسكرية، خاصة منذ تسعينيات القرن الماضي، حيث بدأ الحديث عن مفاهيم مثل “الحرب السيبرانية الباردة” و “سباق التسلح السيبراني” (غراهام، 2004).

وبناءً على ما سبق، يتضح أن الأمن السيبراني أصبح عنصرًا محوريًا في تحليل قضايا الأمن المعاصر، نظرًا لارتباطه المباشر بتحولات القوة، وتعدد الفاعلين، وتعدد طبيعة التهديدات في البيئة الدولية

4- أهداف الأمن السيبراني

تتمثل الأهداف الرئيسة للأمن السيبراني في مجموعة من الغايات الاستراتيجية الرامية إلى حماية البيئة الرقمية وضمان استمرارية عملها بكفاءة. ويأتي في مقدمتها تعزيز أمن الأنظمة التقنية بمكوناتها، سواء ما يتعلق بالأجهزة أو البرمجيات أو البيانات والخدمات المرتبطة بها. كما يسعى الأمن السيبراني إلى مواجهة الهجمات والحوادث المعلوماتية التي تستهدف المؤسسات الحكومية وكيانات القطاعين العام والخاص، إلى جانب توفير بيئة رقمية آمنة وموثوقة تدعم مختلف أشكال التفاعل داخل مجتمع المعلومات. ي شمل ذلك أيضًا ضمان مرونة البنى التحتية الحيوية وقدرتها على الصمود في مواجهة الهجمات الإلكترونية، وتقليل المخاطر المرتبطة بالجرائم السيبرانية التي تستهدف المستخدمين، من خلال معالجة نقاط الضعف وسد الثغرات في الأنظمة المعلوماتية. إضافة إلى ذلك، يهدف الأمن السيبراني إلى الحد من البرمجيات الخبيثة وأنشطة التجسس والتخريب الإلكتروني، سواء على مستوى الأفراد أو المؤسسات، مع اتخاذ التدابير الكفيلة بحماية المستخدمين في مختلف مجالات استخدام الإنترنت. كما يبرز جانب بناء القدرات البشرية من خلال تدريب الأفراد وتأهيلهم للتعامل مع التهديدات السيبرانية المتجددة.

5- خصائص الأمن السيبراني

يتسم الأمن السيبراني بجملة من الخصائص التي تعكس طبيعته المعقدة والمتغيرة، حيث يتمثل هدفه الأساسي في تحقيق القدرة على الوقاية من التهديدات، والاستجابة لها، والتعافي من آثارها، بما يضمن استمرارية الأنظمة الرقمية وحمايتها من الأضرار أو سوء الاستخدام. ويعتمد ذلك على حماية متكاملة للشبكات والأجهزة والبرمجيات والبيانات من الوصول غير المصرح به أو الهجمات المختلفة. كما يتميز الأمن السيبراني بطابعه متعدد التخصصات، حيث يتقاطع فيه البعد التقني مع الأبعاد الاجتماعية والتنظيمية والقانونية، فضلًا عن كونه مجالًا ديناميكيًا يتسم بسرعة التغير، وارتفاع درجة الترابط بين مكوناته، والتفاعل المستمر بين فاعليه. وقد أدى تصاعد التهديدات السيبرانية، خاصة في ظل ما يُعرف بالحروب الإلكترونية، إلى إدراج الأمن السيبراني ضمن أولويات السياسات الوطنية للعديد من الدول، باعتباره عنصرًا أساسيًا في منظومة الأمن القومي.

6- الفاعلون في الفضاء السيبراني

- في إطار تحليل القوة السيبرانية، يميز جوزيف ناي بين عدة فاعلين رئيسيين في هذا المجال. في مقدمتهم الدول، التي تمتلك القدرات التقنية والمؤسسية لتطوير البنى التحتية الرقمية وتنفيذ العمليات السيبرانية، مما يجعلها الفاعل الأكثر تأثيراً في هذا المجال. إلى جانب ذلك، برزت فواعل من غير الدول، التي تلعب أدواراً متزايدة في البيئة السيبرانية، وتشمل:
- الشركات متعددة الجنسيات: التي تمتلك موارد تقنية ومعلوماتية ضخمة، بما في ذلك قواعد بيانات هائلة، ما يمنحها قدرة مؤثرة في الاقتصاد الرقمي وتوجيه الرأي العام.
 - المنظمات الإجرامية: التي تنشط في مجال الجرائم السيبرانية، مثل القرصنة وسرقة البيانات والاحتيال المالي، مستفيدة من فضاءات الإنترنت المظلم.
 - الجماعات الإرهابية: التي توظف الفضاء السيبراني في الدعاية والتجنيد وجمع التمويل وتبادل المعلومات، رغم محدودية قدراتها في تنفيذ هجمات سيبرانية معقدة ضد البنى التحتية الحيوية.
 - الأفراد: الذين أصبحوا، بفضل الأدوات الرقمية، فاعلين مؤثرين في العلاقات الدولية، كما يظهر في حالات تسريب المعلومات ونشر الوثائق الحساسة، على غرار ظاهرة "ويكيليكس".
- وبناءً على ذلك، يتضح أن الأمن السيبراني يشكل مجاًلاً مركزياً في تحليل التحولات المعاصرة، نظراً لتعدد أهدافه، وتعدد خصائصه، وتنوع الفاعلين المنخرطين فيه.

7- الردع السيبراني كآلية لتحقيق الأمن السيبراني وتعزيز الأمن الوطني

يُعدّ الردع أحد المفاهيم المركزية في دراسات الأمن والعلاقات الدولية، إذ يهدف إلى بناء منظومة من الحوافز والقيود التي تحول دون إقدام الخصوم على شن هجمات أو القيام بسلوك عدائي مستقبلي. غير أن تطبيق هذا المفهوم في الفضاء السيبراني يكتسب خصوصية متميزة مقارنة بأشكال الردع التقليدي، لاسيما النووي، نظراً لاختلاف طبيعة البيئة العملية وحدود القدرة على إلحاق تدمير شامل بالخصم. فخاصية "الإخفاء" (Anonymity) التي تميز الفضاء السيبراني تعيق عملية الإسناد (Attribution)، مما يجعل تحديد هوية الفاعل ومصدر الهجوم أمراً معقداً، ويضعف من فعالية استراتيجيات الردع القائمة على التهديد بالعقاب.

تتفاقم هذه الإشكالية في ظل نظام دولي يتسم بتعدد مراكز القوة وتزايد عدد الفاعلين، من دول وغير الدول، الذين يمتلكون قدرات سيبرانية متفاوتة ويستخدمونها في إدارة التفاعلات والصراعات الدولية. كما أن التقدم التكنولوجي المتسارع يسهم في توسيع نطاق التهديدات وتعقيدها، بما يعزز احتمالات توظيف الأدوات السيبرانية كخيار استراتيجي في إدارة النزاعات، خاصة في ظل تصاعد التوترات الإقليمية والدولية، وتنامي أدوار الفواعل المسلحة من غير الدول (كلاع، 2022، ص 307).

في هذا السياق، تبرز الحاجة إلى تطوير مقاربات متكاملة تجمع بين الردع والدفاع السيبراني، من خلال وضع أطر تنظيمية لضبط السلوك في الفضاء السيبراني، وتعزيز القدرات الوطنية في مجال الحماية والاستجابة (خليفة، ص 100). ويُعدّ الدفاع السيبراني الوقائي أحد المرتكزات الأساسية لهذه المقاربة، حيث يقوم على جملة من الآليات، من أبرزها: الكشف المبكر عن التهديدات عبر توظيف أنظمة الاستشعار (Sensors) والاستخبارات السيبرانية لرصد الأنشطة غير الطبيعية في الزمن الحقيقي؛ وتبني استراتيجيات استباقية تهدف إلى تحديد التهديدات قبل تفعيلها، بما في ذلك استخدام أدوات برمجية متقدمة قادرة على اكتشاف البرمجيات الخبيثة وتعطيلها؛ فضلاً عن اعتماد تقنيات الخداع والتمويه السيبراني (Cyber Deception) لتضليل الخصوم وإرباك عملياتهم.

وعلى المستوى التطبيقي، اتجهت العديد من الدول إلى إدماج الفضاء السيبراني ضمن عقائدها العسكرية، واعتباره مجالاً خامساً للعمليات إلى جانب البر والبحر والجو والفضاء. وقد تجسد ذلك في إنشاء قيادات سيبرانية متخصصة ووحدات عملياتية ذات قدرات هجومية ودفاعية متقدمة، كما هو الحال في الولايات المتحدة والصين وروسيا ودول أخرى. وتعكس هذه التطورات إدراكاً متزايداً لأهمية القوة السيبرانية كأداة استراتيجية في تحقيق التفوق وتعزيز الأمن القومي.

وعليه، فإن فعالية الردع السيبراني لا تتحقق بمعزل عن القدرات الدفاعية، بل من خلال تكامل ديناميكي بين الردع بالعقاب (Deterrence by Punishment) والردع بالمنع (Deterrence by Denial)، بما يضمن حماية البنى التحتية الحيوية، وتأمين الأنظمة المعلوماتية، وصون البيانات الاستراتيجية، وهو ما يشكل في مجمله ركيزة أساسية لتعزيز الأمن السيبراني والأمن الوطني في العصر الرقمي.

كيف يؤثر ضعف الدولة على الردع السيبراني؟

يقوم الردع السيبراني على إقناع الخصم بأن أي هجوم إلكتروني سيؤدي إلى اكتشافه ومعاقبته أو إفشال أهدافه، وعندما تكون الدولة ضعيفة سيبرانياً، فإن هذا الإقناع يتراجع.

كما يمكن أن يظهر ضعف الدولة في:

- ضعف البنية التحتية الرقمية .
 - نقص الكفاءات والخبراء .
 - محدودية قدرات الاستخبارات السيبرانية .
 - ضعف التشريعات وآليات الاستجابة .
 - الاعتماد الكبير على التكنولوجيا الأجنبية دون حماية كافية .
- وإذا ما أدرك المهاجم أن الدولة لا تستطيع اكتشاف الاختراق بسرعة أو تحديد مصدر الهجوم وكذا الرد بعقوبات أو هجمات مضادة فإن تكلفة الهجوم بالنسبة إليه تنخفض، وبالتالي يفشل الردع. يُقصد بالإسناد معرفة المسؤول الحقيقي عن الهجوم.
- وهذه المشكلة تُعد من أكبر تحديات الأمن السيبراني لأن المهاجم يستطيع:
- استخدام خوادم في عدة دول .
 - إخفاء عنوانه الحقيقي .
 - استغلال أجهزة مختربة لأطراف أخرى .
 - استخدام جماعات واجهة أو وكلاء .

الخاتمة:

بناءً على ما تم تناوله في هذا البحث، يتضح أن الأمن السيبراني لم يعد مجرد مسألة تقنية محضة، بل تحول إلى قضية استراتيجية متعددة الأبعاد تتداخل فيها الاعتبارات الأمنية والسياسية والاقتصادية والتكنولوجية. فقد أفرزت التحولات التي شهدتها الفضاء الرقمي، لا سيما مع تسارع الاعتماد على الشبكات والأنظمة المعلوماتية،

بيئة معقدة تتسم بتزايد التهديدات وتنوع الفاعلين وتداخل مستويات التأثير، الأمر الذي جعل من الفضاء السيبراني ساحة مركزية للتفاعلات الدولية الحديثة.

وفي هذا السياق، يبرز الردع السيبراني كأحد الأدوات المفاهيمية والعملية التي تسعى الدول من خلالها إلى الحد من التهديدات السيبرانية وتعزيز قدرتها على حماية مصالحها الحيوية. غير أن خصوصية الفضاء السيبراني، خاصة ما يتعلق بصعوبة الإسناد وارتفاع درجة التخفي وتعدد الفاعلين، تجعل من تطبيق آليات الردع التقليدية أمراً معقداً، مما يستدعي تطوير مقاربات مبتكرة تجمع بين الردع والدفاع، وتستند إلى التكامل بين القدرات التقنية والاستخباراتية والتنظيمية.

كما أظهر البحث أن نجاح السياسات السيبرانية للدول يرتبط بمدى قدرتها على تبني استراتيجيات شاملة تشمل الكشف المبكر عن التهديدات، وتعزيز القدرات الوقائية، وتطوير آليات الاستجابة السريعة، إلى جانب الاستثمار في العنصر البشري من خلال التدريب والتأهيل المستمر. وفي المقابل، فإن تنامي أدوار الفاعلين من غير الدول، مثل الجماعات الإجرامية والشركات متعددة الجنسيات، يفرض تحديات إضافية على منظومة الأمن السيبراني، ويستدعي تعزيز التعاون الدولي وتبادل المعلومات لمواجهة هذه التهديدات العابرة للحدود.

وعلى مستوى العلاقات الدولية، أسهم ظهور القوة السيبرانية في إعادة تشكيل موازين القوى، حيث لم تعد القوة محصورة في الأبعاد العسكرية التقليدية، بل امتدت لتشمل القدرات الرقمية والتكنولوجية التي باتت تمثل عنصراً حاسماً في تحديد مكانة الدول ونفوذها. وقد أدى ذلك إلى بروز الفضاء السيبراني كمجال تنافسي جديد، يتقاطع فيه البعد الأمني مع البعد الاستراتيجي، مما يعزز من أهمية تطوير مفاهيم الحوكمة العالمية للأمن السيبراني.

وفي ضوء ما سبق، يمكن القول إن تحقيق الأمن السيبراني وتعزيز الأمن الوطني يتطلبان تبني رؤية شاملة ومتكاملة تقوم على التوازن بين الردع والدفاع، وبين السياسات الوطنية والتعاون الدولي، مع مراعاة الطبيعة الديناميكية للتهديدات السيبرانية. كما يستلزم ذلك الاستثمار المستمر في تطوير البنى التحتية الرقمية، وتعزيز الوعي المجتمعي بمخاطر الفضاء السيبراني، بما يضمن بناء منظومة أمنية قادرة على مواكبة التحديات المتسارعة للعصر الرقمي والتكيف معها بفعالية.

لقد أضحى الفضاء السيبراني في السياق الدولي المعاصر بديلاً استراتيجياً لأشكال الصراع المباشر بين الدول، حيث أتاح توظيف التقنيات الرقمية الحديثة إمكانية تجاوز الحدود الجغرافية والسيادية التقليدية، وفتح

المجال أمام أنماط جديدة من التهديدات والهجمات التي تستهدف أمن الدول واستقرارها. وفي ظل هذه التحولات، لم يعد الأمن الوطني منفصلاً عن الأمن السيبراني، بل أصبح هذا الأخير عنصراً مكملاً لمفهوم السيادة، خاصة في ظل ما تفرضه الهجمات السيبرانية من حالات انكشاف أمني قد تمس البنى التحتية الحيوية والأنظمة المعلوماتية للدول.

كما أبرزت الدراسة أن تصاعد التهديدات السيبرانية، بما في ذلك الاختراقات الإلكترونية وأنشطة التجسس الرقمي، يعكس طبيعة البيئة الدولية المتغيرة التي تتسم بارتفاع درجة عدم اليقين وتعدد الفاعلين وتداخل مستويات التهديد. وهو ما يدفع الدول إلى تبني استراتيجيات أمنية متكاملة قائمة على حماية المعلومات وتطوير القدرات الدفاعية والهجومية في الفضاء السيبراني، بما يضمن تعزيز الجاهزية لمواجهة مختلف المخاطر المحتملة.

وفي ضوء ما سبق، توصل البحث إلى مجموعة من التوصيات التي من شأنها الإسهام في تعزيز الأمن السيبراني، ويمكن إجمالها فيما يلي:

- ضرورة تنظيم دورات تدريبية مكثفة، سواء على المستوى التأسيسي أو المتقدم، بهدف نشر الوعي بمفاهيم الأمن السيبراني ومبادئه الأساسية.
- أهمية ترسيخ الثقافة السيبرانية لدى الأفراد والمؤسسات، من خلال الاستخدام الواعي والأمن للتقنيات الرقمية، ومواكبة المستجدات في هذا المجال.
- العمل على تطوير برامج تكوينية تطبيقية تركز على إكساب المهارات العملية المتعلقة بكيفية استخدام أدوات وتقنيات الأمن السيبراني والتعامل مع التهديدات المحتملة.

وبناءً عليه، فإن تحقيق أمن سيبراني فعال يتطلب مقاربة شاملة تجمع بين التوعية، وبناء القدرات، وتحديث السياسات، بما يواكب التطورات المتسارعة في الفضاء الرقمي، ويعزز قدرة الدول على حماية أمنها الوطني في ظل البيئة التكنولوجية المعاصرة.

قائمة المراجع والمصادر:



- Orji, U. J. (2014). Deterring Cyberterrorism in the Global Information Society: A Case for the Collective Responsibility of States. *Defence against Terrorism Review*, 6(1).
- إبراهيم مصطفى ، و سلمان الشمري. (01 جوان، 2021). الأمن السيبراني وأثره في الأمن الوطني العراقي. *مجلة العلوم القانونية والسياسية* (10).
- منى الأشقر جبور . (2016). *السيبرانية هاجس العصر*. بيروت: جامعة الدول العربية: المركز العربي للبحوث القانونية والقضائية.
- Idris, N., & Shanmugam, B. (2007). *Hybrid Intelligent Intrusion Detection System*, *Information Technology and national security Conference*. Riyadh.
- أميرة عبد العظيم ، و محمد عبد الجواد. (2020). المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام. *مجلة الشريعة والقانون* (3).
- إيفانز غراهام. (2004). *نوينهام جيفري. قاموس بنغوين للعلاقات الدولية*. (مركز الخليج للأبحاث، المحرر) الامارات العربية المتحدة: مركز الخليج للأبحاث.
- إيهاب خليفة. (بلا تاريخ). *القوة الإلكترونية: كيف يمكن أن تدير الدول شؤونها في عصر الأنترنت*.
- إيهاب خليفة. (بلا تاريخ). *تنامي التهديدات السيبرانية للمؤسسات العسكرية*.
- إيهاب خليفة. (بلا تاريخ). *مجتمع ما بعد المعلومات: تأثير الثورة الصناعية الرابعة على الأمن القومي*. القاهرة: العربي.
- باسكال بونيفاس. (2020). *الجيوپوليتيك: مقارنة لفهم العالم في 48 مقالا*. (اياد عيسى، المحرر) دمشق: منشورات الهيئة العامة السورية للكتاب - وزارة الثقافة.
- برونو تيرتري. (2011). *السلاح النووي بين الردع والخطر*. (عبد الهادي الإدريسي، المحرر) الإمارات العربية المتحدة: هيئة أبو ظبي للثقافة والتراث (كلمة).

- جوزيف هينروتين . (2019). حرب واستراتيجية: نهج ومفاهيم. (أيمن منير، المحرر) الكويت: المجلس الوطني للثقافة والفنون والآداب.
- رغدة البهي. (18, 11, 2022). الردع السيبراني: المفهوم والإشكاليات والمتطلبات. تم الاسترداد من موقع المركز الديمقراطي العربي: <https://democraticac.de/?p=43837>
- شريفة كلاع. (2022). الأمن السيبراني وتحديات الجوسسة والاختراقات الالكترونية للدول عبر الفضاء السيبراني. مجلة الحقوق والعلوم الانساني، 15(01).
- عبد الرزاق عادل . (30 أبريل، 2012). القوة الإلكترونية: أسلحة الانتشار الشامل في عصر الفضاء الإلكتروني. مجلة السياسة الدولية (47).
- علي زياد العلي. (2020). الصراع والأمن الجيوسبيبراني في الساحة الدولية: دراسة في استراتيجيات الاشتباك الرقمي. عمان: دار أمجد للنشر والتوزيع.
- منى الأشقر جبو. (2012). الأمن السيبراني: التحديات ومستلزمات المواجهة. اللقاء السنوي في امن وسلامة الفضاء السيبراني. جامعة الدول العربية -المركز العربي للبحوث القانونية والقضائية-.
- نورة شلوش. (2018). القرصنة الإلكترونية في الفضاء السيبراني: التهديد المتصاعد لأمن الدول. مجلة مركز بابل للدراسات الإنسانية (08).