مجلة مؤشر للدراسات الاستطلاعية
Journal index of exploratory studies
المجلد 07، العدد 20
ISSN: 2701-9233

الحرب السيبرانية: التهديدات، الاستراتيجيات، وتحديات الردع في الفضاء الرقمي

Cyber Warfare: Threats, Strategies, and Deterrence Challenges in Cyberspace

د. محمد إبراهيم قانصو
الجامعة الاسلامية في لبنان
m-kanso@hotmail.com

DOI: https://doi.org/10.63939/JIES.2025-Vol7.N20.38-61

الملخص

يهدف هذا البحث إلى مقاربة ظاهرة "الحرب السيبرانية"، وتحليل طبيعتها المهددة للأمن القومي والدولي في العصر الرقمي، واستكشاف الاستراتيجيات المتبعة للردع. يتناول البحث نشأة وتطور مفهوم الحرب السيبرانية، ويحدد طرائق الهجمات وأنماطها التي تتجاوز الحدود الجغرافية، مع إبراز المميزات التي تجعلها سلاحًا ذا كلفة منخفضة وتأثير فاعل ومخفي. اعتمد البحث على المنهج الوصفي التحليلي، مستعرضاً أبرز نماذج الصراع السيبراني الدولي (كالهجمات بين الولايات المتحدة وإيران). خلص البحث إلى أن الطبيعة غير الملموسة والمجهولة المصدر لهذه الهجمات تقوض من فعالية الردع السيبراني التقليدي، مما يفرض تحديات قانونية وموثوقية. ويوصي البحث بضرورة تطوير استراتيجيات ردع مرنة تشمل الأنظمة البديلة وإعادة التأسيس السريع للأنظمة المُخترقة، وتنمية الوعي الفردي والمؤسساتي لمواجهة هذه التهديدات التي باتت تمثل الجيل الخامس من الحروب.

الكلمات المفتاحية : الكلمات المفتاحية :الحرب السيبرانية؛ الأمن السيبراني؛ الردع السيبراني؛ الهجمات السيبرانية؛ الفضاء الرقمي؛ حرب الأصفار والأحاد.

Abstract

This research aims to contextualize and critically analyze the phenomenon of "Cyber Warfare" and its inherent threat landscape to national and international security in the digital age, while exploring emergent deterrence strategies. The study traces the genesis

and evolution of the cyber warfare paradigm, meticulously cataloging the vectors and topologies of attacks that transcend geopolitical boundaries. A key focus is placed on the characteristic features that position cyber operations as low-cost, high-impact, and covert asymmetrical capabilities. Utilizing a descriptive-analytical methodology, the research examines salient models of international cyber conflict (e.g., between the United States and Iran). The findings conclusively demonstrate that the intangible and ambiguous attribution inherent in these attacks significantly degrades the efficacy of conventional cyber deterrence frameworks, thereby introducing critical legal and credibility challenges. Consequently, the study recommends the architecting of resilient deterrence strategies that incorporate redundant systems, rapid system reconstitution capabilities following compromise, and the cultivation of heightened individual and institutional cyber vigilance to effectively counter these threats, which represent the fifth generation of conflict.

Keywords: Cyber Warfare; Cybersecurity; Cyber Deterrence; Cyber Attacks; Digital Cyberspace; Binary Warfare (Zero–One Warfare).

المقدمة

مَثَّلَ بزوغُ الثورة الرقمية وانتشار الإنترنت منعطفاً حاسماً، نقل الفضاء الإلكتروني من مجرد أداة اتصال إلى نسيج حيوي مُعقَّد تُمارس عليه كافة أنشطة البشرية، من الاقتصاد إلى السياسة إلى الأمن القومي. هذا التحول الجوهري أوجد بيئة خصبة لنشوء شكل جديد من الصراعات، تُعرف بالحرب السيبرانية، التي لم تعد مجرد تهديد نظري، بل أصبحت واقعاً ملموساً يُشكِّل الجيل الخامس من الحروب.

لم تعد هذه الحرب مقصورة على دوائر المخابرات التقليدية، بل أصبحت ساحة معقدة تتداخل فيها أدوار الفواعل، وغيرها فإلى جانب الوحدات المتخصصة في الجيوش النظامية، وبرزت مجموعات قرصنة إلكترونية مدعومة أو متسامح معها من قبل بعض الدول، تعمل في منطقة رمادية بين الحرب والسلم. هذا التشابك يجعل من "حرب البتات والبايتات "ساحة صراع غير تقليدية بالغة الغموض.

تتميز هذه المواجهات السيبرانية بطابعها اللامتماثل، حيث يمكن لفاعل صغير نسبياً أن يلحق أضراراً جسيمة بدولة عظمى. وهي حرب مبهمة المعالم :يصعب تحديد هوية المهاجم بدقة) مشكلة نسب الهجوم، وتكون الأهداف غالباً استباقية ومدروسة لتعطير البنى التحتية الحيوية أو سرقة الملكية الفكرية أو تقويض الاستقرار السياسي. وغالباً ما تكتشف الدولة أو المؤسسة المستهدفة الهجوم بعد فوات الأوان، بعد أن تكون الخسائر قد وقعت، ما يجعل الردع والاحتواء تحدياً استراتيجياً شائكاً.

وهكذا، لم يعد الفضاء السيبراني مجرد تقنية، بل تحول إلى مجال جيوسياسي حاسم، تُعيد فيه هذه الحروب الخفية تعريف مفاهيم القوة والسيطرة والهيمنة في النظام العالمي المعاصر.

1.1. إشكالية البحث

تتمحور إشكالية هذا البحث حول التساؤل الرئيسي التالي: إلى أي مدى أدت الطبيعة الخاصة للهجمات السيبرانية (المجهولة المصدر وغير المتماثلة) إلى إعادة تعريف مفهومي القوة والصراع في العلاقات الدولية، وإلى أي مدى يمكن تحقيق الردع الفاعل في ظل هذه الطبيعة الاستثنائية والتحديات المصاحبة لها؟

ويتفرع عن هذا التساؤل أسئلة فرعية يسعى هذا البحث للإجابة عنها:

- كيف أعادت الهجمات السيبرانية تعريف مفهومي القوة والصراع في العلاقات الدولية؟
- ما مدى فعالية استراتيجيات الردع السيبراني في مواجهة إشكالية إخفاء هوية المهاجم؟
- ما مدى قدرة الأطر القانونية الدولية الحالية على تنظيم الفضاء السيبراني ومواجهة تحدياته؟

أهداف البحث

يسعى هذا البحث إلى تحليل الآثار الناجمة عن الحرب السيبرانية على مفاهيم القوة والصراع في العلاقات الدولية، وتقييم إمكانية تحقيق الردع الفاعل في هذا المجال. ولتحقيق ذلك، يهدف البحث إلى:

تحليل المرتكزات المفاهيمية للحرب السيبرانية وسماتها التي أعادت بها تعريف طبيعة الصراع الدولي.

تحديد وتصنيف آليات الهجمات السيبرانية وتحليل تأثيرها على هيكل وتوزيع القوة بين الفواعل الدوليين.

دراسة السياقات التطبيقية للصراع السيبراني من خلال تحليل نماذج حالات لمواجهات بين قوى دولية.

تقييم مدى جدوى وفعالية استراتيجيات الردع السيبراني الحالية في ظل التحديات العملية والقانونية التي تفرضها طبيعة هذه الحرب.

2.1. فرضيات البحث

لإرشاد عملية التحليل، يفترض البحث ما يلي:

- أدت الهجمات السيبرانية إلى بروز "قوة السايبر "كشكل جديد من أشكال القوة، مما أحدث تغييراً في علاقات القوى الدولية.
- صعوبة الإسناد وعدم توفر المصداقية يشكلان التحدي الأبرز الذي يُقوض فعالية الردع السيبراني التقليدي.
- الاستراتيجيات الكلاسيكية غير كافية لمواجهة التهديدات السيبرانية، وتفعيل الردع يتطلب الاعتماد على خيارات مرنة مثل الأنظمة البديلة وإعادة التأسيس السريع.

3.1. أهمية البحث

تتحدد أهمية هذا البحث من خلال مساهمته المتعددة المستويات، والتي تجمع بين القيمة الأكاديمية والتطبيق العملي على النحو التالي:

1.3.1. الأهمية العلمية والنظرية

- يقدم البحث إطاراً تحليلياً متكاملاً لظاهرة الحرب السيبرانية في الأدبيات العربية، التي لا تزال تعاني من ندرة في الدراسات الاستراتيجية العميقة في هذا المجال.

- يسهم في تطوير الفهم النظري لتحولات مفاهيم القوة والسيادة والصراع في العلاقات الدولية في عصر الرقمنة.

2.3.1. الأهمية التطبيقية والعملية

- يقدم تحليلاً استراتيجياً يمكن أن يكون مرتكزاً لصياغة سياسات أمنية وطنية فاعلة وبناء استراتيجيات شاملة للدفاع السيبراني.
- يساعد في تحديد متطلبات تحقيق الردع السيبراني وتصميم أنظمة أكثر فاعلية للإنذار المبكر والاستجابة للحوادث.
- يرفع مستوى الوعي الاستباقي لدى الأفراد والمؤسسات بأهمية الأمن السيبراني، ويقدم إطاراً لبناء القدرات في مجال الحماية من التهديدات الإلكترونية.

2. المنهج المعتمد

اعتمد البحث على المنهج الوصفي التحليلي، حيث تم استخدام الجانب الوصفي لتعريف الظاهرة وتحديد طرائقها ونماذجها التاريخية، واستخدام الجانب التحليلي في تفكيك الإشكالية المعقدة للردع السيبراني وتقييم التحديات التي تعترض تطبيقه.

1.2. السيبرانية (لغة واصطلاحا)

من أجل الوقوف على مفهوم السيبرانية، سنبحث في نطاق تعريفها لغةً واصطلاحاً في ضوء المعاجم اللغوية، وما أدرج عليها المختصون في القانون الدولي العام، وخبراء تكنولوجيا المعلومات.

أ- <u>في اللغة</u>

كلمة سايبر(Cyber) يونانية الأصل وترجع إلى مصطلح (kybernetes)، الذي ورد بداية في مؤلفات الخيال العلمي، ويعني القيادة أو التحكُّم عن بعد (Cresswell , 2010)

والسيبرانية في قاموس (المورد) هي علم الضبط، ومصدرها (Cybernetics)، (البعلبكي،٢٠٠٤) وهو مصدر يتطابق مع مفهوم الهجمات السيبرانية، أي ضبط الأشياء عن بعد والسيطرة عليها.

وأول من استخدم مصطلح السيبرانية عالم الرياضيات نوربرت وينر (Norbert wiener) وذلك في عام ١٩٤٨، في أثناء دراسته لموضوع القيادة والسيطرة والاتصال في عالم الحيوان، فضلاً عن حقل الهندسة الميكانيكية (Wiener, 1948)

وبالرجوع إلى المختصين في اللغة العربية نجد أن تحدياً يواجهونه في اختيار مصطلح مقارب لمصطلح (Cyber) في اللغة الانكليزية، لعدم وجود مصطلح مناظر في اللغة العربية. إلا ان الترجمة العربية لعنوان اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية كانت ترجمة صائبة، إذ تُرجِم العنوان (Cybercrime on Conven) إلى اللغة العربية (الاتفاقية المتعلقة بالجريمة الالكترونية) (مجلس أوروبا حول اتفاقية مجلس أوروبا المتعلق بالجريمة الالكترونية، 2001).

فيما عرف قاموس مصطلحات الأمن ألمعلوماتي، مصطلح السيبرانية بالقول: "هجوم عبر الفضاء الالكتروني يهدف إلى السيطرة على مواقع الكترونية أو بنى محمية الكترونياً لتعطيلها أو تدميرها أو الأضرار بها (Kissel, 2013).

أما سبب اختيار هذا البحث لمصطلح السيبرانية ، فيعود إلى المصطلح الذي استخدمه نوربرت وينر في كتابه الذي ذكرناه سابقا (Cybernetic) ، لعدم وجود مصطلح متفق عليه في اللغة العربية من جهة، ولأن الوثائق الصادرة عن الأمم المتحدة باللغة العربية، استخدمت مصطلح السيبرانية نفسه من جهة أخرى (مكتب الأمم المتحدة المعني بالمخدرات والجريمة، 2013).

ب- اصطلاحا

تبرز عدة مصطلحات حول موضوع البحث فنجد مصطلح الهجمات السيبرانية(Cyber Attack) ومنهم من تبنى مصطلح الفضاء السيبرانيلسيج، (Cyber Space)لورنس. (2006)، بالاستناد إلى المحيط الذي تجري فيه العمليات السيبرانية الناشئة عن أداء أنظمة الكترونية مهمتها متابعة وجمع المعلومات التي تعمل الكترونياً

وتحليلها ومن ثم اتخاذ إجراءات محددة لمهاجمتها عن طريق أنظمة الكترونية أخرى مخصصة لهذا الغرض (. Lewis, 2010)وتبنى آخرون مصطلح الحرب السيبرانية (Cyber Warfare) بالاستناد إلى أيدلوجية أمنية أو عسكرية، تضع منهاجاً لتحقيق أهداف على الصعيد الأمني أو العسكري تجاه (العدو المفترض) (Shin, 2011). وفي هذا البحث سوف نعتمد مصطلح الهجمات السيبرانية كونها أقرب للواقع الحالي المعاش على مستوى الدول. فالمقصود بالهجمات السيبرانية وأشهر تعريف لها " إنها الأفعال الصادرة من أجهزة الحاسوب وشبكات المعلومات التابعة لدولة ما بشكل منظم ومدروس على أجهزة حاسوب وشبكات معلومات لدولة أخرى بغرض التجسس Espionage أو التخريب **Sabotage او** التوجيه". (Saalbach, 2014).

ومن الممكن أن تكون الهجمات السيبرانية وسيلة وطريقة في الوقت نفسه، وبعبارة أخرى يعتمد ذلك على الهدف من استخدامها ، فقد تسهم في توجيه العمليات العسكرية الأخرى كالصواريخ بعيدة المدى أو الطائرات بدون طيار (Drawn) لتحديد أهداف عسكرية منتخبة وتدميرها أو لتعطيل أجهزة الكشف المبكر للهجمات التي يقوم بها سلاح جو معادي أو وقف عمليات الاتصال في المطارات العسكرية أو المدنية (الهجوم الذي قامت به إسرائيل عام 2007 ضد سوريا، إذ توقفت أجهزة الرادار وباقي منظومات الاتصال في المطارات العسكرية والمدنية عن العمل ، في أثناء الهجوم الذي نفذه سلاح الجو التابع لها على مواقع سورية زعمت إسرائيل أنها منشآت ، و في هذه الحالة يعد الهجوم السيبراني طريقة قتالية، إذ يدخل ضمن الخطط العسكرية لمفاعل نووي وبالتالي هو طريقة قتالية.) (Rid & Mcburney, p. 6).

وعلى العكس قد تكون الهجمات السيبرانية وسيلة قتالية ، من خلال استخدامها بذاتها، للتسلل إلى أنظمة الكترونية معدة لحماية أو لتنظيم سير عمل منشآت حيوية، كمحطات توليد الطاقة النووية أو السدود أو وسائل النقل كالمطارات، بهدف تطويعها والسيطرة عليها، لتدمير ذاتها بذاتها من خلال تغذيتها بمعلومات خاطئة لأجهزة التحكم والحماية الالكترونية (ما تعرضت إليه محطة (نطانز) النووية الإيرانية من هجوم سيبرآني عام 2009، وأعلنت عنه الولايات المتحدة في عام 2011، إذ استخدمت برنامجاً ويدعى (Stuxnet) عطل بعضاً من العمليات الحساسة والحق أضراراً جزئية في عمليات تخصيب اليورانيوم، وهو ما يمكن معه عد هذا الهجوم سابقة في حقل الهجمات السيبرانية) (Gervais, 2012, p. 46).

إن التمييز بين وسائل وطرائق القتال، إنما يعتمد على الهدف من استخدامها والنتيجة التي ستؤديها، فكلما كانت تتسبب بطريق مباشر أو غير مباشر بقتل أو جرح أو تدمير أو تعطيل كلي أو جزئي، فتعد وسيلة قتالية، أما إذا استخدمت كجزء من مخطط عسكري فتعد طريقة قتالية تخضع للنظام القانوني الدولي (الجمعية العامة للأمم المتحدة، 1977). وهو ما تتصف به الهجمات السيبرانية في الاثنين معاً.

2.2. **طرائق الهجمات السايبرانية ومميزاتها**

1-تعتمد الهجمات السيبرانية أساسا على الوحدات السيبرانية التي تضم الجنود السيبرانيين وهم بالأصل قراصنة رقميون يتم استخدامهم على شكل فرق متخصصة واعطائهم إمكانات لوجستية وسيرفرات على شبكات المعلومات وتوجيههم لأغراض محددة مثل مراقبة كل شبكات المعلومات الحساسة (شبكات الطاقة، المياه، الكهرباء، الاتصالات، الأمور المالية في البنوك..) او الرد على أي هجمات او التجسس او توجيه راي العام لدول معادية. وكانت معظم الهجمات الالكترونية سابقا تُشن بواسطة أشخاص أو مبرمجين لأهداف شخصية أما في العقدين الأخيرين دخلت المنظمات الأمنية والحكومات إلى هذه الساحة وأخذت تنفق الملايين لتطوير قدراتها وبناء جيوش إلكترونية للدفاع عن منشآتها وشن الهجمات المضادة. وبرزت إسرائيل وأميركا والصين وروسيا وإيران والمملكة المتحدة وكوريا الشمالية وفرنسا في مقدمة الدول المتقدمة في تقنيات الحرب الإلكترونية.

تنقسم الهجمات السيبرانية الى نوعين رئيسين:

- هجمات تعطيل جهاز الكمبيوتر المستهدف.
- هجمات يكون الغرض منها الوصول الى بيانات جهاز الكمبيوتر المستهدف وربما الحصول على امتيازات المسؤول عنه.

ومن طرائق الهجمات السيبرانية نذكر:

- الطريقة الأولى

إرسال روابط بشكل واسع عن طريق برامج التراسل لعدة مستخدمين وتعزز هذه الرسائل بخاصية تتيح التحكم بحساب كل من يفتحها حيث تمكن القراصنة الالكترونيين من الوصول الى بيانات وحسابات للمستخدمين المصرفية حتى او كلمات سر تابعة لهيئات حكومية رسمية.

- الطريقة الثانية

أن يقوم الهاكر بتجهيز عدة سيرفرات سريعة تقوم بإرسال ملايين الطلبات بوقت واحد الى موقع او عدة مواقع الكترونية مما يؤدي الى توقف عملها وهذا يكلف خسائر مالية خصوصا اذا كانت هذه الخدمات المقدمة حكومية او تابعة لهيئات مالية حيوية، فيجري استهداف البنوك أو المواقع الحكومية التي تحتوي على بيانات مهمة، أو حتى استهداف منشآت صناعية.

- الطريقة الثالثة

أن يقوم الهاكر بإنشاء مواقع بأسماء تكون قريبة جدا من أسماء مواقع عالمية موثوقة مثل apple او google ويرسل emails يطلب فيها فحص كلمة السر أو تغييرها ، فيظن المستخدم أنها الشركة العالمية ذاتها وبمجرد وضعه لكلمة السر يتحكم الهاكر ببيناته الخاصة وهذا له تأثير كبير إذا تم على مستوى الدول.

تُشكل الهجمات السيبرانية تحديًا استراتيجيًا غير مسبوق في العلاقات الدولية، حيث تجمع بين خصائص فريدة أعادت تعريف مفهوم الصراع المعاصر. فمن ناحية، تتميز هذه الهجمات بطبيعة غامضة تسمح للدول والفواعل من غير الدول.

بممارسة أعمال عدائية تحت عتبة الحرب التقليدية، مما يخلق منطقة رمادية تتحدى الأطر القانونية والسياسية القائمة. وتتعمق هذه الإشكالية مع صعوبة نسب الهجمات لمصادرها الأصلية، حيث تتداخل التقنيات المتطورة وآليات التمويه والتغطية، مما يخلق بيئة خصبة لإنكار المسؤولية ويضعف آليات الردع التقليدية.

وتمثل هذه الهجمات تحديًا للسيادة التقليدية، حيث تذوب الحدود الجغرافية وتصبح البنى التحتية الحيوية - سواء أكانت أرضية أم فضائية - عرضة للاستهداف. وهذا يوسع بشكل غير مسبوق من نطاق الصراع، حيث تتحول الشبكات الرقمية إلى ساحة معركة مفتوحة على مدار الساعة. وتتفاقم هذه التحديات مع الميزة النسبية لهذه الهجمات من حيث التكلفة، حيث تتيح للدول الصغيرة والفواعل من غير الدول منافسة القوى العظمى بتكاليف محدودة، مما يعيد رسم خريطة توازنات القوى الدولية.

وتتميز هذه الهجمات بطبيعة ازدواجية معقدة، حيث يمكن لنفس الأدوات والتقنيات أن تستخدم لأغراض دفاعية وهجومية، وأن تنتقل بسرعة بين أغراض التجسس والإعاقة والتدمير. وهذا الازدواجية تخلق تحديات كبيرة في التمييز بين الأنشطة العدائية والعمليات الروتينية، وتجعل من الصعب وضع ضوابط واضحة للاستخدام المشروع. كما تبرز الآثار الجيوسياسية العميقة لهذه الهجمات، حيث تصبح الشركات التقنية العالمية فواعل رئيسية في المشهد الجيوسياسي، وتتحول البيانات إلى سلعة استراتيجية، وتتأثر سيادة الدول بقدرتها على حماية فضاءها السيبراني.

ولا يمكن إغفال القدرة التدميرية المتصاعدة لهذه الهجمات، حيث تطورت من مجرد أعمال تخريبية محدودة إلى تهديد وجودي يمكن أن يعطل البنى التحتية الحيوية ويؤدي إلى خسائر بشرية واقتصادية كارثية. وأخيرًا، تتفرد هذه الهجمات بعنصري التوقيت والسرعة، حيث تتميز بغياب المؤشرات التحذيرية التقليدية، وتنفذ بسرعة البرق، مما يحول دون الاستباق ويحد من فرص التصدي الفعال. وهذه الخصائص مجتمعة تجعل من الهجمات السيبرانية تحديًا استراتيجيًا يستدعي تطوير أطر تحليلية جديدة وأدوات استجابة مبتكرة.

3.2. المبحث الثالث: الصراع الدولي السيبراني بين النشأة والنماذج

بات الفضاء السيبراني أحد الركائز الأساسية التي تُشكّل هيكل النظام الدولي المعاصر، حيث يمثل منصة استراتيجية توفر أدوات تكنولوجية متطورة لدعم عمليات الحشد والتعبئة على المستوى العالمي. كما يمارس تأثيراً عميقاً في تشكيل القيم السياسية السائدة، وقد ازداد نطاق هذا التأثير مع سهولة الاستخدام وانخفاض التكلفة، مما وسّع من قدرته على اختراق مختلف المجالات الحياتية.

فلم يعد التأثير مقتصراً على الجوانب السياسية والعسكرية التقليدية، بل امتد ليشمل القطاعات الاقتصادية والأنسجة الاجتماعية وحتى البنى الأيديولوجية. وأصبح من الواضح أن القدرة على توظيف هذا الفضاء بكفاءة تشكل عاملاً حاسماً في تحقيق الأهداف الاستراتيجية للدول والجهات الفاعلة، كما تزيد من قدرتها على توجيه سلوكيات المستخدمين داخل هذه البيئة الرقمية.

ومن الأمور المتعارف عليها في العلاقات الدولية أن مصادر قوة الدولة وأشكالها تتغير، فإلى جانب القوة الصلبة ممثلة في القدرات العسكرية والاقتصادية، تزايد الاهتمام بالأبعاد غير المادية للقوة، ومن ثم بروز القوة الناعمة التي تعتمد على جاذبية النموذج والإقناع، ومع ثورة المعلومات ظهر شكل جديد من أشكال القوة هو قوة السايبر (power Cyber)، ويعد جوزيف ناي (Nye. Joseph) من أبرز المهتمين بالقوة السيبرانية، حيث يعرفها بأنها: "القدرة على الحصول على النتائج المرجوة من خلال استخدام مصادر المعلومات المرتبطة بالفضاء السيبراني، أي أنها القدرة على استخدام الفضاء السيبراني لإيجاد مزايا للدولة، والتأثير على الأحداث المتعلقة بالبيئات التشغيلية الأخرى وذلك عبر أدوات سيبرانية " (Nye, 2010, p. 3).كما يوضح ناي أن مفهوم القوة السيبرانية يشير إلى "مجموعة الموارد المتعلقة بالتحكم والسيطرة على أجهزة الحاسبات والمعلومات والشبكات الالكترونية والبنية التحتية المعلوماتية والمهارات البشرية المدربة للتعامل مع هذه الوسائل ، والتي لها تأثير كبير على المستوى الدولي والمحلي، فمن ناحية أدت إلى توزيع وانتشار القوة بين عدد أكبر من الفاعلين مما جعل قدرة الدولة على السيطرة موضع شك، ومن ناحية أخرى منحت الفاعلين الأصغر قدرة أكبر على ممارسة كل من القوة الصلبة والقوة الناعمة عبر الفضاء السيبراني، وهو ما يعني تغيرا في علاقات القوى في السياسة الدولية .

والجدير ذكرنه أن التسللات ليست بالأمر الجديد، فبقدر قَدم العصور الرومانية، كانت الجيوش تعترض اتصالات العدو. في الحرب الأهلية الأمريكية (Glantz, 2011, p. 57). استخدم جنرالات الاتحاديين والكونفدراليين (الانفصاليين) أجهزة التلغراف الجديدة لإرسال أوامر مزيفة إلى العدو. أثناء الحرب العالمية الثانية، Kahn, (1996) كسر خبراء التشفير البريطانيون والأمريكيون رموز الشفرة الألمانية واليابانية، وكان هذا عنصرا أساسيا في انتصار الحلفاء (ظل بعد ذلك سرا طوال أعوام كثيرة). وفي العقود القليلة الأولى من الحرب الباردة أيضا كان الجواسيس الأمريكيون والروس يعترضون على نحو دوري ومنتظم اتصالات بعضهم ببعض من إشارات راديوية

(لاسلكية)، وبث للموجات الميكروية (الميكروويف)، واتصالات هاتفية. ولم يقتصر الهدف على جمع معلومات استخباراتية بشأن نوايا وقدرات الطرف الآخر، بل إضافة إلى ذلك، الحصول على أفضلية في الحرب الجسيمة المخيفة المقبلة.

أ- النشأة:

هناك من يجد أنّ أفكار الهجمات السيبرانية بدأت في أمريكا منذ الثمانينات خلال عهد الرئيس رونالد ريغان، الذي رأى أنه من الممكن أن تتعرّض بلاده لخطر مثل هذه الهجمات، فأفرز فكرة مميزة وسابقة لأوانها، أنتجت "وحدة السياسة القومية بشأن الاتصالات وأمن نظم المعلومات" التي تطوّرت خلال التسعينيات، واستخدمها الجيش في عمليات الاستشعار عن بعد، وظهرت الحاجة إليها وإلى تقنياتها خلال "الحرب على العراق في 2003" (كابلان، 2019) أن استراتيجية الهجمات السيبرانية الأمريكية كانت ولا تزال، متأثرة بالأولويات الجديدة للصناعة العسكرية الإسرائيلية، المصنفة بالبالغة السرية، والتي تستهدف تباعاً الصناعة النووية الإيرانية (المركز الاستشاري للدراسات والتوثيق، 2014، ص. 17) والصناعات الدفاعية الأوروبية المفترض أنها تعود لبلدان حليفة. وفي الجهة الأخرى من العالم كانت هنالك توجهات للخصم التقليدي، ونقصد به روسيا الاتحادية (Giles, 2011, p. 47)، فقد كانت الأسبق في نطاق الاستعداد للهجمات السيبرانية. ولقد قامت بعض دول العالم بالفعل نفسه في السنوات الأخيرة وعملت على تطوير استخدام مهارات الإنترنت والحواسيب كأدوات هجوم ودفاع واستخبارات وحروب نفسية. فقد أنشأت كل من بريطانيا وفرنسا وكوريا الجنوبية وحدات خاصة في قوّاتها المسلحة مسؤولة عن الحرب الإلكترونية أو حرب المعلومات. وفي مايو 2009، أدخلت شركة American Security اسم إيران بين الدول الخمسة التي تتمتع بأقوى قدرات إنترنت في العالم، وتجمع هذه الوحدات الخاصة ما بين العقل العسكري والمهارات التقنية التي تمكّنها من الدفاع وصدّ الهجمات أو إحداث خسائر. من ناحية أخرى، يتزايد استخدام الإنترنت بشكلٍ عام، ووسائل التواصل الاجتماعي بشكلٍ خاص، كأداة فعالة في الحرب التي تشنها التنظيمات المسلحة لا سيما في الشرق الأوسط. فقد وجدت هذه المجموعات في الفضاء الإلكتروني وسيلة مفيدة في صراعها، فاستخدمت وسائل التواصل الاجتماعي لتجنيد المقاتلين. كما استفادت هذه

التنظيمات من الفضاء الإلكتروني كمنصّة لإطلاق الحرب النفسية ضد الخصوم بتصوير مشاهد العنف ونشرها على نطاق واسع لبثّ الرعب والذعر.

وعليه نجد أن العديد من الدول، اليوم، تصرف المليارات على الأنشطة السيبرانية استعداداً لحروب المستقبل، حيث تبني استراتيجيات حرب المعلومات، والتي يتمّ خوضها بهدف التشتيت، وإثارة الاضطرابات في عملية صناعة القرار لدى الخصوم، عبر اختراق أنظمتهم، واستخدام ونقل معلوماتهم حتى لا تذهب الحروب لمصلحة من يملك القوة فقط، وإنما القادر على شلّ القوة، والتشويش على المعلومة، بل وربما تغيير البيئة الثقافية والفكرية للخصوم والتأثير بها قدر الممكن.

ب- نماذج عن الهجمات السيبرانية

يسجل لنا التاريخ المعاصر، نماذج للهجمات السيبرانية، سوف نأتي على ذكر بعضها فقط، وأولها الهجوم السيبراني الذي نفذته الولايات المتحدة الأمريكية وصرحت به عام 1982 ضد منظومة التحكم العالية صناعياً في أنبوب نفط (Chelyabinsk) التابع للاتحاد السوفياتي السابق، وهو ما نفاه الاتحاد السوفياتي السابق آنذاك (Canabarro & Borne, 2013, p. 10).

أما النموذج الآخر، فهو ما تعرضت له أنظمة الاتصال الالكترونية التابعة لوزارة الدفاع الأمريكي (Pentagon)ووكالة الفضاء الأمريكية(NASA) ووكالة الطاقة الأمريكية (Department -Energy) لهجمات سيبرانية بين الأعوام 1998 -2000، والذي أدى إلى الاستحواذ على الآلاف من الملفات المصنفة بأنها عالية السرية، وقد وجهت الولايات المتحدة التهمة رسمياً إلى روسيا الاتحادية، في حين أنكرت الأخيرة -آنذاك- مسؤوليتها عن هذا الهجوم.

وفي كانون الثاني من العام 2017، كشف تقرير لوكالة الاستخبارات الأميركية عملية قرصنة على الانتخابات الرئاسية الأميركية الأخيرة حيث افاد التقرير «أنّ الرئيس الروسي فلاديمير بوتين أمر بحملة تأييد لمصلحة الرئيس ترامب، خلال الانتخابات» وأوضح «أن الروس حاولوا تقويض إيمان المواطنين بالعملية الديمقراطية الأميركية، وتشويه سمعة الوزيرة هيلاري كلينتون، والتأثير في حظوظها الانتخابية». وذلك، حسب التقرير، بسبب رغبة

روسيا في تقويض النظام الديمقراطي الحر الذي تقوده الولايات المتحدة الأميركية، وهذه العمليات الروسية باتت أكثر تصعيدًا في مباشرتها ومستوى نشاطها وسِعَة جهودها، إذا ما قورنت بعملياتها السابقة.

وقد تكون أكثر الهجمات حداثةً، ما تقوم به الولايات المتحدة وإسرائيل بشأن البرامج النووية الإيرانية، لقد شنّت الولايات المتحدة الأميركية قبيل أعوام من توصل المجتمع الدولي إلى الاتفاق النووي مع طهران (2015)، حربًا سيبرانية على مشروع إيران النووي بهدف إضعاف قدراتها النووية، وإجبارها على التنازل على طاولة المفاوضات. لكنّ الولايات المتحدة نفسها لم تكن بمأمن من الحرب السيبرانية، ففي عام 2018 وجّهت وزارة العدل الأميركية اتهامات جنائية وفرضت عقوبات على شركة إيرانية و9 إيرانيين ناشطين في معهد «مبنا» الإيراني، لاختراقهم أنظمة مئات الجامعات والشركات، بهدف سرقة البحوث والبيانات الأكاديمية والملكية الفكرية. وكانت إيران قد استهدفت الأنظمة الإلكترونية لشركة نفط أرامكو عام 2017، حيث أجبرت قوة الهجوم السلطات على استبدال مجمل الشبكة الالكترونية التي تعمل عليها الشركة، وتبع ذلك تغيير كثير من الأجهزة العاملة (Jawal Max, 2018). فهل الحرب السيبرانية هي أكثر ميدان مرشح للتصاعد خلال الفترة القادمة بين الولايات المتحدة وإيران؟ سيما وأن هناك تعامل متبادل بين إيران وروسيا من جهة وإيران والصين من جهة أخرى ، وروسيا والصين تعتبران من "الطبقة الأولى" في امتلاك القدرات الالكترونية والهجمات السيبرانية، كما وأن القدرات الفنية للقوات السايبرانية الإيرانية أصبحت واضحة جدًا، حيث تمكنت من التسلل مرارًا إلى الحكومات الغربية وشبكات الاستخبارات الإقليمية، فعلى الرغم من كل الإجراءات الأمنية التي تم اتخاذها في ديسمبر 2011، أشار المدير التنفيذي لشركة Google إريك شميدت، في مقابلة مع شبكة CNN الأمريكية، إلى أن الإيرانيين موهوبين على نحو غير معتاد في الحروب السيبرانية الحديثة، وذلك لأسباب لا تفهمها الولايات المتحدة.

و في الآونة الأخيرة وتحديدا في نيسان من العام 2020 أعلنت إسرائيل عن هجوم سيبراني استهدف شبكات المياه الخاصة بها واتهم الإسرائيليون إيران بالمسؤولية عن الهجوم في حين ان إسرائيل والولايات المتحدة الأميركية قد اطلقتا اكثر من فيروس لاستهداف المنشآت النووية الإيرانية وآخرها ما وقع في شباط وايار وتموز من العام 2020 بحيث اقر وزير الأمن الإيراني " محمود علوي" بان هناك اكثر من مليوني هجوم سيبراني وقع بين عامي 2019

و2020 وبحسب وزير الأمن ان إسرائيل وأميركا والسعودية مصدرها علما ان الأخيرة تعمل على تدريب 5000 عنصر في البانيا لهذا الغرض.

ويمكن القول في ضوء تلك النماذج، إنه رغم اختلاف غرض وهدف كل حالة من الحالات السابقة، إلا أنه من الواضح أن حجم الهجمات السيبرانية يتزايد بشكل حاد، ولذا يصعب تحديد حجمها الحقيقي وبخاصة أن عديد منها لا يتم التبليغ عنه .وتتمثل القواسم المشتركة بين تلك الحالات في صعوبة تحديد مرتكبي تلك الهجمات على وجه الدقة، وغياب الرد المضاد، كنتيجة لها. والأهم أنها ليست حكرًا على الدول المتقدمة ذات أنظمة المعلومات الهائلة والمتطورة فحسب. وعليه نرجح بأن حروب المستقبل حتما ستكون حروبا سيبرانية، وعلى الأقل في جزء منها؛ حيث ان الفضاء السيبراني قد وِسم رسميا على أنه «ميدان» للحرب، مثل الجو، والبر، والبحر، والفضاء الخارجي. ونظرا إلى سلاسة وانسيابية الشبكة الحاسوبية العالمية، وبسبب حزم البيانات، وإنترنت الأشياء، فإن الحرب السيبرانية لن تشتمل على الجنود، والبحارة، والطيارين فقط؛ ولكنها، حتما ستتضمن البقية منا. حينما يكون الفضاء السيبراني في كل مكان، فإن الحرب السيبرانية يمكن أن تتسرب وتنضح عبر كل المسام الرقمية.

4.2. العمليات السيبرانية بين الأمن والردع

الأمن السيبراني (cybersecurity) مصطلح حديث، ويطلق عليه أيضا " امن المعلومات" وأمن الحاسوب" وهو فرع من فروع التكنولوجيا يعنى بممارسة حماية الأنظمة والممتلكات والشبكات والبرامج من الهجمات الرقمية، التي تهدف عادة الوصول الى المعلومات الحساسة او تغييرها او اتلافها او ابتزاز المال من المستخدمين أو تعطيل العمليات. ويعرفه "ادوارد اموروسو (Edward Amoroso) " بانه مجموع الوسائل التي من شأنها الحد من خطر الهجوم على البرمجيات او أجهزة الحاسوب او الشبكات. وتشمل تلك الوسائل الأدوات المستخدمة في مواجهة القرصنة وكشف الفيروسات الرقمية ووقفها، وتوفير الاتصالات المشفرة " (هارفارد بزنس ريفيو العربية، تاريخ غير متوفر).

تؤدي الطبيعة الخاصة للهجمات السيبرانية، التي تتسم بالمجهولية وعدم التماثل، إلى إعادة تعريف مفهومي القوة والصراع في العلاقات الدولية بشكل جذري. في السابق، كانت القوة تُقاس غالبًا من خلال العوامل

العسكرية والاقتصادية، ولكن مع ظهور الهجمات السيبرانية، أصبح الفضاء الرقمي يمثل ساحة جديدة للصراع. يمكن للدول أو الجماعات الصغيرة أن تستهدف القوى الكبرى بطرق غير تقليدية، مما يغير من ديناميكيات القوة التقليدية. هذا التحول يسلط الضوء على أهمية المعلومات والقدرة على الوصول إليها، حيث يمكن لمهاجم مجهول أن يؤثر على بنى تحتية حيوية أو ينشر معلومات مضللة، مما يعيد تشكيل موازين القوى.

في سياق استراتيجيات الردع، تواجه الدول تحديات كبيرة. فالهجمات السيبرانية غالبًا ما تُنفذ من قبل جهات غير معروفة، مما يجعل من الصعب تحديد هوية المهاجمين وتطبيق الردود المناسبة. هذا الإخفاء يعقد من قدرة الدول على الرد الفعال، حيث يمكن أن يؤدي إلى ردود فعل مبالغ فيها أو غير متناسبة، مما يزيد من حدة الصراع. بالتالي، تصبح استراتيجيات الردع السيبراني أكثر تعقيدًا، حيث تحتاج الدول إلى تطوير أدوات جديدة للتعامل مع هذه التهديدات، بما في ذلك تعزيز القدرات الاستخباراتية والقدرات الدفاعية في الفضاء السيبراني.

أما بالنسبة للأطر القانونية الدولية، فهي تواجه تحديات كبيرة في تنظيم الفضاء السيبراني ومواجهة تحدياته. القوانين الحالية غالبًا ما تكون غير كافية للتعامل مع الطبيعة المتغيرة للهجمات السيبرانية. تفتقر العديد من الدول إلى القوانين الملائمة التي تعالج قضايا مثل المسؤولية الدولية عن الهجمات السيبرانية، وحقوق الأفراد والدول في الفضاء الرقمي. لذلك، يتطلب الأمر تطوير آليات قانونية جديدة تتناسب مع طبيعة الهجمات السيبرانية وتسمح بتحقيق العدالة ومحاسبة المتورطين.

علاوة على ذلك، تتطلب هذه الديناميكيات الجديدة تعاونًا دوليًا موسعًا، حيث يجب على الدول العمل معًا لتحديد معايير مشتركة وتطوير استراتيجيات فعالة لمواجهة التهديدات السيبرانية. يشير البحث إلى أن الفهم التقليدي للقوة والصراع بحاجة إلى إعادة نظر، ويجب على المجتمع الدولي تعزيز التعاون وتطوير استراتيجيات جديدة لمواجهة هذه التحديات المعقدة. إن معالجة هذه الإشكاليات تتطلب أيضًا زيادة الوعي بين الأفراد والمؤسسات حول أهمية الأمن السيبراني ودوره في حماية المصالح الوطنية.

بالمجمل، يبرز هذا التحليل الحاجة إلى إعادة تقييم شاملة لمفاهيم القوة والصراع، مع التركيز على أهمية تكامل الجهود الأمنية والتشريعية لمواجهة التحديات المتزايدة في الفضاء السيبراني.

ومن هنا نجد أن ظهور الأمن السيبراني ارتبط بظهور الهجمات السيبرانية كونها باتت تشكل خرقا للأمن القومي، وهذا بسبب تأثير التكنولوجيا على المفاهيم ذات الصلة كالقوة powerوالسيادة ,sovereignty الحوكمة العالمية global governanceوالأمنية . securitization ، ونظرا لطبيعة الفضاء السيبراني، حيث انه ساحة عالمية عابرة لحدود الدول، تمتد قضية الأمن السيبراني من داخل الدولة إلى مجموعة النظام الدولي، ومع وجود مخاطر تهدّد الفاعلين جميعًا في مجتمع المعلومات العالمي تصبح القضية مرتبطة بالأمن العالمي. ومن هنا كانت اول محاولة لوضع معاهدة دولية لمراقبة الفضاء السيبراني وما يتصل به في العام 2001، وأسهمت اللجنة الدولية للصليب الأحمر بصفتها مراقبًا، في نشر ما يُعرف بـ«دليل تالين للقانون الدولي المُطبَّق على الحرب الإلكترونية". هذ بالإضافة إلى بروز اتجاهات متعدّدة لتحقيق هذا الأمن، وذلك عبر التنسيق بين أصحاب المصلحة من الحكومات، والمجتمع الأهلي، والشركات التكنولوجية، ووسائل الإعلام، وغيرها للحفاظ على خصوصية وحرية وتفكير وحق الفرد في حفظ بياناته دون اختراق .و قد بات الأمن السيبراني يشكل جزءاً أساسياً من أي سياسة أمنية وطنية، حيث بات معلوماً أن صناع القرار في الولايات المتحدة الأمريكية، الاتحاد الأوروبي، روسيا، الصين، إيران وغيرها من الدول، أصبحوا يصنفون مسائل الدفاع السيبراني/الأمن السيبراني كأولوية في سياساتهم الدفاعية الوطنية، هذا بالإضافة الى تشييد قوة سيبرانية تقوم بالهجوم من خلال برمجيات خاصة . فنجد بأن أغلب الجيوش في العالم يمتلك وحدة امن الكتروني ووحدة امن الدفاع عن الهجمات السيبرانية، لذا نجد بأن الأمن المعلوماتي لم يعد حكراً على الشركات أو المؤسسات صاحبة العلاقة، بغية حفظ البنوك ومعطياتها من أي استهداف، بل أضحى أيضاً يشكّل رهاناً قوياً وتحدياً كبيراً بوجه الدول والحكومات، بحيث تحولت وحدة الأمن الالكتروني الى قيادة قتالية منفصلة عند الدول الكبرى. وهنا تتجلى استراتيجيات المواجهة لتطرح إشكالية مدى إمكانية تحقيق الردع السيبراني لمنع الأعمال الضارة ضد الأصول الوطنية في الفضاء، والذي يرتكز على ثلاثة ركائز هي: مصداقية الدفاع، والقدرة على الانتقام، والرغبة فيه (بوفر، 1970، ص. 31). ولعل ما شهده الواقع المعاصر من حالات متباينة تطال الدول المتقدمة والنامية على حد

سواء، يؤكد ويعزز تلك الحاجة، ولكن إلى أي مدى يمكن ردع تلك الهجمات، وما هي طبيعة التحديات التي تعترض ذلك المدى؟

5.2. تحديات الردع السيبراني

إن عملية الردع تواجه تحديات أبرزها:

- أولا: الإسناد (تحديد مرتكب الهجمات بدقة)، من شأن الردع السيبراني أن يفشل طالما لم يعلن الجاني رسميًا عن مسؤوليته عن الهجوم؛ اذ يمكن لأي شخص أن يكون هو الجاني في الهجمات السيبرانية، وبخاصة أن المعدات اللازمة لشن هجوم سيبراني يمكن الوصول لها، وليست مكلفة، ويمكن شنها من أي مكان تتوافر فيه خدمة الإنترنت. فلكي يعمل الردع لابد من أن يقلق المهاجم من كشف هويته، ومن ثم تعرضه للعقاب أو الانتقام، بيد أن صعوبة تحديد مرتكب الهجمات بدقة، قد يسفر عن استهداف طرف ثالث لا علاقة له بالهجوم الاولي، وهو الأمر الذي لا يُضعف فقط من منطق الردع وفلسفته، لكنه يخلق عدوًا جديدًا أيضًا. فعدم التغلب على تلك الإشكالية يعني تكرار الهجمات مرة أخرى دون تعرض المهاجم للعقاب، أو بعبارة أخرى، تحسين سبل الإسناد ضرورة لفعالية الردع.
- ثانيا: العقبات القانونية، التي لا يمكن تطبيقها حاليا على الهجمات السيبرانية إلا بشكل غير مباشر، لان جرم القانون الدولي منسوب الى العدوان العسكري، ولكن ماذا عن الهجوم السيبراني الذي أسفر عن انفجار قاعدة عسكرية؟ وهل يحق للدولة – إعمالًا لحقها الأصيل في الدفاع عن النفس – استهداف أهداف عسكرية ضد تلك الدولة أو حتى شن هجوم سيبراني مضاد؟! لا يزال النقاش دائرًا حول المسائل القانونية المتعلقة بالهجمات السيبرانية. وعليه، قد يبدو الرد الانتقامي عملًا عدوانيًا غير مبرر أو مخالفًا لقواعد القانون الدولي (Wei, 2015).
- ثالثا: الفاعلون من غير الدول، الذين يمكن لهم إحداث أضرار بدرجات مختلفة، مما يضفي مزيدًا من التعقيد على الردع السيبراني نظرًا لصعوبة استهداف هؤلاء الفاعلين، وهنا المقصود المنظمات الإجرامية، والجماعات الإرهابية، والنشطاء السياسيين، وغيرهم، مما يدعو للتساؤل عن جدوى الرد

الانتقامي، ماذا إذا وُجد هذا الفاعل داخل دولة ما، ووفرت له دولة أخرى الحماية، أيهما يتحمل المسؤولية؟

- رابعا: المصداقية، فهي غير متوفرة في الفضاء السيبراني لكلا الجهتين، بسبب عدم توفر اسناد الهجوم الى مرتكبيه من جهة، ولان الأسلحة السيبرانية خفية وغير مرئية إلى أن يُقدم طرف ما على استخدامها. ولذلك، لا يمكن للمهاجم أن يعرف إذا امتلك الخصم القدرة على الرد أو الانتقام هذا من جهة ثانية (Cohen, 2005).

ولا يمكن تجاهل ثغرة اتساع مفهوم الردع السيبراني حيث انه يطال مجالات عدة مثل: الاتصالات، والتجارة، والأعمال التجارية، والتعليم، والتدريب، وأكثر من ذلك. لذا، بناء استراتيجية فاعلة للردع في الفضاء السيبراني يتطلب تجاوز الحديث عن المجال ككل إلى الحالات التي يمكن للردع أن يكون فاعلًا فيها، الا ان الحديث اليوم عن الردع السيبراني بات أكثر مرونة، وذلك من خلال مقاربات مختلفة، ويمكن تداولها بخيارين مختلفين:

الخيار الأول:

استخدام الأنظمة البديلة: ذلك يكون من خلال اعتماد الدولة أنظمة بديلة وليس الاعتماد على نظام واحد، يتم اختراقه بسهولة، ما يؤدي الى نتائج وخيمة؛ وبخاصة إذا تعلق هذا النظام بالبنية التحتية الرئيسية للدولة، وهذا يمكن الدولة من استخدام خيارات أخرى في حال تعرضها الى هجوم سيبراني، بحيث تلجأ الى الاستعانة بتلك الأنظمة البديلة أو الاحتياطية.

الخيار الثاني:

إعادة التأسيس: **وهذا يعتمد على التوقيت**، فإذا تمكنت الدولة التغلب على الهجوم الذي تتعرض له بسرعة، وإعادة تشغيل النظام، ستكون الآثار هامشية. ولكن الطريقة الوحيدة لتجنب الهجوم هي الاحتجاب عن الجميع، ورغم كونه السبيل الأفضل للردع، إلا أنه يكتنفه مسائل قانونية عدة.

وبناء على ما تقدم سعى هذا البحث إلى تحليل الآثار الناجمة عن الحرب السيبرانية على مفاهيم القوة والصراع في العلاقات الدولية، وتقييم إمكانية تحقيق الردع الفاعل في هذا المجال. إذ تناول المرتكزات المفاهيمية

للحرب السيبرانية وسماتها الفريدة التي تعيد تعريف طبيعة الصراع الدولي، لا سيما من خلال عدم التماثل الذي يتيح للفاعلين الضعفاء استهداف القوى الكبرى بطرق غير تقليدية. كما هدف إلى تحديد وتصنيف آليات الهجمات السيبرانية، مثل الهجمات على البنية التحتية الحيوية والهجمات المعلوماتية، وتحليل تأثيرها على هيكل وتوزيع القوة بين الفواعل الدوليين. بالإضافة إلى ذلك، وتناول السياقات التطبيقية للصراع السيبراني من خلال نماذج حالات لمواجهات بين قوى دولية، مما يتيح فهماً أعمق لاستراتيجيات الردع المتبعة ومدى فعاليتها في مواجهة التهديدات السيبرانية. من خلال هذه الأهداف، يسعى البحث إلى تقديم توصيات لتحسين الردع السيبراني وتعزيز الأمن في الفضاء الرقمي، ما يعكس ضرورة إعادة التفكير في استراتيجيات القوة والصراع في عصر المعلومات.

الخاتمة

في ختام هذ البحث، يتضح أن الواقع العالمي اليوم يتميز بتعقيدات متزايدة، حيث أصبح الفضاء السيبراني ساحة للنزاع ووسيلة لتعزيز المصالح مع تقليل المخاطر. تشكل الخصائص الجديدة لهذا الوسط التقني محفزًا قويًا للأطراف لتسوية نزاعاتها بطريقة تصادمية، في ظل صعوبة تحديد المسؤوليات عند وقوع الهجمات السيبرانية. فمع انطلاق النزاعات في الفضاء الرقمي، تبرز تحديات جديدة تتعلق بالسيادة والأمن، مما يتطلب من الدول إعادة التفكير في استراتيجياتها الدفاعية.

إن بروز عدد كبير من الفاعلين في هذا المجال، من دول وجماعات غير حكومية، أدى إلى تعقيد المشهد السيبراني وجعل من الصعب التحكم في النزاعات. فقد أصبحت المصطلحات الحربية التقليدية تتداخل مع مفاهيم جديدة مثل الإرهاب السيبراني، مما يستدعي تطوير استراتيجيات جديدة لمواجهتها. لذا، فإن المطالبة بعقد اتفاقيات دولية للحد من التسلح في الفضاء الإلكتروني، على غرار الاتفاقيات التي أُبرمت في مجالات الانتشار النووي والكيماوي، أصبحت ضرورة ملحة. يمكن أن تسهم هذه الاتفاقيات في وضع قيود على الحروب الإلكترونية واستخدامها وتوزيعها وتطويرها.

إن الاعتماد المتزايد على تقنيات المعلومات والاتصالات من قبل الدول والأفراد يفرض على الحكومات اتخاذ تدابير فعالة لإدارة المخاطر المرتبطة بالهجمات السيبرانية. ويتطلب ذلك فهمًا عميقًا لطبيعة هذه التقنيات وقدرتها على تجاوز الحدود بين الدول والمجتمعات. لا بد من تعزيز التدابير الأمنية لحماية مجتمعات المعلومات، حيث تُقوض طبيعة العمليات السيبرانية من دور الردع التقليدي. فتعرض دولة ما لهجوم يؤثر على اقتصادها أو بنيتها التحتية أو على أرواح مواطنيها، دون معرفة مصدره أو دوافعه، يقلل من فاعلية الردع.

تظل أهمية الردع قائمة، خاصة في ظل هشاشة الدول في مواجهة الهجمات السيبرانية. وبالتالي، يتطلب الأمر وعيًا متزايدًا بأساليب الوقاية وتعزيز البنية التحتية الدفاعية. كما ينبغي على الدول الاستثمار في تطوير قدرات الاستخبارات السيبرانية، لتكون قادرة على اكتشاف هوية المهاجمين وتحليل دوافعهم، مما يسهل وضع استراتيجيات ردع فعالة.

ويبقى التحدي الأكبر هو تحقيق توازن بين تعزيز القدرات السيبرانية وحماية الأمن الوطني في عالم متغير. يتطلب ذلك تعاونًا دوليًا شاملاً، حيث يمكن أن تسهم الشراكات بين الدول في تبادل المعلومات والخبرات لتعزيز الأمن السيبراني. كما يجب أن تكون هناك جهود متواصلة لتوعية الأفراد والمؤسسات حول أهمية الأمن السيبراني وطرق الوقاية، ما يؤدي إلى خلق بيئة أكثر أمانًا في الفضاء الرقمي.

النتائج

استنادًا إلى ما تقدم حول "الحرب السيبرانية: التهديدات، الاستراتيجيات، وتحديات الردع في الفضاء الرقمي"، يمكن تلخيص النتائج الرئيسة بالتالي:

- :انتقل مفهوم الحرب السيبرانية من نظرية إلى واقع ملموس يهدد الأمن القومي والدولي، ما يستدعي فهمًا شاملًا لطبيعته وآلياته.
- تعتبر الهجمات السيبرانية المتنوعة سلاحًا ذا كلفة منخفضة مع تأثيرات كبيرة، ما يشجع الفاعلين على اعتمادها كوسيلة غير تقليدية للصراع.

- تثير الحرب السيبرانية بتحدياتها قضايا قانونية تتعلق بالمسؤولية، ما يستدعي تطوير أطر قانونية جديدة.
- **ضرورة** تطوير استراتيجيات ردع تشمل تعزيز الأنظمة البديلة وإعادة التأسيس السريع للأنظمة المُخترقة وتعزيز الوعي الفردي والمؤسساتي حول التهديدات السيبرانية لتعزيز القدرة على التصدي لها.

التوصيات

استنادًا إلى النتائج الرئيسة حول "الحرب السيبرانية: التهديدات، الاستراتيجيات، وتحديات الردع في الفضاء الرقمي"، يمكن تقديم التوصيات التالية:

- يتعين على الدول والمنظمات الدولية العمل على وضع أطر قانونية جديدة تعالج القضايا المتعلقة بالمسؤولية في الهجمات السيبرانية. ويجب أن تشمل هذه الأطر معايير واضحة للتصدي للهجمات وتحديد المسؤوليات القانونية تجاه الفاعلين.
- **تعزيز التعاون الدولي** وضرورة بناء شراكات دولية قوية لمواجهة التهديدات السيبرانية، وتنسيق الجهود لمواجهة الهجمات المشتركة، وتطوير استراتيجيات ردع فعالة تعزز الأمن السيبراني على مستوى عالمي.
- تعزيز برامج التوعية والتدريب للأفراد والمؤسسات حول التهديدات السيبرانية وأساليب التصدي لها وتوفير الموارد التعليمية والدورات التدريبية لتعزيز القدرة على التعرف إلى الهجمات والرد عليها بشكل فعال.

قائمة المراجع

- البعلبكي، منير .(2004). المورد: قاموس إنكليزي –عربي .دار العلم للملايين.
- بوفر، أندريه .(1970). الردع والاستراتيجية)ترجمة أكرم ديري). دار الطليعة للطباعة والنشر.
- الجزيرة نت .(تاريخ غير متوفر) https://www.aljazeera.net/midan/reality/politics

- الجمعية العامة للأمم المتحدة .(2013) .دراسة شاملة عن مشكلة الجريمة السيبرانية والتدابير التي تتخذها الدول الأعضاء والمجتمع الدولي والقطاع الخاص للتصدي لها الوثيقة فيينا(UNODC/CCPCJ/EG.4/2013/2).
- كابلان، ف .(2019) .المنطقة المعتمة: التاريخ السري للحرب السيبرانية (ترجمة لؤي عبد المجيد). المجلس الوطني للثقافة والفنون والآداب (سلسلة عالم المعرفة) .
- لسيج، لورنس .(2006) .الكود المنظم للفضاء الإلكتروني (ترجمة: محمد سعد طنطاوي). (ط. 2). مؤسسة هنداوي للتعليم والثقافة.
- المركز الاستشاري للدراسات والتوثيق .(2014) .التحولات في العقيدة العسكرية الأمريكية: دعائم الضعف السبع (أوراق استراتيجية، العدد 2). بيروت: المركز الاستشاري للدراسات والتوثيق.
- هارفارد بزنس ريفيو العربية .(تاريخ غير متوفر). https://hbrarabic.com

- Canabarro, D. R., & Borne, T. (2013). Reflection on the fog of Cyber War (Policy working Paper). National Center for Digital Government.
- Cohen, H. (2005). The Approaches and Limitations of Cyber Deterrence. Retrieved from http://www.cs.tufts.edu/comp/116/archive/fall2015/hcohen.pdf
- Cresswell, J. (2010). Cybernetics. In Oxford Dictionary of word Origins. Oxford University Press.
- Gervais, M. (2012). Cyber Attacks and the Laws of War. Berkeley Journal of International Law, 30(2), Article 6.
- Giles, K. (2011). Information Troops a Russia Cyber Command? In legal paper third international conference on Cyber Conflicts. Tallinn Estonia.
- Glantz, E. J. (2011). Guide to Civil War Intelligence. The Intelligencer: Journal of U.S. Intelligence Studies.
- Jawal Max. (تاريخ غير متوفر). Learn about the highlights of 2018 and 2019 cyber attacks. Retrieved from https://jawalmax.com/learn-about-the-highlights-of-2018-and-2019-cyber-attacks/
- Kahn, D. (1996). The Codebreakers (Rev. ed.). Scribner.
- Kissel, R. (2013). Glassory of Key Information Security Terms. National Institute of Standards and technology, U.S Department of Commerce.
- Lewis, J. A. (2010). Sovereignty and the role of Government in Cyberspace. Center for Strategic and International Studies Journal, 16(2).
- Nye, J. S., Jr. (2010). Cyber Power. Harvard Kennedy School.
- Saalbach, K. (2014). Cyber War, Methods and Practice (Version 9.0). University of Osnabruck.
- Shin, B. (2011). The Cyber Warfare and the Right of Self–Defense: Legal Perspectives and the Case of the United States. IFANS, 19.

- Wei, M. L. H. (2015). The Challenges of Cyber Deterrence. Journal of the Singapore Armed Forces, 41(1), 13-22.
- Wiener, N. (1948). Cybernetic or control communication in the animal and the machine (2nd ed.). M.I.T. Press.