

الردع السيبراني: مقاربة للطبيعة، الفواعل وقيود القانون الدولي

Cyber Deterrence: An Approach to Nature, Actors and the Constraints of International Law



عبد القادر بوعازي^{*1}

¹ جامعة عبد الحميد ابن باديس- مستغانم- الجزائر

abdelkader.boughazi@univ-mosta.dz

تاريخ الإرسال: 2025/03/01 تاريخ القبول: 2025/05/22 تاريخ النشر: 2025/06/01

ملخص: تعكف هذه الدراسة على تحليل أهم المفاهيم المرتبطة بمجال الفضاء السيبراني بالتركيز على تعريف القوة السيبرانية كمفهوم جديد في العلاقات الدولية، وتسابق الدول في تطوير واكتساب القوة في المجال السيبراني، حيث بات هذا الفضاء مرتبطا بمناحي الحياة في جميع المجالات سواء المالية والاقتصادية منها أو الاجتماعية والعسكرية، وهو المدخل المؤدي إلى التعرّيج على الهجمات السيبرانية ودورها في تدمير البنى التحتية والخوادم والحواسيب وتعطيلها وسبل الاجتهاد في بناء استراتيجيات في مجال الردع السيبراني، إلى جانب الإشكالات المطروحة حول مدى فعالية الردع في المجال السيبراني على غرار الردع النووي ذو الفاعلية.

الدراسة أيضا ركزت على بعضا من نماذج استراتيجيات الردع والعقبات التقنية والقانونية التي تعترض الردع السيبراني ومدى تحقيقه من خلال تعدد الفواعل السيبرانيين، اتساع الفضاء الإلكتروني، وتشاركه بين المدنيين والعسكريين وكذا صعوبة تحديد العدو ومصدر العدوان، إضافة إلى التقييدات القانونية والتي تنصب على مدى تطبيق القانون الدولي وقانون الحرب في المجال السيبراني.

الكلمات المفتاحية: الردع السيبراني، الهجمات السيبرانية، الفضاء الإلكتروني، الردع بالاستيعاب، القانون الدولي.

Abstract: This study analyzes the most important concepts related to the field of cyberspace, focusing on defining cyber power as a new concept in international relations, and the competition between countries to develop and gain power in the cyberspace, as this space has become linked to aspects of life in all areas, whether financial, economic, social or military, which is the gateway to cyber-attacks and their role in destroying and disabling infrastructure, servers and computers, and ways to strive to build strategies in the field of cyber deterrence, in addition to the problems raised about the effectiveness of deterrence in the cyberspace, similar to effective nuclear deterrence.

The study also focused on some models of deterrence strategies and the technical and legal obstacles that hinder cyber deterrence and the extent of its achievement, through the multiplicity of cyber actors, the expansion of cyberspace, and its sharing between civilians and the military, as well as the difficulty of identifying the enemy and the source of aggression, in addition to legal restrictions, which focus on the extent of the application of international law and the law of war in the cyberspace.

Key words: Cyber deterrence, cyber-attacks, cyberspace, deterrence by accommodation, international Law.

مقدمة:

ساهمت الطفرة التكنولوجية والمعلوماتية في ارتباط العالم المتزايد بالفضاء السيبراني، من خلال بنيته التحتية التي تشمل الطاقة والنقل والخدمات الحكومية والتجارة الالكترونية والمصارف والمؤسسات الاقتصادية التي أصبحت متداخلة فيما بينها، حيث اتجهت معظم الدول والحكومات لتبني نماذج من الحكومات الذكية والإدارات الالكترونية ليتعدى الأمر نحو بناء المدن الذكية، إلى جانب التزايد الهائل لمستخدمي الإنترنت عبر العالم.

إن الطفرات السابقة التي عرفها العالم أدت إلى زيادة الاستخدامات ذات الطبيعة المدنية والعسكرية، وهو الأمر عينه الذي جعل هذا الفضاء كحالة من التعارض في المصالح والقيم بين الفاعلين الدوليين سواء أكانوا دولاً أم غير الدول بغية حيازة أكبر مساحة من النفوذ والتأثير السيبراني.

لقد خلق هذا السباق بين الفواعل صراعاً داخل هذا الفضاء يدور حول القدرة على امتلاك أنظمة حماية إلكترونية وكذا تطوير القدرات الهجومية والتحكم في المعلومات، مما زاد من الهجمات السيبرانية وتعددتها لتشمل التهديدات بالحروب، الإرهاب، التجسس الرقمي، حيث أصبح هذا الفضاء مجالاً للحرب والصراع في إطار إيجاد استراتيجيات للردع من الهجمات السيبرانية.

إن هذه التوطئة تدفعنا إلى محورة الإشكالية حول التالي:

إلى أي مدى يمكن القول إن قواعد القانون الدولي استطاعت فرض قيود جديدة جاهدة للتهديدات

والهجمات السيبرانية ومحددة لها؟

تتفرع عن الإشكالية الأسئلة الفرعية التالية:

1- فيما يتمثل الردع والردع السيبراني؟

2- ما هي الهجمات السيبرانية ومن هم أهم فواعلها؟

3- كيف ينظر القانون الدولي للهجمات السيبرانية؟

للإجابة على الإشكالية المطروحة والأسئلة المتفرع عنها يتم المرور في هذه الورقة عبر ثلاث محاور، حيث خصص المحور الأول لمفهمة مصطلحي الردع والردع السيبراني، ليتم الانتقال إلى تحديد طبيعة الهجمات السيبرانية والفواعل المحركة لها، مع التعرّيج على مجمل التقييدات التقنية والقانونية المعارضة لهاته الظاهرة وهو ما تم التطرق له في المحور الثالث.

المبحث الأول

الردع والردع السيبراني: إطار نظري.

إن التطور الهائل والطفرة التكنولوجية والرقمية والإلكترونية التي عرفها العالم في العصر الحديث أو ما أصبح يسمى بالموجة الثالثة من التطور التكنولوجي دفع الكل إلى المزيد من الاعتماد الكلي على الإنترنت والتطبيقات الإلكترونية الذكية، وذلك من خلال إنشاء الإدارة الذكية والمدن الذكية التي تعتمد كلياً على الانترنت، وهو الأمر ذاته الذي حتم على الدول والحكومات اعتماد سياسات تتماشى والعالم الرقمي لارتباط ذلك بأمنها القومي من جهة، ونتيجة لتداخل جميع معلوماتها الأمنية والعسكرية والاقتصادية والخدماتية في مجال السيبراني من جهة ثانية.

في هذا الصدد نسعى إلى تسليط الضوء على المفاهيم والاستخدامات المرتبطة بالفضاء الإلكتروني أو السيبراني، من خلال:

1- القوة السيبرانية:

يعتبر "جوزيف ناي" من بين المهتمين بهذا المفهوم، حيث يعرفها بأنها: "القدرة على الحصول على النتائج المرجوة من خلال استخدام مصادر المعلومات المرتبطة بالفضاء الإلكتروني، لإيجاد مزايا للدولة والتأثير على الأحداث المتعلقة بالبيئات التشغيلية الأخرى وذلك عبر أدوات إلكترونية"¹.

حيث يطرح "جوزيف ناي" للقوة السيبرانية مجموعة عوامل وجب توافرها كأجهزة الحاسوب، المعلومات والشبكات الإلكترونية والبنية التحتية للمعلومات والمهارات البشرية، كما يعتبر أن القوة السيبرانية فريدة من نوعها من خلال أنها من صنع واختراع الإنسان، إذ تخضع لتغيرات تكنولوجية أكثر سرعة من مجالات تقليدية أخرى.

ومنه فإن جغرافية الفضاء السيبراني هي بيئة قابلة للتأثير والتغيير من خلال سهولة الولوج إليها بأرخص الوسائل والموارد وبأقل وقت، عكس السيطرة على الفضاء الجوي والبحري الذي يتطلب قوة بشرية وعسكرية وتكاثف جهود واستراتيجيات وتكنولوجيات من الجيل الخامس لتحقيق تفوق جوي أو بحري للسيطرة على جزء منه فقط، وهو الأمر المخالف تماماً للفضاء السيبراني حيث عوائق وتكلفة الولوج إليه أقل نظراً لتعدد اللاعبين وسهولة الدخول وسرعة الاخفاء².

¹. إيهاب خليفة، نمط جديد لممارسة التأثيرات غير تقليدية في العلاقات الدولية، مجلة اتجاهات للأحداث، ع.06، يناير 2015، ص. 3.

². Joseph S. Nye, *Cyber Power: The Future of Power in the 21st Century* (Belfer Center for Science and International Affairs, Harvard Kennedy School, 2010), P.03,04

2- الجريمة السيبرانية:

لقد عرفت منظمة التعاون والتنمية في الميدان الاقتصادي الجريمة السيبرانية أنها الجريمة ذات الصلة بالحاسوب، وبأنها أي سلوك غير مشروع وغير أخلاقي أو غير مرخص به، ويشمل الإرسال أو معالجة المعطيات وكل جريمة متصلة بالجانب الإلكتروني بواسطة توجيه النظام الحاسوبي نحو هدف الجريمة واتخاذ كوسيلة لارتكابها، أي أنها بعبارة أخرى تلك الجريمة المتصلة بالتكنولوجيا الرقمية المستخدمة للشبكة الدولية للمعلومات والانترنت.¹

3- الإرهاب السيبراني:

إن الإرهاب في الفضاء السيبراني يتكون من الجريمة السيبرانية والإرهاب، حيث هي فئة تسعى إلى الاستخدام الغير القانوني للحواسيب والبنية التحتية للاتصالات الموصولة بشبكة الانترنت لتنفيذ أعمال وهجمات تخريبية بغية عرقلة تشغيل هذه البنى الحيوية، أو أنه التهديد بهجمات على أجهزة الكمبيوتر والشبكات والمعلومات المخزنة فيه من أجل تخويف أو إكراه الدول والحكومات وكذا ترويع الشعوب لتنفيذ مطالب أو إرغامها على تنازلات.²

4- مفهوم الردع:

يتمثل الردع في أهم معانيه على أنه عملية إقناع الجهة المعادية أو المحتملة، حيث أن أي عدوان أو عملية عسكرية ستكون كثر في شكل أضرار غير مقبولة مقارنة بالمكاسب التي يمكن تحقيقها ماديا، سياسيا، ومنه فالردع عملية تفاعل اجتماعي معقد تتعلق بدرجة كبيرة بالطبيعة البشرية والمشاعر الإنسانية والخوف.³

5- مفهوم الردع السيبراني: تباين السيبراني والنووي واستراتيجيات المجابهة.

أ- مفهوم الردع السيبراني: الاتجاهات المتباينة بين السيبراني والنووي.

يعرف الردع السيبراني بأنه منع الأعمال الضارة ضد الأصول الوطنية في الفضاء، حيث يركز الردع السيبراني على ثلاثة ركائز هي مصداقية الدفاع، والقدرة على الانتقام والرغبة في الانتقام.⁴

إلا أنه هناك من يرى صعوبة إسقاط نظرية الردع أو بالأحرى الردع النووي على الفضاء السيبراني، وذلك لوجود عدة عقبات وعتبات بين الفضاء السيبراني، وفضاء الردع النووي الذي مساحته الجو والبر

². دليل الامن السيبراني للبلدان النامية، الاتحاد الدولي للاتصالات، 2006.

². Uchenna Jerome Orji, **Detering Cyber terrorism in the Global Information Society: A Case for the Collective Responsibility of States**, Defense Against Terrorism, Vol. 6, No. 1, Spring 2014, p.32.

⁴. (حول مفهوم الردع) مجلة الناتو، تاريخ الزيارة. 2025/01/28

⁴. رغبة البهي، الردع السيبراني إشكالات ومتطلبات، مجلة مفاهيم استراتيجية، المركز العربي لأبحاث الفضاء الإلكتروني، تاريخ الزيارة 2025/01/29، في الموقع: http://accronline.com/article_detail.aspx?id=28706

والبحر- الطبيعة الجغرافية-، أما الفضاء السيبراني هو من صنع الانسان، وهو الاتجاه الأول المحلل لعملية التباين بين الردع السيبراني والنووي.

إن أصحاب هذا الاتجاه يبنون رأيهم حول مدى وجود القدرة على استعمال القوة التدميرية الفورية في حال الانتقام النووي، وهو الأمر الصعب التكهن به في مجالات أخرى كالفضاء السيبراني، وذلك للاعتبارات التالية:

أ- صعوبة تحديد الخصم بشكل مؤكد، مما يشكل مشكلة إجراء حوار "الردع".
ب- صعوبة التحكم في آثار الانتقام، والتأكد من نجاح الضربة السيبرانية، أو التأكد من وصول آثار الضربة إلى أهدافها.

ج- الإخفاء والتخفي من الآثار المادية على العملية.

د- اتهام عدد كبير من الجهات الفاعلة مما تمنع النظر في ردعها.

هـ- ضرورة الحفاظ على مستوى عال من السرية حول وجود معين من الأدوات المتاحة للمدافع.¹

ومنه تجدر الإشارة هنا إلى صعوبة التعامل مع الهجمات الإلكترونية والرد عليها بطريقة رادعة للأسباب الآتية، عكس العمل الهجومي على الأرض الذي يمكن من خلاله تحديد مكان الضربة، ومكان إطلاق الصاروخ الباليستي، الشيء الذي يمد حق الرد في مكان الاعتداء ومتابعة المعتدي، أما في الفضاء السيبراني ففيه صعوبة بمكان في تحديد هوية الفاعل وخاصة إذا كان خارج الإقليم القانوني للدولة، مما يستدعي تعاون قضائي وتحقيق أمني مع دولة مصدر العدوان السيبراني.²

من جانب آخر هناك اتجاه ثاني يرى بحتمية الردع في الفضاء السيبراني لغاية الحاجة الملحة لحماية القواعد البيانية والبنية التحتية وحماية الخصوصيات والملكيات الفكرية والعلمية، وكذا حماية التجارة والاقتصاد الرقمي من التعطيل، حيث يعتبرون الردع السيبراني أحد أهم استراتيجيات الأمن القومي للدول والحكومات³، وهنا تشير التقارير الدولية أن الردع السيبراني أكثر فعالية من الأسلحة الأخرى، إذ القليل من الدول كانت قد تمكنت من صنع القنبلة النووية، في حين الأسلحة السيبرانية أصبحت تطورها موجود في أكثر من 140 دولة، كما أن أكثر من 30 دولة قامت وتقوم بتطوير وإنشاء وحدات الإنترنت في قواتها المسلحة⁴.

¹ . Bruno Grumelle. Bruno Terrais, Alain Esterle, **Cyber Dissuasion**. Édité et diffusé par la Fondation pour la Recherche Stratégique, 2012, p.44

² . Amir Ludovici, **Cyber Warfare and Deterrence**, Trends and Challenges in Research : visited a 30/01/2025. p.09

<https://i-hls.com/wp-content/.../Cyber-Warfare-and-Deterrence.pdf>

². رغدة البهي، نفس المرجع.

⁴. Eric Talbot Jensen, **cyber deterrence**, law memory, vol.26, n.2, p.780

أما الاتجاه الثالث فيقر بوجودية الردع في المجال السيبراني، لكن لابد من توفر بناء مفاهيمي ونظري لإسقاط مفهوم الردع في الفضاء السيبراني على غيره من أنواع الردع، لأنه يختلف كلياً عنهم وخاصة الردع في المجال النووي محل التحليل، إضافة إلى وجود ترسانة قانونية وتعاون دولي مكثف في هذا المجال، وعليه نكون أمام إشكالية كبرى وهي عسكرة الفضاء السيبراني.¹

ب- استراتيجيات مجابهة الردع السيبراني:

يتم هنا رصد مجموعة من الاستراتيجيات لمجابهة هذا الخطر، يمكن اختصارها في استراتيجيات الردع السيبراني بالاستيعاب، وكذا خيارات وسبل تقليدية أخرى للردع، حيث تشتمل الأولى على الاستراتيجيات التخفيف من حدة الهجمات الإلكترونية وكيفية التعامل معها، والعمل على التقليل من حدة التأثير على البنية التحتية، وذلك من خلال:

- نظم الإنذار المسبق: وذلك بالعمل على التنبيه على الهجمات فور وقوعها قبل انتشارها لتحطيم كامل البنية التحتية، مما يستدعي التدخل المبكر.

- تعدد مصار الطاقة وإيجاد بدائل إلكترونية: يعني في حال ارتباط المنشآت بالبنية السيبرانية لابد من بقاء نظم تقليدية تشتغل لتفادي الشلل التام، وهنا لابد من إنشاء بدائل إلكترونية تعمل كبدايل في حال تعرضها للهجمات الإلكترونية خاصة في المرافق الحساسة.

- إنشاء بيانات "back up" المهمة مع تشفيرها: أي العمل على إنشاء نسخ احتياطية للبيانات، مع العمل على تحديثها دورياً- نظام أرشفة-، من خلال تشفير البيانات الحساسة والأكثر أهمية، ووضع خطة شاملة تضم القطاع العام والخاص مع تأطير كوادرو خبراء وتقنيين للتعامل مع هكذا هجمات، إلى جانب العمل على تطوير شبكات ودروع إلكترونية غير قابلة للاختراق تجرب دورياً لمعرفة مواطن الضعف والخلل.²

أما الاستراتيجية الثانية فتختص بخيارات وسبل الردع التقليدية، حيث الردع السيبراني هنا لا يصل إلى درجة الردع النووي، وعليه تم طرح مجموعة من المتطلبات التقليدية للردع متمثلة في:

- الردع السلبي: ويتمثل في عدم مجارة الخصم أو المهاجم والعمل على تطوير البنية الإلكترونية لتجنيبها الوقوع في الهجمات والاختراق، وكذا تحسين تدابير الأمن الإلكتروني.

- الاحتجاج الدبلوماسي: أي العمل على الضغط على الدول مصدر الهجوم بتقليص التمثيل الدبلوماسي والإحراج الدولي مما يسيء بسمعة الدولة.

¹ . WilliamJ. Lynn, III. **Cyber territory, One Year Later Defending Against the Next Cyber-attack**, in:

<https://www.foreignaffairs.com/articles/2011-09-28/pentagons-cyberstrategy-one-year-later>

² . إيهاب خليفة، إمكانيات تحقيق الردع في صراعات الفضاء الإلكتروني، مجلة اتجاهات الأحداث، ع.13، أوت 2015،

- التدابير القانونية: مثل رفع شكاوى للمحاكم الدولية والإقليمية ولورمزيا.

- العقوبات الاقتصادية: بفرض حزمة من العقوبات الاقتصادية، كالحصار وتجميد الأصول وحجز السفن.

إلى جانب ما يسمى بالانتقام في الفضاء السيبراني والانتقام العسكري، وذلك بالرد على الهجمات السيبرانية بأخرى إلكترونية إلى حد احتمال التصعيد المتبادل، أو التهديد أو شن ضربة عسكرية مضادة على حسب الضرر المتسبب في كارثة.¹

المحور الثاني: الهجمات السيبرانية من حيث الطبيعة والفواعل.

مع التطور التكنولوجي تحول الفضاء الإلكتروني إلى ساحة للتفاعلات الدولية لكافة الاستخدامات العسكرية والمدنية، حيث ظهرت الهجمات السيبرانية على نمطين، إذ الأول منه يتعلق بالقوة الناعمة من خلال استخدام حروب الأفكار والعمليات النفسية، والنمط الآخر مرتبط بالقوة الصلبة كإستخدام الفيروسات والهجمات الإلكترونية، وفي هذا السياق تحول الفضاء الإلكتروني إلى ساحة للصراعات ما بين الفواعل الدولية وغير دولانية.² سيتم تحليل هذا المحور من خلال:

أولاً: الفواعل الدولية وغير دولانية:

أ- الفواعل الدولية:

وهنا وجب التأكيد على قدرة الدولة على السيطرة على المجال البري والبحري والجوي، وكذا الفضاء الإلكتروني لما تملكه من مقومات وأمن ومرافق وتنظيم ومنشآت الدالة على المفهوم الصلب للسيادة، بمعنى آخر الدولة كفاعل محوري داخل هذا الفضاء³، إذ تعد الدول الفاعل الأكثر قوة في المجال الإلكتروني وهو الأمر عينه الذي يمكن إثباته واقعياً، ففي سنة 2008 تمكنت حوالي 180 دولة من أن تمتلك ترسانة من الأسلحة الإلكترونية موسعة بذلك من قدراتها وتفوقها الإلكتروني، الشيء الذي حولها من موقع الدفاع إلى موقع الهجوم.

ب- الفواعل غير دولانية:

حيث يلعب الفواعل من غير الدول دورا كبيرا في مجال الفضاء الإلكتروني سواء من حيث التفاعل أو من حيث التأثير، ويعود ذلك إلى انخفاض تكلفةولوج إلى هذا المجال وعدم وجود حواجز ومعوقات، إلى

². رغدة البهي، مرجع سابق، ص.55.

². عادل عبد الصادق، الهجمات السيبرانية انماط وتحديات للأمن العالمي، دورية مفاهيم استراتيجية، تاريخ الزيارة 2025/01/29، في الموقع: http://accronline.com/article_detail.aspx?id=29088

³. لطفي لمن بلفرد، الفضاء السيبراني، هندسة وفواعل، المجلة الجزائرية للدراسات السياسية، ع.05، 2016، ص.148.

جانب سهولة الحصول على الأدوات اللازمة من الإنترنت مما يسهل شن هجمات على أهداف موجهة للدول أو غير دول¹. في هذا الصدد يمكن رصد الفواعل التالية:

1- المنظمات غير الحكومية:

إذ تعد المنظمات غير الحكومية من بين الفواعل التي تقوم بهجمات إلكترونية، يبدأ أنها لا تملك مقومات الدولة وقدراتها ضعيفة مقارنة مع الدولة، حيث تقتصر هجماتها على أهداف قليلة الأهمية نسبياً كالمواقع الإلكترونية من أجل تحقيق ربح ضئيل قبل أن يتم اكتشافها وتطبيق القانون عليها، وهنا يمكن إدخال المنظمات العادية والاجرامية في هذا السياق، هذه الأخيرة التي تتخذ الفضاء الرقمي لها كمجال وحيد فقط مثل منظمة "yakuza" اليابانية، او منظمة "asian triads" التي تتمتع بغسيل الأموال والابتزاز والاحتيال المالي، القرصنة، والتجسس الصناعي، وكذا توظيف مبرمجين لإنتاج تهديدات وبيع معلومات عبر الإنترنت عن طريق سمسة البيانات والأنشطة².

2- الافراد:

ويقصد بهم الأفراد ذوو الخبرة التقنية والكفاءة في استعمال التكنولوجيات الرقمية والقدرة على توظيفها، حيث يكونون مجهولوا الهوية مما يصعب الكشف عنهم وملاحقتهم³، وتجدر الإشارة هنا إلى إمكانية تقسيمهم إلى أربع فئات قادرة على شن هجمات إلكترونية، وهم:

● الافراد المبتدئون:

يملك المبتدئون مجموعة من البرمجيات المحدودة التي يكون الهجوم من خلالها غير معقد الهدف من خلالها هو الإثارة والمغامرة كعربون لتقبلهم في فئة القرصنة.

● القرصنة:

الهدف الذي يصبوا إليه القرصنة هو الوصول إلى البيانات المشغلة للحواسيب الآلية وتعطيلها وتدمير شبكتها من خلال هجمات معقدة ومنظمة، الهدف منها تحقيق الشهرة والمكاسب المالية.

● القرصنة السياسية:

الهدف من القرصنة السياسية هو الدوافع السياسية لتحقيق منافع شخصية، يلجؤون إلى استخدام الديدان والفيروسات. ومن الأمثلة التي يمكن أن نسوقها هنا اسم "Anonymous" والتي جرائها اعتقل "مانينج برادلي" الذي اتهم بتسريب معلومات لويكليكس.

¹ .نوران شفيق، أثر التهديدات الإلكترونية على العلاقات الدولية: دراسة في ابعاد الأمن الإلكتروني (مصر: المكتب العربي للمعارف، 2018)، ص. 40

² . Paul Cornish et Rex Hughes and David Livingstone, **cyber space and the national security of the unit kingdom**, a Chatham house report. Mars 2009. P.15

³ . إيهاب خليفة، مرجع سابق، ص. 03.

● جماعات الإرهاب الإلكتروني:

تشابه من حيث الأهداف مع القراصنة السياسيين، لكن نطاق الهجمات هو إلحاق الضرر بالدولة والمجتمع على المستوى السياسي والاقتصادي والاجتماعي¹.

ثانياً: أسباب ودوافع الهجمات السيبرانية.

إن المهاجمون السيبرانيون ينقسمون كلاسيكياً حسب اعتبارات مختلفة، ويمكن حصر هذه الاعتبارات في الدافع، الإيديولوجيات والأداء، وكذا التقنية المستخدمة وجهة التمويل، إضافة إلى الأفراد العسكريين المدربين للقيام بأعمال هجومية في الفضاء السيبراني، حيث تنقسم الهجمات السيبرانية إلى نوعين، الأول يتمثل في الاختراقات التي يسعى المهاجم من خلالها إلى التجسس الرقمي، والثانية من أجل إيقاف شبكات الأعداء وإتلاف بنيتها التحتية².

يستخدم الفاعلون في المجال السيبراني الإنترنت لتأكيد مواقفهم الإيديولوجية، سواء كانت سياسية أو دينية أو أخلاقية³، إذ كانت الهجمات في مراحلها الأولى فردية قائمة على أصول الدولة القومية من أجل لفت الأنظار أو شغل حيز إعلامي للعملية، لكن مع التطورات المتلاحقة في هذه الأنظمة تطورت الأساليب والأهداف خاصة مع الفواعل الجدد من غير الدول، والتي أصبحت أسعى غاياتها حيازة أهداف سياسية أو الاعتراض على سياسات معينة، الشيء الذي أضحى يطلق عليه مصطلح "القرصنة الوطنية"، ويمكن إظهار بعضاً من الأمثلة في هذا السياق شنت فيها هجمات على الدول مثل الهجوم على إستونيا 2007 والهجوم على جورجيا في 2008⁴.

ثالثاً: أهم الهجمات السيبرانية بعد سنة 2000.

من بين الحروب السيبرانية التي لاقت ذيعاً واسعاً في النظام الدولي ما سميت بهجمات "فان أليك" والتي كان هدفها إعادة بث معلومات مزيفة والخداع، وكذا فيروس "سينما فورست جانب" الذي يستعمل في تضليل الجيوش، وكذا فيروس "شامون وديستراك" والذي هدفه استهداف شركات الطاقة والبتروك. وقد أصبحت هذه الهجمات تعمل على نشر وإنشاء برمجيات وفيروسات إلكترونية "قنابل إلكترونية"، هدفها هو محو البيانات إلى جانب استعمال ديدان الحواسيب التي تعمل على التدمير الذاتي حين استقبالها إشارات استشعارية، وتتشكل من أبواب سرية تقوم بنقل المعلومات للجهة المرسل.

¹. نوران شفيق، مرجع سابق، ص. 46، 47.

². كريستينا كوش، الجيوبوليتكس السيبرانية والاستقرار في الشرق الأوسط، ترجمة عادل رفيق (مصر: المعهد المصري للدراسات، 2018)، ص. 02.

³. Bruno Gruselle. Bruno Tertrias. Alain Esterle, Cyber **Dissuasion**. Édité et diffusé par la Fondation pour la Recherche Stratégique, mars 2012, p.14

⁴. نوران شفيق، نفس المرجع، ص. 34.

وفي سياق ذاته أصبحت الدول تواجه أخطر الحروب الإلكترونية، ونخص بالذكر هنا تلك التي تكون هجماتها موجهة للمنشآت والمفاعلات النووية، كالهجوم الأمريكي - الإسرائيلي على مفاعل "بوشهر" النووي الإيراني بفيروس "ستكسنت" سنة 2010¹، وفي نفس السنة حدث هجوم مماثل من طرف كوريا الجنوبية على البيت الأبيض ووكالة الأمن القومي واتحادية الطيران².

إن الأمثلة كثيرة في هذا المجال والتي وقعت فيها هجمات عن طريق استخدام الفيروسات والتي كان من أهمها أيضا ما حدث سنة 2012 من تدمير حواسيب وأجهزة "أرامكو" السعودية لتخريب صادرات النفط، إلى جانب اختراق الموقع الإلكتروني للحكومة القطرية والذي كانت الغاية منه إثارة الأزمات في مجلس التعاون الخليجي سنة 2017³.

المحور الثالث: الإشكالات والقيود التقنية والقانونية للردع السيبراني.

يطرح الفضاء الإلكتروني جملة من الإشكالات التقنية والقانونية في ردع الجناة السيبرانيون سواء من الناحية التقنية، أو من ناحية إمكانية تطبيق القانون الدولي الإنساني على الحروب الإلكترونية، إلى جانب إشكالية التمييز بين الفاعلين الدوليين وغير الدوليين.

أولاً: الإشكالات التقنية.

من بين الإشكالات التقنية التي تعترض إنجاح عملية ردعية للمهاجم الإلكتروني نذكر:

أ- الإسناد:

وهو صعوبة إسناد عملية أو هجمة إلكترونية وإلصاق التهمة به مادام لم يعترف بالجرم حيث الجاني افتراضي، وهو الأمر الذي يعقد توجيه الهجمة التي من الممكن أن تكون من طرف ثالث لا دخل له في العملية. إن هذا يستوجب تعاون دولي في هذا المجال في تقديم معلومات رقمية عن هوية أشخاص محتملين.

ب- تجنب الانتقام:

فمن إشكاليات الهجمة السيبرانية أنه لا يمكن التنبؤ بها، وعليه فالمستهدف لا يحدد زمن ومكان الرد ووسيلة الرد التي إما أن تكون تقليدية أو سيبرانية، والمثال على هذا تلويح روسيا في عام 1998 الرد على أي هجوم سيبراني بأي سلاح من أسلحتها الاستراتيجية.

د- الفاعلين من غير الدول:

¹. ايمن السيسي، هدفها تفكيك الدولة، وتقسيم المنطقة، حروب المعلومات ومن يواجهها، مجلة الاهرام، ع. 139،

13 يوليو 2015، على الموقع: <http://www.ahram.org.eg/NewsQ/414060.aspx>

². كريستينا كوشش، مرجع سابق، ص. 01

³. رغدة البهي، مرجع سابق، ص. 12.

والعقبة هنا حين يكون المهاجم فرد أو جماعة أو منظمة إجرامية، إذ نكون أمام اللاتماثل السيبراني بين الدولة والأفراد والجماعات، وعليه استهدافهم وهم داخل دول غير دولهم يطرح إشكالا قانونيا وخاصة إذا ما وفرت الدولة الأخرى الحماية، إلى جانب إشكالات أخرى تتعلق بمن باستطاعته تحمل المسؤولية الجنائية في هذا الصدد.

هـ - اتساع الحيز الفضائي:

حيث يشمل الفضاء الإلكتروني مجالات التجارة، الاقتصاد، البنوك والاتصالات وجميع مناحي الحياة، لذا توجد صعوبة في بناء استراتيجية للردع السيبراني من خلال اختيار مجال أو مجالات محددة لبناء استراتيجية ردعية.¹

ثانيا: إشكالية تطبيق القانون الدولي العام وقانون الحرب في الفضاء السيبراني.

لعبت العولمة دورا كبيرا في التأثير على التفاعلات الإنسانية على الأصعدة السياسية والاجتماعية والاقتصادية والثقافية والتقانية، وعليه غير التطور التكنولوجي من المفهوم التقليدي للقوة لما أحدثته الثورة التقنية من طفرات هائلة في الشؤون العسكرية، الأمر الذي أدى إلى صعوبة التمييز بين الأهداف المدنية والعسكرية وكيفيات إلحاق الضرر بالمنشآت المختلفة، وهو الشيء عينه الذي يعد من التصرفات التي تؤدي إلى انتهاك القانون الدولي الإنساني.

كما أنه على الصعيد الدولي لم يعد الدول هم الفاعلون الأساسيون في العلاقات الدولية رغم عدم اكتساب بعض الفواعل صفة الشخصية القانونية الدولية، إلا أن هذا الأمر لم يمنع من التنصيص القانوني على مبدأ عدم استخدام القوة في العلاقات الدولية وذلك منذ اتفاقيات واستفاليا 1648، وبالموازاة عمل المجتمع الدولي على تطوير ترسانة قانونية مماثلة كاتفاقيات "لاهاي وجنيف" التي كانت الغاية من وراء تشريعها حماية الأشخاص وقت الحروب وذلك دون الإشارة إلى أسلحة محددة الاستخدام.

ينعطف على هذا تحول الحروب في العصر الحديث من حروب تدور بين عسكريين وأعداء معينين وبأهداف معينة إلى حروب غير مرئية تتم بوقع إلكتروني متقن ومنظم، وعليه أفرزت هاته النقلة واقعا جديدا حتم على القانون الدولي ضرورة التكيف معه، إذ بعد ما كان القانون الدولي يطبق على الفضاء الجغرافي أصبح لزاما على قواعده أن تعيد النظر في التطبيق على هذا الفضاء الجديد وهو الفضاء الإلكتروني، وذلك بضرورة إعادة النظر في مجمل المفاهيم القانونية كمبدأ الشرعية والمشروعية، والسيادة والنفوذ، والاختصاص القضائي والإقليمي للجرائم السيبرانية.²

¹ . رغدة البهي، مرجع سابق، ص. 24.

² عادل عبد الصادق، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، الدراسات المستقبلية، ع. 23، 2016، ص. 83-84.

والحقيقة أن القانون الدولي أنتج مساطر قانونية تخص ما تم التطرق إليه سابقا يمكن أن نشير هنا على سبيل المثال لا الحصر إلى:

أ- مبدأ حضر استخدام القوة في العلاقات الدولية والأسلحة الإلكترونية:

لقد أقر القانون الدولي مجموعة استثناءات تخص حق الدول المشروع في اللجوء إلى استعمال القوة خاصة في حال تعرضها للعدوان، ومنه يمكن المقاربة بين الهجمات الإلكترونية والهجمات التقليدية من حيث العدوان على الدول وكذا النتائج والأضرار.

إن هذه الميزة تدخل في تصنيف الهجمات الإلكترونية في خانة الخطر، حيث تنص المادة 58 من البروتوكول الإضافي الأول الملحق باتفاقات "جنيف" على أن الهجمات الانتقامية تعد شكلا من أشكال العدوان، وعليه تم فرض حماية للمنشآت التي تحتوي على مواد خطيرة أو تقدم خدمات اجتماعية.

ب- قانون "تالين" كأساس قانوني للحرب الإلكترونية:

يعد دليل "تالين" الوثيقة القانونية التي تتضمن قواعد القانون الدولي المطبقة أثناء الحروب السيبرانية في 95 قاعدة، حيث يقدم "دليل تالين" رؤية هامة متمسكا فيها على سبيل المثال بالثنائية التقليدية للنزاعات المسلحة الدولية والنزاعات المسلحة غير الدولية، ويقر بأن العمليات الإلكترونية وحدها قد تشكل نزاعات مسلحة تبعا للظروف لا سيما الآثار المدمرة لتلك العمليات.

وفي هذا السياق يقدم تعريفا "للهجوم السيبراني" بموجب القانون الدولي الإنساني بوصفه "عملية إلكترونية سواء هجومية أو دفاعية يتوقع أن تتسبب في إصابة أو قتل أشخاص أو الإضرار بأعيان أو تدميرها"¹، وعليه ما ينبغي أن يستنتج على أنه "ضرر" في العالم الإلكتروني.

رغم هذا التوصيف لحجم الخطر إلا أن الكثيرون يعتبرون "قانون تالين" لا يزال يترنح في بدايات التكوين القانوني والتشريعي على المستوى الدولي خاصة في إرساء مبادئ عامة تنظم قانون الحرب السيبراني، إذ يعتبر ما تطرق له القانون هو قواعد الاشتباك ما بين الدول لا غير، وأن الهجمات السيبرانية الحالية هل تصنف ضمن عمل مسلح دولي أو غير دولي لتتنطبق عليها قواعد قانون الحرب السيبراني أم لا، أو بعبارة أخرى متى نكون أمام عمل مسلح دولي لابد أن تتوافر فيه شروط المادة 08 من ميثاق الأمم المتحدة التي يتحدد من خلالها مسؤولية الدولة بشكل واضح.

ورغم هذا النقد إلا أن "قانون تالين" أوجد بعضا من الحلول القانونية المجابهة للهجمات السيبرانية وخاصة حظر الإصابات لدي المدنيين، حيث يقسم الفضاء السيبراني إلى فاعلين سيبرانيين أو ما

¹ . اللجنة الدولية للصليب الأحمر، ماهي القيود التي يفرضها قانون الحرب على الهجمات السيبرانية، الزيارة 2025/01/30/03، على الموقع:

يسمى بالمقاتل السيبراني (cyber combattants)، وما بين المستخدم العادي، كما يحدد الهجمات نحو الأهداف العسكرية الإلكترونية فقط باعتبارها فضاء يتقاسمه المدنيين والعسكريين، وهذا ما نصت عليه المادة 14 و71 و74 من "قانون تالين" بالضرورة العسكرية والتناسب وتحديد الأهداف بدقة.

وفي نفس المنحى ينص "قانون تالين" على مجموعة من القواعد المتعلقة بالاشتباك الإلكتروني في ظل القانون الدولي الإنساني، إذ يؤكد على ضرورة اعتماد استراتيجيات للرد العسكري بالكيفيات اللازمة للتعامل مع العدو، وكذا وجوبية التمييز بين عملية عسكرية تحت غطاء وحماية دولة أو عبث القرصنة وأفراد من أجل التسلية وسرقة الحسابات، إذ يدعوا إلى وجوبية التوجه للحل الدبلوماسي في حالة العمليات المغطاة بغطاء حكومي تم التدرج إلى الرد العسكري بالتنسيق مع الأجهزة المخولة لذلك، الأمر الذي يدفعنا للقول أن "قانون تالين" يتفق ومبادئ اتفاقيات جنيف لعام 1949 والبروتوكولات الإضافية لعام 1977.¹

في الأخير يمكن القول إنه لا تزال الدول تتنصل من مسؤولية عدم الامتثال للقانون الدولي في الفضاء السيبراني حتى ولو طبقت مبادئ قانون الحرب عليه، ولهذا لا بد من إيجاد قواعد ومعايير ملزمة من الناحية السياسية لتحقيق اتفاق مبدئي مشترك بين الدول قبل الشروع في بلورة قوانين دولية ملزمة في المجال الإلكتروني.

هذا ويبقى التحدي قائم في مجال تعريف "النزاع المسلح" عبر الفضاء الإلكتروني وشبه عجزه - القانون الدولي الإنساني - على سن قوانين وإجراءات تنظيمية حول أساليب ووسائل الحرب الجديدة²، وما يبرر هذا العجز الدولي هو عدم الاستطاعة في التسريع لإيجاد قوانين ردعية للهجمات السيبرانية وتحميل مرتكبيها المسؤولية الدولية، وذلك من خلال عدم التصريح بآثار الهجمة وتكتم الدول عليها وكذا تفردا بهذه الاستخدامات بالنظر إلى حجمها الدولي ومدى تطورها في المجال الإلكتروني³.

خاتمة:

بناء على ما سبق يمكن القول إن الطفرة في المجال التكنولوجي وخاصة في الفضاء السيبراني غيرت الكثير من المفاهيم في العلاقات الدولية، حيث مفهوم القوة في المجال الجغرافي الذي كانت تتحكم فيه الدول دون سواها أصبح تقليديا، إذ تم الانتقال إلى ضرورة امتلاك القوة في الفضاء الإلكتروني والذي لم يعد مقتصرًا

¹. سعيد درويش، ماهية الحرب الإلكترونية في ضوء قواعد القانون الدولي، حولية جامعة الجزائر 1، ع. 29، ج. 02، 2018، ص. 122.

². عادل عبد الصادق، مرجع سابق ص. 93.

³. أحمد عيسى نعمة الفتلاوي، الهجمات السيبرانية مفهومها والمسؤولية الدولية الناشئة في ظل التنظيم الدولي المعاصر، مجلة المحقق العلمي للعلوم القانونية والسياسية، ع. 04، 2019، ص. 18.

على الدولة كوحدة بل توزع ذلك على فواعل دولاتية أخرى من خلال تمكّنها من إنتاج أسلحة سيبرانية والعمل بها على الهجوم والدفاع في المجال السيبراني.

ومنه حدثت نقلة نوعية في المجال الحربي، إذ تم الانتقال أيضا من هذا المجال إلى الفضاء السيبراني، هذا الفضاء الذي أصبح يشترك فيه العسكريين والمدنيين على حد سواء، وأن الهجمات فيه تؤدي إلى ضرب البنية التحتية لمجالات عدة وبأساليب متعددة كالقرصنة وسرقة المعلومات والتجسس الإلكتروني، مما استدعي تبني استراتيجية فعالة وموازية للردع السيبراني، هذا الأخير الذي كان محل تضارب في مدى جديته من عدمها بسبب ضبابية الهدف والمعتدي، ومدى تحقق الهجوم من عدمه، وطريقة التصعيد في حالة تحقق الهجوم.

هي إشكالات واجهت مفهوم الردع السيبراني في إسناد الهجمات الإلكترونية وتحديد العدو ومصدر العدوان، إضافة إلى الانتقام من خلال عدم استطاعة التنبؤ بالهجمات، وذلك لتعدد الفاعلين واتساع الحيز السيبراني، الأمر الذي لا يزال يطرح حزمة من الإشكالات القانونية التي مازالت في بدايتها، مقتصرة على تبني "قانون تالين" لتنظيم الحرب في الفضاء الإلكتروني وكذا تنظيم الاشتباك الإلكتروني ما بين الفواعل الدولية.

قائمة المراجع:

أولا: الكتب:

أ- باللغة العربية:

1- نوران شفيق، أثر التهديدات الإلكترونية على العلاقات الدولية: دراسة في ابعاد الأمن الإلكتروني (مصر: المكتب العربي للمعارف، 2018).

2- كريستينا كوسش، الجيوبوليتكس السيبرانية والاستقرار في الشرق الأوسط، ترجمة عادل رفيق (مصر: المعهد المصري للدراسات، 2018).

ب- باللغة الأجنبية:

1- Joseph S. Nye, **Cyber Power: The Future of Power in the 21st Century** (Belfer Center for Science and International Affairs, Harvard Kennedy School, 2010).

2- Bruno Grumelle. Bruno Terrais, Alain Esterle, **Cyber Dissuasion** (France : Édité et diffusé par la Fondation pour la Recherche Stratégique, 2012).

ثانيا: المجلات:

أ- باللغة العربية:

1- إيهاب خليفة، نمط جديد لممارسة التأثيرات غير تقليدية في العلاقات الدولية، مجلة اتجاهات للأحداث، ع.06، يناير 2015.

2- لطفي لمين بلفرد، الفضاء السيبراني، هندسة وفواعل، المجلة الجزائرية للدراسات السياسية، ع.05، 2016.

3- عادل عبد الصادق، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، الدراسات المستقبلية، ع.23، 2016.

4- سعيد درويش، ماهية الحرب الإلكترونية في ضوء قواعد القانون الدولي، حولية جامعة الجزائر 1، ع.29، ج.02، 2018.

5- أحمد عيسى نعمة الفتلاوي، الهجمات السيبرانية مفهومها والمسؤولية الدولية الناشئة في ظل التنظيم الدولي المعاصر، مجلة المحقق العلمي للعلوم القانونية والسياسية، ع.04، 2019.

ب-باللغة الأجنبية:

1- Bruno Gruselle. Bruno Tertrias. Alain Esterle, Cyber **Dissuasion**. Édité et diffusé par la Fondation pour la Recherche Stratégique, mars 2012.

2- Eric Talbot Jensen, **cyber deterrence**, *law memory*, vol.26, n.2, 2012.

3- Paul Cornish et Rex Hughes and David Livingstone, **cyber space and the national security of the unit kingdom**, a Chatham house report. Mars 2009.

4- Uchenna Jerome Orji, **Deterring Cyber terrorism in the Global Information Society: A Case for the Collective Responsibility of States**, *Defense Against Terrorism*, Vol. 6, No. 1, Spring 2014.

ثالثاً: منشورات صادرة عن المنظمات وهيئات دولية:

1- دليل الأمن السيبراني للبلدان النامية، الاتحاد الدولي للاتصالات، 2006.

2- (حول مفهوم الردع) مجلة الناتو، تاريخ الزيارة: 2025/01/28.

3- اللجنة الدولية للصليب الأحمر، ماهي القيود التي يفرضها قانون الحرب على الهجمات السيبرانية، الزيارة: 2025/01/30/03، على الموقع:

<https://www.icrc.org/ara/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm>

رابعاً: المواقع الالكترونية:

1- رغدة البهي، الردع السيبراني إشكالات ومتطلبات، مجلة مفاهيم استراتيجية، المركز العربي لأبحاث الفضاء الالكتروني، تاريخ الزيارة: 2025/01/29، في الموقع:

http://accronline.com/article_detail.aspx?id=28706

2- عادل عبد الصادق، الهجمات السيبرانية أنماط وتحديات للأمن العالمي، دورية مفاهيم استراتيجية، تاريخ الزيارة: 2025/01/29، في الموقع:

http://accronline.com/article_detail.aspx?id=29088

ايمن السيبي، هدفها تفكيك الدولة، وتقسيم المنطقة، حروب المعلومات ومن يواجهها، مجلة الاهرام، ع. 139، 13 يوليو 2015، على الموقع:

<http://www.ahram.org.eg/NewsQ/414060.aspx>

5- Amir Ludovici, Cyber **Warfare and Deterrence**, Trends and Challenges in Research : visited a 30/01/2025, in:

<https://i-hls.com/wp-content/.../Cyber-Warfare-and-Deterrence.pd>

6- William J. Lynn, III. **Cyber territory, One Year Later Defending Against the Next Cyber-attack**, in:

<https://www.foreignaffairs.com/articles/2011-09-28/pentagons-cyberstrategy-one-year-later>