

من الردع النووي الى الردع السيبراني: دراسة لمدى تحقيق مبدأ الردع في الفضاء السيبراني

From Nuclear Deterrence to Cyber Deterrence: A study of the extent achievement of the principle of deterrence in cyberspace

علاء الدين فرحات

المدرسة الوطنية العليا للعلوم السياسية . Ferhat.alaeddine@enssp.dz

تاريخ الاستلام: 2021/05/10 تاريخ القبول: 2021/06/08 تاريخ النشر: 2021/06/09

ملخص:

تناقش هذه الورقة طبيعة مفهوم الردع السيبراني والجدل المثار حوله، وتحاول تقديم رؤية واضحة حول إمكانية تحقيق الردع في الفضاء السيبراني. كما تصف العديد من حالات الصراع السيبراني لإلقاء الضوء على مشاكل الردع السيبراني وتقييمها.

تخلص الدراسة إلى أنه نظرا لصعوبات إسناد الهجمات السيبرانية إلى مرتكبيها وما يترتب على ذلك من احتمالات الانتقام المرتبطة بها، يمكننا القول أن المجال السيبراني يمثل تحديا لآليات الردع. وهناك رأي آخر يؤسس لفشل نماذج الردع المعروفة في حروب الانترنت، فالردع بالانتقام أو العقاب لا ينطبق على هذه الحروب، حيث انه من الصعوبة بمكان بل ومن المستحيل في كثير من الأحيان تحديد الهجمات الالكترونية ذات الزخم العالي.

كلمات مفتاحية: الردع السيبراني، الردع النووي، الحروب السيبرانية، الفضاء السيبراني، الأمن القومي.

Abstract:

This paper discusses the nature of the concept of "cyber deterrence" and the controversy surrounding it, and provides a clear vision about the possibility of achieving deterrence in cyberspace. And describes several situations of cyber conflict to illuminate and assess cyber deterrence problems.

The study concludes that, the difficulties in attributing cyber attacks to their perpetrators and the consequent potential for retaliation associated with them, we can say that the cyber field presents a challenge to deterrence mechanisms. There is another opinion that establishes the failure of the known deterrence models in internet wars. Deterrence with retaliation or punishment does not apply to these wars, as it is very difficult and often impossible to identify cyber attacks with high momentum.

Keywords: cyber deterrence; nuclear deterrence; cyber wars; cyberspace; national security.

المؤلف المرسل: علاء الدين فرحات، الإيميل: ferhat.alaeddine@enssp.dz

مقدمة

أصبحت الهجمات الإلكترونية مصدر قلق للأمن القومي وأداة جديدة في السياسة الخارجية، تستلزم التكثيف السريع معها عبر تطوير القدرات العسكرية والاستخباراتية السيبرانية، وتماشيا مع هذا الوضع الجيوسياسي قامت القوى الكبرى بتكثيف استراتيجياتها العسكرية مع خصائص البيئة السيبرانية لأن أمنها سيتحدد ليس فقط من خلال المواجهة على الأصعدة العسكرية والاقتصادية والدبلوماسية، لكنه سيتحدد بنفس القدر الذي تدور فيه في الفضاء السيبراني، حيث تكمن كل الفرص وكل المخاطر، جراء هذا باتت الدول القومية في خضم سباق تسلح إلكتروني متسارع، سباق له العديد من الآثار السياسية والإستراتيجية التي تفرض الحاجة إلى إيجاد إجابات سياسية على وجه التحديد لفهم الفضاء السيبراني كمجال سياسي وأمني جديد. فمع تنامي التهديدات السيبرانية باتت فكرة الردع في الفضاء الإلكتروني جزءا من هذه الاستراتيجيات الأمنية للدول، ولمواجهة هذه التهديدات عمل الأكاديميون، السياسيون والأمنيون على البحث عن سبل وآليات للردع في الفضاء السيبراني، لصد الهجمات السيبرانية وتوظيف العمليات السيبرانية الهجومية لردع أنواع أخرى من الضرر المادي. خاصة في ظل سهولة اختراق الشبكة من قبل المتسللين عبر هجمات سيبرانية قد تسفر عن عواقب وخيمة تستنزف الموارد المتاحة، وتتطلب سياسات رادعة لمواجهةها.

مما سبق فإن مشكلة **Problématisation** هذا الموضوع من هذه الزاوية يمكننا من فهم آليات تطبيق الردع في الفضاء السيبراني ومدى نجاعته، ووفق هذا تأتّى دراستنا حاملة الإشكال التالي:

■ الإشكالية:

إلى أي مدى تستطيع الدول ردع أو ثني الآخرين عن إلحاق الضرر بها في الفضاء السيبراني؟

وتنطوي تحت هذه الإشكالية جملة من الأسئلة الفرعية، نبرز بعضها فيما يلي:

■ الأسئلة الفرعية

➤ هل الدول في سباق تسلح إلكتروني؟ إذا كان الأمر كذلك، فما هي خصائصه ودينامياته؟

➤ هل يحقق الردع السبراني الاستقرار والسلام؟

منهجية الدراسة: لتحقيق أهداف الدراسة؛ ونظرا لطبيعة الموضوع فقد اعتمدت الدراسة على المنهج الوصفي التحليلي، نظرا لما يتيح هذا المنهج المتشابه والذي يركز على المعلومات الكافية لفترات زمنية محددة، من أجل الحصول على نتائج علمية يتم تفسيرها بموضوعية تنسجم مع المعطيات الفعلية للظاهرة محل الدراسة، من خلال تحليل العلاقة بين متغيري الدراسة، وتحليل مؤشرات التعاطي الدولي مع هذا التهديد الناشئ وانعكاساته ذلك على الأمن العالمي، والبحث عن إمكانية ردعه.

الهدف من الدراسة: تسعى هذه الدراسة إلى البحث في مفهمة الردع وإمكانية تحقيقه في الفضاء السبراني، كما ستتطرق الدراسة في إطار ذلك لفكرة السلام الإلكتروني كنقطة تستند عليها الأجندات الأمنية للدول لتحقيق نوع من الشفافية والمسؤولية فيما بينها.

1. الثورة في الشؤون العسكرية : والتغير في طبيعة للحرب

عادةً ما يخرج التطور التكنولوجي المعلوماتي من رحم حاجة الجيوش لتطوير وسائل القتال والتواصل والتنظيم اللوجستي، خاصةً أن هذه الوسائل ذات أهمية جوهرية في خوض الحروب والانتصار فيها، إذ تعتمد القدرة على اتخاذ قرارات تكتيكية سريعة وتنسيق عال في مسار المعارك والأساس على سرعة نقل المعلومة، وهذه القدرة هي إحدى أهم الأعمدة في تحديد قدرة الجيوش في التغلب على خصومها. ويخلف التاريخ بأمثلة كثيرة لارتباط تطور تكنولوجيا التواصل مع الحروب المتلاحقة، بدءاً من استخدام البرقيات في الحرب الأهلية الأمريكية في أواسط القرن التاسع عشر، مروراً باستخدام الراديو والرادار في الحربين العالميتين الأولى والثانية، ووصولاً إلى الساتلايت والإنترنت وغيرها في حروب اليوم حيث يوفر التدفق الهائل للمعلومات للقادة الميدانيين الفرصة لاتخاذ قراراتهم بشكل لحظي وبمستوى أعلى من الدقة والسرعة، الأمر الذي يتيح لهم تفوقاً هائلاً على العدو. ويمكن بهذا المنظار النظر إلى الجيوش والبنية العسكرية المتفوقة والتي تشمل القدرات البرية والجوية والبحرية التي يملكها الغرب، فقوة هذه البنية تستند بشكل كبير إلى توافر طرق تواصل فورية، وتدفق سريع وسلس للمعلومات الدقيقة من ساحة المعركة إلى مراكز القيادة والتحكم، والعكس.

وفي ظل التفوق الجوي وعصر المعلومات، تزايدت النقاشات حول طبيعة الحروب وأصبحت مفاهيم كـ "الثورة في الشؤون العسكرية" (Revolution in Military Affairs) هي الغالبة عند الحديث عن القوة الأمريكية وقدرتها على التحكم في الفضاء العملياني، وارتباط هذا التحكم أساساً بالقدرة التكنولوجية التي سهّلت من عمليات التحكم بالقوة الجوية، ومن أبرز الأمثلة على ذلك حرب الخليج الأولى، التي استطاعت فيها القوات الأمريكية التغلب على القوات العراقية بخسائر قليلة، بفضل التطور في تكنولوجيا الاتصال لدى الأمريكان. ومن ثمّ أتت حرب البلقان لتؤكد صحة المقولة حيث لم يقتل في العمليات العسكرية الأمريكية جندي أمريكي واحد، بفضل الاعتماد التام على القوة الجوية المرتبطة أساساً بالثورة التكنولوجية.

ولم يعد الجيش اليوم مكوّناً، كما الجيوش التقليدية، من سلاح البحر والبر والجو فقط، بل أصبحت هناك وحدات جديدة تتواءم مع هذا التطور التكنولوجي. فمثلاً تتصاعد في الوقت الراهن أهمية وحدات السايبر (Cyber)، والتي تقوم بعدة عمليات أهمّها حماية المرافق العامة والمدنية من هجوم إلكتروني عدائي يعطل عملها، أو من عمل تخريبي افتراضي يضرب قلب الدولة وأجهزتها دون الحاجة لإطلاق رصاصة واحدة. كما يفترض من تلك الوحدات تطوير قدرات هجومية إلكترونية تستطيع شلّ قدرات الخصم (ك، 2016).

فالتطورات التكنولوجية والمعلوماتية أدت إلى ثورة في مجال الأسلحة التقليدية وفي استراتيجيات شن الحروب المسلحة **Military Technology Revolution**. وتغيرت الطريقة التي تدار بها الحرب (Sharp, June 2011).

وباختصار حدثت ثلاثة خطوط للتطور العسكري، المدى والسرعة ومستوى القتل كلها وصلت إلى أقصى حدودها في النصف الأخير من القرن العشرين، هذه التغييرات قد حدثت كلها في مدى قصير - في خمسة وثلاثون عاماً - وفي وقت بدأ فيه نوع جديد من الاقتصاد والمجتمع يتشكل (موجة ثالثة أو مدنية ما بعد التصنيع). وهذا يساعد على تفسير أن الثورة العسكرية التي تلوح أمامنا ستكون أعمق بكثير عمّا تصور معظم المحللين حتى الآن، إنها ثورة عسكرية في الإدراك الكامل، تظهر فقط عندما تبرز مدنية جديدة لتتحدى المدنية القديمة، ويجبر أفرع العسكرية أن تتغير على كل المستويات في آن واحد - ابتداء

من التكنولوجيا والثقافة إلى العمليات والاستراتيجيات والتكتيكات والتدريب والعقيدة والشؤون الإدارية (توفلر، 2000، الصفحات 65-66).

فرغم الكلام عن خفض الميزانيات و عن السلام في العالم سنرى عقائد عسكرية حول العالم تتغير تبعا للتحديات الجديدة والتكنولوجيات المستحدثة في عالم حروب الحراب (NICHE)، ومقاتلوا الحراب يمكن أن يزدهروا في عالم يتحول إلى أن يعتمد أكثر من ذي قبل على وسائل الاتصالات الفضائية، وسيزداد اعتماد المؤسسات العسكرية على الفضاء في عالم مصانعه أصبحت آلية وتعمل بالحاسبات بصورة لم يسبق لها مثيل، فإن الحروب أيضا من المتوقع أن تعتمد على الحاسبات الالكترونية والآلية والروبوتية **ROBOTIZATION** و كل من هذه التطورات سيتم مزجها في شكل حروب الموجة الثالثة (توفلر، المرجع نفسه، صفحة 184).

وبسبب الثورة في الشؤون العسكرية أصبحت أنظمة القيادة، السيطرة، الاستخبارات، الاتصالات، الحوسبة، المراقبة والاستطلاع وهي عصب هذه الثورة في خطر من أن تُسدد لها ضربة تُحد من قدرتها وتشلها إذا قام عدو اضعف بالتشويش على خطوط الاتصال التي تربط القوات في شبكة واحدة (كوبلانند، 2003، صفحة 90).

بهذا تتحرك الحرب نحو مستوى جديد كلياً .. !

فالتطورات التكنولوجية ساهمت في تطوير أنظمة التحكم، فضلا عن تسهيل عمل الدفاع الجوي والاستشعار عن بعد ونقل البيانات والاتصالات. كما أن التطورات التكنولوجية أدت إلى تحسين كفاءة أنظمة التسلل، وزيادة دقة توجيه الأسلحة، ورفع كفاءة المحاكاة للعمليات الحربية والمناورات.

وعليه يمكن القول بأن الثورة في الشؤون العسكرية قد أدت إلى اختلاف طبيعة الصراعات وآليات إدارتها بشكل ملحوظ، وقدمت أدوات جديدة يمكن من خلالها إلحاق الضرر بالدول المستهدفة، وفي الوقت ذاته عظم من القدرة التدميرية والقتالية للأسلحة التقليدية، واستدعت الفواعل من غير الدول إلى ساحة الصراع الالكتروني كمساحة جديدة للحركة، وزادت من احتمالية ظهور صراعات مستمرة منخفضة المستوى **Perpetuat Low-level Conflict** أو ما يمكن أن نطلق عليها حروبا

الالكترونية باردة **Cyber Cold Wars**.

وترتب عن ذلك كله أن أصبحت تكنولوجيا المعلومات والاتصالات غاية ووسيلة في الوقت ذاته وأصبح الفضاء الإلكتروني* أحد مجالات الصراع إلى جانب الجو والفضاء والأرض والبحر. ولم يعد من الممكن إتمام عملية عسكرية دون حضور واضح للبعد الإلكتروني. علاوة على ذلك، بدأت الدول الصناعية المتقدمة في استخدام هذه الآليات لخلق شبكات عالمية لتحسين أوضاعها الاقتصادية وتعزيز من قوتها ونفوذها عالمياً (شفيق، 2016، الصفحات 10-11).

2. سباق التسلح الجديد: الانتقال من القوة العسكرية التقليدية إلى امتلاك القوة الإلكترونية

وضع باحثي الأمن السيبراني مصطلح "سباق التسلح السيبراني" لوصف التطورات الجيوسياسية والتفاعل الاستراتيجي للدول في الفضاء الإلكتروني، نستحضر هنا مفهوم "المعضلة الأمنية" لوصف الأمن السيبراني الجيوسياسي، في هذا السياق أجرت شركة **McAfee Corp** إجراء مسح لوضعي السياسات وقادة الأعمال في مجال تكنولوجيا المعلومات والاتصالات، والذين يعتقد 57٪ منهم أن الدول في سباق تسلح للأمن السيبراني. على الرغم من كونها مفيدة كمقياس للآراء، إلا أن هذه الأرقام لا تجيب عما إذا كانت ديناميكيات سباق التسلح الرسمية تحفز بالفعل واضعي السياسات الدفاعية فيما يتعلق بالأمن السيبراني. وبالتالي، ووفق فرضية "المعضلة الأمنية **security dilemma**"، والمعروفة أيضاً باسم "النموذج اللولبي **The spiral model**":

تواجه الدول صراعاً لأنها تشارك في تكوين بيئة فوضوية (أي بيئة تفتقر إلى أي سلطة أعلى)، مما يمنع الدول من الوثوق ببعضها البعض للتخلي عن الاستغلال أو استخدام القوة في حل النزاعات أو إنفاذ الاتفاقيات، فالتحسينات في أمن دولة ما تعتبر خسائر للأخري، وإجراءات الاستجابة المضادة تخلق حلقات ردود فعل سلبية، والتي تمثل سباقات التسلح أحد التعبيرات الخاصة بها.

• فرضية "انتقال السلطة التعديلية" أو "نموذج الردع":

* الفضاء الإلكتروني/ السيبراني هو مجال مركب يشمل عدداً من العناصر هي: أجهزة الكمبيوتر، أنظمة الشبكات والبرمجيات، حوسبة المعلومات، نقل وتخزين البيانات، يعتبر مجالاً حيوياً وجيوسراتيجياً يُخاض فيه العديد من الحروب والهجمات الرقمية، لمعلومات أكثر أنظر: محمود عزت، الفضاء السيبراني وتحديات الأمن المعلوماتي العربي، مقال من موقع المجلة العربية،

تبدأ سباقات التسليح لأن القوة الكلية للدول (وبالتالي الأمن) تنمو بشكل غير متكافئ، وهذا يؤدي بطبيعة الحال إلى حالات تستغل فيها القوى الصاعدة ديناميكيته للبحث عن أهداف غير أمنية مثل الثروة والتأثير من خلال تحدي أنماط الوضع الراهن للتفاعل والتأثير، ولكن الدول التي تقود هذا الوضع الراهن ستقاوم التغيير، يقود هذه القوى التصحيحية إلى تسليح نفسها لدعم توسعها، بينما تستجيب قوى الوضع الراهن من خلال التسليح بينما لا تزال متقدمة على أمل ردع القوى الصاعدة عن السعي وراء أجندات تخريبية. والنتيجة هي سباق تسلح (Jellenc، 2012).

ومع تغير طبيعة الحرب ونوع التهديد ذهب الاستشاري لدى وزارة الدفاع الأمريكية بيتر سينجر P.W.Singer وفي تساؤل مثير عن جدوى الحرب، قائلا: "في أثناء عملية البحث صدمني انهيار آخر للنموذج التقليدي بشأن من يفترض أن يكونوا في حالة حرب"، وتحدث عن تغير الخصوم في القرن الحادي والعشرين واصفا الحرب على أنها "ليست مجرد تدمير بشري، بل إنها خليط من أقصى أشكال الرعب والهدر. نحن نلجأ باستمرار إلى الحرب إما لنشر إيديولوجية رائجة في زمن ما وإما لدمرها." فنحن نعيش في زمن يشهد أهم التطورات في مجال الأسلحة منذ القنبلة الذرية. وقد يرى البعض أيضا صعود هؤلاء المحاربين الرقميين أكثر أهمية على اعتبار أن الروبوتات لا تغير درجة دموية الحرب فحسب، ولكن أيضا هوية المحارب (سينجر، 2010، الصفحات 12-21).

في حين يذهب "ألفين توفلر" Alvin Toffler إلى أن حروب المستقبل ستكون " عبارة عن كومبيوتر ضد الأقمار الصناعية وفكر وأعصاب البشر، وهي لا تتطلب صواريخ أو دبابات بل تتطلب معلومات دقيقة وبرامج كمبيوتر، ويقول خلال 5-10 سنوات سيكون بإمكاننا أن نخاطب الدول المعادية الكترونيا وتقنيا ودون قتل نفس واحدة (المخادمي، 2015، صفحة 153). خاصة في ظل هذا الانفتاح الكوني عبر الأجهزة الالكترونية (العمر، 2013، صفحة 183).

هذا ويعترف ألفين توفلر ضمنا أن العدو لم يختفي باختفاء الاتحاد السوفيتي، بل تحول اسمه وشكله ولم يعد ممكنا تشخيصه بدقة لذلك فنحن لا نعرف من هم أعداؤنا ومن هم أصدقاؤنا على وجه اليقين، فحرب الفضاء الالكتروني ستكون هي الشكل الغالب لحروب المستقبل، والتركيز على الأقمار الصناعية والصواريخ يفرض علينا أسلحة مضادة للأقمار الصناعية، ولكن ليست أسلحة تقليدية بل برامج كومبيوتر فإذا كنا نرغب بتدمير بلد نوجه إشارات إلى أقماره الصناعية لتقوم بتضليل أجهزة استلامه، وهذا

يعني أن الانتقال من القوة العسكرية التقليدية إلى امتلاك القوة العسكرية العقلية معتمدين على الكمبيوتر والمعلومات الاستخباراتية (المخادمي ع.، صفحة 145) .

لهذا تعبر الحرب الالكترونية؛ عن النموذج الجدي الذي ظهر ردًا على العدو غير المتوقع الذي يجارب من خلال الشبكات بدلا من التشكيلات العسكرية المعتادة. حيث لم يكن بالإمكان التعرف على هؤلاء المقاتلين بسهولة على أرض المعركة، حيث استغلوا عنصر عدم وضوح هوياتهم كميزة قتالية إضافية. كما أن أنشطتهم لا تقتصر على ساحات القتال واضحة المعالم أو الأهداف العسكرية المعتادة، هذه الخصائص مكنتهم من مقاومة ميزة القوى الكبرى في مناورات الحروب التقليدية، أو القوة الجوية، الخدمات اللوجستية. وأصبحت هذه المعضلة حافزًا لإعادة التغيير في استراتيجيات الأمن القومي استنادًا إلى الحاجة لتحديد وفحص، واستهداف هؤلاء المقاتلين الفرديين وشبكاتهم (فويلز، 2018، الصفحات 20-21).

على الرغم من اختلاف الصراع السيبراني عن الصراع التقليدي، بالأخص العسكري الذي يعد حكرًا على الدول والجماعات المسلحة، وهي صراعات تدور في بيئة جغرافية معينة، وتستمر لمدة زمنية معينة، إلا أن هذه الصراعات التقليدية قد دخلت فيها أدوات تكنولوجيا سيبرانية، فبمجرد نشوب صراع تقليدي بين الدول تصبح قطاعات الاتصالات، المعلومات، والبنى التحتية المعلوماتية ضمن أهداف الدول، ومن ثم، باتت الأسلحة الالكترونية أساسًا ثابتًا ضمن إستراتيجية الحروب الحديثة، حيث وفر الفضاء السيبراني للفاعلين هامشًا كبيرًا للمناورة، وتحقيق الأهداف دون اللجوء إلى الأعمال العسكرية في طابعها التقليدي (العبودي، الصفحات 345-374).

واستجابة لتطور الرقمنة، استثمرت الحكومات في القدرات الإلكترونية من أجل تأمين شبكات الدفاع الوطني والبنية التحتية. ومع ذلك، نظرًا لأن القدرات الإلكترونية قللت بشكل كبير من التكاليف العسكرية والبشرية للحرب - كما أصبح من السهل الوصول إليها - فإن كل من الحكومات والجهات الفاعلة غير الحكومية على استعداد متزايد لاستخدامها كأدوات هجومية. فخلال السنوات الماضية، أعلنت دول مثل الولايات المتحدة وروسيا اعتماد عقيدة هجومية عبر الإنترنت، تحدد كيف ومتى سيستخدمون الأسلحة السيبرانية (Jellenc, libid) .

في هذا الصدد أُجري تقييم لمعهد الأمم المتحدة لبحوث نزع السلاح العام 2012 مسحًا للمعلومات المتاحة للجمهور لـ 193 عضوًا في الأمم المتحدة ووجد أن 114 دولة لديها برامج وطنية للأمن السيبراني. تعطي 47 دولة منها دورًا للقوات المسلحة، في حين أن 67 دولة لديها برامج مدنية فقط. تشير الدراسة نفسها إلى أن 12 من أصل 15 من أكبر المنفقين العسكريين لديهم أو يطورون وحدات مخصصة للحرب الإلكترونية، ويبدو أن 10 منها تمتلك أو تطور قدرات إلكترونية هجومية، منها الولايات المتحدة والمملكة المتحدة والصين وروسيا، فرنسا (Cirlig, 2014)، وإيران وإسرائيل (الكيان المحتل)، هذه الدول التي تتبادل رسائل الردع الإلكتروني بقليل من الضجيج مما يساهم على الأرجح في انتشار الهجمات الإلكترونية (Goodman, 2010, pp. 102-135)، محولين صد المتسللين الذين يتمكنهم التقنية مثلاً من أن يلوثوا إمدادات المياه، كما يمكنهم تعطيل النظام المالي، وإرسال الطائرات على مسار تصادمي (Nye, 2016, pp. 44-71). وكذا المساس بعدد البنى الحيوية التحتية الرقبة والمادية الأخرى، كأنظمة المفاعلات النووية.

نتيجة لذلك، من المتوقع أن يرتفع الطلب المتزايد على الأدوات والأنظمة الإلكترونية الهجومية بنسبة تصل إلى 39٪ بحلول عام 2027، بتشجيع من الاتجاه المتزايد لميزانيات الدفاع السيبراني في جميع أنحاء العالم. هذا وتقع الشركات الأكثر تقدمًا في هذا المجال بشكل أساسي في الولايات المتحدة وإسرائيل وأوروبا، مثل **BAE Systems** أو **Cisco Systems** أو صناعات الفضاء الإسرائيلية (**IAI**). قاد هذا الاتجاه خبراء الإنترنت إلى تسميته "سباق التسلح الإلكتروني"، والذي من المتوقع أن يتوسع في المستقبل القريب كما أوضح خبير تكنولوجيا المعلومات الفنلندي **ميكو هيبونن**، الذي قال: "من المحتمل جدًا أن نفني الستين سنة القادمة في سباق التسلح الإلكتروني" (Baudouin-Naneix, 2019).

3. الردع السيبراني: طبيعة المفهوم وتداخلاته

يعد التعريف الأبرز والأشهر للردع **Deterrence** هو تعريف الجنرال "أندريه بوفر" الذي قدمه على أنه "منع دولة معادية من اتخاذ قرار باستخدام أسلحتها - أو بصورة أعم - منعها من العمل أو الرد إزاء موقف معين باتخاذ مجموعة من التدابير والإجراءات التي تشكل تهديدًا كافيًا حيالها، والنتيجة التي يراد الحصول عليها بواسطة التهديد هي نتيجة سيكولوجية نفسية (البهي، 2017)

كما يمكن القول أن الردع هو ممارسة تثبيط أو كبح شخص ما - في السياسة العالمية وعادة ما تكون دولة قومية - من اتخاذ إجراءات غير مرغوب فيها، مثل الهجوم المسلح. (قوادري، 2020، الصفحات 518-531)

في هذا الشأن كتب روبرت جيرفيس **Robert Jervis** عن "ثلاث موجات من نظرية الردع **three waves of deterrence theory**" في الحقبة النووية قائلا "إن التنظير حول الردع في العصر السيبراني يخرج من الموجة الأولى فقط (Jervis, 1979, pp. 289-324)

فمع ظهور مفهوم "الدول المارقة"، ظهرت موجة ثالثة من "نظرية الردع"، والتي ارتبطت أيضاً بظهور "فاعلين من غير الدول" وانتشار الإرهابيين، مما يتطلب وجود تدابير وقائية.

منذ هذه العلامة المفاهيمية عالية المستوى، طبق محللون مفاهيم الردع على المشكلات الأمنية المعاصرة، وأصلوها لها أكاديمياً. (Loc.cit, Goodman)

فيما تعود أصول الردع السيبراني إلى عملية عاصفة الصحراء عام 1991، عندما اكتسبت فكرة "الثورة في الشؤون العسكرية" شعبية كبيرة. فخلال المراحل الأولى من العملية شنت الولايات المتحدة الأمريكية "حرب معلومات **Information warfare**" التي وصفها "د.بيتز" **D.Betz** بأنها "سلاح محتمل يحد ذاته" لتتشكل بذلك أولى أدبيات الردع السيبراني في الحروب الحديثة. (حسين، صفحة 521)

يعرف الردع السيبراني على أنه "منع الأعمال الضارة ضد الأصول الوطنية في الفضاء والأصول التي تدعم العمليات الفضائية" ويرتكز الردع السيبراني على ثلاثة ركائز هي عماد إستراتيجية الدفاع السيبراني، تتمثل في: مصداقية الدفاع **Credible Defense**، والقدرة على الانتقام **An Ability to Retaliate**

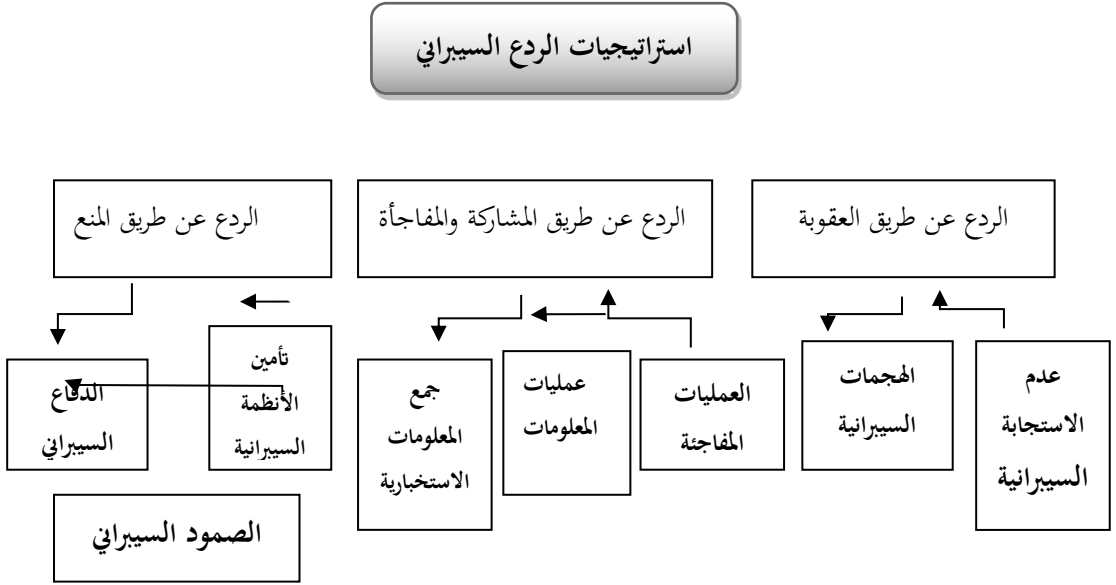
والرغبة في الانتقام **A Will to Retaliate**، فيما تعود استراتيجية الردع على الأقل إلى ثيوسيديدس **Thucydides** والحرب البيلوبونيسية **Peloponnesian War**، وكان للموضوع نهضة كبيرة خلال الحرب الباردة حيث سعت الولايات المتحدة والاتحاد السوفيتي إلى تجنب صراع نووي. (البهي، 2017)

ونظراً للعواقب الوخيمة التي قد تسببها "الحروب السيبرانية"، وجد بعض الكتاب أن ثمة طريقاً لتطبيق نظرية الردع على الفضاء السيبراني، معتمدين على عنصرين هما: ردع الهجمات السيبرانية فيما يُعرف "الردع بالمنع"، والردع بالتهديد بشأن هجمات سيبرانية فيما يُعرف بـ "الردع بالانتقام"، وفق استراتيجيات يوضحها المخطط التوضيحي أدناه.

ويمكن أن نميز بين "الردع بالمنع" و "الردع بالانتقام"، فـ "الردع بالمنع" يكون فعّالاً بمجرد جعل حسابات "التكلفة" لدى المهاجمين سلبية، من خلال إقناع المهاجم بأنه لن تكون هناك مكاسب تتناسب مع تكلفة الهجوم. وبالتالي تتضح أهمية النظم الدفاعية الجيدة التي تجعل فرص نجاح أي هجوم ضئيلة، وعلى الرغم من ذلك، يمكن تجاوز التدابير الدفاعية، فعلى سبيل المثال تم تجاوز إنشاء إيران هياكل متوازية لشبكة وطنية لمنع الهجمات الإلكترونية عالية المستوى، من خلال فيروس "ستكسنت" **Stuxnet** الذي أصاب برنامج المفاعل النووي من خلال **USB- sticks**

أما "الردع بالانتقام أو العقاب"، فينطوي تحت "الردع بالمقاومة" **Resistance**، و "الردع بالصمود" **Resilience**. والصمود هنا يعني القدرة على استعادة الشيء بشكله الأصلي قبل الهجوم الذي تم، وهذا من شأنه أن يحد المكاسب المحتملة، ويمكن أن يقنع الخصم بعدم الهجوم خاصة إذا كانت التكلفة مُفرطة. ويظل الهدف من "المقاومة والصمود" هو تقليل خيارات الطرف الذي ينوي الهجوم، سواء من خلال بناء هياكل دفاعية يصعب التغلب عليها أو من خلال ضمان الاستعادة السريعة لأصل الشيء بعد الهجوم، و يحمل تطبيقه الكثير من التحديات لأن هناك قيود أخرى للانتقام في المجال السيبراني تتمثل في عدم التناسب بين كثافة الهجمات والضرر الناتج، وفكرة تطور الأنظمة عبر مرور الزمن، مما يجعل فرص الاختراق محدودة، لتعقد الأنظمة. وأيضاً مدة الهجمات، فكلما طالت الهجمات كان من الصعب تنفيذ هجمات لاحقة. (الديواني، 2015)

الشكل 1: استراتيجيات الردع السيبراني



المصدر: خالد بن سعد الشايع، الأمن السيبراني مفهومه وخصائصه وسياساته، 2019

تمثل هذه التطورات في السياسية نقطة تحول مهمة أخرى في تطور الردع السيبراني كركيزة ضامنة ومركزية لسياسة الأمن الدولي. تعكس كل استراتيجية من استراتيجيات الردع السيبراني السالفة الذكر تصورات الدول ومصالحها، والاستعدادات للنزاع السيبراني. على هذا النحو، يصبح من الضروري للغاية أن تكون قادرًا على تقييم النجاحات والفشل النسبي لهذه السياسات والأنشطة التي تقوم بها، ويتطلب القيام بذلك مجموعة أدوات تحليلية لمدى نجاعة استراتيجيات الردع.

4. من الردع التقليدي إلى الردع السيبراني.

من الطبيعي في التهديدات الإستراتيجية بأن يكون الإجراء العقابي (إذا فشل التهديد وكان لا بد من تنفيذه) مؤلماً ومكلفاً للجانبين، فالهدف من التهديد هو الردع المتوقع وليس الانتقام المحقق (شيلينج، 2010، صفحة 201)، خاصة وأن قاعدة الردع هي وضعية دفاعية تواجه الخصم باحتمال الفشل

التشغيلي نتيجة العدوان (David Ochmanek, 2015, p. 7) ، فبعد ظهور الأسلحة الذرية - بقوة المدمرة - بدأ التفكير الجدي في الردع بعد حادثي هيروشيما وناغازاكي. وهكذا ظهر نوع غريب من الاستقرار الاستراتيجي في شكل "التدمير المتبادل المؤكد (MAD) ، الذي ما زال العقيدة المستقرة لغاية اليوم.

وقد تتبع الأسلحة السيبرانية مسارا مماثلا في أعقاب هجوم ستكسنت **Stuxnet attack** على إيران، والذي أثبت أن الفيروسات يمكن أن تسبب في تدمير مادي يتم تحقيقه عادة بالقنابل والرصاص، فبمثل هذه الفيروسات والعناصر الأخرى من الترسانات الافتراضية - ذات قابلية الاستخدام الظاهر للهجوم السيبراني - قد تسبب في حدوث خلل يمكن أن يكون تأثيره أكثر من تأثير التدمير الشامل، نتيجة سهولة الوصول إلى مثل هذه القدرة (نظراً لان تكلفتها أقل بكثير، إلى جانب أن هذه الخبرة العالمية منتشرة على نطاق واسع). لذلك ، يجب الاعتراف بأهمية التفكير في الردع في هذا العصر، والنظر في الخطاب الدولي حول الحرب السيبرانية بواقعية.

فكون المهاجمين السيبرانيين قادرين على الاختباء وراء ستار من "عدم الكشف عن الهوية " أو من الإنكار المعقول - تجعل من غير الواضح ضد من وكيف ترد؟.

والحقيقة البسيطة في الأمر هي أنه في غياب التشريع لنوع ما من الاتفاقات الدولية التي تنص على الامتناع عن الهجمات السيبرانية ضد الأهداف المدنية، فإن الردع في حد ذاته شكل ضعيف. نعم ، لا يزال الردع النووي قوياً إلى حد كبير، ولكن عندما يتعلق الأمر بالهجوم السيبراني، فإن عالم الردع بعد ستكسنت يشبه إلى حد كبير عالم الردع قبل هيروشيما.

التحدي الآن هو تصميم نسخة رادعة في عصر المعلومات فيما تشير الدراسات المتوفرة إلى أن معظم دول العالم بعيدة كل البعد عن هذا الهدف. والولايات المتحدة متخلفة بشكل خاص، كما يراها قيصر الإنترنت السابق في واشنطن ريتشارد كلارك **Richard Clarke** . في كتابه " **Cyber War** الحرب السيبرانية" حيث يضع تقييمه للدفاعات الافتراضية للقوى السيبرانية بالولايات المتحدة في المركز الأخير ويؤكد أن أفضل الدفاعات السيبرانية موجودة في كوريا الشمالية، وتبعتها الصين وروسيا وبدرجة أقل إيران. (Arquilla, 2015)

مما سبق نفهم أن مفهوم الردع انتقل من المفهمة التقليدية التي تأتت بعد الحرب الباردة والتي مفادها ردع الدول الأخرى من تنفيذ هجومها النووي لقدرة الدولة على الانتقام الهائل بواسطة الهجوم

النووي إلى الردع في الفضاء السيبراني عن طريق توفير آليات دفاع سيبراني لتفادي الضرر في الفضاء السيبراني الذي يعتبر بعد سيادي جديد تأتي من خلال الثورة في الشؤون العسكرية.

هذا وتعتمد مسألة ما إذا كان الردع يعمل في الفضاء السيبراني على "من وماذا". ليست كل الهجمات الإلكترونية ذات أهمية متساوية؛ لا يمكن ردع كل شيء؛ وليس كل شيء يصل إلى مستوى التهديدات الأمنية الوطنية. والدرس المستفاد لصانعي السياسات هو التركيز على أهم الهجمات وفهم السياق الذي قد تحدث فيه هذه الهجمات، عبر اتخاذ مجموعة كاملة من الآليات المتاحة لمنعها.

إلا أن أكبر مشكلة في الردع الإلكتروني تبقى الردع ذاته على حد تعبير الرئيس الإستوني السابق توماس إلفيس **Toomas Ilves**. في هذا الشأن يجادل ريتشارد كلارك **Richard Clark** وروبرت كناك **Robert Knake** بأن "من بين جميع مفاهيم الإستراتيجية النووية، فإن نظرية الردع هي على الأرجح الأقل قابلية للتحويل إلى الحرب السيبرانية". كما يجادلون بأن الاعتماد الشديد للولايات المتحدة على الاتصال السيبراني يجعلها عرضة بشكل خاص للهجمات الإلكترونية غير المتماثلة: "في العالم الحقيقي، ربما ينبغي ردع الولايات المتحدة عن الشروع في حرب إلكترونية واسعة النطاق خوفاً من الآثار غير المتكافئة التي يمكن أن يحدثها الانتقام على الشبكات الأمريكية."

يقودنا هذا لبناء تصور علمي مفاده أن فهم الردع في الفضاء الإلكتروني أمر صعب في كثير من الأحيان لأن أذهاننا يتم التقاطها من خلال صور الردع في الحرب الباردة على أنها تهدد بالانتقام الكبير للهجوم النووي بالوسائل النووية. ومع ذلك، فإن التشابه مع الردع النووي مضلل، لأن هدف الولايات المتحدة مثلاً (الذي تحقق حتى الآن) كان منعاً تاماً. في المقابل، فإن العديد من جوانب السلوك السيبراني أشبه بالسلوكيات الأخرى، مثل الجريمة، التي تحاول الولايات المتحدة (بشكل ناقص) ردعها. يتضمن منع الضرر في الفضاء السيبراني آليات معقدة مثل التهديد بالعقاب، والحرمان. علاوة على ذلك، حتى عندما يتم استخدام العقاب، لا يجب أن تقتصر التهديدات الرادعة على الاستجابات السيبرانية، بل قد تتعامل مع السلوك العام وكذلك الأفعال المحددة (Nye, Deterrence and Dissuasion in Cyberspace, 2016, pp. 44-71).

فنظراً لصعوبات إسناد الهجمات إلى مرتكبيها وما يترتب على ذلك من احتمالات الانتقام المرتبطة بها، يمكننا القول أن المجال السيبراني يمثل تحدياً للآليات التقليدية للردع. ففي عام 2015، قال أحد كبار

الشخصيات الأمريكية المتخصصة في الفضاء الإلكتروني لمجلس الشيوخ الأمريكي أنه نظرا لأن الردع التقليدي "يتآكل لدرجة مقلقة، فإن معالجة هذا الخطر في مجال الفضاء الإلكتروني" أمر أساسي "من أجل الحفاظ على فعالية الأدوات التقليدية للسلطة الوطنية" (رفيق).

وعلى صعيد آخر، يقترح "يوري تور" (الباحث في المركز البيني بمرتسليا) بأن التركيز على "الردع المطلق" المستمد من خبرة الردع النووي الأمريكي يخلق توقعات زائفة بقدرته على مواجهة كافة الأنشطة الضارة، غير أنه لن يحول دون كافة الهجمات السيبرانية. وعليه، يستند "تور" على خبرة "الردع التراكمي"، الذي جمع بين التهديد والاستخدام الفعلي للقوة لردع العدوان. وهو ما يتطلب مزيجاً من الوسائل السيبرانية وغير السيبرانية.

ولا توجد استراتيجية يمكنها منع كافة الأنشطة الضارة في الفضاء السيبراني، ولكن على عكس الردع النووي، لا يفشل الردع السيبراني تلقائياً في حالة الهجوم. لذا، يجب التركيز على الآثار التراكمية للسلوك العدائي، سواء كان ناتجاً عن هجوم إلكتروني واحد واسع النطاق أو أكثر. (البهي، صعوبات بناء إستراتيجية شاملة في الفضاء السيبراني، 2019)

فالرأي الذي يؤسس لفشل نماذج الردع المعروفة في حروب الانترنت، يحتاج بأن الردع بالانتقام أو العقاب لا ينطبق على سبيل المثال على هذه الحروب، حيث انه من الصعوبة بمكان بل ومن المستحيل في كثير من الأحيان تحديد الهجمات الالكترونية ذات الزخم العالي. بعض الحالات تتطلب أشهر لرصدها وهو ما يلغي مفعول الردع بالانتقام وكثير من الحالات لا يمكن تتبع مصدرها في المقابل وحتى إذا تم تتبع مصدرها وتبين أنها تعود لفاعلين غير حكوميين فإنه في هذه الحالة لن يكون لديهم أصول أو قواعد حتى يتم الرد عليها (الغفار، صفحة 12)، وبالتالي فقد أصبح الفضاء السيبراني مصدراً رئيساً لانعدام الأمن (جواد، 2016، صفحة 145)، وردع الأنشطة السيبرانية السيئة فيه يتطلب تكاتف الجهود التقنية والقانونية على أمل التخفيف منها لا ردعها بصفة نهائية للأسباب سابقة الذكر.

5. من الردع إلى البحث عن السلام الإلكتروني

اليوم، وبعد أن أنشأت أكثر من عشرين دولة وحدات لحرب الفضاء الإلكتروني الهجومية بجيوشها وأجهزة استخباراتها، وبعد أن زاد فهمنا لشكل حرب الفضاء الإلكتروني في المستقبل آن الأوان

لتقوم الدول بمراجعة موقفها بشأن ضبط التسليح الإلكتروني والتفكير فيما إذا كان هناك أي فائدة يمكن أن تجنيها من خلال الاتفاقيات الدولية في هذا الإطار (كلارك، صفحة 258)، ومن ناحية أخرى، نجد بعض المبادرات ما بين الفواعل لتحقيق التعاون في مجال الأمن الإلكتروني في صورة مباحثات أو اتفاقيات مشتركة كتلك التي تمت ما بين الولايات المتحدة الأمريكية وروسيا، وما بين الدول الأعضاء في حلف شمال الأطلسي. وهو الأمر الذي يطرح سؤالاً عن مدى تأثير هذه التفاعلات في تحقيق الأمن الإلكتروني أو السلام الإلكتروني **Cyber peace**، ومن ثم تحقيق الأمن العالمي.

حيث بات ينظر للأمن السيبراني كرافد جديد للأمن القومي وجزء من الأمن الجماعي، بما أن العلاقة بين الأمن والتكنولوجيا علاقة متزايدة مع إمكانية تعرض المصالح الإستراتيجية - ذات الطبيعة الإلكترونية - إلى مخاطر إلكترونية، الأمر الذي يهدد بتحول الفضاء الإلكتروني لوسيط ومصدر لأدوات جديدة للصراع الدولي المتعدد الأطراف ودورها في تغذية التوترات الدولية. ومن جهة أخرى فرضت تلك التطورات إعادة التفكير في مفهوم الأمن القومي الذي يُعنى بحماية قيم المجتمع الأساسية وإبعاد مصادر التهديد عنها، غياب الخوف من خطر تعرّض هذه القيم للهجوم، وبذلك يتوافر أمن الفضاء الإلكتروني حال تحقيق إجراءات الحماية ضد التعرّض للأعمال العدائية والاستخدام السيئ لتكنولوجيا الاتصال والمعلومات.

هذا وقد عني الأمن الإلكتروني بعملية وضع المعايير والإجراءات المتخذة لمنع وصول المعلومات إلى أيدي أشخاص غير مخولين بها عبر الاتصالات ولضمان أصالة وصحة هذه الاتصالات. وجاءت تلك المظاهر لتبرز استخدامات غير سلمية للفضاء الإلكتروني وما يمثله ذلك من تهديد للأمن الإلكتروني العالمي والبنية التحتية الكونية للمعلومات من جانب كافة الفاعلين في مجتمع المعلومات العالمي، وأصبحت هناك مصلحة قُطريّة فضلاً عن دولية في الحفاظ على أمن الفضاء الإلكتروني، على اعتبار أن أمن الدول جزء من الأمن الجماعي، الأمر الذي يستدعي اتخاذ إستراتيجية مرنة تتواءم مع المتغيرات المستمرة، سواء في الآليات أو في التكتيكات الخاصة بالأمن مقابل التطور المستمر في الأخطار. ويرجع ذلك إلى الطبيعة المتغيرة للفضاء الإلكتروني وفقاً للعامل الإنساني. وتساعد مخاطر التهديدات الإلكترونية على البنية التحتية الكونية للمعلومات (الصادق، 2017).

وعلى الرغم من أن الاهتمام بقضايا أمن الفضاء الإلكتروني أكثر وضوحا بالنسبة للقوى الكبرى- والتي لا يتوقف اهتمامها بالأمن الإلكتروني فقط من زاوية رد الفعل أو محاولة التصدي للتهديدات المترتبة عليه، وإنما يمتد إلى وضع استراتيجيات واسعة النطاق في التعامل مع القضايا الخاصة به، والاستناد إلى الآليات الإلكترونية المرتبطة به كإحدى أدوات السياسة الخارجية وإدارة التفاعلات الدولية، ومن ثم تحقيق المصالح- غير أن دول الجنوب والعالم الثالث بشكل عام، قد بدأت أيضا إدراك أهمية الأمن الإلكتروني والتهديدات المرتبطة به، ولذا نجد أنها قد بدأت في تطوير ما يسمى بفرق الطوارئ الخاصة بالحاسب الآلي **Computer Emergency Response Teams**، والتي تهدف بالأساس إلى التصدي للتهديدات الإلكترونية التي قد تتعرض لها الدولة.

ومن ثم، يمكن القول بأن قضايا الأمن الإلكتروني وتهديداته قد باتت تشغل نطاقا واسعا من الفواعل الدولية المختلفة بحثا عن السلام في الفضاء الإلكتروني، ولكن تظل القوى الكبرى هي الأبرز في هذا الاهتمام، نتيجة لامتلاكها قدرات تكنولوجية هائلة، واعتمادها بشكل كبير على أنظمة المعلومات في إدارة شؤون الدولة. لذا نجد أن اهتمامها بهذه القضايا يأتي في إطار استراتيجيات وسياسات، واستخدام الفضاء الإلكتروني ك مجال لإدارة التفاعلات الدولية. في حين يظل اهتمام دول الجنوب بقضايا الأمن الإلكتروني محدودا ومقصورا فقط على محاولة التصدي للتهديدات الأمنية المرتبطة به (شفيق، مرجع سابق، الصفحات 6-7).

في هذا الصدد إذ أكد مبعوث الرئيس الروسي لشؤون التعاون الدولي في مجال أمن المعلومات "أندريه كروتسكيخ" على ضرورة توحيد الجهود لمواجهة الهجمات الإلكترونية، معتبرا أنها "إرهاقا إلكترونيا".. مؤكدا على ضرورة بدء الحوار بين الخبراء الروس والأميركيين لوضع خطط مشتركة لمحاربتها، مشيرا إلى استعداد موسكو للحوار مع واشنطن في جميع القضايا العالمية التي تخص الهجمات الإلكترونية، لكنه قال إن موقف الرئيس الأميركي دونالد ترامب يعيق تشكيل فريق مشترك لبدء التعاون العملي.

أما الصين فقالت على لسان المتحدث باسم وزارة الخارجية "هوا تشان بينغ" إن بلادها تحت المجتمع الدولي على العمل من أجل تعزيز مفهوم الأمن المشترك، وحماية السلام في الفضاء الإلكتروني، ومنع سباق التسلح الإلكتروني، وضمان استخدام التقنيات السيبرانية لرخاء وتقدم البشرية (ك، روسيا والصين تدوعان الى تعاون دولي في أمن المعلومات، 2017)، ومنع وتسوية الصراع والمصالحة أو حتى إدارة الأزمة، ودعم القدرة علي إقامة تحالفات جديدة في صورة شبكات الكترونية بين الحكومات والمنظمات الدولية والمجتمع

المدني والقطاع الخاص وحشد الرأي العام الدولي والتنسيق الفعال مع تجاوز الحدود المكانية والهياكل البيروقراطية، لما للفضاء الإلكتروني من تأثيرات علي التنظيم الاجتماعي والتفاهم الدولي المشترك (الصادق، هل يكون للفضاء الإلكتروني دور في صنع السلام وحل الأزمات الدولية؟ ، 2014) .

فيما دعا مجلس الأمن - في ضوء الاعتراف بتحديات الأنشطة الخبيثة في الفضاء السيبراني - جميع الدول للامتناع عن استخدام الفضاء الإلكتروني لأغراض عسكرية، وأعلن أنها "منطقة خالية من السلاح". وعلى ضرورة بناء الثقة الملزمة، بما في ذلك آلية التشاور الإلزامي، وذلك من أجل منع أي نزاع ينشأ عن استخدام تكنولوجيا المعلومات والاتصالات. كما أنشأت هيئة لتسوية النزاعات في الفضاء السيبراني (ريموندنك، 2019)، وشكلت بداية الجهود التعاونية لمواجهة تهديد الحرب الإلكترونية ووضع معايير دولية للسلوك في الفضاء الإلكتروني (Ibid ، Cirlig).

6. خاتمة

أصبحت فكرة الردع في الفضاء الإلكتروني جزءاً من الإستراتيجية الأمنية السيبرانية لأي دولة؛ ورغم عدم مثاليته تطبيقاً عكس جدواه نظرياً إلا أنه أفضل من عدم وجوده على الإطلاق. كما أن الهجمات السيبرانية تجعل من الضروري البحث في كيفية منعها خشية تكرارها، خاصة في ظل سهولة الحصول على الأسلحة السيبرانية وشن الهجمات باستخدامها، وصعوبة تحديد الخطوط الحمراء التي لا يُمكن تجاوزها على صعيد تلك الهجمات.

هذا وظل الردع جزءاً من الإستراتيجية السيبرانية، وبدأ يلعب دوراً في استراتيجيه الردع السيبراني. هذا يعكس الاتجاه الأوسع المتمثل في لعب الإنترنت دوراً لا يتجزأ بشكل متزايد في الإستراتيجية والعقيدة وبنية القوة الشاملة

كما خلصت الدراسة لجملة استنتاجات نوجزها في التالي:

الاستنتاجات:

- التطورات التكنولوجية والمعلوماتية أدت إلى ثورة في مجال الأسلحة وفي استراتيجيات شن الحروب المسلحة، وغيّرت من الطريقة التي تدار بها الحرب.
- إن تزايد اعتماد الدول على الحرب السيبرانية قد يؤدي إلى تصعيد الصراع إلى مواجهات عسكرية في العالم الواقعي.

- تشير النتائج التي توصلنا إليها إلى أن الدول قد انخرطت بالفعل في سباقات التسلح السيبراني، من خلال الزيادة المتبادلة التنافسية والغير مسبقة في القدرات الإلكترونية. يعزز هذا العمل فهمنا لسلوك الدولة في المجال السيبراني.
- سيؤدي النزوع نحو الحروب السيبرانية لمستقبل يصبح فيه تفويض هياكل الحكم والقيم التي تمثلها أكثر شيوعاً، و ستكون البنية التحتية الرقمية بالغة الأهمية معرضة للقرصنة وسرقة البيانات مما يعرض وبالأساس لاقتصادنا المستقبلي للخطر.
- التهديدات السيبرانية تمثل خطراً على أمن الفضاء الإلكتروني باعتباره أصبح مرفقاً دولياً.
- الردع السيبراني أسهل من الناحية العملية مما يبدو عليه من الناحية النظرية لأن الهجمات الإلكترونية لا تنفصل في النهاية عن المجال المادي، حيث يتمتع الردع بسجل حافل بالنجاح، فيما يقول آخرون بصعوبة تحقيق مبدأ الردع في الفضاء السيبراني لصعوبة تحديد وتتبع مرتكبي الهجمات السيبرانية.
- نظراً لصعوبات إسناد الهجمات إلى مرتكبيها وما يترتب على ذلك من احتمالات الانتقام المرتبطة بها، يمكننا القول أن المجال السيبراني يمثل تحدياً للآليات التقليدية للردع.
- عند مقارنته بالتطورات الحاصلة في مفهوم الردع في المجالات الأخرى، لا يزال الردع السيبراني في مهده. وفي بعض النواحي تتفوق ممارسة الردع السيبراني على نظرية الردع السيبراني حيث يتم تطوير التكتيكات والإستراتيجية والعقيدة والسياسة واستخدامها حتى قبل فهم النظريات المقابلة بشكل صحيح.
- استجابة للتهديد المتزايد للهجمات الإلكترونية من المتوقع أن تولي الحكومات أهمية متزايدة لقضايا الأمن السيبراني وتعزيز مختلف تدابير الحماية التكنولوجية والسياسية، وتكريس سبل التعاون الدولي ضماناً للأمن السيبراني العالمي.

قائمة المراجع:

• المؤلفات:

- ألفين وهايدي توفلر، تر محمد عبد الحليم أو غزالة، الحرب وضد الحرب، (مصر: دار المعارف، 2000)؛
- توماس شيلينج، تر نزهت طيب وأكرم حمدان، إستراتيجية الصراع، ط1، (الدوحة:الدار العربية للعلوم ناشرون، 2010)؛
- توماس كوبلاندي، ثورة المعلومات والأمن القومي، (الإمارات العربية المتحدة: مركز الإمارات للدراسات والبحوث الإستراتيجية، 2003)؛
- نوران شفيق، أثر التهديدات الالكترونية على العلاقات الدولية دراسة في أبعاد الأمن الالكتروني(القاهرة: المكتب العربي للمعارف، القاهرة، 2016)؛
- بيتر سينجر، الحرب عن بعد دور التكنولوجيا في الحرب، ط1، (الإمارات: مركز الإمارات للدراسات والبحوث الإستراتيجية، 2010)؛
- عبد القادر المخادمي، الحرب الناعمة هل تكون بديلا لحروب المستقبل؟ (الجزائر: ديوان المطبوعات الجامعية، 2015)؛
- معن خليل العمر، الجريمة المنظمة والإرهاب، (عمان-الأردن: دار الشروق للنشر والتوزيع، 2013)،
- غلين فويلز، صعود الحرب الالكترونية: الهوية والمعلومات وخصائص الحرب الحديثة، (ليبيا: ترجمة مركز حازم لترجمة الدراسات الإستراتيجية، 2018)؛
- ريتشارد إيه كلارك، روبرت كيه كنيك، حرب الفضاء الالكتروني الخطر القادم على الأمن القومي وسبل المواجهة، ط1 (أبو ظبي: مركز الإمارات للدراسات والبحوث الإستراتيجية، 2012)؛

● المقالات:

- حسين قواري، الردع السيبراني بين النظرية والتطبيق، المجلة الجزائرية للأمن والتنمية، العدد 16 جانفي 2020؛

- علي عبد الكريم العبودي، هاجس الحروب السيبرانية وتداعياتها على الأمن والسلم الدوليين، مجلة قضايا سياسية، العدد 57؛
- انمار موسى جواد، حروب الفضاء الالكتروني المفهوم الأدوات والتطبيقات، مجلة العلوم القانونية والسياسية، الجزائر، عدد 2 مجلد 5، جوان 2016؛

• مواقع الانترنت:

- رغدة البهي (2017)، الردع السيبراني المفهوم والاشكاليات والمتطلبات، مجلة العلوم السياسية والقانون، المركز العربي الديمقراطي:
<https://soo.gd/CBEA> (Consulté le 04/04/2021)
- عادل عبد الصادق (2017)، خطر الحروب السيبرانية عبر الفضاء الالكتروني، مقال في موقع لغة العصر: <https://goo.gl/e3Nm3q> (Consulté le 08/04/2021)
- عبد الغفار الديواني (2015)، القرن السيبراني: الردع الالكتروني بين المنع والانتقام، المعهد الألماني للشؤون الدولية والأمنية. <https://soo.gd/RYM9> (consulté le 07/05/2021)
- رغدة البهي، 2019، صعوبات بناء إستراتيجية شاملة في الفضاء السيبراني، مركز دراسات المستقبل، <https://soo.gd/lgl2> (consulté le 07/05/2021)
- د.ذ.ك (2016)، حرب المعلومات في سياق الحروب اللامتماثلة، مقال من موقع باب الواد :
<https://goo.gl/DMSzWn> (consulté le 17/04/2021)
- د ذ ك (2017)، روسيا والصين تدوعان الى تعاون دولي في أمن المعلومات، موقع الجزيرة الاخباري: <https://goo.gl/qVwvyB> (Consulé le 12/04/2021)
- عادل عبد الصادق (2014)، هل يكون للفضاء الالكتروني دور في صنع السلام وحل الأزمات الدولية؟، المركز العربي لأبحاث الفضاء الالكتروني ACCR: <https://goo.gl/rwqFc8> (Consulé le 25-02-2019)
- باتريك باولاك بروسيلس وناثالي فان ريمدونك (2019)، ماذا لو قادت "الشمس" إلى حروب سيبرانية؟، عرض صباح عبدالصبور، المستقبل للابحاث والدراسات المتقدمة:
<https://goo.gl/cLPBbU> (Consulé le 25-02-2019)

• **Magassine:**

- Joseph S. Nye, 'Deterrence and Dissuasion in Cyberspace', *International Security*, Volume 41, 2016.
- Kristin Lord and Travis Sharp, *America's Cyber Future Security and Prosperity in the Information Age*, volume 1, Centre for A new American Security, June 2011. Will Goodman "Cyber Deterrence Tougher in Theory than in Practice?", *Strategic Studies Quarterly*, 2010.
- Joseph S. Nye, 'Deterrence and Dissuasion in Cyberspace', *International Security*, Volume 41, 2016.
- Robert Jervis, "Deterrence Theory Revisited," *World Politics*, Vol. 31, N° 2, January 1979.
- Joseph S. Nye, *Deterrence and Dissuasion in Cyberspace*, *International Security*, Volume 41, 2016.
- David Ochmanek, Andrew R. Hoehn And others, *America's Security Deficit: Addressing the Imbalance Between Strategy and Resources in a Turbulent World*, RAND Corporation, 2015.

• **Websites:**

- John Arquilla, (August 4, 2015), *Deterrence After Stuxnet*, *Communications of the ACM*, Available at: <https://goo.gl/wR99ff>. (consulté le 08/04/2021)
- Eli Jellenc, (July, 2012), *The Emerging Cyber Arms Race and International Security : Theoretic Explanation and Empirical Foundation*, at the 9th European Conference on Information Warfare Available at: <https://soo.gd/0idN> (consulté le 05/05/2021).
- Carmen-Cri 1 Solène Baudouin-Naneix, 3 September 2019, *Cyber Weapons: The New 'Arms Race'*, European Army Interoperability Centre, Available at: <https://soo.gd/WJqh> (consulté le 10/05/2021)

- stina Cirlig, (2014), *Cyber Defence in the EU, Preparing for Cyber Warfare?*, [online] European Parliamentary Research Service, Available at: <https://soo.gd/YXZB> (Consulté le 09/05/2021).