الردع السيبراني بين النظرية والتطبيق.

Cyber deterrence between theory and practice.

حسين قوادرة

جامعة أم البواقي، الجزائر، hocine751@yahoo.fr

تاريخ الإرسال: 2019/08/13 **تاريخ القبول:** 2019/10/23 **تاريخ النشر:** 2020/01/01

ملخص:

مثلما هو الحال مع ظهور الحرب الجوية والقوة الجوية في النصف الأول من القرن العشرين، شهد المجال السيبراني تدفقًا سريعًا للتكنولوجيا. ليصبح في السنوات القليلة الماضية محور اهتمام صناع السياسات العسكرية، حيث تتسابق الدول لتأكيد هيمنتها وتفوقها. وقد تجاوز هذا التطبيق العملي الصياغة النظرية والتطور المفاهيمي، مما نتج عنه محاولة نقل الاستراتيجيات القديمة إلى المجال الجديد. ويكتسي الردع مكانة رئيسية بين تلك الاستراتيجيات، لكنه يعاني من مشاكل كبيرة برزت بشكل أساسي في العصر النووي. فطبيعة الفضاء السيبراني التي تتميز بعدم الأهمية المادية والقدرة على تجاوز الحدود الوطنية، مع غلبة الفواعل من غير الدول، تجعل القواعد التي تحدد الردع النووي غير قابلة للتطبيق. ومما يفاقم هذه القضايا الصعوبات الحقيقية في تحقيق المصداقية ومشكلة الإسناد. لكن لا يبدو أن استراتيجيات الردع السيبراني تستجيب لهذه القضايا، ولكنها بدلاً من ذلك تشعل خطابًا خطيرًا يغذي سباق التسلح المتفجر بشكل خاص.

الكلمات المفتاحية: *الفضاء السيبراني؛ الردع السيبراني؛ التهديد؛ الإسناد؛ سباق التسلح.*

Abstract:

As with the advent of air warfare and air power in the first half of the 20th century, the cyberspace saw a rapid flow of technology. In the past few years, it has become the focus of military policymakers, as countries race to assert their dominance. This practical application went beyond theoretical formulation and conceptual development, resulting in an attempt to move old strategies into the new field. Deterrence is central to these strategies, but it suffers from major problems that emerged mainly in the nuclear age. The nature of cyberspace, characterized by the insignificance of materiality and the ability to transcend national borders, with the predominance of non-State actors, render the rules defining nuclear deterrence unworkable. These issues are exacerbated by real difficulties in achieving credibility and the problem of attribution. But cyber-deterrence strategies do not seem to respond to these issues, but instead ignite a dangerous rhetoric that fuels a particularly explosive arms race.

Keywords: *cyberspace; cyber deterrence; threat; attribution; arms race.*

* **المؤلف المرسل: حسين قوادرة، hocine751@yahoo.fr**

مقدمة:

مع إرساء وتحول الفضاء السيبراني إلى مجال خامس للحرب، وجدت المفاهيم الكلاسيكية التي طورت في المجالات الأخرى (البرية والبحرية والجوية والفضائية) منفذاً جديداً. ومن بين هذه الأفكار فكرة الردع، التي أضحت موجودة ما دامت البشرية تخوض الحروب، بالرغم من أنها ربما تُذكر بشكل رئيسي على أنها الإستراتيجية الأساسية للعصر النووي. ومع أن القدرات السيبرانية لا تقدم نفس القدرة المدمّرة مثل الأسلحة النووية، فإن الهجمات الإلكترونية على الأنظمة المالية والرعاية الصحية وشبكات النقل والكهرباء - مثل هجوم ديسمبر 2015 الذي ترك 225.000 أوكراني بدون كهرباء- يمكن أن تنطوي على أضرار كبيرة محتملة. وبالنظر إلى أن الردع قد تجنب الصراع النووي ظاهريا، يبدو أن صانعي السياسة اليوم حريصون على اللجوء إلى هذا المفهوم لتجنب التبادل العدواني للضربات الإلكترونية.

ففي سبتمبر 2013، أصدر وزير الخارجية للدفاع "فيليب هاموند" Phillip Hammond بيانًا يتناول فيه جوانب معينة من الإستراتيجية الوطنية للأمن السيبراني للمملكة المتحدة. حيث أكد "هاموند": أن بناء دفاعات إلكترونية أصبح غير كاف كما هو الحال في مجالات الحرب الأخرى، علينا أيضًا استخدام الردع. ستقوم بريطانيا ببناء قدرة مخصصة للهجوم المضاد في الفضاء الإلكتروني، وإذا لزم الأمر يتم شن الهجوم في الفضاء الإلكتروني (Taylor 2013). ليتم تبني الموقف رسميًا في عدة دول بما فيها الولايات المتحدة الأمريكية ودول أخرى في الغرب والشرق على حد سواء، من خلال الاحتفاظ بموقف رادع عن طريق التطوير العلني للقدرات السيبرانية الهجومية، حتى لو لم يتم التذرع بخطاب الردع بشكل صريح.

هذا التركيز على القدرات السيبرانية التي يتم الحصول عليها بقصد الردع يستحق التشريح الدقيق لأنه محفوف بالسوابق التاريخية والآثار المترتبة على مستقبل السياسة الخارجية والعلاقات الدولية. وبالتالي ستتم معالجة الإشكالية التالية: هل يمكن تحقيق خطاب الردع السيبراني في ظل المخاطر الناجمة عن ذلك؟. وللإجابة على هذه الإشكالية سيتم تسليط الضوء على السياق التاريخي للردع، ثم التطرق إلى استعمال الردع في الفضاء السيبراني بما ينطوي عليه من تحول في المفهوم الكلاسيكي للردع الناتج عن تأثير التقنيات الحديثة للمعلومات، مع رصد مختلف التحديات التي تواجه الردع السيبراني الفعّال، وفي الأخير سيتم تحليل مخاطر انتشار خطاب الردع السيبراني.

أولا: السياق التاريخي للردع

الردع Deterrence هو ممارسة تثبيط أو كبح شخص ما - في السياسة العالمية، وعادة ما تكون دولة قومية - من اتخاذ إجراءات غير مرغوب فيها، مثل الهجوم المسلح. كما أنه ينطوي على محاولة لوقف أو منع أي إجراء، على عكس مفهوم "الإرغام" Compellence المرتبط به ارتباطًا وثيقًا ولكنه مختلف عنه، فهو محاولة لإجبار الفاعل على فعل شيء ما (Mazarr 2018).

فكرة الردع بطبيعة الحال ليست جديدة. إلا أن الإحاطة بفهم فكرة الردع الحديثة أمر ضروري من أجل صياغة الحوار السيبراني. ويعتبر الباحث الإيطالي "جيليو دوهيت" Guilio Douhet من المهتمين بموضوع القوة الجوية من خلال كتابه "The Command of the Air "، الذي أشار من خلاله إلى أن "القيادة الجوية" شكلت اتجاها جديدا في الفكر الاستراتيجي في القرن العشرين. فظهور القوة الجوية قدّم بُعدًا جديدًا للصراع. إذ

توقع "دوهيت" أن القوة التدميرية بالمعنى المادي وكذلك المعنى المحبط للحرب الجوية، سوف تمنع الدول في النهاية من شن الحرب على بعضها البعض. وأضاف بأن مثل هذا التقييد سوف ينبع من "طائرة وحيدة، يمكنها أن تحقق تجميد كل هذه الموارد والطاقات بمجرد وجودها المحتمل، دون الحاجة إلى الإقلاع والطيران على الإطلاق (Douhet 2009, p-p.24-28).

واستحوذت هذه الفكرة على خيال المخططين العسكريين، أين أصبح بالإمكان تجنب الحروب أو كسبها دون أي شرط لإنفاق اليد العاملة أو الموارد الباهظة التكلفة. فيشير الاستثمار في القوات الجوية في ثلاثينيات القرن الماضي إلى أن القيادات العسكرية تمكنت من إقناع حلفائهم/ممولهم المدنيين بأن الردع الجوي كان فكرة جيدة. إذ على سبيل المثال، بين عامي 1920 و1939، تلقى سلاح الجو الملكي البريطاني الذي تم إنشاؤه حديثًا زيادة سنوية في التمويل بنسبة 6.6٪، في حين فإن القوات البحرية الملكية التي كانت في السابق الذراع القوي للقوات المسلحة في المملكة المتحدة خسرت 1.1٪ في الفترة نفسها (UK Public Spending).

باندلاع الحرب العالمية الثانية انتهت مرحلة ردع سلاح الجو التي أثارت ضجة كبيرة، فبالرغم من الاستثمار في الأجهزة والمعدات لم يتم تجنب الحروب. ومع ذلك فإن الإنفجارات النووية الأكثر حدة التي أنهت هذه الحرب - القنابل الذرية التي أُسقطت على هيروشيما وناغازاكي في أوت 1945- نقلت فكرة الردع نحو العصر النووي.

فالدمار التام الذي تحدثه الأسلحة النووية بحد ذاته يحبط عملية استخدامها. لأن السمة الأساسية لإستراتيجية الردع، تكمن في عدم الاستخدام الفعلي للأسلحة النووية، بالموازاة مع ذلك يتم الاستغلال الحكيم لحقيقة وجودها. فما عليك سوى إظهارها للأعداء الذين لديك القدرة على تدميرهم، وهذا يكون كافياً لردعهم عن مهاجمتك. من المؤكد أن هذا الأمر قد ثبت خلال الحرب الباردة، خلال الحرب النووية بين الولايات المتحدة والاتحاد السوفيتي، ناهيك عن أي من القوى النووية الأخرى، إذ لم تحدث المواجهة/الحرب النووية، بالرغم من المخاوف الناشئة عن أزمة الصواريخ الكوبية عام 1962. فالردع النووي ليس بالطبع نظرية فحسب، بل هو أيضًا "إستراتيجية لإدارة الصراع"، مع تطبيقها العملي منذ نهاية الحرب العالمية الثانية (Sauer 2015, p.8).

يبدو أن المشكلة هي أن نظرية الردع لم تنتقل من هذا العصر. رغم أن الأسلحة النووية لا تزال موجودة، فقد مر العالم بتغيرات سياسية وتكنولوجية جذرية. علاوة على ذلك، لم يعد توازن القوى مستقطباً بين قوتين عظميين، ولكن بدلاً من ذلك تهيمن عليه الولايات المتحدة الأمريكية كقوة عظمى. ومع ذلك، فإن الفواعل الحكومية وغير الحكومية الجديدة تستعرض قوتها على الساحة الدولية، حيث تسعى الصين ببطء لملئ الفراغ الذي خلفه الاتحاد السوفيتي والجماعات الإرهابية التي تسببت في الفوضى في الشرق الأوسط، فضلا عن مناطق أبعد. لقد نشأت زيادة الصحة الشخصية والثروة من خلال التقدم العلمي والميكانيكي. فقد أدت التقنيات الجديدة - التي تربط جميع أركان الكوكب على الفور وبشكل مستمر- بشكل حاسم إلى عالم متغير حقًا في القرن الحادي والعشرين.

ثانيا: استخدام الردع في الفضاء السيبراني

أصبحت العلاقة بين الحرب الإلكترونية وإستراتيجية الردع تمثل نقطة محورية لدى العديد من الدارسين. حيث بدأ الكثيرون منهم في استكشاف طرق جديدة لتنفيذ أساسيات نظرية الردع الكلاسيكية في

المجال السيبراني، وذلك لردع الهجمات الإلكترونية والحرب الإلكترونية بنجاح (Lupovici 2011, p.p. 49-51). وقد وفر ذلك قوة دافعة لتطوير ما يشير إليه غودمان Goodman، والعديد من الدارسين الآخرين، باسم "نظرية الردع السيبراني" (Goodman 2010, p.p. 102-135).

تعود أصول الردع السيبراني إلى عملية عاصفة الصحراء في عام 1991، عندما اكتسبت فكرة "الثورة في الشؤون العسكرية" شعبية كبيرة. فخلال المراحل الأولى من العملية، شنت الولايات المتحدة "حرب المعلومات" Information Warfare، التي وصفها "د. بيتز" D. Betz بأنها "سلاح محتمل بحد ذاته" (Betz 2006, p.p. 505-533)، ضد الحكومة العراقية، مؤدية إلى شل شبكات اتصالاتها العسكرية. ليكشف هذا الموقف عن أهمية الردع السيبراني ودوره في الحروب المعاصرة.

ففي مرحلة التسعينيات، قدم الدارسون أسسًا صلبة لدراسة الردع وحرب المعلومات، وركزوا بشكل أكبر على استخدام إدارة الإدراك أكثر من الهجمات الرقمية على البنى التحتية للمعلومات. وبعد الأحداث السيبرانية التي حدثت في أواخر سنة 2000، على غرار الهجمات الإلكترونية على استونيا في عام 2007، تحول اهتمام الدارسين إلى التركيز على ردع الهجمات الإلكترونية، أو "الحرب الإلكترونية"، التي لها غايات إستراتيجية وسياسية (Stevens 2012, p.p. 149-151).

من المهم في هذا السياق التمييز بين مفهومي "الهجوم السيبراني" cyber attack و"الحرب السيبرانية" cyber war نظرا للخلط في استخدامهما من قبل الدارسين في الكثير من الأحيان. فيشير مصطلح "الهجوم الإلكتروني" إلى استخدام الخصوم لأكواد الكمبيوتر لأغراض التدخل في "وظيفة نظام الكمبيوتر" أو الشبكة، بما في ذلك وظائف الحكومات والخدمات العسكرية، لتحقيق مزايا إستراتيجية وسياسية عن طريق تعطيل تلك الشبكات والأنظمة، مثل جعلها في وضع عدم الاتصال، أو تدميرها بالكامل (Stevens 2012, p. 151). أما مصطلح "الحرب الإلكترونية" يشير إلى الإجراءات التي تتخذها دولة قومية لاختراق أجهزة الكمبيوتر أو الشبكات الخاصة بدولة أخرى بغرض التسبب في تلفها أو تعطيلها (Clarke and Knake 2010, p.6).

وتجدر الإشارة إلى أن الردع بالمفهوم الكلاسيكي الذي تم تحديده أعلاه يختلف اختلافا جوهريا عن مفهوم الردع السيبراني، وهذا راجع إلى مجموعة من العوامل أهمها:

1- وجود فواعل جديدة من غير الدول

إذا كان القرن العشرون قد حددته الحربان العالميتان اللتان أعقبتهما الحرب الباردة، فقد تم تحديد القرن الحادي والعشرين حتى الآن من خلال سلسلة طويلة من الصراعات المنخفضة الحدة. فقد كانت أفغانستان والعراق من أوائل المتصدرين للعناوين الرئيسية في الغرب، لكن الحروب الأهلية العديدة في إفريقيا والربيع العربي والمشكلات في شرق أوكرانيا تستمر اليوم عند مستويات بديلة. إذ يمكن تحديد الفواعل في هذه الساحات في الغالب على أنها غير تابعة للدولة، وكذلك يمكن تمييز الفواعل البارزة في الفضاء الإلكتروني. فالفواعل من غير الدول المحددة على نطاق واسع متمثلة في الفواعل السياسية المنظمة التي تؤثر على مصالح الدولة من خلال السعي لتحقيق أهدافها دون أن تكون مرتبطة مباشرة بالدولة (Pearlman and Cunningham 2012, p.3).

وبشكل أكثر تحديدًا، تشمل الفواعل من غير الدول مجموعات المصالح الخاصة، والناشطين من أجل قضية واحدة، وحركات الاستقلال، ومقاتلي الحرية، وجماعات الضغط، والمتظاهرين، والمعارضين، وحتى الجهاديين الذين اكتسبوا منابر عالمية عبر الإنترنت يمكنهم من خلالها تعزيز وجهات نظرهم. هذه المجموعات الدولية هي التي تحدد سكان الفضاء الإلكتروني، وليس مواطني الدول القومية. وبطبيعة الحال، يمكن للشخص أن يكون "مستخدمًا على الإنترنت ومواطنا في الوقت نفسه، ولكن على شبكة الإنترنت تتآكل جنسية الدولة القومية كثيرًا نظرًا لخصائص الإنترنت المحددة.

تتجلى مشكلة الردع في أن هذه الفواعل من غير الدول لا تتصرف عمومًا وفقًا لمعايير وقيم نظام الدولة. فهي ليست ملزمة أو مقيدة بنفس المبادئ التي تفرضها الدول. فاللوائح التي تحكم كيفية تفاعل الدول لا تسري على العديد من الفواعل من غير الدول، وخاصة في الفضاء الإلكتروني. إذ يمكن تجاوز المهام الدبلوماسية والقوانين التجارية تمامًا من خلال التفاعلات عبر الإنترنت، على غرار أسواق الويب المظلمة مثل طريق الحرير. وفي الواقع، لا تلعب الفواعل من غير الدول نفس قواعد النظام الدولي التي تدعم إستراتيجية الردع التقليدية.

2- طبيعة الفضاء السيبراني

تعتبر تسمية الفضاء السيبراني تسمية غير دقيقة، لأنه ليس حقا مساحة ملموسة على الإطلاق. إنه بلا شكل، ولا حدود له بطبيعته، ويعتمد هذا الفضاء على البنية التحتية المادية - الخوادم والكابلات وأجهزة الكمبيوتر- لوجوده. لكن النقطة المهمة هي أن مفهوم الإنترنت ينتشر ويحل محل المفاهيم التقليدية للأراضي والملكية في ظل غياب أية حدود إقليمية في هذا الفضاء الجديد، كما أن تكلفة وسرعة انتقال الرسائل في هذا الفضاء يكون بصورة مستقلة تماما عن المواقع المادية (Johnson and Post 1996, p.p. 1370-1371). فمستخدم الإنترنت لا يعيش في المواقع على الإنترنت، ولا يمكن بذلك المطالبة بالحقوق في جزء معين من المواقع الإلكترونية.

يفرض نطاق الإنترنت فوق-الوطني، بطبيعته والمستخدمين على حد سواء، مشاكل كبيرة للردع في الفضاء الإلكتروني. ولتحقيق أهدافه، يعتمد الردع التقليدي على مفاهيم الدولة، بما في ذلك الإقليم والمواطنين باعتبارهم مظاهر مادية. لكن في الفضاء الإلكتروني يصعب تحديد هذه المظاهر، مثل تحديد ما هي أراضي بلد الإنترنت، ومن هم مواطنوها على الإنترنت؟.

النقطة المهمة هي أنه من دون فهم دقيق للغاية لما يتم حمايته، فمن المستحيل معرفة متى تم اختراق الحدود والمعالم. خلال الحرب الباردة، تم ردع القوى العظمى عن مهاجمة بعضها البعض من خلال وضع الأسلحة الفتاكة خلف خطوط، إما مادية (الحدود) أو مجازية (السياسية)، بقصد استخدام هذه الأسلحة إذا تم عبور الخط. لكن في الفضاء الإلكتروني لا يوجد خط، على الأقل ليس خطًا سهل التعريف والتطبيق. إذ بدون مثل هذا الخط، يصبح من الصعب للغاية ردع الخصم، لأن قواعد اللعبة ليست واضحة للعيان.

3- مصداقية التهديد

تعتبر مصداقية التهديد سمة لا غنى عنها لإستراتيجية الردع، من خلال تهديد أحد الأطراف لطرف آخر ببعض الإجراءات العقابية في حالة قيام الطرف الآخر بالتصرف خارج رغبات الطرف الأول. ولكن حتى ينجح هذا التهديد، يجب على الطرف الأول أن يُظهر أن التهديد حقيقي جدًا وليس مجرد كلمات فارغة. وفي هذا السياق كتب *Thomas Schelling* توماس شيلينج (1994): "كقاعدة عامة، يجب على المرء أن يهدد بأنه سوف يتصرف، وليس أنه قد يتصرف إذا فشل التهديد" (Schelling 1994, p.p. 241-244). وبعبارة أخرى، يجب أن يكون المرء مستعدًا للقيام بالعمل الجدي وليس فقط بالأقوال.

ففي العصر النووي، ومنذ عام 1945 حتى اليوم، تم تحقيق هذه المصداقية من خلال التصريحات العلنية للنوايا. إذ يجب على كل من يتحمل مسؤولية التصريح باستخدام الأسلحة النووية أن يعلن بشكل مقنع التزامه بشن ضربة، إذا دعت الحاجة. وإذا فشل هذا الموقف في الإقناع، فإن الرادع سيكون لاغيا وباطلا.

علاوة على ذلك، يمكن القول أن تهديد الردع يجب أن يكون مرئيا أيضا. ففي القرن العشرين، قدمت كل من القوات الجوية والصواريخ الباليستية العابرة للقارات أساسًا ماديًا يمكن من خلاله توجيه تهديدات مرئية. وفي هذا الصدد، كانت Zeppelin زيبلين أول مركبة جوية توفر مثل هذا الأساس وتثير ردود فعل لدى عامة الناس، فقد ألهمت ذلك الرعب بالإضافة إلى الخوف والإثارة والرهبة. واستمر هذا الأمر في صورة أساطيل المهاجمين التي ستستمر دائمًا، وفي وقت لاحق برزت للعيان الصواريخ الباليستية العابرة للقارات. وبالتالي ستساهم هذه الصور في خدمة وتعزيز الغرض من ضمان بقاء خطر الردع مرئيًا أمام أنظار العامة، وبالتالي تعزيز مصداقيته.

أما في الفضاء السيبراني، الذي رأيناه سابقا بأنه لا شكل له، فإن مثل هذه الصور المرئية غير ممكنة. إذ من المستحيل التفاخر بالأسلحة السيبرانية وإظهارها على نفس المنوال بالنسبة الأسلحة التقليدية. فخطوط شيفرات الكمبيوتر، سواء كانت فعلية أو مجرد فكرة، لا يمكنها نقل نفس تهديد الطائرة المهاجمة أو الصاروخ النووي. والواقع أن عدم القدرة على عرض رادع التهديدات السيبرانية يقوض بشدة مصداقية هذه التهديدات التي تبقى مجرد تهديدات افتراضية.

4- عدم الكشف عن الهوية

إن إمكانية مستخدمي الإنترنت إخفاء هويتهم في الحياة الواقعية قد منحتهم القدرة على التصرف بشكل مجهول عبر الإنترنت. ومع عدم اتخاذ أي إجراءات مرتبطة بهم في الحياة الحقيقية، يكون الأشخاص لديهم القدرة والاستعداد للقيام بأشياء قد يكونون مثبطين عن القيام بها، مثل: التعبير عن المعارضة في ظل الأنظمة القمعية. في حين أن حرية التعبير هذه تعد قوة للخير بشكل واضح، ويمكن أيضًا استخدام نفس الهوية من قبل الفواعل الخبيثة malicious actors ذات النوايا الخطيرة. حيث يستطيع المجرمون والإرهابيون والكيانات التي ترعاها الدولة اجتياز الفضاء الإلكتروني لنشر رسائلهم وأداء التجسس وسن الأعمال التخريبية بدرجة عالية جدًا من عدم الكشف عن هويتهم أو على الأقل إتباع نهج الإنكار المعقول.

وفي سياق إخفاء الهوية، يشعر المسؤولون عن حماية الجمهور بالضعف بسبب قدرة المجرمين على ارتكاب جرائم التخفي، لأنه من المستحيل القبض على الجناة، ناهيك عن عدم إمكانية فرض العقوبات، إذا

كانت هويات الجناة غير معروفة. وبالتالي فإن إخفاء الهوية يمثل مشكلة كبيرة في الفضاء الإلكتروني ويسبب مشاكل كبيرة للردع.

وبالتالي، أصبحت حقيقة صعوبة تحديد الهوية في الفضاء الإلكتروني واضحة بشكل متزايد. فعلى سبيل المثال، لا يزال فيروس Stuxnet مجهولا بخصوص الطرف المسؤول عنه والمعترف به رسميًا، بالرغم من اكتشافه منذ حوالي تسع سنوات. فقد تم توجيه الاتهام إلى كل من الولايات المتحدة وإسرائيل. وبينما لمّح كلا البلدين بقوة إلى تورطهما في تطويره ونشره بهدف تدمير بعض أجهزة الطرد المركزي لإبطاء البرنامج النووي الإيراني (Denning 2012, p. 676)، لا تزال هناك درجة صغيرة من عدم اليقين، وهو ما يكفي للحفاظ على الإنكار المعقول.

انطلاقا من العناصر السابقة، تجدر الإشارة إلى أن تحديد الفواعل في الفضاء الإلكتروني أمر صعب. إذ أن طبيعة المجال السيبراني وعدم مصداقية التهديدات فيه، إضافة إلى إمكانية إخفاء الهوية ورفض المشاركة في الأنشطة في الفضاء السيبراني، من شأنها تقويض قابلية الحفاظ على إستراتيجية الردع السيبراني.

ثالثا: تحديات الردع السيبراني الفعّال

بعد التطرق للسياق التاريخي للردع، والإحاطة بتطور استعمال الردع في الفضاء السيبراني، فإن الخطوة التالية هي النظر في التحديات المرتبطة بتطبيق الردع السيبراني على الفضاء الإلكتروني، وفي هذا السياق فإن أحد أهم العوائق التي تحول دون الردع السيبراني الفعال هو مشكلة الإسناد، علاوة على قضية فهم الدوافع العدوانية ومستوى تحمل المخاطر.

1- مشكلة الإسناد

تعتبر مشكلة الإسناد من بين المسائل الحرجة التي تجعل من الردع السيبراني عديم الجدوى، كما أنها من العوامل الحاسمة التي تحتل مكان الصدارة عند مناقشة قضايا الردع السيبراني عن طريق الانتقام. فكما هو معلوم، تم تصميم الإنترنت بطريقة لا يمكن أن تعرف بها هوية الخادم حيث تم إطلاق الهجوم الإلكتروني ولا يمكن للمعتدي السيبراني في معظم الحالات أن يكون معروفًا. بسبب بنية الإنترنت وباعتبارها "وسيلة بلا حدود جغرافية"، حيث تصبح لا أهمية للمكان (Goldsmith And Wu 2006, p.49).

لا يبدو بأن إخفاء هوية الجاني السيبراني هي مجرد مشكلة عابرة. إذ يشير في هذا الصدد الباحث John Markoff إلى أن بعض دارسي الحرب الإلكترونية يشيرون إلى "بريّة المرايا" wilderness of mirrors (Markoff 2009). ونتيجة لذلك، تميل مشكلة الإسناد في الأدبيات إلى تصويرها باعتبارها عاملاً حاسماً في الحد من الردع السيبراني الفعال، وتحديداً في الردع عن طريق الانتقام. في المجال السيبراني، يتوقع الجاني مستوى معين من الإفلات من العقاب. لذلك، يُعتقد أنه لا توجد إستراتيجية للردع السيبراني قد تكون فعالة في منع الهجمات الإلكترونية التي ينظر إليها على أنها "جولات مجانية"free rides (Kugler 2009, p.326). بسبب عدم التأكد من هوية المهاجم، مما سيقوض مصداقية التهديد بالانتقام، بصرف النظر عن مدى قدرة المهاجم، من خلال جعل الردع غير فعال.

في الفضاء الإلكتروني، قد يؤدي عدم اليقين في نسب مصدر الهجوم إلى عرقلة الردع بطرق مختلفة (Lynn III 2010, p.99). بادئ ذي بدء، تفترض الإستراتيجية النووية التي تتبناها الولايات المتحدة أنه يمكن تتبع

أصل الهجوم النووي على الأراضي الأمريكية من خلال وسائل تنفيذ المهاجمين. بمعنى آخر، كان من الواضح بشكل عام تحديد من فعل ذلك خلال المواجهة النووية بين القوى العظمى (Libicki 2009, p.p. 39-40). وعلى النقيض من ذلك، في الفضاء السيبراني غالبًا ما يظل مصدر الإجراءات السيبرانية الخبيثة، أو الجهة المسؤولة عنها غير معروف ومن الصعب اكتشافه (Lin 2016, p.77).

لكي يكون الردع السيبراني من خلال العقوبة فعالا، يجب أن يكون المدافع قادرًا على تحديد هوية المهاجم بثقة عالية، ويجب أن يعتقد المعتدي المحتمل أن المدافع سيكون قادرًا على تحقيق إسناد عملي للهجوم. ونظرًا للصعوبات الفنية المتأصلة في المجال السيبراني، يمكن للمعتدين على الإنترنت إخفاء هوياتهم بسهولة، مما يقلل من مصداقية الطرف الرادع، والذي بدوره يجعل الردع السيبراني غير فعّال. حتى إذا كان الطرف الرادع قادرًا على تحديد أصل الهجوم وهوية الجاني السيبراني من خلال وسائل تقنية مثل عنوان بروتوكول الإنترنت (IP) واسم مستخدم، فإن هذه الوسائل التقنية قد لا تؤدي إلى الدليل القاطع الذي يشير إلى المهاجم الفعلي. قد يكون السبب في ذلك هو أن المعتدي السيبراني قد استخدم توقيعات هجومية مضللة أو خادعة، مثل استخدام أجهزة الكمبيوتر المعرضة للخطر في الروبوتات لتحويل مصدر الهجوم، وبالتالي إخفاء الهوية بشكل فعال (Solomon 2011, p.5). قد يعود الأمر كذلك إلى أن الهدف ربما لم يدرك أنه تعرض للهجوم السيبراني، ولكنه بدلا من ذلك، ربما أرجع المشكلة بشكل غير صحيح إلى "خطأ أو عطل" في أنظمة الكمبيوتر (Hollis 2011, p.378).

وبالتالي كلما كان المهاجم أكثر تعقيدًا، كلما زادت نسبة الإسناد. حيث سيتخذ هؤلاء المهاجمون إجراءات لإخفاء موقعهم الحقيقي وجعله يبدو أن مهاجمًا آخر أو دولة قومية أخرى قد قاموا بالهجوم. زيادة على ذلك، قد تجعل العقبات القانونية والسياسية الإسناد أمرًا صعبًا ويستغرق وقتًا طويلًا، خاصةً عندما يكون التعاون الدولي بين منظمات ووكالات وحكومات متعددة مطلوبًا لتحديد مصدر الهجوم. إذ يمكن لأي منظمة تختار عدم المساعدة في التحقيق (أو ليس لديها القدرة الفنية على المساعدة) أن تمنع أو تعيق تحديد هوية المهاجم. نتيجة لذلك، قد يكون الحصول على بعض الإسناد في الوقت المناسب في بعض الأحيان أمرًا بالغ الصعوبة (خاصة ضد مهاجم متطور) لردع الأعمال الإلكترونية الإجرامية.

2- مشكلة فهم الدوافع العدوانية ومستوى تحمل المخاطر

التحدي الآخر للردع السيبراني يتمثل في فهم الخصم وكيف سيكون رد فعله على إستراتيجية الردع المحددة. وفي هذا السياق يمكن تصنيف التهديدات السيبرانية إلى عدة فئات وفقا لطبيعة الفواعل، وسيكون لكل فئة دوافع ومستويات مختلفة من المهارات أو القدرات السيبرانية. وتتمثل أهم هذه الفئات في: الفواعل الإجرامية criminal actors، الفواعل العنيفة من غير الدول violent nonstate actors، والفواعل الحكومية أو التي ترعاها الدولة state or state-sponsored actors.

بالنسبة للنشاطات الإجرامية السيبرانية، تعتبر أكبر مجموعة من التهديدات السيبرانية والتي يصعب ردعها على نحو فعال. تتراوح هذه المجموعة في التطور والتعقيد ما بين القراصنة ذووا القدرات المنخفضة، إلى القراصنة على مستوى النخبة بدافع المكاسب المالية. كما أن القدرة على معاقبة هذه المجموعة وردعها محدودة في بعض الأحيان، وتعتمد إلى حد كبير على إنفاذ القانون والتعاون الفعال من قبل الدول الأجنبية. بحيث سوف

يبحث القراصنة المتطورون عن الأماكن التي تسهل فيها شروط الإدارة والسياسة لإخفاء هوياتهم (Yannakogeorgos 2013).

يمكن أن تكون معاقبة هذه المجموعة معقدة لعدة أسباب، من ضمنها أن الإسناد الدقيق لمصدر الهجمات السيبرانية يعد إشكالية ويستغرق وقتًا طويلاً. إضافة إلى أن الحجم الهائل للنشاط يجعل ملاحقة جميع القضايا والمسائل أمرا متعذرا من الناحية العملية. فوفقًا لتقرير صادر عن مكتب محاسبة الحكومة الأمريكية لعام 2013 حول الأمن السيبراني، ارتفع عدد حوادث أمان الكمبيوتر التي أبلغت عنها الوكالات الفيدرالية لفريق الاستعداد للطوارئ بالكمبيوتر بالولايات المتحدة (US-CERT) على مدار فترة ست سنوات من 5,503 في عام 2006 إلى 48,562 في عام 2012 بزيادة قدرت بـ 782 % (US Government Accountability Office).

وطبقًا لتقرير جرائم الإنترنت لعام 2010 الصادر عن مركز شكاوى الإنترنت، تلقى مكتب التحقيقات الفيدرالي 303,809 شكاوى تتعلق بجرائم الإنترنت مما أسفر عن إعداد 1,420 قضية جنائية، وهذا ما أدى إلى ستة إدانات فقط (Grimes 2012). بالإضافة إلى انخفاض معدل الإدانة، تعد جرائم الإنترنت من بين أكثر أشكال الإجرام التي لا يتم الإبلاغ عنها. إذ يشير أحد التقديرات إلى أن 17 % من الشركات تبلغ عن إنفاذ القانون عن الخسائر المتعلقة بجرائم الإنترنت (Kshetri 2006, p.p. 35-36).

وبالتالي، يتعين على القراصنة ذوي النية الإجرامية أو المالية تقييم إمكانية القبض عليهم ومحاكمتهم على جرائمهم ضد الأرباح المحتملة. ومع ذلك، سيستمر القراصنة الماهرين الذين يعرفون كيفية إخفاء هوياتهم ومواقعهم في ارتكاب هذه الجرائم حتى يزداد التعرف على جرائم الإنترنت وإسنادها وملاحقتها. لذلك، فالقدرة على ردع الجماعات المتطرفة السياسية منخفضة لجميع الأسباب نفسها. باعتبار أن القراصنة هم نشطاء بدوافع سياسية أو دينية، أو الرغبة في فضح ذلك من ارتكاب مخالفات أو الانتقام الفعلي. فإلى أن تتمكن الدول من زيادة خطر ملاحقة هذه الجرائم بشكل ملحوظ، لا يمكنها توقع أن يكون لديها إستراتيجية فعالة للردع السيبراني على المستوى الوطني ضد القراصنة الإجراميين أو القراصنة السياسيين.

أما بالنسبة للفئة الثانية المتمثلة في المنظمات العنيفة من غير الدول مثل الجماعات الإرهابية. قد تكون هذه المجموعة أكثر تنظيماً ولها هدف واضح لإلحاق الأذى بالدول أو بمصالحها الرئيسية. وبالتالي فالقدرة على ردع هذه المنظمات عن مهاجمة شبكات المعلومات تبدو منخفضة في الوقت الحالي. لأن هذه المنظمات العنيفة عازمة على التسبب في ضرر لمختلف الدول بأي ثمن تقريبًا، ومن المرجح أن تعلن عن نجاحها في إحداث الفوضى على أنظمتها. إذ تدرك أي جماعة إرهابية غير خاضعة للرقابة أنها لا تستطيع محاربة الدول القوية عسكريا في معركة حقيقية، لذلك تلجأ إلى أشكال الحرب غير النظامية.

تقع مهاجمة الدول في المجال السيبراني بالتأكيد ضمن نطاق الحرب الحديثة غير النظامية. التي تكون تكلفة الدخول فيها منخفضة مقارنة بتكلفة الحصول على أنظمة أسلحة تقليدية قادرة على هزيمة القوات العسكرية في حرب نظامية. فالأسلحة والتقنيات السيبرانية تتوفر بسهولة أكبر من أنظمة الأسلحة التقليدية المتقدمة، وتمنح الأسلحة الإلكترونية الإرهابيين القدرة على مهاجمة أي دولة معادية. فقد رأينا هذه الجماعات تجند أشخاصًا على استعداد للموت كمفجرين انتحاريين خدمة لقضاياهم. ليس من الصعب تصور إحدى هذه المجموعات التي تجند قراصنة ماهرين لدعم قتالها ضد الدول المعادية. ونظرًا لارتباط الدول بشدة

بالشبكات وأن هذه المجموعات مصممة على ذلك، فإن الاحتمال المعقول هو أنه في مرحلة ما في المستقبل، ستؤثر إحدى هذه المجموعات على مصالح الدول المعادية لها.

من غير المحتمل حاليا أن يكون لدى جماعة إرهابية القدرة على شن هجوم إلكتروني من شأنه أن يثير مخاوف جماعية لدى عامة الناس. ومع ذلك، من الممكن أن تهاجم هذه الجماعات البنية التحتية الخاصة والحكومية، مسببة خسائر مالية كبيرة للأفراد أو الشركات.

على عكس القراصنة الإجراميين والجماعات العنيفة من غير الدول (المنظمات الإرهابية)، يمكن تحقيق الردع بالنسبة للمجموعات التي ترعاها الدولة بشكل فعال. لأن الفرق بين هذه المجموعات الحكومية وغيرها هو القدرة على فرض مستوى مناسب من العقوبة على الدولة القومية لردع السلوك غير المواتي الذي تسترشد به تلك الدولة. في هذه الحالة، يمكن للدولة المستهدفة استخدام جميع الأدوات الكاملة (الدبلوماسية، الإعلامية، العسكرية والاقتصادية) للقوة الوطنية لتشكيل سلوكيات الدول الأجنبية.

إن التهديد بفرض عقوبات اقتصادية أو عمل عسكري أو أي ردود سياسية / دبلوماسية أخرى من جانب الدولة المستهدفة يمكن أن يؤثر بشكل ملحوظ على بعض الدول. سيتعين على الدولة القومية أن تقيس خطر تصاعد الأعمال العدائية ضد أي قوة عظمى مع المكاسب المحتملة للهجوم السيبراني. ومع ذلك يُتوقع من معظم الدول القومية تطوير أسلحة إلكترونية هجومية لاستخدامها ضد القوى العظمى بسبب كلفتها المنخفضة واعتماد الدول العظمى على الأنظمة الشبكية. وبالتالي، يجب أن توضح إستراتيجية الردع السيبراني الفعالة لأي دولة أن أي هجوم سيبراني ضد مصالحها سوف يُنظر إليه على أنه شكل من أشكال العدوان ولا يختلف عن أي هجوم حركي أو مسلح. فالهدف هو وجود إستراتيجية ردع تمنع الدول من استخدام الأسلحة الإلكترونية خارج الحرب المعلنة ضد أية دولة عظمى.

رابعا: المخاطر الناجمة عن انتشار خطاب الردع السيبراني

من خلال ما سبق، جادلنا بأن الردع كمفهوم لا يترجم من العالم التماثلي للقنابل والقذائف الباليستية إلى عالم الفضاء الإلكتروني الرقمي. لذلك يتم إساءة فهم محاولات ممارسة استراتيجيات الردع السيبراني، بما ينطوي على ذلك في الواقع من إثارة خطابات خطيرة ومثيرة للاستفزاز. لقد تبلور وتطور الشكل الحديث للردع في عصر نشأت فيه الحروب نتيجة لتمسك القوى الأوروبية بالإمبراطوريات العالمية وزيادة الاستقطاب بين الفوارق الجيوسياسية والإيديولوجية، وارتفاع مستويات الإنفاق على التسلح والاستعداد العسكري. ومن خلال محاولة مواصلة خطاب الردع، فإن احتمال صدى هذه الظروف وآثارها الكارثية، هو احتمال حقيقي على نحو خطير.

في أعقاب عملية "فيروس ستيكسنات" لعام 2010، تزايدت المخاوف والشواغل الرئيسية التي عبر عنها الأكاديميون والقادة العسكريون وواضعو السياسات على حد سواء، بخصوص تنامي السباق نحو تسلح متطور وجديد. فعلى عكس سباقات التسلح التاريخية التي سعت فيها الدول لتطوير وبناء سفن حربية ودبابات ومقاتلات نفاثة وصواريخ كروز، فإن سباق التسلح الجديد هذا يتعلق بتطوير الأسلحة السيبرانية.

وكما سبق وأن أشرنا سابقا، فإن الفارق الرئيسي بين الأسلحة السيبرانية والأسلحة التقليدية-المادية هو وجودها بلا شكل وبدون معالم، مع ما ينجم عن ذلك من عدم رؤيتها في الواقع. إن تقييم قدرات الخصم

من خلال الفحص التجريبي، كما هو متاح مع السفن الحربية والقذائف، يعتبر ذلك غير ممكن مع الأسلحة الإلكترونية. لذلك، فإن عالم اليوم مليء بنقص شديد وواضح في المعرفة الدقيقة بشأن القدرات الإلكترونية الهجومية والدفاعية للفواعل المختلفة. مثل هذا الجهل، إلى جانب الخوف المتزايد، هو ما من شأنه أن يدفع ويغذي سباقات التسلح (Schneier 2013).

ومع ذلك، لن يكون لسباق التسلح في الفضاء الإلكتروني نفس خصائص سباق التسلح التقليدي، نظرًا للتكوين الخاص للأسلحة السيبرانية. حيث يمكن للأسلحة التقليدية أن تتغلب على دفاعات الخصم باستخدام القوة الغاشمة. كما قد يساعد العثور على نقاط الضعف في الدفاعات على نشر الأسلحة بشكل أكثر دقة وكفاءة. ولكن على النقيض من ذلك بالنسبة للأسلحة السيبرانية، فإنها تعتمد على نقاط الضعف في الدفاعات لأداء مهامها. إذ تعمل الأسلحة السيبرانية من خلال الاستعانة باستغلال نقاط الضعف الموجودة في أنظمة الكمبيوتر. على سبيل المثال، استخدمت عملية فيروس Stuxnet ما لا يقل عن أربعة من هذه الثغرات الأمنية لاختراق أنظمة الكمبيوتر، لأن الفيروس من هذا النوع عادة ما يكون قادرا على الانتشار عبر أجهزة الكمبيوتر غير المؤمنة وغير المتطابقة (Falliere 2011, p.7). وبالتالي، أصبح العثور على نقاط الضعف هذه مشروعًا تجاريًا، من خلال استعداد الشركات لدفع مبالغ نقدية كبيرة للأفراد لإفشاء نقاط الضعف في برامجهم، وأصبحت مثل هذه المشاريع معروفة باسم برامج مكافأة الأخطاء bug bounty programmes. على سبيل المثال لا الحصر، تقدم شركة فيسبوك وعودا بمكافآت لا تقل عن 500 دولار مقابل الكشف عن الخلل.

ربما ليس من المستغرب أن يكون هناك سوق سوداء تطورت حيث يتداول الفاعلون الأقل شرعية نقاط الضعف. على الرغم من المكافآت الوفيرة المتاحة للأشخاص الذين يكشفون عن نتائجهم بطريقة مسؤولة، إلا أنه لا يزال من الممكن الحصول على أسعار أعلى من خلال الوصول إلى مصادر أكثر خطورة في أعماق الشبكة المظلمة. لا تقتصر جاذبية إخفاء الهوية على المجرمين، ولكن يشمل أيضًا الفواعل الشرعية التي قد لا ترغب في نشر تعاملاتها بصفة علنية.

ربما أدت الهجمات الإلكترونية الأخيرة على غرار Stuxnet وFlame إلى زيادة الطلب في السوق العالمية على شراء وبيع الأسلحة الإلكترونية للتجسس أو التدمير. حيث اكتشف الباحثون الفنيون المستقلون ذوو المهارات العالية أنه يمكن بيع الأسلحة السيبرانية المتطورة في سوق عالمي سري بمبالغ ضخمة. ويشمل العملاء كلا من الدول والشركات، والأسلحة السيبرانية المطلوبة هي تلك التي لديها آثار يمكن أن تبقى على أجهزة الكمبيوتر المصابة لعدة أشهر أو سنوات قبل أن يتم اكتشافها (Wilson 2013, p.16).

مما لا شك فيه أن سباق التسلح السيبراني من شأنه أن يشعل السوق السوداء بالطلب على نقاط الضعف، مما يعزز التجارة التي تنافس بالفعل تجارة المخدرات غير المشروعة من أجل الربحية. وبالتالي، تهدد استراتيجيات الردع السيبراني بالمساهمة في هذا النمو، وهو أمر يستحق الشجب أخلاقياً كما أنه يعتبر مصدرا لزعزعة الاستقرار نتيجة لصعوبة تنظيم الأسواق، فأي محاولة لفرض قواعد صارمة سيتم التحايل عليها بواسطة تقنية إخفاء الهوية، في ظل فضاء سيبراني ذو طابع دولي معيق لعملية تنظيمه على نحو خاص.

خـــاتمة

يُعد غزو معظم الدول في المجال السيبراني أمرا موضع ترحيب كبير، نظرًا لأهمية هذا المجال للمجتمع بشكل عام والجيوش بشكل خاص. ومع ذلك، فإن برامج اكتساب القدرة السيبرانية، خاصة تلك المصحوبة بتركيز واضح على الردع، أصبحت تشكل سببا مهما للقلق والتوجس بشأنها.

لقد استعرض هذا البحث السياق التاريخي للردع من أجل تقييم ما إذا كانت مثل هذه الإستراتيجية قابلة للتطبيق في الفضاء الإلكتروني. من خلال تحليل العديد من جوانب الردع، وُجد أن هذا المفهوم كما هو معروف تقليديًا، لا يترجم بشكل جيد من الفضاء التماثلي إلى الفضاء الإلكتروني. وهذا راجع للعديد من المشكلات التي تعيق ذلك، وأبرزها مسألة عدم الكشف عن الهوية، باعتبارها معرقلة لممارسة الردع بفعالية في الفضاء السيبراني. علاوة على ذلك، تعمل محاولات ردع الفواعل غير المحددة بقدرات غير محددة في الواقع على زعزعة الاستقرار وتفاقم الفضاء الإلكتروني فيما يتعلق بسباق التسلح وتقلبه.

فالفضاء السيبراني هو مجال لم يتم فهمه بالكامل بعد من قبل المخططين العسكريين وواضعي السياسات كما يتضح من الاستراتيجيات التي لا تعد ولا تحصى، والتي تتسم بصياغة سيئة مثل الردع السيبراني. تعني الخصائص المميزة للمجال السيبراني أن السياسات والمفاهيم التقليدية الراسخة لا يمكن نقلها وتطبيقها بسهولة داخل هذا الفضاء الجديد. إذ سلط هذا البحث الضوء على بعض الطرق الدقيقة التي تظهر بها هذه المشكلة، إلى جانب العواقب المحتملة الناجمة عن خطأ التعامل معها. نظرًا لأن فهم نضوج الفضاء السيبراني وقدرات الإنترنت أصبحت أكثر فاعلية، فإن الحجج المقدمة هنا ستكون بمثابة مبادئ توجيهية لصياغة الاستراتيجيات والسياسات المستقبلية.

قائمة المراجع:

1. Douhet, G. (2009). The Command of the Air. translated by : Harahan, J, P and Kohn R, H. Tuscaloosa : The University of Alabama Press.
2. Sauer, F. (2015). Atomic Anxiety: Deterrence, Taboo and the Non-Use of U.S. Nuclear Weapons. Hampshire/ New York : Palgrave Macmillan.
3. Clarke, R, A. and Knake, R. (2010). Cyber War: The Next Threat to National Security and What to Do About It. New York : HarperCollins Publishers.
4. Schelling, T. (1994). The threat that leaves something to chance. in : Freedman, L. War. Oxford :Oxford University Press,
5. Goldsmith, J. And Wu,T. (2006).Who Controls the Internet?: Illusions of a Borderless World. New York : Oxford University Press.
6. Kugler, R, L. (2009).Deterrence of cyber attacks, in : Kramer, F, D. Starr, S, H. and Wentz, L, K (Eds), Cyberpower and national security. Washington, DC: Potomac Books,
7. Libicki, M, C. (2009).Cyberdeterrence and cyberwar, Santa Monica, CA: RAND Corporation.
8. Wilson, C. (2013). Cybersecurity and Cyber Weapons: Is Nonproliferation Possible?. in : Martellini M (Editor). Cyber Security: Deterrence and IT Protection for Critical Infrastructures. New York / London : Springer.

2- المقالات في مجلات محكّمة

9. Goodman, W. (2010). Cyber Deterrence Tougher in Theory than in Practice?. trategic Studies Quarterly 4 (3), 102-135.
10. Lupovici, A. (December 2011). Cyber Warfare and Deterrence: Trends and Challenges in Research. Military and Strategic Affairs 03 (3), 49-62.
11. Betz, D, J. (2006). The more you know, the less you understand: The problem with information Warfare. Journal of Strategic Studies 29 (3), 505-533.
12. Stevens, T. (2012). A cyberwar of ideas?: Deterrence and norms in cyberspace. Contemporary Security Policy 33 (1), 148-170
13. Pearlman, W. and Cunningham, K, G. (2012). Nonstate actors, fragmentation, and conflict processes. Journal of Conflict Resolution 56 (01), 3-15.
14. Johnson, D, R. and Post, D, G. (May 1996). Law and borders: the rise of law in cyberspace. Stanford Law Review (48) , 1367–1402.
15. Denning, D, E. (2012). Stuxnet: What Has Changed. Future Internet 4 (4) , 672-687.
16. Lynn III, W, J. (September 2010). Defending a New Domain: The Pentagon's Cyberstrategy. Foreign Affairs 89 (5), 97-108.
17. Lin, H. (Winter 2016). Attribution of malicious cyber incidents: From soup to nuts. Journal of International Affairs 70 (1), 75-137.
18. Solomon, J. (Spring 2011). Cyberdeterrence between nation-states: Plausible strategy or a pipe dream?. Strategic Studies Quarterly 5 (1) , 1-25.
19. Hollis, D, B. (Summer 2011). An e-SOS for cyberspace. Harvard International Law Journal 52 (2) , 374-432.
20. Kshetri, N. (January/February 2006). The Simple Economics of Cybercrimes. IEEE Security and Privacy 4 (1), 33- 39.

3- روابط الأنترنت:

1. Taylor, R, N. (30 Sept 2013). Britain plans cyber strike-force—with help from GCHQ. The Guardian. Retrieved 20/05/2019, from :

https://www.theguardian.com/uk-news/defence-and-security-blog/2013/sep/30/cyber-gchq-defence

2. Mazarr, M, J. (2018). Understanding Deterrence. RAND corporation (perspective). Retrieved 20/05/2019, from :

https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE295/RAND_PE295.pdf

3. -UK Public Spending. Retrieved 21/05/2019, from :

https://www.ukpublicspending.co.uk/past_spending

4. Markoff, J. (July 16, 2009). Internet's Anonymity Makes Cyberattack Hard to Trace. The New York Times. Retrieved 12/08/2019, from :

https://www.nytimes.com/2009/07/17/technology/17cyber.html

5. Yannakogeorgos, P, A. (May 17, 2013). Keep Cyberwar Narrow. The National Interest. Retrieved 15/07/2019, from :

https://nationalinterest.org/commentary/keep-cyberwar-narrow-8459

6. US Government Accountability Office. Key Issues: Cybersecurity. Retrieved 15/07/2019, from : https://www.gao.gov/key_issues/overview

7. Grimes, R, A. (January 10, 2012). Why Internet crime goes unpunished. Retrieved 15/07/2019, from : https://www.csoonline.com/article/2618598/why-internet-crime-goes-unpunished.html

8. Schneier, B. (March 14, 2013). Rhetoric of Cyber War Breeds Fear-and More Cyber War. Schneier On Security. Retrieved 17/07/2019, from : https://www.schneier.com/essays/archives/2013/03/rhetoric_of_cyber_wa.html

9. Falliere, N. (February 2011). W32.Stuxnet Dossier. Version 1.4. Retrieved accessed 18/07/2019 , from : https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf