مجلة الناقد للدراسات السياسية | المجلد: 06/ العـدد: 02 (2022)، ص 678-695

الحرب السيبرانية ومستقبل الأمن العالمي

Cyber war and the Future of Global security

علاء الدين فرحات

المدرسة الوطنية العليا للعلوم السياسية (الجزائر)، Alaferhat@gmail.com

تاريخ الاستلام: 2021/05/04 تاريخ القبول: 2021/09/07 تاريخ النشر: 2022/10/10

ملخص:

تطمح ورقة البحث هذه إلى تسليط الضوء على مؤشرات تصاعد توظيف الحرب السيبرانية في العلاقات بين الدول، والوقوف على أسباب هذا التطور، كما توجه القارئ نحو شك صحي لبعض "الحقائق" المقبولة حول الحروب السيبرانية، فضلاً عن الإشارة إلى أبرز السياسات التي اعتمدتها الفواعل الدولية في محاولة منها لضبط، احتواء أو تحجيم تداعيات هذه الحرب من خلال تنظيم قواعد الاشتباك السيبراني، والتعامل مع مسرح الحرب الجديد هذا.

كما تحاول الدراسة إزالة الغموض عن المفاهيم المحيطة بدراسة التهديدات السيبرانية، ولا سيما احتمالية حدوث الحرب السيبرانية من خلال التركيز على بعض الحوادث التاريخية والمناقشات الرئيسية داخل الدوائر الحكومية والأكاديمية وتقديم رؤية واضحة حول سيناريوهات مستقبل الأمن العالمي في ظل النزوع نحو الحروب السيبرانية.

كلمات مفتاحية: الحرب السيبرانية، الفضاء السيبراني، الجيش السيبراني، الأمن العالمي.

Abstract:

This research paper aspires to highlight on the indicators of the escalation of the use of cyber warfare in relations between countries, and to find out the reasons for this development. It guides the reader toward a healthy skepticism of some accepted “truths” about cyber warfare, as well as the most prominent policies adopted by international organizations. An attempt to control, contain or quantify the ramifications of this war by organizing cyberspace rules of engagement and dealing with this new warfield.

The study also attempts to demystify the concepts surrounding the study of cyber threats, especially the possibility of cyber warfare by focusing on some historical events and major discussions within the government and academic departments and providing a clear vision about scenarios for the future of global security in light of the trend towards cyber wars.

Keywords: Cyber warfare; cyberspace; Cyber weapons; cybersecurity; global security.

المؤلف المرسل: علاء الدين فرحات، **الإيميل**: Alaferhat@gmail.com

مقدمة:

يعد موضوع الحرب السيبرانية من المواضيع التي باتت تحظى باهتمام المجتمع البحثي كظاهرة صاعدة على المستوى الاستراتيجي، وتُهيمن على الجدل العام في العالم خاصة بعد الثورة الكبيرة التي جلبتها الحضارة التقنية في عصر المعلومات، وظهور العالم الافتراضي في الشؤون الإستراتيجية (الفضاء الخامس في علم الإستراتيجيا)، وتداعياته على الأمن العالمي، هذا الوضع ذهب بالبعض لوصف هذا الجيل الجديد من الحروب بأنها حرب باردة جديدة، تخلق واقعًا عالميًّا جديدًا يتميز بكثير من التعقيد والتشابك، قد تنتهي بنزاعات مسلحة تبعا للظروف التي تولدت منها وخلفتها هذه البيئة الأمنية الجديدة، الأمر الذي استحث أقلام الكثير من الباحثين والعسكريين للحديث عن مرحلة جديدة لتحولات الحرب، وذلك من خلال اقتراح مفردات تحليل جديدة تماشيا مع توسع الدراسات العسكرية نظريا وميدانيا، الأمر الذي زامن أكبر عملية هدم للأطر الإبستيمولوجية والأنطولوجية لما جاءت به تفسيرات مواجهات الحروب التقليدية، ودعوا إلى رفع مستوى الفهم التقليدي للحرب والطريقة التي تتعامل بها الدول مع الدفاع والردع، خاصة وأن الطبيعة غير التقليدية لهذه الحروب تتطلب حلولًا أو معايير غير تقليدية للتعاطي معها.

ومما سبق فإن معالجة هذا الموضوع، من خلال تقديم مسح تحليلي للوضع الحالي للبحوث في مجال الحرب السيبرانية، فتحليل وجهات النظر المتفاوتة والبحوث التي أجريت حتى الآن يوفّر نقاشًا يمكن من خلاله تحديد مجال البحث وتوجهاته التي تتيح صياغة أسئلة بحثية جديدة. ووفق هذا تأتي هذه الدراسة حاملة الإشكال التالي:

- **الإشكالية:** ما مدى تأثير الحروب السيبرانية على الأمن العالمي؟

والإجابة عن هذا السؤال المحوري تتطلب مجموعة من الأسئلة الفرعية لتقريب وتوضيح الرؤية أكثر. نوجزها على النحو التالي:

الأسئلة الفرعية:

- ماهي الحروب السيبرانية؟ وما نوع الأسلحة المستخدمة فيها؟
- ما مستقبل الأمن العالمي في ظل النزوع نحو الحروب السيبرانية؟

فرضية الدراسة: أثرت الحروب السيبرانية على البنية التحتية الرقمية المتحكمة بالبنى الحيوية للدول كالمستشفيات وشبكات الكهرباء والقواعد النووية والقدرات العسكرية مما أثر سلبا على الأمن القومي والعالمي بسبب الأضرار المادية الناتجة عنها وما تخلفه من تجاذبات سياسية وعسكرية بين الدول.

أولا: الحرب السيبرانية: الذراع الرابعة

عادة ما تتشكل الجيوش من ثلاث أذرع عسكرية وهي القوة الجوية والقوة البرية والقوة البحرية، ولكن في عصر الانترنت تدور رحى المعارك في الفضاء الالكتروني، وبين خصوم معظمهم مجهول الهوية، يهاجمون البنية التحتية الرقمية للدول التي يصنفونها في خانة العدو، حيث تهدف الهجمات الرقمية إلى الحصول على معلومات مخابراتية حساسة أو تدمير بنية الاقتصاد المعتمد على المعلومات بشكل كبير، أو لمجرد إشعار العدو أنهم موجودون على الجبهة الرقمية[1].

تميل تعريفات الحرب الإلكترونية إلى أن تكون أوصافًا لعمليات تقوم بها دولة ما تستهدف اتلاف أجهزة الكمبيوتر أو الشبكات، إلا أن هذه المفاهيم تبقى غامضة للغاية وتفتقر إلى الدقة الوصفية الكافية، فمن الضروري وضع تعريف أكثر تحديداً للعمل العدواني الذي نسعى إلى تجنبه[2].

في هذا السياق، يذهب ريتشارد إيه كلارك في تعريفه للحرب السيبرانية على أنها " اختراق شبكة أو حاسوب دولة أخرى اختراقا غير مصرح به بواسطة حكومة ما، أو نيابة عنها، أو دعما لها، أو أي نشاط آخر يؤثر على نظام حاسوبي بغرض إضافة أو تغيير أو تزييف البيانات، أو التسبب في تعطيل جهاز حاسوب أو إتلافه، أو تعطيل أو إتلاف جهاز متصل بشبكة أو الأشياء التي يتحكم فيها نظام الحاسوب[3]".

كجزء من هذا النقاش، يقدم أندرو راثمل Rathmeml Andrew تصورا مفاده: أن التطورات التكنولوجية والسوسيو-سياسية تشير إلى أن حرب المستقبل سيكون لها شكلا إلكترونيا محوره المعلومات، وأن هناك قرائن تشير إلى إمكان انهيار كل البنى التحتية الخاصة بأنظمة المعلومات في العالم، وليس في بعض المؤسسات الكبرى أو الدول المستهدفة، وذلك بفعل الهجمات المعلوماتية، التي يتم الإعداد لها بطريقة جيدة والتي تتوخى مهاجمة عدد كبير من الأهداف الحيوية المنتقاة بعناية في مناطق مختلفة من العالم.

وكان رجال السياسة والعسكريون —الذين قالوا بأن حروب المستقبل سوف تعتمد على الفضاء المعلوماتي- يعتقدون بأن هذه الحروب يمكن تحقيق النصر فيها دون إراقة دماء عن طريق الهيمنة المعلوماتية

وتدمير المنظومة المعلوماتية للأعداء[4]، ومع تزايد الاعتماد العالمي على هذه الأخيرة تزايد أيضاً التعرض للهجمات على البنية التحتية الحرجة من خلال الفضاء السيبراني. ورغم أن المعالم الدقيقة لأي "حرب سيبرانية" لا تزال غير محددة فإن الهجمات الكبيرة ضد البنية التحتية للمعلومات وخدمات الإنترنت في العقد الأخير تُعطي صورة ما عن الشكل والنطاق المحتملين للنزاع في الفضاء السيبراني. وقد رُبطت الهجمات في كوريا الجنوبية والولايات المتحدة بالحرب السيبرانية، ورُبطت انقطاعات الكهرباء المتعددة في البرازيل بهجمات سيبرانية، وفي عام 2008 تمكّن القراصنة من الدخول إلى الموقع الشبكي للحكومة والسيطرة عليه لمدة تزيد عن أسبوع. وتوضح انقطاعات الكهرباء في البرازيل الاتساع المحتمل للأنواع الجديدة من الهجمات السيبرانية[5]، كما تزعم مجموعتان من لوائح الاتهام الفيدرالية –إحداهما في فيفري والآخر في جويلية – بالتفصيل كيف عملت شركة خاصة مرتبطة بوتين والجيش الروسي على استقطاب الخطاب السياسي الأمريكي والتأثير على الانتخابات الرئاسية الأمريكية عام 2016[6]، من خلال اختراق الإيميل الخاص بمرشحة الحزب الديمقراطي هيلاري كلينتون، وكذلك الإيميلات الخاصة بـ "اللجنة الوطنية الديمقراطية" من أجل إقناع الرأي العام بعدم التصويت لها، وهو ما صب في النهاية لصالح الرئيس الأمريكي دونالد ترامب، إذ يسود اقتناع راسخ لدى أجهزة الاستخبارات الأمريكية، خاصة وكالة الاستخبارات المركزية (السي آي إيه) بأن موسكو استخدمت أطرافاً ثالثة لتسريب تلك الإيميلات إلى موقع ويكيليكس، والذي قام بدوره بنشرها [7].

كما أنه وفي العقد الأخير من القرن الحادي والعشرين برز وبوضوح دور الفضاء الإلكتروني كمجال جديد في العمليات العدائية، كان أهم صوره الصراع بين إستونيا وروسيا في 2007، والحرب بين روسيا وجورجيا في عام 2008، وبين كوريا الجنوبية والولايات المتحدة الأمريكية في عام 2009 والتي شهدت هجمات إلكترونية كورية على شبكات البيت الأبيض. وجاء الهجوم الإلكتروني بفيروس "ستوكسنت" على برنامج إيران النووي عام 2010 ليمثل نقلة مهمة في تطور واستخدام الأسلحة الإلكترونية، ثم الدور السياسي الذي لعبته شبكات التواصل الاجتماعي في إدارة الفوضى في عدد من الدول العربية خلال عامي 2011، 2012، والهجوم على آلاف من أجهزة كمبيوتر في شركة النفط السعودية "أرامكو" في عام 2016، وهجمات القراصنة ضد قطاعات الطاقة والصناعة والنقل وشركات الطيران المدني في بعض دول الخليج [8].

- **مظاهر التدمير الرقمي:**

ذهبت العديد من دول العالم في السنوات الأخيرة إلى تطوير استخدام مهارات الإنترنت والحواسيب كأدوات هجوم ودفاع واستخبارات وحروب نفسية، فقد أنشأت الولايات المتحدة وبريطانيا وفرنسا وكوريا الجنوبية وحدات خاصة بالقوات المسلحة مسؤولة عن الحرب الإلكترونية أو حرب المعلومات، وتجمع هذه الوحدات الخاصة ما بين العقل العسكري والمهارات التقنية التي تمكنها من إحداث خسائر أو الدفاع وصد الهجمات.

علاوة على ذلك، يُستخدم الإنترنت في شن هجمات إلكترونية من شأنها إلحاق خسائر بالخصم، غالبًا ما تكون مالية؛ فيجري استهداف البنوك أو المواقع الحكومية التي تحتوي على بيانات هامة، أو حتى استهداف منشآت صناعية، كما حدث لبرنامج إيران النووي.

وبالرغم من الطبيعة الافتراضية لهذا النوع من العمليات العسكرية، فإن الأضرار والمعاناة الناتجة عنها لا تقتصر على العالم الافتراضي. ففي عصر يجري فيه التحكم بكل شيء إلكترونيًّا، قد تستهدف بعض الهجمات الإلكترونية مؤسسات البنية التحتية لمنطقة ما، مما يسبب حرمان عدد كبير من المدنيين من الخدمات أو المواد الأساسية كالمياه أو الكهرباء أو الرعاية الطبية، وقد يترتب على ذلك معاناة كبيرة وربما فقدان البعض لحياتهم. لذا فمن المهم متابعة النقاشات الدائرة في هذا المجال، بالإضافة لمتابعة التطورات التقنية من أجل تقليل المعاناة الناجمة عن «العنف الرقمي»[9].

ثانيا: الأسلحة السيبرانية: تطور تكنولوجيا وعقيدة لحرب

في منتصف التسعينات، أوضحت دراسة أجرتها مؤسسة راند RAND Corporation أن تكاليف تطوير الأسلحة السيبرانية اللازمة لإجراء الحرب السيبرانية متواضعة للغاية. وفي هذه الحالة تستطيع كل الدول تقريبًا تحمل هذه التكاليف. ونقلت الصحيفة عن "لاني كاس" Lani Kass كبير مستشاري رئيس أركان القوات الجوية الأمريكية USAF الجنرال "مايكل موسلي" T. Michael Moseley تأكيده على ضرورة تطوير الولايات المتحدة لأسلحة هجومية على الإنترنت.

هذا وينظر إلى الأسلحة السيبرانية على أنها أسلحة الضربة الأولى first strike weapons التي تستخدم لتعطيل قيادة العدو ومراقبته والبنى التحتية التشغيلية، وربما خلق اضطرابات مدنية من خلال وقف

البنية التحتية والخدمات الأساسية. وفي تقرير وضعته Spy-Ops في خريف عام 2007، هناك حوالي 140 دولة لديها برامج نشطة لتطوير الأسلحة السيبرانية في مكانها وتشغيلها.

ويمكن حصر الأسلحة السيبرانية في معظم الأنواع الشائعة من الأسلحة السيبرانية الهجومية: فيروسات الكمبيوتر، والأجهزة الكهرومغناطيسية العابرة، والبرامج الضارة، والبرمجيات الملوثة، برامج التهكير، برنامج Rootki، والديدان Worms، ومفاتيح تشفير والقنابل المنطقية[10] logic bombs ، الأبواب الخلفية Back Doors ، الانتحال، هجمات الحرمان من الخدمة الموزعة.. الخ[11].

كما أن الأدوات السيبرانية تتميز كثيراً عن الأدوات التقليدية ذات التأثير الدولي في ميدان المعركة الجيوسياسية وذلك من نواح أخرى كثيرة؛ لهذه الهجمات قدرة عالية على التخريب بكُلفة اقتصادية منخفضة نسبيا للمهاجمين. وكذلك تُعتبر الكُلفة السياسية – في شكل إمكانية التعرض لخطر الانتقام- منخفضة جداً، نظرا للتحديات التي تعترض إمكانية تحديد هوية من قام بالهجوم. كما أن إغفال القانون الدولي لعقوبات ونصوص واضحة وقاطعة لمواجهة العمليات السيبرانية العابرة للحدود يجعلها أكثر جذباً للبعض. وحيث أنها تجمع بين القدرة التخريبية العالية والانتشار السريع بتكلفة سياسية واقتصادية منخفضة، فإن الهجمات السيبرانية تنتشر بشكل كبير بين الجهات الفاعلة التي تتبع إستراتيجية جيوسياسية موسعة ذات موارد و / أو قدرات دفاعية محدودة[12].

يقودنا هذا للقول أن حروب الانترنت هي حروب لا تناظرية Asymmetric فالتكلفة المتدنية نسبيا للأدوات اللازمة لشن هكذا حروب قد تعني أنه ليس هناك حاجة لدولة ما مثلا أن تقوم بتصنيع أسلحة مكلفة لكي تفرض تهديدا خطير وحقيقي على أية دولة[13]، يضاف إلى ذلك أن أهمية الآليات التكنولوجية وانتشارها قد يؤدي إلى تزايد فداحة الأضرار المترتبة على الحروب السيبرانية في حال وقوعها، هذه القدرة التدميرية تجعلها وسيلة مثلى لتحقيق الإكراه والتأثير في تحركات الفواعل الدولية المختلفة، دون أن يتضمن ذلك إيذاء بدنيا للأفراد مما يجعل عديد الفواعل الدولية تلجأ إلى استخدام الآليات الالكترونية في الهجوم حتى تلك الجماعات التي لا تميل إلى استخدام العنف بشكل عام، مما قد يوسع نطاق الفواعل التي تقوم باستخدام هذه الوسائل في الهجوم، نظرا لان الحواجز المفروضة على الفضاء الالكتروني محدودة للغاية [14].

في هذا الصدد يقول النائب السابق لرئيس أركان القوات الجوية الأمريكية للتخطيط طويل المدى بيري سميث Perry M. Smith: " يجب على المخططين العسكريين أن ينظروا إلى ما وراء استخدام القنابل والصواريخ لمهاجمة الأهداف بدقة، فالتكنولوجيا قد تسمح قريبا بتدمير العناصر الحيوية دون قتل الجنود أو التدمير الكامل للهدف، وإذا أمكن جعل دبابة معادية غير فعالة بمنع المحرك من العمل أو تدمير حاسب جهاز إدارة النيران قد يصبح الفوز بالحرب من خلال وسائل ليست قاتلة بوجه عام ممكنا".

وهو الأمر الذي أقرته وزارة الدفاع الأمريكية رسميا تحت مسمى: تطوير تكنولوجيات وعقيدة لحرب غير قاتلة – " قتل لين SOFT KILL "[15]، يدخل هذا في إطار الأسلحة الذكية التي يتشكل منها ميدان الحرب الالكترونية، والتي تعد بديلا عن الأسلحة التقليدية، وإذا نظرنا إلى جميع حروب المستقبل سنجدها تستهدف النفاذ إلى داخل دورة اتخاذ القرار للخصم وإفقاده السيطرة، وتدميره بأقل خسائر ممكنة، وبأقل تكاليف ممكنة، وأقل زمن متاح، كما تؤدي إلى شل الخصم وسهولة فرض الإرادة السياسية[16]. من خلال الأشكال العديدة للحرب الالكترونية والتي منها: الحجب الضار والتحييد وسرقة أو تغيير البيانات والتسلل وبرمجيات التجسس والعديد من الأسلحة السيبراتية المدمرة لأنظمة الإعلام الآلي من طرف الـ "هاكرس" Hackers أو الـ "كراكرس" Crachers [17]عن طريق الهجوم العاصفي Tempest-attackK، حصان طروادة Trogan Horse[18]، هذا الأخير يعتبره الكثيرون أقوى آداة لهجمات حجب الخدمة الموزعة DDoS وهي نوع جديد من برامج الهجوم الالكترونية التي تعمل على تجنيد أجهزة الحاسوب المتصلة بالأنترنت وتوجيهها إلى بث الرزم الشبكية إلى مزود معين، بهدف إيقافه عن العمل، نتيجة ضغط البيانات المستقبلة؛ ومن أشهر البرامج المستخدمة في إجراء هذه الهجمات TRINPP Stasheldraht, Tribe FloodNet.[19]

وقد تحدث "جوديت دوناث" Judith Donath من جامعة هارفارد عن فيروس "ستكسنت" ويرى فيه مثالا لنوع جديد من الأسلحة التي يمكن تطويرها. ويجدر بأي مفكر عسكري استراتيجي يظن أن تداعياته ستقتصر على مجالات مثل: التجسس فقط، أن يزور محطات الطاقة للقواعد العسكرية، أو غرف محركات السفن الحربية التي تعمل باستخدام برامج التحكم، والاستحواذ على البيانات ذاته (SCADA) الذي صمم فيروس "ستكسنت" لاستهدافه، فمن الأهمية بمكان ملاحظة أن "ستكسنت" بمجرد إطلاقه قام بمهمة معقدة بحثا عن هدفه وتدميره، ويرى جاسون هيلي Jason Healey –وهو مسؤول سابق في

البيت الأبيض، ويدير الآن "مبادرة فنون الإدارة السيبرانية" Cyber Statecraft Initiative في المجلس الوطني- أن "ستكسنت" كان" أول سلاح مستقل يضغط على الزناد بواسطة معادلة خوارزمية، وليس بيد بشرية"[20].

هذا هو السبب الذي يدعوا الكثيرين إلى القلق من أن تفضي هذه الأسلحة إلى ظهور نوع جديد من التصعيد يحمل مخاطر عالمية. وفي هذا الاطار كتب ميكو هايبونين Mikko Hypponen المفكر في مجال الفضاء السيبراني: " لقد غير فيروس "ستكسنت" قواعد اللعبة بشكل قاطع"، وأضاف: " ندخل سباق تسلح حيث تبدأ فيه الدول بتخزين الأسلحة، الحديث هنا لا يقتصر عن طائرات ومفاعلات نووية فقط، بل تخزين أسلحة سيبرانية ايضا".

ووصف "رالف لانجنر" Ralph Langner الخبير الأمني في مجال الحاسوب، ومكتشف "ستكسنت" للعالم السلاح الجديد بقوله: يمكن أن تعتبره نموذجا لنهج "حرب عادلة". فلم يقتل أحدا، وهذا شيء جيد. غير أنني أخشى أن يكون هذا على المدى القصير فقط، فعلى المدى الطويل سيفتح صندوق باندورا [صندوق الشر]، الأمر الذي يقودنا للقول أن مآلات الحروب المستقبلية قد تحسمها الحروب السيبرانية، خاصة مع التوجه العسكري الجديد، والتنافس على تطوير الأسلحة السيبرانية بمختلف أصنافها الدفاعية والهجومية.

الجدير بالذكر أيضا أن التنافس اليوم أضحى أكثر اتساعا من ذي قبل. وبات عدد الدول التي يمكنها بناء أو حتى استغلال المنصات التي كانت توفر في السابق الهيمنة على المعركة مثل البوارج أو القاذفات الإستراتيجية، يعد على أصابع اليد الواحدة. بالمقارنة، هناك ما لا يقل عن 87 جيشا له منظومات جوية غير مأهولة، ولدى أكثر من 100 جيش برامج حرب سيبرانية، بينما لدى نحو 20 منها قدرات سيبرانية متطورة[21]، مما يعكس أهمية تضمين البعد السيبراني في استراتيجيات الدول للدفاع والأمن.

من نافلة القول، إن التأثير غير المؤكد للأسلحة ومعدات الحرب الالكترونية وأساليبها على طبيعة الحرب في المستقبل قد يزيد أو يقلص فرص الحرب، كما أن تعقيد تكتيكات وتقنية الحرب السيبرانية وتأثيرها الواسع جدا في المعركة قد يتسبب في تردد بعض القادة قبل وضع ثقتهم بقدرة قواتهم على تحقيق نصر سريع وحاسم، ولكن إذا وضع القادة ثقتهم بالمزاعم التي يؤكدها العسكريون بأن الحرب السيبرانية ستساعدهم على

تحقيق نصر سريع، فربما يصبحون أكثر رغبة في المخاطرة بشن الحرب. رغم أن استحالة التنبؤ بالحرب السيبرانية يجعل الحرب أكثر خطورة فإنها أيضا تفتح مجالا للخطأ في التقديرات السياسية والعسكرية[22].

هذا ويجادل بعض المراقبون بأن الاستخدام الفعال للحرب الالكترونية سيخفض الخسائر البشرية وتكاليف الحرب بشكل كبير مقارنة بالخسائر الدامية في الحروب التقليدية، لكن ذلك لن يكون صحيحا إلا إذا أمكن شن الحرب الالكترونية بشكل فعال وأدت بالفعل إلى الانتصار في الحرب، وليس في معركة واحدة.

ربما ستدعم الحرب الالكترونية حجج المنادين بـ" مبدأ المناورة"، الذين يقولون إن الحرب الالكترونية الخاطفة يمكن أن تتيح للقوات الأضعف أن تهزم القوات الأقوى، وأن المهارات العسكرية يمكن أن تمنع الحرب من التفاقم عن طريق الاستنزاف[23].

ثالثا: الالتزام بقواعد الحرب في المجال السيبراني.

ذهب البعض لوصف الحروب السيبرانية بأنها حرب باردة جديدة، تخلق واقعًا عالميًّا جديدًا يتميز بكثير من التعقيد. وأصبحنا الآن أمام مصطلحات حربية تقليدية تضاف إليها الصفة الافتراضية أو الرقمية أو الإلكترونية، مثل: سباق التسلح الإلكتروني، ساحات الحرب الإلكترونية، الجهاد الإلكتروني، المقاتلين الإلكترونيين، وأخيرًا الإرهاب الإلكتروني.

حدا هذا الوضع الجديد مجموعة من الخبراء لأن يطالبوا بعقد اتفاقيات دولية للحد من التسلح داخل الفضاء الإلكتروني، مثل تلك التي تمت في مجال الانتشار النووي والكيماوي، ويمكن لهذه الاتفاقيات أن تساهم – في حال تطبيقها – في وضع قيود على الحروب الإلكترونية؛ استخدامها، وتوزيعها، وانتشارها، وتطويرها.

في عام 2013، ساهمت اللجنة الدولية للصليب الأحمر بصفتها مراقبًا في نشر ما يُعرف بـ "دليل تالين للقانون الدولي المطبَّق على الحرب الإلكترونية" اختصارا دليل تالين[24].

1- دليل تالين كرافد قانوني لتنظيم الحروب السيبرانية:

دليل تالين Tallin Manual (الذي يُطلق عليه اسم العاصمة الإستونية، حيث يوجد مركز الأبحاث) هو وثيقة قانونية غير ملزمة تتضمن قواعد القانون الدولي المعمول به أثناء الحروب السيبرانية، يتكون

من 95 قاعدة، تم إطلاق هذا المشروع على أمل تحقيق قدر من الوضوح للمسائل القانونية المعقدة المحيطة بالعمليات السيبرانية[25]، الوثيقة الصادرة عن حلف الناتو والتي أتت لتعزيز الوعي العالمي، كمحاولة لتقديم النصح للدول حول كيفية العمل بشكل قانوني في هذا المجال الحربي الجديد والمثير للقلق العالمي[26].

وفي هذه الحالة تعكس القواعد المنصوص عليها في دليل تالين توافقاً في الآراء بين الخبراء على القانون الذي يحكم وينظم حالياً النزاع السيبراني مراعاة لقواعد القانون الدولي الإنساني، فدليل تالين وفي القاعدة العاشرة منه يحظر التهديد أو استخدام القوة Prohibition of Threat or Use of Force[27]، كما ينص في القاعدة 32 على حظر مهاجمة المدنيين Prohibition on Attacking Civilians[28] ، في حين تضمنت المادة 37 حظر مهاجمة كل ما يتعلق بأغراض المدنيين Prohibition on Attacking Civilian Objects[29].

كما يحاول دليل تالين تحديد الأهداف التي لا يمكن الوصول إليها (المدارس والمستشفيات على سبيل المثال) ويبين تحت أية ظروف يمكن للدولة الاستجابة لهجوم سيبراني بالقوة العسكرية. ولكن كما يشير دليل تالين على أنه "ليس وثيقة رسمية" و "يجب أن يُفهم فقط كتعبير عن آراء مجموعتين دوليتين من الخبراء فيما يتعلق حالة القانون ".

هذا وقد اتفقت عشرات الشركات التكنولوجية، بما في ذلك شركة مايكروسوفت وشركة فيسبوك، على أنهم "لن يساعدوا الحكومات على شن الهجمات الإلكترونية ضد المواطنين الأبرياء والمؤسسات". وقد شُبِّه ما يسمى باتفاقية الأمن السيبراني مع نسخة رقمية من اتفاقيات جنيف، وهي الاتفاقيات الدولية التي تعنى بحماية حقوق الإنسان الأساسية في حالة الحرب[30].

2- اتفاقية جنيف الرقمية:

هناك جدل كبير بين الدول الرائدة حول ما إذا كان يجب تطبيق قانون النزاع المسلح على الأنشطة على الإنترنت[31]، حيث يعد غياب الشفافية في المجال السيبراني أمرا يجعل من الصعب تطبيق استراتيجيات الحد من التسلح بالنسبة للأسلحة الالكترونية المستخدمة لعدم القدرة على تحديد هوية القائم بالهجوم، وذلك على عكس الأسلحة النووية التي تمنح الفاعلين قدر من الشفافية يمكنهم القيام بالتفاوض من أجل الحد من التسلح.

كما يتسم الفضاء الالكتروني بعدم وجود قواعد مقبولة للسلوك والتي من المفترض أن تمكن الفاعلين من التنبؤ بالنتائج المحتملة لما يقومون به من أفعال. فعلى الرغم من وجود عدد من القواعد والقوانين الدولية التي تحكم المجالات الأخرى وتقوم بتعريف الفعل العدواني، إلا أن ذلك يغيب في مجال الفضاء السيبراني، فالفاعل قد يقوم بإحداث تدمير واسع النطاق دون أن يتضمن ذلك استخدام أي نوع من أنواع العنف. وهو الأمر الذي قد لا يؤدي إلى إحداث هجوم مضاد بالضرورة، فوجود قدر من القواعد الحاكمة للسلوك يؤدي إلى وجود تنبؤ بإمكانية قيام قوى عظمى بالرد، حتى وإن تضمن ذلك استخدام القوة المسلحة في حال تعرضها للهجوم، ومن ثم يتم تبرير هذا الهجوم المضاد في هذه الحالة وفق مبدأ مشروعية الدفاع عن النفس[32].

ومن الواضح أن صياغة استجابة فعالة لهذا النوع المتنامي من الأسلحة السيبرانية تقع على عاتق الحكومات الوطنية، نقلاً عن رئيس مايكروسوفت براد سميث Brad Smith : "يتعين على حكومات العالم أن تتخذ نهجا مختلفًا وأن تلتزم في الفضاء الإلكتروني بنفس القواعد المطبقة على الأسلحة في العالم المادي، وهذا هو أحد أسباب "اتفاقية جنيف الرقمية" بما في ذلك مطلب جديد للحكومات بالإبلاغ عن نقاط الضعف إلى جانب تطوير القدرات الهجومية، و من المرجح أن تزداد سرقة وتسرب الأسلحة السيبرانية الهجومية واستخدامها اللاحق، مما قد يخلق توترات دولية جديدة بين الحكومات وبينها وبين صناع التكنولوجيا[33].

علما أن اتفاقية جنيف الرقمية والتي دعت إليها شركة مايكروسوفت على لسان رئيسها تهدف إلى وضع قواعد فيما يخص التهديدات الإلكترونية، وتحث حكومات العالم على تشكيل هيئة دولية لحماية المدنيين من القرصنة التي ترعاها الدول، وضرورة تواجد معاهدات وهيئة تحكيم محايدة لمحاسبة الحكومات العالمية عند ارتكابها لهجمات وجرائم إلكترونية.

ودعا رئيس شركة مايكروسوفت إلى وضع معاهدات رقمية مماثلة لمعاهدات جنيف [34]، وصرح " نحن بحاجة إلى اتفاقية جنيف الرقمية التي من شأنها أن تلزم الحكومات بتنفيذ المعايير اللازمة لحماية المدنيين على شبكة الإنترنت في أوقات السلم " .

في نفس السياق، أشار أيضاً إلى الحاجة لمنظمة محايدة مستقلة تتبع معايير مستقلة بحيث يمكنها تحديد التهديدات الإلكترونية، وتمتلك القوة اللازمة للتحقيق في جميع القطاعات العامة والخاصة، وتجبر الحكومات على نشر تقارير حول الثغرات الأمنية، و يوجد حالياً عدد قليل جداً من القواعد التي تعمل على تنظيم الهجمات الإلكترونية الدولية، حيث تعهدت الولايات المتحدة و الصين في عام 2015 بالامتناع عن قرصنة الشركات من أجل سرقة الملكية الفكرية، كما وقع المنتدى الاقتصادي الدولي المعروف باسم مجموعة الـ 20 تعهداً مماثلاً في العام نفسه، وقال سميث أيضاً أنه ينبغي على الشركات التقنية التعهد بالوقوف على الحياد فيما يخص الصراعات السيبرانية، وأنه يفترض بقطاع التقنية أن يحمي مستخدمي الإنترنت من خلال عدم مساعدة الحكومات في الهجمات السيبرانية لتحقيق الأمن بشكليه العام والخاص كرافدين للأمن العالمي [35].

رابعا: مستقبل الأمن العالمي في ظل النزوع نحو الحروب السيبرانية

1- اتساع نطاق الصراع والفاعلين فيه

إن انتشار الفضاء الإلكتروني وسهولة الدخول إليه يمكن أن يوسع دائرة الاستهداف بالإضافة إلى زيادة عدد المهاجمين، ولتدور تلك الهجمات المتبادلة على نحو من الكر والفر ليعبر عن حالة صراع ممتد يرتبط بطبيعة الفضاء الإلكتروني المختلفة. ودفعت الأهمية المتصاعدة للفضاء الإلكتروني في الاستحواذ على القوة إلى الصراع حول امتلاك مقدراتها وأدواتها من أجل العمل على الحماية والدفاع وتطوير القدرات الهجومية في سبيل تعظيم القوة والتفوق والهيمنة بين الدول والفاعلين من غير الدول وتعزيز التنافس حول السيطرة والابتكار والتحكم في المعلومات، لزيادة النفوذ والتأثير ليس على نطاق محلي فقط، بل على نطاق دولي أيضًا[36].

خاصة وأن حجم الهجمات السيبرانية ينمو بشكل مطرد، ويتوقع الكثيرون احتمال وقوع هجمات الكترونية كارثية في المستقبل. لقد رأينا بالفعل هجمات على نطاق وطني، لذلك ليس من المستبعد أن نتخيل وباء رقمي بهجمات تشل اقتصادات بأكملها. كما وصفها أحد محللي الصناعة في أمريكا بـ"بيرل هاربور الرقمية قادمة ..."

في حين يتوقع أنه سيزداد تهديد الصراع السيبراني المدمر على مدار العقد المقبل، ولن يقتصر على الدول القومية فحسب، بل أيضًا من قِبل بدائلها، ومن خلال الحركات السياسية المستقلة والجهات الفاعلة الخاصة. وستقترن أعمال الصراع السيبراني بالمعلومات المضللة والدعاية لزعزعة استقرار الدول والاقتصادات. سيؤدي هذا لمستقبل يصبح فيه تقويض هياكل الحكم والقيم التي تمثلها أكثر شيوعًا، وستكون البنية التحتية الرقمية معرضة للقرصنة وسرقة البيانات مما يعرض وبالأساس اقتصادنا المستقبلي للخطر[37]. وهنا، تري الدول الكبرى أن من يحدد مصير تلك المعركة المستقبلية ليس من يملك القوة فقط، وإنما القادر على شل القوة، والتشويش على المعلومة[38].

2- الأسلحة السيبرانية كسمة معيارية للحرب.

يشير الأمين العام لحلف الناتو "ينس ستولتنبرغ" إلى استخدام الأسلحة الإلكترونية ضد داعش في العراق وسوريا مؤكدا على أن الإنترنت سيكون جزءًا لا يتجزأ من أي صراع عسكري، ونظرًا لأن الجيوش و أجهزة الاستخبارات ينفقون أكثر على بناء مخزونها من الأسلحة الالكترونية فستحدث ضغوط لا محالة لإثبات قيمة هذا الاستثمار[39].

كما من المتوقع أن ينمو سوق الأسلحة الإلكترونية أكثر والتي يتم فيها توظيف المجرمين أو القراصنة أو المتطوعين بما يعمل على سرعة انتشارها ويفاقم من تأثيرها ويحد من قدرة الدول على تنظيم استخدام القوة عبر الفضاء الإلكتروني، بالإضافة إلى التطور الملحوظ في امتلاك دول لقدرات تطوير واستخدام الأسلحة الإلكترونية، وهو ما يجعل تلك التهديدات تمثل خطرا على أمن الفضاء الإلكتروني باعتباره أصبح مرفقا دوليا، 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، كالدول والمنظمات الإرهابية والأفراد وعناصر إجرامية وآخرين[40].

كما يمكن استخدام الأسلحة الإلكترونية والحرب الإلكترونية لتحقيق مكاسب سياسية بين القوى الكبرى، لكن من غير المؤكد ما إذا كان سيؤدي هذا الوضع إلى اضطرابات كبيرة في الشبكة أم لا، وربما يقلل من ثقة مستخدمي الإنترنت بها.

3- الاستجابة والاستعدادات السيبرانية.

استجابة للتهديد المتزايد للهجمات الإلكترونية من المتوقع أن تولي الحكومات أهمية متزايدة لقضايا الأمن السيبراني، عن طريق تعزيز مختلف تدابير الحماية التكنولوجية والسياسية، وتكريس سبل التعاون الدولي ضمانا للأمن السيبراني العالمي[41]، وستستمر الدول بالاستعداد لتلك التحديات الأمنية الجديدة من خلال العمل على تحديث النشاط الدفاعي لمواجهة مخاطر الحرب السيبرانية، ومن جهة أخرى الاستثمار في البنية التحتية المعلوماتية وتأمينها، وتحديث القدرات العسكرية في مجال الحرب الالكترونية وتدشين وحدات حرب خاصة بها، ورفع كفاءة الجاهزية للحرب السيبرانية عن طريق التدريب والمشاركة الدولية في حماية البنية المعلوماتية، والاستثمار في رفع القدرات البشرية داخل الأجهزة الوطنية المعنية، ويتعلق التوجه الأخطر بنقل تلك القدرات من الدفاع إلى الهجوم عن طريق استخدام تلك الهجمات في إطار إدارة الصراع والتوتر مع دول أخرى.

كما يتطلب من المجتمع الدولي التركيز على العلاقة بين الأمن الإلكتروني وبقضايا التنمية الاقتصادية والاجتماعية والاستقرار السياسي، وصياغة إستراتيجية دولية لمواجهة تصاعد الأخطار الإلكترونية، وأهمية تعاون كافة الفاعلين في مجتمع المعلومات العالمي لترسيخ ثقافة عالمية لأمن الفضاء الإلكتروني، وأهمية الموازنة بين اعتبارات الأمن وحرية استخدام الفضاء الإلكتروني، وما بين الاحتكار العالمي للتكنولوجيا والعمل على انتقالها في دول العالم، ومن ثم فإن التعامل مع النمط الجديد من التهديدات يتطلب تعاونا دوليا، وأهمية الحاجة إلى فتح الطريق أمام التعاون المثمر بين الحكومات والأفراد والشركات العاملة في تكنولوجيا الاتصال والمعلومات، ما يستوجب تعزيز دور الفضاء الإلكتروني في النمو الاقتصادي وتحسين حياة المواطنين، وحرية الرأي والتعبير، وتعزيز التسامح بين الثقافات، وبذل جهود دولية عاجلة ومتكاتفة لمواجهة تهديدات أمن الفضاء الإلكتروني بإمكانية العمل على حل الصراعات على أرض الواقع لمنع انتقالها إليه، والعمل على توافق القوانين المتعلقة بالصراع الإلكتروني مع القانون الدولي وأهمية المبادرات الدولية لحماية الفضاء الإلكتروني فضلا عن البحث والتطوير في مجال الدفاعات ضد الأخطار الإلكترونية[42]، وتعزيز أشكال التعاون الدولي في سبيل مكافحتها من أجل تعزيز أمن الفضاء الإلكتروني باعتباره مرفقا دوليا وتراثا مشتركا للإنسانية[43] ، فضلاً عن توعية الرأي العام بمخاطر هذا النمط الجديد من الحرب، وتعزيز التعاون بين الوكالات الأمنية العاملة في مجال الأمن السيبراني والوكالات الأمنية التقليدية[44]، وتكافل القطاعين العام والخاص على المستويين الوطني والدولي لخلق ثقافة عالمية للأمن السيبراني، حيث يصبح الأمن السيبراني مسؤولية الجميع[45].

خاتمة:

بات جليا أن الاتكالية التي تسيطر على العالم في كثير من مفاصله، واعتماده الكبير على الانترنت والتكنولوجيا، ستقودنا حتما إلى حروب مدمرة باستخدام جيوش حديثة منظومتها القتالية سيبرانية، لتصبح ميدانا رابعا من ميادين الحرب، فالدول اليوم أدركت أنه لا بد من تطوير استراتيجيات تتيح لها إخضاع الخصوم بدون الدخول في حروب تقليدية قد تكلف خسائر مادية ومعنوية كبيرة، في حين تم تطوير الأسلحة السيبرانية واستخدامها في الغالب من قبل وكالات الاستخبارات كجزء من المهام السرية، إلا أنها أصبحت الآن خيارًا عسكريًا معمولا به أثناء النزاعات، و امتلاك القدرة على الحرب الإلكترونية هو أحدث ما يجب أن يكون بالنسبة للعديد من الدول القومية، الأمر الذي أثار سباق تسلح عبر الإنترنت لا يظهر أي علامة على التباطؤ. كما أن تزايد اعتماد الدول على الحرب السيبرانية قد يؤدي إلى تصعيد الصراع إلى مواجهات عسكرية في العالم الواقعي، خاصة وأن التهديدات السبرانية تمثل خطرا على أمن الفضاء الإلكتروني باعتباره أصبح مرفقا دوليا.

واستجابة للتهديد المتزايد للهجمات الإلكترونية من المتوقع أن تولي الحكومات أهمية متزايدة لقضايا الأمن السيبراني وتعزيز مختلف تدابير الحماية التكنولوجية والسياسية، وتكريس سبل التعاون الدولي ضمانا للأمن السيبراني العالمي على اعتبار انه رافد جديد للأمن القومي وجزء من الأمن الجماعي.

الهوامش:

[1] عباس بدوان، الحروب الالكترونية الاشتباك في عالم المعلومات، (بيروت: مركز دراسات الحكومة الالكترونية، 2010)، ص 4.

[2] Daniel Dobrygowski, "What would a cyberwar look like?, world economic forum", April 25. 2018, available from :https://goo.gl/RqF7wo

[3] ريتشارد إيه كلارك، روبرت كيه كنيك، حرب الفضاء الالكتروني الخطر القادم على الأمن القومي وسبل المواجهة، ط 1 (أبو ظبي: مركز الإمارات للدراسات والبحوث الإستراتيجية، 2012)، ص 267

[4] محمد طوالبية، الأمن في العالم الافتراضي دراسة في سيكولوجية الإرهاب الالكتروني، مجلة الأكاديمية للدراسات الاجتماعية والإنسانية، العدد 18، (جوان 2017) ، ص 55-67.

[5] حمدون.أ.توريه، الفضاء السيبراني وتهديد الحرب السيبرانيي، البحث عن السلام، (الاتحاد الدولي للاتصالات، جانفي 2011)، ص 9-12.

[6] Timothy Summers, How the Russian government used disinformation and cyber warfare in 2016 election – an ethical hacker explains, the conversation, July 27, 2018, available from : https://goo.gl/cNFKZZ

[7] سرحات شوبوأوجلو، تزايد استخدام الأسلحة السيبرانية في الصراعات الدولية، مجلة اتجاهات الأحداث (نوفمبر 2017)، ص 59.

[8] عبد الغفار عفيفي الدويك، "الأزمات والحروب السيبرانية.. تهديدات تتجاوز الفضاء الالكتروني"، شوهد في 2021/01/01، انظر: https://goo.gl/HTtUe4

[9] *محمد علام فرغلي،" العنف الرقمي: أحدث صيحات الحروب الجديدة"، مجلة الإنسان عدد 59، 2015، شوهد في 2021/03/14، انظر:* https://goo.gl/YRTBHQ

[10] القنبلة المنطقية هي قطعة من الكود مدرجة عمداً في نظام برمجي يقوم بإطلاق وظيفة ضارة عند استيفاء شروط محددة.. للاستزادة انظر :

Tommy Armendariz, What Is a Logic Bomb?, available from: https://goo.gl/N9351U

[11] Kevin Coleman, "The Cyber Arms Race Has Begun", CSO, JAN 28, 2008, available from: https://goo.gl/xKcvK4

[12] عادل رفيق، "الجيوبوليتكس السيبرانية والاستقرار في الشرق الأوسط"، المعهد المصري للدراسات، شوهد في 2020/12/25 انظر: https://goo.gl/Fzq8jW

[13] فيصل محمد عبد الغفار، الحروب الالكترونية، (الأردن: الجنادرية للنشر والتوزيع، 2015)، ص 11.

[14] نوران شفيق، السياسة الدولية والاستراتيجية أثر التهديدات الإلكترونية على العلاقات الدولية دراسة في أبعاد الأمن الالكتروني،(االقاهرة: لمكتب العربي للمعارف، 2016)، ص 8-9.

[15] الفين وهايدي توفلر، تر محمد عبد الحليم أو غزالة ،الحرب وضد الحرب ،(مصر: دار المعارف ، 2000) ص ص 65-66.

[16] خليل حسين، حسين عبيد، الإستراتيجيا: التفكير والتخطيط الاستراتيجي استراتيجيات الأمن القومي والحروب وإستراتيجية الاقتراب غير المباشر،ط1(بيروت: منشورات الحلبي الحقوقية، 2013)، ص ص320-321.

[17] يمكن ملاحظة الفرق الرئيسي بين الـ hackers الـ crackers من خلال النقاط التالية: الهاكرز هم الأشخاص الذين يستخدمون معارفهم لغرض جيد ولا يتلفون البيانات،وذلك بالاعتماد على دراستهم للشبكات والبرمجة

والاستراتيجيات وطرق التسلل والاستغلال، في حين أن الكراكرز هم الأشخاص الذين يخترقون النظام بغرض خبيث ويتلفون البيانات عمدا، وغالبا ما يكون هدفهم المال.

[18] خلفاوي محمد، الاستعلام رهان حرب صامت، (دراية–الجزائر :سارة للنشر، 2016)، ص 228–231.

[19] أسامة سمير حسين، الاحتيال الالكتروني الوجه القبيح للتكنولوجيا، ط1 (عمان: الجنادرية للنشر والتوزيع، 2011)، ص 146.

[20] يتر سينجر، الحرب عن بعد دور التكنولوجيا في الحرب، ط1 (الإمارات: مركز الإمارات للدراسات والبحوث الإستراتيجية 2010)، ص89.

[21] بيتر سينجر، **مرجع سابق**، ص 93.

[22] بيتر سينجر، **مرجع سابق**، ص89– 96

[23] عبد الكريم محمود برم، التقنية في الحرب: البعد الإلكتروني، ط1(أبو ظبي: مركز الإمارات للدراسات والبحوث، 2010)، ص 453.

[24] *محمد علام فرغلي،" العنف الرقمي: أحدث صيحات الحروب الجديدة"، مجلة الإنسان عدد 59، 2015، شوهد في 2021/03/14، انظر:* https://goo.gl/YRTBHQ

[25] Tallinn Manual, NATO Cooperative Cyber Defence Centre of Excellence, Cambridge University Press, UK, 2013, p17

[26] Michael Robinsona, Cyber Warfare: Issues and Challenges, Journal of Computers and Security, 18 March 2015, p 2.

[27] Tallinn Manual, ***Op.Cit,*** p 45.

[28] ***Ibid,*** p 97.

[29] ***Ibid***, p 106.

[30] Jordan Robertson and Laurence Arnold, Cyberwar: How Nations Attack Without Bullets Or Bombs, available from: https://goo.gl/fZd35o

[31] Daniel Dobrygowski, What would a cyberwar look like?, world economic forum, April 25. 2018, available from :https://goo.gl/RqF7wo .

[32] نوران شفيق، ***مرجع سابق***، ص 9.

[33] Gil Baram, "from Net Politics and Digital and Cyberspace Policy Program The Theft and Reuse of Advanced Offensive Cyber Weapons Pose A Growing Threat", Council Foreign Relations, 20-01-2019, available from: https://goo.gl/UKjwrE

[34] تعتبر اتفاقيات جنيف لعام 1949 بمثابة معاهدات جرى وضعها بعد الحرب العالمية الثانية، و التي تهدف إلى وضع قواعد تمنع التطرف وسط الصراعات المسلحة ، بحيث تصنف الإنتهاكات لهذه المعاهدات على أنها جريمة حرب

[35] أحمد عنتر، "مايكروسوفت تدعو لإيجاد اتفاقية جنيف الرقمية"، موقع المركز العربي لأبحاث الفضاء الالكتروني، شوهد في 2021/02/06، انظر:https://goo.gl/fLnsn5

[36]عادل عبد الصادق، "خطر الحروب السيبرانية عبر الفضاء الالكتروني"، مقال في موقع لغة العصر،2017 ، شوهد في 2021/02/11، انظر: https://goo.gl/e3Nm3q

[37] Internet Society Global Internet Report 2017, Paths to our Digital Future, 2017, P 55-61, available from: https://goo.gl/2N2Ywu

[38] عادل عبد الصادق، "أنماط الحرب السيبرانية وتداعياتها على الأمن العالمي"، السياسية الدولية، 2017، شوهد في 2021/01/3 انظر: https://goo.gl/e5xw6F

[39] Steve Ranger, The future of cyberwar: Weaponized ransomware, IoT attacks and a new arms race, Tech Republic; Nov 15. 2017, available from: https://goo.gl/R1V4tG

[40] عادل عبد الصادق، القوة الالكترونية :أسلحة الانتشار الشامل في عصر الفضاء الالكتروني، **مجلة** السياسية الدولية، العدد 188، أفريل 2012.

[41] Internet Society Global Internet Report 2017, Paths to our Digital Future, P 55-61, available from: https://goo.gl/2N2Ywu

[42] عادل عبد الصادق، القوة الالكترونية :أسلحة الانتشار الشامل في عصر الفضاء الالكتروني، **مرجع سابق**، ص121.

[43] المرجع نفسه.

[44] شوبوأوجلو، **مرجع سابق**، ص 59.

[45] عادل عبد الصادق، "أنماط الحرب السيبرانية وتداعياتها على الأمن العالمي"، السياسية الدولية، شوهد في 2021/01/3 انظر: https://goo.gl/e5xw6F