الجهود الفقهية لمواجهة مخاطر الأمن السيبراني

م.م. رائد حميد صالح

جامعة التراث

Abstract

We live today in the digital age thanks to the tremendous development in information and communication technology, because of the intertwining and interdependence between communication networks, which led to the emergence of a new environment for interaction between individuals, societies, and countries, which is termed as cyberspace, which is characterized by its rapid development and extreme ambiguity, and the misuse of this space has created The existence of risks and threats to states in their security and led to the emergence of cyber security as a basic pillar in building the national security of states, so states rushed to form civil and military bodies and institutions to defend their cyber security, and to enact legal legislation to confront this technological development, and among them was the jurisprudence efforts of legal scholars To face the risks and threats to countries, individuals and society in their cybersecurity, and to create a safe and stable cyberspace.

Keywords: yberspace, cyber risks, cyber attacks, cybersecurity, cyber wars

الملخص

نعيش اليوم في العصر الرقمي بفضل التطور الهائل في تكنولوجيا المعلومات والإتصال, فبسبب التشابك والترابط بين شبكات الإتصالات ادى الى ظهور بيئة جديدة للتفاعل بين الأفراد والمجتمعات والدول, وهو ما أصطلح عليه بالفضاء السيبراني, المتميز بتطوره السريع والغموض الشديد, وقد خلق الإستخدام السيئ لهذا الفضاء الى وجود مخاطر وتهديدات تتعرض لها الدول في أمنها وأدى الى بروز الأمن السيبراني كركيزة أساسية في بناء الأمن القومي للدول, لذلك سارعت الدول الى تشكيل هيئات ومؤسسات مدنية وعسكرية للدفاع عن أمنها السيبراني, وسن تشريعات قانونية لمواجهة هذا التطور التكطنولوجي, وكان من بينها الجهود الفقهية لفقهاء القانون لمواجهة المخاطر والتهديدات التي تتعرض لها الدول والأفراد والمجتمع في أمنها السيبراني, وخلق فضاء سيبراني آمن ومستقر.

الكلمات الدالة: الفضاء السيبراني, المخاطر السيبرانية, الهجمات السيبرانية, الأمن السيبراني, الحروب السيبرانية

١. المقدمة

في إطار غياب توجه رسمي من الأمم المتحدة ظهرت إجتهادات فقهية عديدة لمعالجة مخاطر الأمن السيبراني التي تتعرض لها الدول وتقع في مقدمتها مسألة الهجمات السيبرانية, والإستجابة الدولية الأهم والأبرز لمعالجة هذه المسألة جاءت فيما يسمى بـ "دليل تالين Tallinn Manual" للقانون الدولي المنطبق على الحرب السيبرانية والذي قام بإعداده مجموعة من أبرز فقهاء القانون الدولي, إذ تم نشر الإصدار الأول منه عام ٢٠١٣ وأحتوى على ٩٥ قاعدة قانونية إرشادية لعمل أو سلوك الدول في سياق الحرب السيبرانية, وصدر الإصدار الثاني منه عام ٢٠١٧ وأحتوى على ١٥٤ قاعدة قانونية لُيشكل مستوى أكثر أتساعاً لمعالجة العمليات السيبرانية ومراجعة وحسم لنقاط عدم الإتفاق في الإصدار الأول, بالإضافة الى جهود الخبراء الدوليين صدرت مبادئ في إعلان "إيريتشي" بشأن الأستقرار والسلام السيبراني والذي أعده فريق الرصد الدائم المعني بأمن المعلومات التابع للأتحاد العالمي للعلماء "WFS " [1].

٢. دليل تالين والهجمات السيبرانية

([1]) See, Priyanka R. Dev, " Use of Force" and "Armed Attack" Thresholds in Cyber Conflict: The Looming Definitional Gaps and the Growing Need for Formal U.N. Response", Texas International Law Journal, Vol. 50, Issue 2, 2015, P: 380. See also, Eric Talbot Jensen, "The Tallinn Manual 2.0: Highlights and Insights", Research Paper, No. 17, Georgetown Journal of International Law, 2017, P: 01.

عرّف فريق الخبراء (لدليل تالين ٢) العمليات السيبرانية بأنها (تعتبر العملية السيبرانية التي تشكل تهديداً أو استخداماً للقوة ضد السلامة الإقليمية أو الاستقلال السياسي لأي دولة، أو التي تتعارض بأي طريقة أخرى مع أغراض ومقاصد الأمم المتحدة، غير شرعية) [٢], وهو ما يتفق مع المادة (٢/ فق ٤) من ميثاق الأمم المتحدة والتي تنص على انه (يمتنع أعضاء الهيئة جميعاً في علاقاتهم الدولية عن التهديد بإستعمال القوة أو أستخدامها ضد سلامة الأراضي أو الأستقلال السياسي لأية دولة أو على أي وجه أخر لا يتفق ومقاصد الأمم المتحدة).

كما ذكر فريق الخبراء الدولي ان العملية السيبرانية تُشكل إستخداماً للقوة عندما يكون حجمها وأثارها قابلة للمقارنة مع العمليات غير السيبرانية التي تصل لمستوى أستخدام القوة, وذلك في القاعدة (٦٩) من (دليل تالين ٢), التي تنص على انه (تشكل العملية السيبرانية استخداماً للقوة عندما يكون نطاقها وآثارها قابلة للمقارنة مع العمليات غير السيبرانية التي ترتفع الى مستوى استخدام القوة) [٣], ففي سياق النص المقدم اعلاه أقر الخبراء الدوليين أنهم قد أستندوا الى معيار الحجم والتأثير في تحديد فيما إذا كانت الهجمة السيبرانية ترتقي الى إستخدام غير مشروع للقوة, وايضاً فيما إذا كان هجوماً عسكرياً يبرر الدفاع عن النفس وفقاً للمادة (٥١) من ميثاق الأمم المتحدة [٤].

من ثم ووفقاً لدليل تالين, تعتبر العمليات السيبرانية إستخداماً للقوة عندما يكون مستواها وتأثيرها متقارباً مع العمليات غير السيبرانية, وذلك إعتماداً على معيار النطاق والأثر في تحديد الدرجة التي يجب ان يصل إليها الهجوم السيبراني كإستخدام للقوة أو هجوماً مسلح, وعليه, يمكن إعتبار هجوم سيبراني كهجوم مسلح إذا أحدث ضرر, أو يصل الى درجة من الشدة, ويُقصد بذلك ان يُحدث أضراراً مادية جسيمة, وأستند الخبراء الدوليين في إعتماد هذا الأختبار على رأي محكمة العدل الدولية في قضية الأنشطة العسكرية وشبة العسكرية (نيكاراغوا ضد الولايات المتحدة الإمريكية) عام ١٩٨٦, على اساس انه الأنسب لتحديد الدرجة المناسبة للأعمال التي تصل الى حد إستخدام القوة والهجمات المسلحة [٥], وبالقياس على الهجمات السيبرانية أتفق فريق الخبراء (دليل تالين ٢), على ان قيام دولة بتزويد قوات أفراد بأجهزة وتدريبهم لشن هجمات سيبرانية ضد دولة أخرى يعد إستخدام غير مشروع للقوة [٦].

ووفقاً لفريق الخبراء الدوليين تُعرف الحرب السيبرانية بالإستناد الى لقانون الدولي الإنساني بأنها (إستخدام وسائل واساليب القتال التي تتألف من عمليات في الفضاء السيبراني وترتقي الى مستوى النزاع المسلح أو تجري في سياقه), وتشمل وسائل الحرب السيبرانية الاسلحة السيبرانية والأنظمة الإلكترونية المرتبطة بها, كما تشمل أساليب الحرب السيبرانية التكتيكات والتقنيات والأجراءات الإلكترونية التي يتم من خلالها تنفيذ الأعمال العدائية [٧], وطُبق هذا المعنى بصورة واضحة في الهجمات السيبرانية في الحرب بين جورجيا وروسيا عام ٢٠٠٨, وفي الهجمة السيبرانية العالمية التي طالت أكثر من (٦٠) دولة على مستوى العالم عام ٢٠١٧, وأدى ذلك الى ظهور الفضاء السيبراني على الساحة الدولية على نحو مباشر وعلني في النزاعات الدولية, وكأداة ووسيلة في النزاع المسلح, لذلك ثار الجدل حول مدى إعتبار تلك الهجمات عملاً من أعمال الحرب, إذ تُقارب الهجمات السيبرانية الهجمات التقليدية في النتائج مع أختلاف الوسائل وأستراتيجيات التنفيذ, مما أدى الى خلق حرب مفتوحة, الأمر الذي يمكن ان يكون معها صعوبة في تحديد أطرافها, لذلك تسعى الدول الى تطوير أساليب جديدة في الحروب المستقبلية [٨].

وقد وضع فريق الخبراء الدوليين مجموعة من الصفات التي يجب ان تتسم بها الهجمات السيبرانية حتى ترتقي الى درجة الهجوم المسلح وبالتالي تعطي الدولة المعتدي حق الدفاع الشرعي وتفعيل المادة (٥١) من ميثاق الأمم المتحدة, وهو ما جاء في القاعدة (٧١) من (دليل تالين ٢) التي تنص على انه (يجوز للدولة التي تكون هدفاً لعملية سيبرانية ترتفع الى مستوى هجوم مسلح أن تمارس حقها الأصيل في الدفاع عن النفس, ويعتمد ما إذا كانت العملية السيبرانية تُشكل هجوماً مسلحاً أم لا

([2]) See, Michael N. Schmitt, Tallinn Manual 2.0 On The International Law Applicable to Cyber Operations, Cambridge University Press 2017, Rule 68. P: (329 – 330).

([3]) See, Michael N. Schmitt, Tallinn Manual 2.0, Op. Cit. Rule 69. P: (330 – 338).

([٤]) تنص المادة ٥١ من الميثاق على انه "ليس في هذا الميثاق ما يُضع أو يُنقص الحق الطبيعي للدول، فرادى أو جماعات، في الدفاع عن أنفسهم إذا اعتدت قوة مسلحة على أحد أعضاء" الأمم المتحدة "وذلك إلى أن يتخذ مجلس الأمن التدابير اللازمة لحفظ السلم والأمن الدولي، والتدابير التي اتخذها الأعضاء استعمالاً لحق الدفاع عن النفس تبلَّغ إلى المجلس فوراً، ولا تؤثر تلك التدابير بأي حال فيما للمجلس - بمقتضى سلطته ومسؤولياته المستمرة من أحكام هذا الميثاق - من الحق في أن يتخذ في أي وقت ما يرى ضرورة لاتخاذه من الأعمال لحفظ السلم والأمن الدولي أو إعادته إلى نصابه".

([5]) See, Case Concerning Military and Paramilitary Activities in and Against Nicaragua, (Nicaragua v. United States of America), Merits, ICJ, Reports of Judgments. Advisory Opinions and Orders, Judgment of 27 June 1986. Para 191.

([6]) See, Michael N. Schmitt, Tallinn Manual 2.0, Op. Cit. Rule 69. Para 9, Rule 71. Para 3.

([7]) See, Michael N. Schmitt, Tallinn Manual 2.0, Op. Cit. Rule 103. P: 452.

([8]) See, Tim Jordan, Cyberpower: The culture and politics of cyberspace and the Internet, 1999, P: (160 – 169).

على حجمها وتأثيراتها) [٩], وأعتبر الفريق الدولي ان أهم المعايير التي يجب الأستناد إليها في تحديد المستوى المطلوب لوصول العمليات السيبرانية الى درجة الهجوم المسلح يتمثل في جسامة هذا التصرف أو حدته ومدى تأثيره على الدولة المعتدى عليها, وأن يكون هناك ضرراً مادياً حالاً على الأفراد والممتلكات في الدولة المعتدى عليها بهجوم سيبراني, وفي سبيل ذلك قام الفريق الدولي بالمقارنة بين أثر الهجمات العسكرية التقليدية والهجمات السيبرانية أستناداً الى قياس نتائج الأخيرة, وفيما إذا كانت منتجة لأضرار مماثلة للهجمات العسكرية التقليدية أم لا [١٠].

ان الهجمات السيبرانية يمكن ان تنتج مثل هذا الضرر المماثل للهجمات العسكرية التقليدية أو يفوقه كما لو حدث أعتداءً سيبرانياً على شبكات الحاسوب الخاصة بمطار إحدى الدولة مما أدى الى مقتل المئات من الأشخاص بسبب الخلل الذي أحدثته الهجمة السيبرانية وأدى الى تصادم الطائرات, ففي مثل هذه الحالة تعتبر العملية السيبرانية هجوماً عسكرياً [١١], أما تلك الصفات التي لا تلحق مثل هذا النوع من الضرر فتخرج حسب رأي الفريق الدولي من دائرة الهجوم العسكرية, إلا في الحالة التي تضر فيها هذه العمليات السيبرانية بمصلحة وطنية حساسة للدولة المعتدى عليها دون ان تتصل بضرر مادي محسوس, وقد قام الفريق الدولي بإخراج مجموعة من العمليات السيبرانية من دائرة كونها تُشكل هجوماً مسلحاً كتلك المؤدية الى نشوء "حالة من الأنزعاج" في الدولة المتضررة, دون ان تقترن تلك المجموعة بضرر في مصلحة أساسية من مصالح الدولة, فهذه الحالة التي خلفها الإعتداء على الدولة لا ترتقي الى كونها هجوماً مسلحاً تستدعي تطبيق المادة (٥١) من الميثاق, إلا ان العملية السيبرانية المؤثرة مباشرةً على حركة الطائرات, فأنها تُضيف الى أنزعاج الدولة المعتدى عليها ضرراً بمصلحة أساسية للدولة, ومن ثم, تُشكل هجوماً عسكرياً يُبيح اللجوء الى الدفاع عن النفس [١٢].

ان الضرر المادي على الأفراد والممتلكات والذي أعتبره فريق الخبراء الدولي محققاً لمعيار الجسامة, جاء متوافقا مع موقف محكمة العدل الدولية في قضية الأنشطة العسكرية وشبه العسكرية, عندما فرق بين الأعمال الأكثر خطورة والأقل خطورة, إذ قرر الفريق الدولي في هذا الشأن بأن الاضرار غير الجسيمة على الافراد أو الممتلكات لا تُشكل هجمة عسكرية وهو ما عبرت عنه المحكمة بمصطلح (الأعمال الأقل خطورة), مثل المناوشات الحدودية إذ لا يمكن ان تعتبر شكلاً من أشكال استخدام القوة, ومع ذلك تبقى هناك حاجة قائمة لوضع معيار لتحديد ما يُعتبر جسيماً وما يُعتبر أقل جسامةً [١٣].

يلاحظ ان شرط وقوع الضرر من بين الشروط الجوهرية للهجمات السيبرانية والذي أعتدّ به الفريق الدولي لكي ترتقي العملية السيبرانية الى مستوى الهجوم المسلح, وهو شرط متباين عن فكرة المسؤولية الدولية للدول والتي تُبنى على خرق الإلتزم بغض النظر عما إذا كان هذا الخرق مصاحباً للضر أم لا [١٤], ويتحقق هذا الشرط في حالتين, الأولى عندما يقع الضرر فعلاً على الدولة المعتدى عليها, والحالة الثانية, عندما لا يكون الضرر قد وقع فعلاً وإنما هو ضرر وشيك الوقوع, وهو بحسب رأي الفرق الدولي منتج للحق في الدفاع عن النفس, وقد استند الفريق الدولي في هذا الإطار الى معيار (الفترة الزمنية الكافية) التي يمكن ان تستغلها الدولة المعتدى عليها لتجنب وقوع الضرر من خلال تواصلها بدولة مصدر الإعتداء للتراجع عن هذا التصرف, فلا يمكن للتصرف وفقاً لهذا المعيار ان يرقى الى كونه إستخداماً للقوة إذا أثبت ان الدولة المعتدى عليها في هذا الهجوم قد فرطت بإي نافذه زمنية كان بالإمكان إستغلالها لدرء الضرر عنها, وبمعنى أخر ان الخطر الأني أو الحال هو الذي سوف يقع دون أي قدرة للدولة المعتدى عليها ولا بأي طريقة لدرءه [١٥].

ان أهم الفروقات بين الهجمات التقليدية والهجمات السيبرانية ان الهجوم يجب ان يكون ذا أثر مباشر, وان نتائج الأخيرة قد لا تكون واضحة, بمعنى عدم تحديد العلاقة السببية بين الفعل والضرر, وذلك نتيجة لما يطلق عليه الأنفصال الزمني بين التصرف الاساسي الذي يعد مخالفة والنتائج التي يمكن ان يرتبها هذا التصرف, وهذه صفه ملازمة للهجمات السيبرانية [١٦],

---

([9]) See, Michael N. Schmitt, Tallinn Manual 2.0, Op. Cit. Rule 71. P: 339.

([10]) See, Stephen Herzog, Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses, Journal of Strategic Security, Volume. 4. No. 2, Summer 2011. P: (54 – 55).

([١١]) يُنظر, د. أميرة عبد العظيم محمد عبد الجواد, المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام, مجلة الشريعة والقانون, العدد الخامس والثلاثون, الجزء الثالث, ٢٠٢٠, ص ٥٠٦.

([١٢]) يُنظر, رزق أحمد سمودي, حق الدفاع عن النفس نتيجة الهجمات الإلكترونية في ضوء قواعد القانون الدولي العام, مجلة جامعة الشارقة للعلوم القانونية, المجلد ١٥, العدد ٢, كانون الأول ٢٠١٨, ص (٣٥١ – ٣٥٢).

([13]) See, Case Concerning Military and Paramilitary Activities in and Against Nicaragua, (Nicaragua v. United States of America), Op. Cit. Para 191.

([١٤]) يُنظر, حولية لجنة القانون الدولي, المجلد الثاني, الجزء الثاني, ٢٠٠١, مشروع المسؤولية الدولية للدول عن الأفعال غير المشوعة دولياً, المادة (٢)

([15]) See, Daniel Bethlehem, Principles Relevent to the Scope of Self-Defence Against Imminent or Actual Armed Attack by Nonstate Actors, American Journal of International Law, Vol. 106, Iss. 4, 2012. P: (770 – 777).

([16]) See, Haitao Du and Shanchieh Jay Yang, Temporal and Spatial Analyses for Large-Scale Cyber Attacks, Handbook of Computational Approaches to Counterterrorism, November 2013, P: (559 – 578).

على سبيل المثال لو ان عمليات سيبرانية وجهّت الى سوق الأوراق المالية في دولةٍ ما وأثر بشكل سلبي وببطء شديد في إداء الأسواق بشكل عام وبالتالي ترتب علية إنكماش أقتصادي في تلك الدولة , ففي هذه الحالة يمكن لهذه العمليات السيبرانية ان تقرأ في شقيت, الأول, ان الأنكماش الإقتصادي كان نتيجة مباشرة للعملية السيبرانية, إلا ان هذا الأنكماش ظهرة بعد فترة من الزمن, اما الشق الثاني, فأن إقتصاد تلك الدولة كان ضعيفاً والعملية السيبرانية لم تكن هي السبب الجوهري وراء هذا الأنكماش وإنما كانت العملية كاشفة له, ومن ثم, لا توجد علاقة مباشرة بين التصرف والنتيجة [١٧].

أما بالنسبة لدليل تالين فإستناداً الى شرط (الإتصال المباشر) الوراد فيه فأن هذا الشق الأخير لا يمكن ان يرتقي بالتصرف الى درجة الهجوم المسلح استناداً اللى عدم القدرة على تحديد العلاقة السببية بين التصرف والضرر, لذلك يجب عدم الخلط بين الأنية والمباشرة كشرطين متميزين جاء بهما الدليل, إذ يتمثل الأول في ظهور الضرر الى حيز الوجود, والثاني يرتبك بالتصرف والضرر [١٨], بالأضافة الى ذلك جاء دليل تالين متضمناً شرط العدائية والذي يتمثل في النية خلف العملية السيبرانية, فبحسب هذا الشرط ترتقي العملية السيبرانية الى درجة الهجوم المسلح كلما كانت الدولة المعتدى عليها قادرة على إثبات ان هذا التصرف يسعى الى تحقيق أهداف عدائية في الدول الأخرى كإضعاف القدرة العسكرية من خلال التأثير على برامجها السيبرانية العسكرية [١٩].

ان شرط أتصال التصرف بالدولة يعد من أهم وأبرز الشروط لنهوض المسؤولية الدولية عموماً, حيث يتضمن هذا الشرط ضرورة ان يكون التصرف صادراً عن من يُمثل الدولة, سواء السلطة التشريعية أو التنفيذية أو القضائية أو اي جهة أخرى يعهد إليها مهمة القيام بعمل معين بالنيابة عن الدولة [٢٠], إذ يُثير هذا الشرط أمرين:

- يتمثل في صعوبة تحديد ما أذا كان هذا العمل منسوباً للدولة فعلاً وهذا مرتبط بالقدرة التكنولوجية المتنامية والتي يمكن ان تمكن الدولة مصدرة التصرف ان تُخفي هوية الفاعل الحقيقي, أضافة الى ذلك فأن عملية نسبة العمل الدولية تزداد تعقيداً في الحالة التي لا تكون الشبكات السيبرانية هي الوسط الذي تمت من خلاله هذه الهجمات, كإرسال فيروسات توضع مباشرةً في أجهزة الحاسوب الخاصةبالدول المستهدفة, أو في الحالة التي يُستخدم فيها إفليم دولة أخرى لتنفيذ هذه الهجمات, على سبيل المثال, قيام الدولة (أ) بإستخدام البُنية التحتية السيبرانية للدولة (ب) للقيام بتنفيذ هجمة سيبرانية عن طريق وكلاء لها تستهدف الدولة (ج).
- يتمثل في الحالة التي يُنسب فيها التصرف الى جهات فاعلة من غير الدول, ولكن هذه المجموعة إستخدمت إقليم الدولة لتنفيذ العملية السيبرانية الضارة, حيث أثارت هذه الحالة نقاشاً مستفيضاً بين فريق الخبراء الدوليين (لدليل تالين٢), إذ أقر الفريق الدولي بشكل ضمني في الفقرة الثانية من القاعدة (٧١), ان التحكم الفعّال هو فقط ما ينهض بالمسؤولية في مواجهةالدولة مصدرة الإعتداء, وهو موقف متوافق مع قرار محكمة العدل الدولية في قضية الأنشطة العسكرية وشبة العسكرية [٢١].

أضافة الى الشروط السابقة, قام الفريق الدولي بوضع شروط أخرى تتمثل في وضوح نتائج الهجمات أو القدرة على قياسها, بمعنى قدرة الدولة المعتدى عليها في تحديد الضرر الذي تسببت به الهجمة السيبرانية, أضافة الى شرط الطابع العسكري للعملية السيبرانية وهو شرط مستمد من مجمل مواد ميثاق الأمم المتحدة الخاصة بإستخدام القوة والتي تربط بين إستخدام القوة وبين الطبيعة العسكرية لهذه النشاطات [٢٢].

٣. إعلان إيريتشي بشأن مبادئ الأستقرار والسلام السيبراني الصادر عن الأتحاد العالمي للعلماء

أعد إعلان إريتشي بشأن مبادئ الاستقرار السيبراني والسلام السيبراني بواسطة فريق الرصد الدائم المعني بأمن المعلومات التابع للأتحاد العالمي للعلماء (WFS) [٢٣], حيث أعتمدته الجلسة العامة للأتحاد العالمي للعلماء في الدورة الثانية والأربعون

---

(١٧) يُنظر, رزق أحمد سمودي, حق الدفاع عن النفس نتيجة الهجمات الإلكترونية في ضوء قواعد القانون الدولي العام, المرجع السابق, ص ٣٥٤.

(١٨) يُنظر, د. أميرة عبد العظيم محمد عبد الجواد, المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام, المرجع السابق, ص ٥٠٩.

(١٩) يُنظر, رزق أحمد سمودي, حق الدفاع عن النفس نتيجة الهجمات الإلكترونية في ضوء قواعد القانون الدولي العام, المرجع السابق, ص ٣٥٥.

(٢٠) وهو ما أقرته المادة (٤), من مشروع مواد المسؤولية الدولية للدولة, عن الأفعال غير المشروعة. يُنظر, حولية لجنة القانون الدولي, المجلد الثاني, الجزء الثاني, ٢٠٠١, المرجع السابق, ص ٥٠.

(21) See, Case Concerning Military and Paramilitary Activities in and Against Nicaragua, (Nicaragua v. United States of America), Op. Cit. Para 115.

(٢٢) يُنظر, رزق أحمد سمودي, حق الدفاع عن النفس نتيجة الهجمات الإلكترونية في ضوء قواعد القانون الدولي العام, المرجع السابق, ص ٣٥٧.

(٢٣) في عام ١٩٧٣ قامت مجموعة من العلماء البارزين بإنشاء الاتحاد العالمي للعلماء في إيرتشه بجزيرة صقلية .ومنذ ذلك الحين انضم كثير من العلماء الأخرين إلى الاتحاد، والاتحاد تجمع حر آخذ ينمو حتى أصبح يضم أكثر من ١٠٠٠ عالم من ١١٠ دولة, ويتقاسم جميع الأعضاء نفس الأهداف والمثل العليا ويساهمون طواعية في الدفاع عن مبادئ الاتحاد .ويُشجع الاتحاد على التعاون الدولي في العلم والتكنولوجيا بين العلماء والباحثين من كل أنحاء العالم . ويسعى الاتحاد وأعضاؤه إلى تحقيق حرية تبادل المعلومات كهدف مثالي، بحيث لا تكون الاكتشافات والتقدمات العلمية قاصرة على قلة مختارة .والهدف هو تقاسم هذه المعارف بين شعوب كل الدول ليتمتع كل شخص بفوائد تقدم العلم, وكان إنشاء الاتحاد العالمي للعلماء ممكناً بفضل وجود مركز للثقافة العلمية أُقيم في إريتشه لتخليد ذكرى عالم الفيزياء إيتوري مايورانا باسم "مؤسسة إيتوري مايورانا ومركز الثقافة العلمية (المركز) وأصبح، هذا المركز الذي أُطلقت عليه تسمية "جامعة الألفية الثالثة" قوة تعليمية

للحلقات الدراسية الدولية بشأن الطورائ العالمية في إريتشي (صقلية) في ٢٠ أب ٢٠٠٩, وكان من أبرز التقارير لهذا الأتحاد التقرير المعنون بـ (نحو نظام عالمي للفضاء السيبراني, إدارة التهديدات من الجريمة السيبرانية الى الحرب السيبرانية), والذي يعد إحدى الوثائق الرئيسية التي قدمها المجتمع المدني الى القمة العالمية لمجتمع المعلومات والتي عقدتها الأمم المتحدة في جنيف عام ٢٠٠٣ [٢٤].

وقد نشر فريق الرصد عدة أوراق بشأن الأمن السيبراني والحرب السيبرانية, ويتناول بإنتظام قضايا أمن المعلومات بإعتبارها موضوعاً من موضوعات الطورائ الحرجة أثناء الدورات العامة للأتحاد العالمي للعلماء والتي تنعقد في شهر أب من كل عام في إريتشي, وقد أعرب الفريق في عام ٢٠٠٩, عن قلقه من أمكانية وقوع حرب سيبرانية تُعطل المجتمع الدولي وتُسيب ضرراً ومعاناة لا لزوم لها, لذلك عمد الى صياغة **إعلان إيرتشي لمبادئ الاستقرار السيبراني والسلام السيبراني,** والذي اعتمدته في الجلسة العامة للإتحاد في نفس العام وتم توزيع هذا الأعلان على كل الدول الأعضاء في الأمم المتحدة [٢٥].

يبين هذا الأعلان ان تحقيق الأستقرار السيبراني والسلام السيبراني أمران متداخلان تداخلاً وثيقاً ويتسم الإعلان بالإيجاز ويركز على العناصر التشغيلية الأساسية للسلام السيبراني وهي [٢٦]:

- ينبغي لجميع الحكومات الاعتراف بأن القانون الدولي يضمن للأفراد التدفق الحر للمعلومات والأفكار؛ وتنطبق هذه الضمانات أيضاً على الفضاء السيبراني .وينبغي عدم فرض القيود إلا عند الاقتضاء، على أن تخضع لعمليةمراجعة قانونية.
- ينبغي لجميع البلدان العمل معاً لوضع مدونة مشتركة للسلوك السيبراني وإطار قانوني عالمي منسق، بما في ذلك أحكام إجرائية تتعلق بالمساعدة في التحقيق والتعاون بما يكفل احترام الخصوصية وحقوق الإنسان, وينبغي لجميع الحكومات وموزودي الخدمات والمستعملين دعم الجهود المبذولة في سبيل إنفاذ القانون الدولي ضد مرتكبي الجرائم السيبرانية.
- ينبغي لجميع المستعملين وموزودي الخدمات والحكومات العمل معاً لضمان ألا يستخدم الفضاء السيبراني بأي شكل من شأنه أن يفضي الى استغلال المستعملين، لا سيما الشباب والمستضعفين منهم، من خلال العنف أو الإذلال.
- ينبغي للحكومات والمنظمات والقطاع الخاص بما في ذلك الأفراد، تنفيذ برامج شاملة للأمن وتحديثها بناءً على أفضل الممارسات والمعايير المقبولة دولياً واستعمال تكنولوجيات حماية الخصوصية والأمن.
- ينبغي لمطوري البرمجيات والمعدات السعي الى تطوير تكنولوجيات آمنة تعزز القدرة على التصدي وتقاوم نقاط الضعف.
- ينبغي للحكومات أن تشارك بفعالية في جهود الأمم المتحدة الرامية الى النهوض بالأمن السيبراني والسلام السيبراني في العالم وأن تتفادى استعمال الفضاء السيبراني من أجل النزاعات.

يمكن أن نستشف من وراء هذه المبادئ، ولا سيما المبدأ السادس، الإرادة الصارمة من أجل كبح إمكانية النزاعات في الفضاء السيبراني .وفي الواقع لا بد، في إطار السعي إلى السلام السيبراني، وفي ضوء الزيادة المهولة لقدرات "الحرب السيبرانية" العدوانية، من التركيز بشكل خاص على الجانب الحربي للأنشطة في الفضاء السيبراني التي تقوم بها الحكومات وجهات فاعلة غير حكومية على حد سواء, وقد دعا الاتحاد العالمي للعلماء منذ سنة ٢٠٠٢ إلى العمل من أجل وضع قانون عالمي للفضاء السيبراني, وأنه من الأفضل أن يكون تحت رعاية الأمم المتحدة [٢٧], فضلا عن ضرورة وجود إطار قانوني لتعريف ما الذي يشكل خرقاً للسلام، وقد اقترح الأمين العام للاتحاد الدولي للاتصالات، في مفهومه الذي ينطلق من المبادئ الخمسة للاتحاد، أنه ينبغي للأمم أن تتعهد في هذا الإطار بألا تبدأ بالعدوان السيبراني ضد أمة أخرى [٢٨].

٤. الخاتمة

لا شك أن التطور السريع في تكنولوجيا الحاسوب، دفع المجتمع الدولي للدخول في مرحلة جديدة أصبح فيها للأمن السيبراني دوراً أساسيw سواء في الإستحواذ على عناصره الأساسية أو في تعظيم القوة، لظهور محددات جديدة لهذه القوة

عالمية, وقام هذا المركز منذ إنشائه في عام ١٩٦٣ بتنظيم ٤٨٤ مشاركاً منهم (١٢٥ من ١٢٣ مدرسة و ١٤٩٧ دورة دراسية حضرها ١٠٣ الحاصلين على جائزة نوبل) من ٩٣٢ جامعة ومختبراً في ١٤٠ دولة.

([٢٤]) يُنظر, د. أميرة عبد العظيم محمد عبد الجواد, المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام, المرجع السابق, ص (٥١٢ – ٥١٣).

([٢٥]) يُنظر, حمدون أ. توريه, السلام السيبراني, الأتحاد العالمي للعلماء, كانون الثاني ٢٠١١.

([26]) See, World Federation of Scientists - Erice Declaration on Principles for Cyber Stability and Cyber Peace, 2009. P: (1 – 2)

([27]) See, Toward a Universal Order of Cyberspace: Managing Threats from Cybercrime to Cyberwar, Report & Recommendations, World Federation of Scientists, August 2003, P: 07.

([٢٨]) يُنظر, د. أميرة عبد العظيم محمد عبد الجواد, المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام, المرجع السابق. ص (٥١ – ٥١٧).

سواء من حيث طبيعتها أو أنماط استخدامها أو طبيعة الفاعلين فيها، وانعكاس ذلك على قدرات الدول وعلاقاتها الخارجية مما جعل هذه البيئة السيبرانية حقيقة غير مسبوقة، واتجهت الدول إلى الحفاظ على أمنها القومي لمواجهة ما يعرف بصراع "عصر المعلومات".

وقد انتهينا إلى جملة من الأستنتاجات والتوصيات تتمثل في:

٤-١- الأستنتاجات

أن الفضاء السيبراني قد فرض على الدول والعديد من المنظمات الدولية إعادة التفكير في مفهوم الأمن الدولي، والذي يتعلق بتلك الدرجة التي تتمكن الدول من أن تصبح في مأمن من المخاطر التي تتعرض لها سواء في سلامة أراضيها أو استقلالها السياسي أو حماية البنى التحتية لمنشأتها الحيوية ومن كافة أوجه الاستخدام غير المشروع لتكنولوجيا الاتصال والمعلومات, وأن من أهم الإشكاليات التي تواجه المجتمع الدولي هو ما يتعلق بالجدل حول مدى اعتبار الأسلحة السيبرانية كالأسلحة غير التقليدية من إمكانية إخضاعها لقيود الاتفاقيات الدولية، وممارسة حق الدفاع الشرعي وفق المادة (٥١) من الميثاق سواء عبر ممارسات فردية أو جماعية.

أن فقه القانون الدو متمثل في فريق الخبراء القائمين على دليل تالين، والاتحاد العالمي للعلماء يدعم اعتبار الأسلحة السيبرانية كالأسلحة غير التقليدية بمحددات معينة، وذلك استنادا إلى آراء محكمة العدل الدولية والتي كانت مهيأة في العديد من القضايا التي عرضت أمامها كما في قضية "النشاطات العسكرية وشبه العسكرية في نيكاراجوا" ١٩٨٦, إلى ضم فئات أخرى غير الهجوم المادي لكي يعطي الحق للدولة التي تتعرض إلى هجوم الارتكاز إلى المادة ٥١ والدفاع عن نفسها ولكن ضمن شروط أبرزها الحجم والتأثير.

أن محكمة العدل الدولية قد ركزت على نتائج الهجوم أكثر من تركيزها على الوسائل المستخدمة في تنفيذ الهجوم مما يفيد أن المحكمة مهيأة لإدخال الهجمات السيبرانية ضمن فئة الهجمات التقليدية لما لها من حجم وتثير في الدول محل الهجوم السيبراني.

بالرغم من ذلك تبقى مسألة المقارنة بين الهجوم المسلح المادي والهجوم السيبراني غير عملية وذلك بسبب الفوارق الجوهرية بين هاتين الفئتين من الهجمات وعدم إمكانية إسقاط بعض الشروط الواجب توافرها من أجل تفعيل المادة ٥١ على الهجمات السيبرانية, على وجه التحديد فإنه من الصعوبة بمكان إسقاط شروط الضرورة والسرعة والفورية في رد الهجوم لكي تقوم الدولة المعتدى عليها باتخاذ إجراءات الدفاع عن النفس , وذلك بسبب الصعوبة التي تصاحب عملية تحديد الجهة مصدر الهجوم إلا بعد مدة زمنية طويلة والتي يمكن عندها أن ينتفي المنطق من إعطاء الدولة الحق في الدفاع عن نفسها دون اللجوء إلى مجلس الأمن صاحب السلطة الأساسية في حفظ الأمن والسلم الدوليين.

ومن ثم, لابد من تضافر وتكاتف الجهود لإبرام اتفاقيات دولية تكون مهمتها الأساسية مواجهة المخاطر السيبرانية واحتوائها ومحاولة التخفيف منها.

٤-٢- التوصيات

- ضرورة العمل على وضع قواعد دولية موحدة تحكم حالات الحرب والنزاع في الفضاء السيبراني، وإدخال العدوان السيبراني ضمن صور العدوان من أجل دعم الاستخدام السلمي للفضاء السيبراني، ووضع الأمن السيبراني ضمن استراتيجيات الأمن القومي للدول من أجل تحقيق السلم والأمن الدوليين.
- وضع أطر قانونية لحماية حقوق الإنسان الرقمية وعدم المساس بها وجعل الأمن السيبراني الجماعي أحد أشكال الأمن الجماعي الإنساني الجديد.
- وضع استراتيجيات لتطوير نموذج التشريعات السيبرانية يكون قابلاً للتطبيق محلياً وعالمياً بالتوازي مع التدابير القانونية الوطنية والدولية المعتمدة.
- وضع استراتيجية لتحديد الحد الأدنى المقبول عالمياً في موضوع معايير الأمن ونظم تطبيقات البرامج والأنظمة.
- تقديم المشورة بشأن إمكانية اعتماد إطار استراتيجي عالمي لأصحاب المصلحة من أجل التعاون الدولي والحوار والتعاون والتنسيق في جميع المجالات.
- توظيف الخبراء وتدريبهم لمواكبة أحدث التطورات التكنولوجية وفهمها وتطوير القوانين الوطنية وفق ذلك.
- تكاتف الجهود الداخلية والدولية لإنشاء منظمات دولية وإقليمية، وإبرام اتفاقيات ثنائية وجماعية وتكون متخصصة مهمتها الأساسية التنسيق بشأن مواجهة الجرائم السيبرانية واحتوائها ومحاولة التخفيف منها.
- تبادل الخبرات بين الدول كافة، وخاصة التي لها خبرات واسعة في هذا مجال مكافحة المخاطر السيبرانية.

٥. المصادر

٥-١- المصادر العربية

١. رزق أحمد سمودي, حق الدفاع عن النفس نتيجة الهجمات الإلكترونية في ضوء قواعد القانون الدولي العام, مجلة جامعة الشارقة للعلوم القانونية, المجلد ١٥, العدد ٢, كانون الأول ٢٠١٨
٢. د. أميرة عبد العظيم محمد عبد الجواد, المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام, مجلة الشريعة والقانون, العدد الخامس والثلاثون, الجزء الثالث, ٢٠٢٠
٣. حولية لجنة القانون الدولي, المجلد الثاني, الجزء الثاني ٢٠٠١.
٤. حمدون أ. توريه, السلام السيبراني, الأتحاد العالمي للعلماء, كانون الثاني ٢٠١١.

٥-٢- المصادر الأجنبية

1. Case Concerning Military and Paramilitary Activities in and Against Nicaragua, (Nicaragua v. United States of America), Merits, ICJ, Reports of Judgments. Advisory Opinions and Orders, Judgment of 27 June 1986.
2. Daniel Bethlehem, Principles Relevent to the Scope of Self-Defence Against Imminent or Actual Armed Attack by Nonstate Actors, American Journal of International Law, Vol. 106, Iss. 4, 2012.
3. Eric Talbot Jensen, "The Tallinn Manual 2.0: Highlights and Insights", Research Paper, No. 17, Georgetown Journal of International Law, 2017.
4. Haitao Du and Shanchieh Jay Yang, Temporal and Spatial Analyses for Large-Scale Cyber Attacks, Handbook of Computational Approaches to Counterterrorism, November 2013.
5. Michael N. Schmitt, Tallinn Manual 2.0 On The International Law Applicable to Cyber Operations, Cambridge University Press 2017.
6. Priyanka R. Dev, " Use of Force" and "Armed Attack" Thresholds in Cyber Conflict: The Looming Definitional Gaps and the Growing Need for Formal U.N. Response", Texas International Law Journal, Vol. 50, Issue 2, 2015.
7. Stephen Herzog, Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses, Journal of Strategic Security, Volume. 4. No. 2, Summer 2011.
8. Toward a Universal Order of Cyberspace: Managing Threats from Cybercrime to Cyberwar, Report & Recommendations, World Federation of Scientists, August 2003.
9. World Federation of Scientists - Erice Declaration on Principles for Cyber Stability and Cyber Peace, 2009.