الانتهاكات السيبرانية للقانون الدولي
وتحديات مواجهته

دكتور
أحمد حسن فولي
أستاذ القانون الدولي العام المشارك
كلية القانون – جامعة المدينة عجمان
2023

المقدمة:

مع نهايات القرن العشرين تغير شكل التواصل بين البشر عما كان علية من قبل، وكانت البداية بقرار اتخذته الولايات المتحدة الأمريكية بشأن شبكة الاتصالات التي أنشأتها بين أجهزة الكمبيوتر للأغراض العسكرية، والمعروفة وقتها باسم (الأربنت Arpanet)، حيث قررت القيادة الأمريكية إتاحة هذه الشبكة للتواصل وتبادل المعرفة وانتقال المعلومات بين البشر على المستوى العالمي، وعرفت الشبكة باسم (الانترنت Internet)، وبعدها عملت الشركات المتخصصة على إنشاء النظم الإلكترونية التي تتيح لكافة الاشخاص والمؤسسات في العالم إنشاء صناديق بريد إلكترونية لتبادل الرسائل وإنشاء المواقع الإلكترونية وتخزين المعلومات وإتاحتها للجماهير.[1]

ومع ظهور الانترنت وقدرة البشر على تخزين البيانات في أجهزة الكمبيوتر شهد العالم ثورة حقيقية في مجال تكنولوجيا المعلومات، ثورة بكل ما تحمله الكلمة من معان في مختلف المجالات الاقتصادية والإدارية والثقافية والاجتماعية، وأصبحت إدارة أي عمل أكثر سهولة ويسراً في ظل القدرة الفائقة لأجهزة الكمبيوتر على تخزين المعلومات وتنظيمها بما يتيح سهولة استرجاعها ومعالجتها وتبادلها عبر الاتصال بالأنترنت.

وكلما ازداد كم المعلومات تزداد الحاجة لاستخدام الوسائل التكنولوجية لتخزينها ومعالجتها، ولا مبالغة في القول بأن تقدم الدول أصبح يقاس بقدرتها على التعامل الإلكتروني مع كافة شئونها الداخلية، فمستوى الخدمات الصحية والتعليمية والمصرفية وغيرها من الخدمات الحكومية يرتقي بقدر قدرة الدولة على تدريب مؤسساتها على التعامل الإلكتروني ونشر ثقافته بين المنتفعين بهذه الخدمات.

ومع ظهور الفضاء الإلكتروني الذي خزن فيه البشر هذا الكم الهائل من المعلومات، إلى أن أصبح بمثابة خزانة معلومات الأرض بمن عليها من دول وشركات وأشخاص، ومع استخدام الفضاء الالكتروني كوسيله جديده للاتصال على المستوى الدولي والداخلي، ظهر مجال جديد للعلاقات الدولية، أطلق علية المجال الخامس استنادا لوجود أربع مجالات تقليدية لهذه العلاقات وهي المجال البري والبحري والجوي والفضاء الخارجي.

وكما شهدت المجالات التقليدية للعلاقات الدولية صراع محموم بين الدول على مدار تاريخها، امتد الصراع الدولي إلى مجال الفضاء الإلكتروني، حيث سعت الدول إلى فك شفراته للحصول على المعلومات الخاصة بالدول الأخرى أو إتلافها أو التحكم فيها وإدارتها بالشكل الذي يحقق مصالحها الاستراتيجية ويضر بمصالح الدولة المخزنة لهذه المعلومات.

وإن كان النطاق التقليدي للعلاقات الدولية بما يحتويه من ارض وبحر وجو وفضاء خارجي يتسم بطابع مكاني محدد والتصرفات فيه تكون ذات طبيعة حركية يمكن رصدها، فإن الطبيعة الافتراضية للفضاء السيبراني عكست تحديات حقيقية أمام وضع الإطار القانوني الدولي الضابط لمشروعية التصرفات السيبرانية للدول.

---

[1]) د. محمد المجذوب، الوسيط في القانون الدولي العام، الطبعة السابعة، ٢٠١٨، منشورات الحلبي الحقوقية، ص 814

ورغم الاختلاف الشاسع بين التصرفات الحركية والسيبرانية، تسعى المنظمات الدولية مؤيده بجانب من الفقه الدولي إلى محاولة شمول التصرفات السيبرانية للدول بقواعد وأحكام القانون الدولي الموضوعة لتحديد مدى مشروعية تصرفاتها الحركية.

والدافع لهذا التوجه هو إدراك مدى صعوبة وضع قواعد دولية جديدة لتحديد مشروعية التصرفات السيبرانية للدول، لما يكتنف ذلك من تحديات تتمثل في الطبيعة الخاصة لهذا الفضاء الجديد، وأيضاً عدم رغبة الدول في توقيع اتفاقات تحد من حرية تصرفاتها فيه.

إشكالية البحث

تتمثل إشكالية البحث في صعوبة تطبيق قواعد القانون الدولي التي وضعت لضبط تصرفات الدول ذات الطبيعة الحركية على التصرفات التي تقوم بها الدول في الفضاء السيبراني والمعروفة باسم التصرفات السيبرانية، وصعوبة تحديد الجهات التي تنتهك قواعد القانون الدولي في الفضاء السيبراني نظراً لطبيعته الخاصة.

هدف البحث

إبراز مفهوم الانتهاكات السيبرانية للقانون الدولي، والتعرف على صورها، وإلقاء الضوء على الجهود الدولية التي بذلت لمواجهتها، والتحديات التي تعرقل مكافحة تلك الانتهاكات، وتسارع سباق التسلح السيبراني، وتحديد العقبات التي تواجه تطبيق القانون الدولي الإنساني في الفضاء السيبراني، والعقبات التي تواجه إعمال قواعد المسؤولية الدولية في هذا الفضاء.

تساؤلات البحث

- ما هي صور الانتهاكات السيبرانية للقانون الدولي؟
- ما مدى فاعلية الجهود الدولية المبذولة لمواجهة الانتهاكات السيبرانية للقانون الدولي؟
- ما هي ملامح سباق التسلح السيبراني؟
- هل يمثل الردع السيبراني وسيلة ناجعة لحماية الأمن السيبراني للدول؟
- ما هي التحديات التي تواجه تطبيق القانون الدولي الإنساني في الفضاء السيبراني؟
- ما هي التحديات التي تواجه إعمال قواعد المسؤولية الدولية لمحاسبة الدول التي ترتكب الانتهاكات السيبرانية للقانون الدولي؟

منهجية البحث

استخدم الباحث المنهج التحليلي الاستنباطي وذلك بتحليل المبادئ والقواعد العامة للقانون الدولي، بما في ذلك مبدأ السيادة، ومبدأ عدم التدخل في الشؤون الداخلية للدول، والقواعد العامة للمسؤولية الدولية والقواعد المنظمة لاستخدام القوة في العلاقات الدولية، وتعرض البحث لدراسة انتهاكات هذه المبادئ في الفضاء السيبراني، والعقبات التي تواجه فرض احترامها على الدول.

خطة البحث

المبحث الأول: الانتهاكات السيبرانية للقانون الدولي: صورها وتعريفها وجهود مواجهتها.

المطلب الأول: صور الانتهاكات السيبرانية للقانون الدولي.

المطلب الثاني: مفهوم الانتهاكات السيبرانية للقانون الدولي وفاعلية جهود مواجهتها.

المبحث الثاني: التسلح السيبراني وحق الدول في الدفاع عن نفسها ضد الهجمات السيبرانية.

المطلب الأول: التسلح السيبراني للدول وانتشار القوى السيبرانية غير المنظمة.

المطلب الثاني: الردع السيبراني وحق الدول في الدفاع عن نفسها في مواجهة الهجمات السيبرانية.

المبحث الثالث: تحديات مواجهة الانتهاكات السيبرانية للقانون الدولي.

المطلب الأول: تحديات تطبيق قواعد القانون الدولي الإنساني على الانتهاكات السيبرانية.

المطلب الثاني: تحدي إسناد المسؤولية الدولية في الفضاء السيبراني وسبل مواجهته.

المبحث الأول

الانتهاكات السيبرانية للقانون الدولي: صورها وتعريفها وجهود مواجهتها

لم تعد الحرب كما كانت، نزاعات تُستخدم فيها القوة المسلحة المباشرة بشكل صريح، [2] لكنها اصطبغت بألوان عدة، واتخذت صوراً وأشكالاً متباينة، وهو ما يثبت أن الحرب حقاً حرباء تتلون بلون زمانها[3]، ويقف القانون الدولي عاجزاً أمام تطورها وتلونها، فما أسرع تطور أدوات الحرب وآلياتها، وما أبطأ تطور أدوات مكافحتها في القانون الدولي.

رغم تطور أدوات الحرب وآلياتها خلال العقود السبع الماضية، نجد اتفاقيات جينيف وبروتوكولاتها الملحقة ظلت جامده، ولم يطرأ عليها التحديث اللازم لمواجهة أساليب الحروب الحديثة، ولم تُبرم الدول اتفاقات جديدة للحد من مخاطر الحروب المستحدثة التي أصبح جهاز الكمبيوتر فيها موازياً للطائرة الحربية في المخاطر، إن لم تكن بعض الفيروسات التي تطلقها أجهزة الكمبيوتر أكثر تدميراً من بعض أنواع الصواريخ التي تطلقها الطائرات الحربية.

افرزت هذه المعطيات صراعات دولية أخطر ما فيها صعوبة توصيفها، فلا هي بالحرب التي عرفتها المواثيق الدولية، ولا هي بالسلم الذي ينشده القانون الدولي، ومن هذه الصراعات ما عرف بالحرب السيبرانية، [4] ذلك المفهوم الذي اثار الكثير من اللبس والغموض بسبب تداخله مع مفهومي (حرب الشبكات) [5] و (حرب المعلومات) [6]. تلك

---

[2]) الحرب وفقاً للقانون الدولي بمفهومها التقليدي صراع تستخدم فيه القوة المسلحة بين أطرافها، يرمي به كل طرف فيها إلى حماية مصالحه وصيانه حقوقه في مواجهة الأطراف الأخرى، ولوصف الصراعات التي تنشب داخل أي دولة - بين قواتها المسلحة وإقليم ثائر في مواجهة حكومته - بالنزاع المسلح، يشترط القانون الدولي أن يكون القتال منظم وأن يكون للثوار قوات نظامية تشرف عليها سلطة مسؤولة تمارس باسمها أعمال السيادة على الإقليم الذي في حوزتها وتسعى للاستئثار بها في مواجهة الحكومة الأصلية، كما يجب الاعتراف لهؤلاء الثوار بصفة المحاربين، سواء صدر هذا الاعتراف من الحكومة الأصلية أو من حكومات الدول الأجنبية. أنظر د. على صادق أبو هيف، القانون الدولي العام، منشأة المعارف، الإسكندرية، ٦٧٩، بدون تاريخ

[3]) للمزيد من التفصيل عن تطور أجيال الحرب راجع، شادي عبد الوهاب منصور، حروب الجيل الخامس، أساليب "التفجير من الداخل" على الساحة الدولية، الطبعة الأولى، العربي للنشر والتوزيع، القاهرة – مصر، 2019، ص 101

[4]) منزر رابح، درويش سعيد، الطبيعة القانونية للهجمات السيبرانية التي تقع بين الدول، مجلة صوت القانون، المجلد الثامن، 2021، ص ص 542

[5]) حرب الشبكات فهي مصطلح طوره الباحثان الأمريكيان (جون أركيلا) و (ديفيد رونفيلدت) للدلالة على استخدام أحد أطراف الحرب نظام الخلايا البشرية المتناثرة والمترابطة بشكل معقد يصعب فهمه، والتي تجتمع على أفكار أيديولوجية أو عقائدية، ولا تتضح القيادة الهرمية أو المركزية لهذه الشبكات وهو الأسلوب الذي تستخدمه الجماعات الإرهابية في إدارة تنظيمها، ومن أشهر أمثلتها تنظيم القاعدة الذي فرقته القوات الأمريكية في أفغانستان، وتعتمد حرب الشبكات على تقدم تقنية الاتصال الإلكتروني التي اتاحة استخدام الإنترنت والاتصال الإلكتروني في تأمين الاتصال بين عقد الشبكة وبينها وبين العالم الخارجي

John Arquilla and David Ronfeldt, In Athena's Camp: Preparing for Conflict in the Information Age, Santa Monica, RAND, 1997.

[6]) حرب المعلومات هو مصطلح يُستخدم للدلالة على مجموعة موضوعات متنوعة، مما يؤدى لاختلاط المفاهيم، فمن جهة نجد حرب المعلومات تشير إلى استخدم تكنولوجيا المعلومات الحديثة في الحرب، ولهذا يتداخل مفهومها مع حرب الشبكات، وعلى الجانب الأخر يستخدم مفهوم حرب المعلومات للدلالة على المعارك التي تغلب عليها الطبيعة السياسية حيث يتم خلالها التلاعب بالمعلومات لتضليل الرأي العام الوطني والدولي أو لفضح قادة الدولة المستهدفة من الحرب بإعلان الفضائح، ومن جانب ثالث يستخدم

الحروب التي تدور رحاها في الفضاء السيبراني وترتكب خلالها الكثير من الانتهاكات للقانون الدولي، وتأبى الدول الإفصاح عن الاسلحة التي تستخدمها فيها أو ما وصلت إليه من تطور في مجالاتها.

وسأحاول من خلال هذا المبحث إلقاء الضوء على صور الانتهاكات التي ترتكبها الدول في الفضاء السيبراني من خلال مطلب أول، ثم احاول وضع تعريف للانتهاكات السيبرانية للقانون الدولي واستعرض الجهود الدولية المبذولة لمواجهتها بغية الوقوف على مدى فاعليتها.

المطلب الأول

صور الانتهاكات السيبرانية للقانون الدولي

ظهرت خلال السنوات الأخيرة ثلاث صور للانتهاكات السيبرانية للقانون الدولي، الأولى هي الانتهاكات التي ترتكب خلال النزاعات المسلحة، والثانية هي ارتكاب فعل من أفعال العدوان من خلال الفضاء السيبراني والمعروفة باسم "العدوان السيبراني"، أما الصورة الثالثة فهي الهجمات السيبرانية التي لا تُشن في زمن النزاعات المسلحة ولا ترتقي لمستوى الخطورة المطلوب لوصفها بالفعل العدواني.[7]

وغني عن البيان أن هناك صورة أخرى للانتهاكات السيبرانية تتمثل في الجرائم السيبرانية الوطنية، والتي يبتغي مرتكبها تحقيق منفعة مالية شخصية، وهذه الانتهاكات السيبرانية تخضع للقوانين الوطنية، [8] ولن اتعرض لها بالبحث، حيث يقتصر البحث على التصرفات التي تُنسب للدول سواء التي تقوم بها مؤسسات الدولة أو يقوم بها أشخاص أو مؤسسات بتعليمات أو توجيهات من أحد الدول، أي أنها تخضع لقواعد القانون الدولي العام. [9]

أولاً: الهجمات السيبرانية التي تشن في زمن النزاعات المسلحة.

تستخدم الدول الفضاء السيبراني في زمن النزاعات المسلحة، حيث تقوم بتنفيذ هجمات سيبرانية الغرض منها اكتشاف أو تغيير أو تدمير أو تعطيل أو نقل البيانات المخزنة

مصطلح حرب المعلومات كمرادف لمصطلح الحروب السيبرانية وإمكانية توجيه هجمات على نظم المعلومات. بول روبنسون، قاموس الأمن الدولي، مركز الإمارات للدراسات والبحوث الاستراتيجية، الإمارات العربية المتحدة، 2009، ص 145، ص ١٩٨

[7]) Gianpiero Greco, Cyber-attacks as aggression crimes in cyberspace in the context of international criminal law, European Journal of Political science studies, volume 4, Issue 1, 2020, p 40

[8]) Philip Hemen Fage The Implications of transnational cyber threats in international humanitarian law: analyzing the distinction between cybercrime, cyber-attack, and cyber warfare in the 21st century. Baltic Journal of law & Politics, 2017, vol (10) , p. (1-34)

[9]) Jonathan A.OPHARD, "Cyber warfare and the crime of aggression: the Need for individual Accountability on tomorrow Battlefield, Duke law and technology" DUKE LAW & TECHNOLOGY REVIEW, 2010, p No3, and, Solce, The Battlefield of Cyberspace: The Inevitable New Military Branch - The Cyber Force, 18 ALB. L.J. SCI. & TECH. 293, 301 (2008). p No 300

في اجهزة كمبيوتر الدولة الخصم بما يعزز قدرات الدولة التي شنت الهجوم على الانتصار في النزاع المسلح.

وقد تكون الهجمات السيبرانية سابقة في التوقيت على بدأ العمليات الحركية بغرض إضعاف القوة العسكرية للخصم لتيسير الهجوم علية وتدمير معداته العسكرية، وهو ما حدث في عام ٢٠٠٨ اثناء النزاع بين روسيا وجورجيا. فقبل بدء الهجمات العسكرية الروسية بيوم واحد شهدت جورجيا هجمه سيبرانية أدت إلى تعطيل نظم الاتصال الإلكترونية للقوات الجورجية بالكامل، خاصة في إقليم أوسيتا عقب إعلان انفصاله عن جورجيا، مما أدى إلى إضعاف وسائل الدفاع الجورجية، هذا بالإضافة لتعطل وسائل الإعلام وقطاع المواصلات عن العمل لاشتراكهم في البنية التحتية السيبرانية مع المواقع العسكرية المستهدفة بالهجمات. (10)

وقد توجه الهجمة السيبرانية في نفس توقيت شن الهجمات الجوية، ومن أمثلة هذا النوع من الهجمات ما قامت به إسرائيل في عام ٢٠٠٧ عندما وجه سلاح الجو الإسرائيلي ضربات لمواقع سورية اشتبهت في احتوائها على مفاعلات نووية، وفي نفس التوقيت وجهت إسرائيل هجمات سيبرانية استهدفت شبكة التحكم في الرادارات والاتصالات السورية مما أدى إلى تعطيلها عن العمل بالكامل. (11)

وتمثل الهجمات السيبرانية التي تشن في زمن النزاعات المسلحة انتهاكاً للقانون الدولي إذا أدت لأضرار غير مبرره للسكان المدنيين أو إذا وجهت تلك الهجمات لمواقع مدنية، حيث أن استخدام القوة بما في ذلك القوة السيبرانية يجب أن يكون في إطار الضوابط التي يحددها القانون الدولي الإنساني.

وبالتالي فالقانون الدولي الإنساني هو الذي يحدد الانتهاكات السيبرانية الي ترتكبها الدول في زمن النزاعات المسلحة، وهو الذي يحدد مدى مشروعية الهجمات التي تشنها الدول، سواء العمليات السيبرانية التي تشن كسلاح قتال مساعد للعمليات العسكرية الحركية التقليدية البرية والبحرية والجوية، أو العمليات السيبرانية المستقلة التي تشن بهدف تدمير البنية التحتية للدولة المستهدفة إذا نُفذت في زمن النزاع المسلح (12) مثل حالات الهجوم على أنابيب نقل الغاز والبترول والمفاعلات النووية. (13)

ثانياً: العدوان السيبراني

---

[10] Jonathan A.OPHARD, “Cyber warfare and the crime of aggression: the Need for individual Accountability on tomorrow Battlefield, Duke law and technology” O.P, p3

[11]) Thomas Rid and peter McBurney, cyber – weapons, Routledge publisher, The RUSI Journal, February 2012, p9.https://www.tandfonline.com/doi/pdf/10.1080/03071847.2012.664354?needAccess=true

[12]) في التمييز بين العمليات السيبرانية التي تتم كوسيلة مساعدة للحرب البرية والبحرية والجوية والعمليات السيبرانية التي تشن لتحقيق أهداف اقتصادية وسياسية وتدمير البنية التحتية راجع حسن فياض، الهجمات السيبرانية من منظور القانون الدولي الإنساني، الموقع الرسمي للجيش اللبناني، 2020، ص 4

[13]) تشكل العملية السيبرانية استخدام للقوة عندما يكون حجمها وآثارها قابلة للمقارنة مع العمليات غير السيبرانية التي تصل لمستوى استخدام القوة. أنظر القاعدة الحادية عشر من دليل تالين

الصوره الثانية للانتهاكات السيبراينة للقانون الدولي تتمثل في الهجمات التي لا تشن في زمن الحرب ولكنها تؤدى لتحقيق نتائج ترتقي لمستوى العدوان، ويرى Gianpiero Greco إمكانية تحديد مفهوم العدوان السيبراني من خلال تطبيق مفهوم العدوان التقليدي الوارد في الفقرة الأولى من المادة الثامنة مكرر من النظام الأساسي للمحكمة الجنائية الدولية، [14] وعلية يكون العدوان السيبراني هو قيام أي دولة بتنفيذ أو توجيه أو تخطيط أو إعداد أو شن عملية سيبرانية، تمثل بحكم خصائصها وخطورتها ونطاقها انتهاكاً واضحاً لميثاق الأمم المتحدة".

ويتفق Jonathan A.OPHARD مع هذا الرأي قائلاً أن وصف فعل معين بأنة عملاً عدوانياً يستند في الأساس على الانتهاك الواضح لميثاق الأمم المتحدة، ووقوع الانتهاك الذي يمثل الفعل المادي للعدوان من عدمه يُحدد من خلال الوقوف على خصائص الفعل وخطورته ونطاقة. [15]

ومثال ذلك، العملية السيربانية الموجهة للمفاعل النووي الإيراني عام 2010، والمعروفة باسم "دودة ستوكسنت"، حيث حققت هذه العملية اضراراً مادية بأجهزة الطرد المركزية للمفاعل النووي الإيراني، واحتوت دودة ستوكسنت على عنصرين الأول منهم صمم بغرض خروج نظام الطرد المركزي للمفاعل عن السيطرة الإيرانية، والجزء الثاني هو خداع الإيرانيين واخفاء ما يتم في الواقع واعتقادهم بأن الأجهزة تعمل بشكل طبيعي، ونُسب هذا الهجوم بنسبة كبيرة للولايات المتحدة الأمريكية وإسرائيل.[16] ومعيار خطورة هذه العملية يجعلها ترتقي لمستوى العدوان الالكتروني.

وعلى الرغم من اتفاق جانب كبير من فقهاء القانون الدولي على أن العدوان الإلكتروني يمثل أحد أخطر صور العدوان، إلا أن هذا الأمر لم يلقى استجابة على مستوى الواقع من الأمم المتحدة أو المحكمة الجنائية الدولية لمحاولة تحديد الإطار القانوني لمحاكمة مرتكبي جريمة العدوان السيبراني. [17]

ويرى Kevin Miller أن المحكمة الجنائية الدولية يمكنها مكافحة حالات العدوان السيبراني من خلال تفسيرها لنص المادة الثامنة مكرر التي أضيفت في كمبالا، دون الحاجة لإدخال تعديلات جديدة على النظام الأساسي، كما أن مجلس الأمن يمكنه مكافحة أي شكل من أشكال العدوان المستحدثة وفقاً لما يملكه من سلطات واسعة في تحديد ما إذا كان أي فعل

---

[14]) Gianpiero Greco, Cyber-attacks as aggression crimes in cyberspace in the context of international criminal law, O.P p 43

[15]) Jonathan A.OPHARD, "Cyber warfare and the crime of aggression: the Need for individual Accountability on tomorrow Battlefield, Duke law and technology" O.P , p1

[16]) Micheal Gervais, "Cyber Attacks and the law of warfare'', Berkeley Journal of international law, vol:30. Issue.2 article 6, 2012, p.570 https://lawcat.berkeley.edu/record/1125035?ln=en

[17]) Albi Kociblli, Aggression, from Cyber-Attacks TO ISIS: Why International law Struggles to Adapt,2017 vol39.

تقوم به الدول يمثل عدوان أم لا بالاستناد على ما يمثله ذلك الفعل من تهديد للسلم والأمن الدولي. [18]

ويتفق الباحث مع أن المحكمة الجنائية الدولية يمكنها محاكمة مرتكبي أفعال العدوان السيبراني استناداً على أن نص المادة الثامنة مكرر لم يحدد صور العدوان بشكل حصري ولكنها اشارت لبعض الصور على سبيل المثال وليس الحصر، كما أن مجلس الأمن يمكنه توصيف أي فعل بالعمل العدواني وفقاً لسلطاته في هذا الشأن، وإن كان ذلك سيواجه عقبة تحديد الجهة المنفذة للهجمات العدوانية، وسيتم مناقشة ذلك في الأجزاء التالية من البحث.

ثالثا: العمليات السيربانية التي لا ترتكب في زمن الحرب ولا ترتقي لمستوى العدوان وتمثل انتهاك للقانون الدولي.

إذا كانت هناك عمليات سيبرانية ترتكب في زمن النزاع المسلح وبالتالي تخضع لقواعد القانون الدولي الإنساني، وعمليات أخرى تعكس خطورتها وجود حالة عدوان صريح من الدولة التي نفذت العملية، فهناك حالات أخرى تثير إشكاليات بالغة التعقيد بسبب أن خصائصها وخطورتها ونطاقها لا يرتقي لمستوى العدوان الدولي. [19] مثل اختراق موقع إخباري أو وكالة من وكالات الأنباء، [20] أو العمليات التي تستهدف سرقة أو تدمير البيانات التي تخزنها الدولة المستهدفة، أو عمليات سرقة الأموال المملوكة للدولة، وهي تصرفات غير مشروعة دولياً لما ينتج عنها من أضرار تصيب الدولة المستهدفة، ولكنها لا تصل لحد العدوان الذي يتطلب مستوى عالي من المخاطر الناشئة عن التصرف السيبراني الدولي. [21]

والأمثلة على هذه العمليات كثيرة، ولا مبالغة في القول بأن هذه العمليات هي الأكثر انتشاراً على الساحة الدولية خلال السنوات السابقة، ومنها العمليات السيبرانية التي تنفذ لتحقيق أهداف سياسية كاختراق الشبكات ونشر والوثائق السرية المرتبطة بالعلاقات السياسية الدولية، ومن أشهر هذه العمليات تسريبات ويكيليكس، وهو الموقع الذي تم اختراقه وسرقة آلاف الوثائق السرية الرسمية لمخاطبات بين وزارة الخارجية الأمريكية وبعثاتها في مختلف دول العالم وتم نشرها مما تسبب في توتر حاد في العلاقات مع العديد من الدول، بالإضافة لحالة التوتر الداخلي التي شهدتها عدة دول بسبب المعلومات التي تم تسريبها عن قيادات حكومية في مختلف المواقع في هذه الدول. [22]

ومن أمثلة هذه العمليات التي لا تشن في زمن الزاعات المسلحة ولا ترتقي لوصف العدوان ايضاً، نجد العملية السيبرانية التي وجهت إلى الولايات المتحدة الأمريكية في عام

---

[18]) Kevin L. Miller, The Kampala Compromise and Cyberattacks: Can there Be an international Crime of Cyber-Aggression? Southern California Interdisciplinary law Journal, 2014, vol.23, p.217,

[19]) Jonathan A.OPHARD, "Cyber warfare and the crime of aggression: the Need for individual Accountability on tomorrow Battlefield, Duke law and technology" O.P, p 5

[20]) في عام 2013 اخترق حساب وكالة اسوشيتد برس الامريكية على تويتر من خلال عملية سيبرانية، وقامت الجهة المنفذة للعلمية بنشر تغريدات كاذبة تشير إلى حدوث هجوم على البيت الأبيض، وأدت هذه الهجمة السيبرانية إلى هبوط حاد في أسعار البورصة الأمريكية، وتبنى الجيش السوري الالكتروني الهجوم.

[21]) Micheal Gervais, "Cyber Attacks and the law of warfare'' O.P, p.537

[22]) سارة عبد العزيز، الحرب السيبرانية، التداعيات المحتملة لتصاعد الهجمات الإلكترونية على الساحة الدولية، مركز المستقبل للأبحاث والدراسات المتقدمة، 2017

2003 وعرفت باسم "تايتن راين" وخلال هذه العملية نجحت الجهة المنفذة في استخراج بيانات حساسة من منظمات تشمل وكالة ناسا، ومكتب التحقيقات الفيدرالية الأمريكية، ووزارة الدفاع الأمريكية ووزارة الدفاع البريطانية. [23] وبعد عامين من التحقيقات نسبت الحكومية الأمريكية تنفيذ هذه العملية للصين وهو ما عارضته الصين قائلة إن الولايات المتحدة لا تملك ما يثبت صحة ادعائها. [24]

كما تعرضت اليابان وكوريا الجنوبية وماليزيا لعدد هائل من الهجمات التي استهدفت سرقة وتدمير المعلومات المخزنة على أجهزة كمبيوتر خاصة بشخصيات سياسية وعسكرية ودبلوماسية، ومواقع رسمية للدولة مثل الموقع الرسمي لرئاسة الجمهورية في كوريا الجنوبية. [25]

وفي عام 2016 وجهت هجمه سيبرانية لشبكة كهرباء أوكرانيا، مما أدى لانقطاع الكهرباء لعدة ساعات عن 225000 مستهلك، واتهم مسؤولين أوكرانيون روسيا، إلا أن عمليات التتبع الإلكتروني لمنفذي الهجوم والتي قام بها عدد من شركات الامن الإلكتروني الخاصة انتهت إلى صعوبة التحقق مما إذا كانت الجهة المنفذة للهجمة تابعة للحكومة أم أنها نفذت من قبل مجرمين إلكترونيين. وفي عام 2016 أيضاً وجهت هجمة سيبرانية للبنك المركزي في بنغلاديش، تم خلالها سرقة 81 مليون دولار من حساب البنك لدى البنك الاحتياطي الفيدرالي في نيويورك باستخدام نظام الاتصالات المصرفية العالمي SWIFT [26] ،

---

[23]) Jonathan A.OPHARD, "Cyber warfare and the crime of aggression: the Need for individual Accountability on tomorrow Battlefield, Duke law and technology" O.P, p 10

[24]) شهد عام 2012 مثال أخر لهذه الهجمات حيث وجهت عملية سيبرانية للقطاع الموزع للخدمة على المصارف الأمريكية، واستهدفت ما يزيد عن 46 من أبرز المؤسسات المالية في الولايات المتحدة الأمريكية، وبعد أربع سنوات من التحقيق لمحاولة التعرف على الجهة المنفذة للعملية - في مارس 2016 - قالت الولايات المتحدة أن هذا التصرف السيبراني تم من جانب جهات فاعلة في الحكومة الإيرانية.
وفي عام 2014 تم تنفيذ هجمة سيبرانية على البيت الأبيض ووزارة الخارجية الأمريكية وعزي هذا الهجوم بدرجة كبيرة لروسيا ولكن الحكومة الأمريكية لم تستطع تحديد المصدر رسمياً، وفي العام التالي (2015) تم توجيه هجوم على المكتب الأمريكي لشؤون الموظفين وسرقة 21.5 مليون سجل خاص بموظفي حكومة الولايات المتحدة، عزي بدرجة كبيرة للصين، ولكن الحكومة الأمريكية لم تحدد رسمياً مصدر الهجوم، وفي (2016) نُفذ هجوم سيبراني على اللجنة الديمقراطية الوطنية في الولايات المتحدة الأمريكية، وتم خلال هذه العملية استخراج وثائق الحملة الانتخابية ونشرها، ونسبه تقرير مدير مكتب الاستخبارات في 2017 لجهات فاعلة حكومية روسية. ومن الأمثلة الأشهر على الهجمات السيبرانية على البيانات ما حدث في عام 2012 حين وجهت هجمة سيبرانية لشركة أرامكو السعودية، مما نتج عنه مسح وتدمير للمعلومات الموجودة على 35000 جهاز كمبيوتر تابع للشركة، وتسببت هذه الهجمة في خسائر مالية بالغة للمملكة العربية السعودية وللاقتصاد العالمي وقتها ونسبت الحكومة الأمريكية هذا الهجوم لإيران. كما شهدت ألمانيا هجمه سيبرانية في عام 2015 حيث تم توجيه عملية سيبرانية للبرلمان الألماني، نتج عنها استخراج ونشر 2420 ملف حساس من ملفات الاتحاد الديمقراطي المسيحي الألماني، وبعد تحقيقات استمرت لمده عام نسب المكتب الفيدرالي لحماية الدستور هذه الهجمة لمجموعة (آي بي تي 28) تهديدات مجهولة المصدر: نحو مساءلة دولية في الفضاء الإلكتروني، مجموعة باحثين، مؤسسة RAND، 2017، ص 7 - 12

[25]) راجع: عمر حمد شاكر، المجال الخامس – الفضاء الإلكتروني، دراسات استراتيجية، المعهد المصري للدراسات، 2019، ص 22.

[٢٦]) د. علم الدين بانقا، مخاطر الهجمات الإلكترونية، السيبرانية، دراسات تنموية، المعهد العربي للتخطيط، الكويت، العدد 63، 2019، ص20

وبعد قرابة عام من التحقيقات، في عام 2017 نسب تقرير وكالة الاستخبارات الأمريكية تنفيذ الهجمة إلى دولة كوريا الشمالية. [27]

ومن خلال استعراض هذه العمليات السيبرانية يتضح أن درجة خطورتها لا ترتقي لوصف العدوان كما أنها لم ترتكب في زمن النزاعات المسلحة، وبالتالي لا يطبق عليها القانون الدولي الإنساني، ولكنها تبقى انتهاكات سيبرانية للقانون الدولي، كما أن الانتهاكات السيبرانية السابق ذكرها أظهرت عجز النظام القانوني الدولي مكافحتها.

وما يزيد من صعوبة مكافحة هذه الانتهاكات أن الدول لديها أكثر من خيار لاقتحام المواقع الإلكترونية للدول الأخرى وسرقة أو تدمير معلوماتها، وعند تحليل هذه الخيارات نجد تباين في الوسائل الي تستخدمها الدول وفي النهاية تحقق غايتها في تدمير المعلومات أو سرقتها. [28]

الاختيار الأول الذي تلجأ إلية الدول هو مراقبة الأنشطة السيبرانية للدولة المستهدفة من خلال خرق شفرة الإشارات التي تمر عبر الخوادم الموجودة على إقليم الدولة التي تقوم بالمراقبة، وهذا الاختيار لا يمثل انتهاك للقانون الدولي، ذلك لأن القانون الدولي لا يحظر أعمال التجسس أو العمليات التي لا تتضمن عنف أو أعمال قسرية. والاختيار الثاني هو ارسال أحد الدول لبرنامج تجسس لشبكة تابعة للدولة المستهدفة عن بعد، ولا يوجد في القانون الدولي أيضاً ما يحرم سلوك الدولة التي أرسلت البرامج أو يمنعها من ذلك بشكل واضح. والاختيار الثالث هو قيام الدولة بزرع شريحة الكترونية يضعها أحد عملائها في شبكة النظام الالكتروني لدى الدولة المستهدفة، وهذا الاختيار هو الوحيد الذي يمكن القول بأنه محظور دولياً لأنه يمثل انتهاك لحرمة إقليم الدولة المستهدفة بإدخال شخص وزرع الشريحة الإلكترونية وهو ما ينطوي على تصرف مادي تم على إقليم الدولة المستهدفة دون علمها أو موافقتها. [29]

وبالتالي فإن لجوء الدول للاختيار الأول أو الاختيار الثاني يُظهر فراغ قانوني في القانون الدولي يستوجب ابرام اتفاقية دولية تحظر هذه الأفعال التي تلجأ إليها الدول في حروبها المعاصرة ضد الدول الأخرى.

المطلب الثاني

مفهوم الانتهاكات السيبرانية للقانون الدولي وفاعلية جهود مواجهتها

يحاول هذا المطلب صياغة تعريف يجمع كافة التصرفات السيبرانية التي تمثل انتهاكاً للقانون الدولي، حيث أن الكثير من الباحثين اتجهوا لتعريف العدوان السيبراني، أو عقبات تطبيق القانون الدولي الإنساني في الفضاء السيبراني، إلا أنهم لم يتعرضوا للانتهاكات التي تتم في غير حالات النزاع المسلح، والحالات التي لا تمثل حالة من حالات العدوان.

---

[27]) تهديدات مجهولة المصدر: نحو مساءلة دولية في الفضاء الإلكتروني، مجموعة باحثين، مؤسسة RAND، 2017، ص 10

[28]) Michael N.Schmidt, the law of cyber warfare, STANFORD LAW & POLICY REVIEW, 2014, Vol. 25,p.275

[29]) Micheal Gervais, "Cyber Attacks and the law of warfare'', Berkeley Journal of international law, vol:30. Issue.2 article 6, 2012, p.533

ولذا سأحاول من خلال هذا المطلب وضع تعريف للانتهاكات السيبرانية للقانون الدولي يشمل أي شكل من اشكال الانتهاك للقانون الدولي في الفضاء السيبراني بغض النظر عما أذا كان تنفيذه في زمن النزاع المسلح، أو ما إذا كان الفعل يرتقي لوصف العدوان من عدمه.

أولاً: مفهوم الانتهاكات السيربانية للقانون الدولي.

يضم القانون الدولي العام عدد من المبادئ الأساسية التي تمثل النواه الصلبة التي تنبت من داخلها كافة القواعد المنظمة لتصرفات الدولة، وتمثل تلك المبادئ الإطار المحدد لمشروعية اي تصرف او وصفه بأنه ينتهك القانون الدولي.

فالتصرفات المباحة دولياً توصف بالمشروعية لكونها تتفق مع المبادئ المستقرة للقانون الدولي، والتصرفات المحرمه توصف بالانتهاكات لتعارضها مع تلك المبادئ، وارى أن احترام هذه المبادئ الأساسية هو المعيار الذ يحدد مدى مشروعية أي تصرف، بغض النظر عما إذا كانت هناك قاعدة محدده تصف هذا التصرف بكونه مشروع أو ممنوع دولياً.

وتتمثل أهم مبادئ القانون الدولي العام في مبدأ السيادة الوطنية ومبدأ عدم التدخل في الشئون الداخلية للدول الأخرى ومبدأ عدم استخدام القوة وحظر التهديد بها في مجال العلاقات الدولية، وقد انبثقت عن تلك المبادئ التي يمكننا وصفها بالمبادئ الموضوعية الكثير من القواعد القانونية التي هدفت إلى تطبيق تلك المبادئ على مستوى كافة العلاقات الدولية.

وفي هذا الشأن يقول Michael Schmidt أن تطبيق مبادئ القانون الدولي يقتضي تطور تفسيرها وتطبيقاتها بشكل مستمر لتستجيب لتحولات بيئة الأمن الدولي وتظل قادرة على حفظ السلام الدولي الذي وضعت من أجل حمايته. [30]

فمثلاً مبدأ السيادة الوطنية، انبثقت عنه الكثير من المفاهيم التي تُطبق مضمون فكرة السيادة على إقليم الدولة بما يحتويه من بر وبحر وجو، فيأتي مفهوم السيادة البرية ليعبر عن سيطرة الدولة على إقليمها البري وكل ما علية، ومفهوم السيادة البحرية ليطبق فكرة السيادة في المسطحات المائية الواقعة في إقليم الدولة، ومفهوم السيادة الجوية يُطبق فكرة السيادة في المنطقة الجوية التي تعلو إقليم الدولة وتخضع لسلطاتها الوطنية. ويشار في هذا الشأن إلى أن كل مجال من هذه المجالات شهد خلافات واقعية بين الدول وجهود فقية استمرت لسنوات طويلة حتى استقر العمل الدولي على تحديد المناطق الخاضعة لسيادة الدولة سواء في البحر أو في الجو [31].

ومن خلال بيان صور الانتهاكات السيبرانية للقانون الدولي التي سبق التعرض لها يبات جلياً أن العلاقات الدولية دخلت حقلاً جديداً، ولم تعد محدودة في مجالات البر والبحر والجو، وإذا كان القانون الدولي مناط به تنظيم علاقات الدول في تلك المجالات التقليدية، فأن

---

[30]) Michael N.Schmidt, the law of cyber warfare, O.P ,p.271

[٣١]) لمزيد من التفصيل عن مبدأ السيادة الإقليمية على المسطحات المائية على سبيل المثال، راجع، د. صلاح الدين عامر، مقدمة لدراسة القانون الدولي العام، دار النهضة العربية، الطبعة الحادية والعشرون، 2020، ص 555 - 565

تطبيقه على أي مجال مستجد للعلاقات الدولية هو أمر واجب ليحقق هذا القانون غايته في تنظيم علاقات الدول أينما وجدت هذه العلاقات. [32]

وإن كان ذلك كذلك، فيمكننا القول أن الأطار العام لمصطلح الانتهاكات السيربانية للقانون الدولي قد اتضح وظهرت ملامحه الرئيسية، والتي تتمثل في أنه مصطلح يعبر عن أي انتهاك لمبادئ القانون الدولي من خلال عمليات سيبرانية أسوة بما هو مطبق على التصرفات الحركية في المجالات التقليدية للعلاقات الدولية.

ولذا اتجه الفقة إلى تطبيق مبدئي السيادة وعدم التدخل في الشئون الداخلية للدول الأخرى على الفضاء السيبراني، فاعتُرف للدول بامتلاك حق السيطرة الكاملة على البنية التحتية التي تقع داخل أراضيها السيادية، كما انتهى فريق الخبراء الحكوميين الذي أنشأته الأمم المتحدة والمعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي إلى أن المبادئ الدولية التي تستمد من سيادة الدول تنطبق على سلوك الدول في مجال الأنشطة المتصلة بالفضاء السيبراني وتكنولوجيا المعلومات والاتصالات وعلى ولايتها القضائية فيما يتعلق بالبنية التحتية المرتبطة بهذه التكنولوجيا الموجودة على أرضها. [33]

كما انسحب مبدأ عدم التدخل في الشئون الداخلية للدول الأخرى على الفضاء السيبراني، حيث اعتُرف بأن أي تدخل من قبل الدول في البنية التحتية السيبرانية على متن منصه تتمتع بالحصانة السيادية للدول الأخرى أينما وجدت تشكل انتهاك لسيادة الدولة صاحبة السيادية على تلك البنية. [34]

كما انسحب مبدأ عدم استخدام القوة أو التهديد بها في مجال العلاقات الدولية على مجال الفضاء السيبراني، وذلك بالاعتراف بأن العمليات السيبرانية التي تتضمن تهديد أو استخدام للقوة ضد سلامة الأراضي أو الاستقلال السياسي لأي دولة، [35] أو التي لا تتفق بأي وجه مع مقاصد الأمم المتحدة، تعتبر عمليات غير مشروعة، [36] أي أنها تمثل انتهاكات سيبرانية للقانون الدولي.

وبالتأكيد لم يقتصر استخدام الفضاء السيبراني على تصرفات الدول، بل أنه أضحى مجالاً جديداً لعلاقات البشر بكافة مستوياتها بما في ذلك علاقات الأشخاص والمؤسسات على المستوى الداخلي، وإن كانت العمليات السيربانية التي تتم على المستوى الوطني وتمثل تهديد لاستقرار مجتمع الدولة تخضع للتشريعات الوطنية التي تضعها الدول، فإن العمليات السيبرانية التي تتم على المستوي الدولي في مجال علاقات الدول وبعضها البعض وتمثل تهديد للسلام والأمن الدولي يجب أن تخضع لقواعد وأحكام القانون الدولي وأن تكون في سياق احترام مبادئه الأساسية.

---

[32]) Micheal Gervais, "Cyber Attacks and the law of warfare'' O.P p.536

[33]) تقرير فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي وثائق الأمم المتحدة (A/68/98) ص2

[34]) القاعدة الرابعة من دليل تالين

[35]) Micheal Gervais, "Cyber Attacks and the law of warfare'', O.P p.536

[36]) القاعدة العاشرة من دليل تالين.

وتتضح ضرورة إبراز مفهرم الانتهاكات السيبرانية للقانون الدولي من أن هذا المفهوم يعكس انتهاك العلميات السيبرانية للقانون الدولي ولا علاقة له بالقانون الوطنية، فمن الممكن أن يكون التصرف مشروع على مستوى القانون الوطني أو غير مُجرم بموجب التشريعات الوطنية للدولة التي نُفذ على إقليمها إلا أنه يمثل انتهاكاً للقانون الدولي لمخالفته أحد مبادئة أو قواعدة الرئيسية.

واستناداً على ما سبق يمكننا تعريف الانتهاكات السيبرانية للقانون الدولي بأنها: "قيام أحد أشخاص القانون الدولي العام بعمليات سيبرانية موجهة لشخص دولي أخر بغرض تحقيق أهداف تمثل انتهاك لمبادئ القانون الدولي العام أو أي قاعدة من قواعدة".

ثانياً: مدى فاعلية الجهود المبذولة لمواجهة الانتهاكات السيبرانية للقانون الدولي

مع نهاية القرن المنصرم بدأت مخاطر استخدام الفضاء السيبراني على السلام والأمن الدوليين تلوح في الأفق، [37] وبادرت الجمعية العامة للأمم المتحدة بمحاولة محاصرة تلك المخاطر من بداياتها، ففي ٢٣ ديسمبر ١٩٩٩ أصدرت الجمعية العامة قرارها المعنون بالتطورات في ميدان المعلومات والاتصالات السلكية في سياق الأمن الدولي، والذي أشارت فيه لأهمية التقدم في مجال تكنولوجيا المعلومات واستخدام الانترنت، وما يمثله هذه التطور من إتاحة لتطور الحضارات وتوسيع لفرص التعاون الدولي، وعلى الجانب الأخر ما ينتج عن هذا التقدم من مخاطر تهدد السلام والأمن الدولي، ولذا بدأت الجمعية العامة العمل على وضع تعريف للمفاهيم الأساسية المتصلة بأمن المعلومات، بما فيها التدخل غير المأذون به في نظم المعلومات والاتصالات السلكية واللاسلكية وموارد المعلومات وإساءة استخدامها، واتجهت الجمعية العامة إلى وضع مبادئ دولية يكون من شأنها تعزيز أمن نظم المعلومات والاتصالات السلكية واللاسلكية. وفي 7 يناير 2002 عاودت الجمعية العامة التأكيد على مخاطر استخدام الفضاء السيبراني وقررت إنشاء فريق من الخبراء الحكوميين معني بدراسة الأخطار القائمة والمحتملة من استخدام هذا الفضاء الإلكتروني وما يمثله من تهديد لأمن المعلومات، وقررت أن يبدأ هذا الفريق عملة في 2004، إلا أن إنشاء هذا الفريق – مع الأسف - استغرق خمس سنوات إضافية من النقاشات، ولم يبدأ الفريق عملة إلا في عام 2009 رغم أن موضوع مخاطر استخدام الفضاء السيبراني ظل مطروح للمناقشة أمام الجمعية العامة طوال تلك الفترة ورغم تأكيدها على تصاعد هذه المخاطر عام بعد عام [38].

وقدم فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي ثلاث تقارير في 2010[39]، 2013[40]،

---

[37]) Scott Shackelford, From Nuclear War to War: Analogizing Cyber Attacks in International law, Berkley Journal of International Law (BJIL), VOL.25, NO.3, 2009, P. 192.

[38]) أنظر القرارات الصادرة الجمعية العامة للأمم المتحدة بعنوان "التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي"، رقم (A/RES/45/49)، ورقم (A/RES/56/19)، ورقم (A/RES/28/32)، ورقم (A/RES/60/45)، ورقم (A/RES/62/17)، ورقم (A/RES/64/25)، ورقم (A/RES/66/24)، ورقم (A/RES/66/24).

[39]) أنظر وثائق الأمم المتحدة رقم (A/65/201)

[40]) أنظر وثائق الأمم المتحدة رقم (A/68/98)

2015[41]، أكدت في مجملها على تعاظم مخاطر الفضاء السيبراني وانتهاكات القانون الدولي التي تزداد يوماً بعد يوم في هذا المجال الجديد للعلاقات الدولية.

ويلاحظ أن الجمعية العامة للأمم المتحدة لم تستطع تحقيق تقدم يُذكر في مجال مواجهة الانتهاكات السيبرانية للقانون الدولي، فعلى مدار عقدين من الزمن تدور المناقشات التقليدية ويتم التأكيد سنوياً على مخاطر الفضاء السيبراني، والانتهاكات التي ترتكب فيه، ولم يصدر إلى الأن اتفاق دولي يضع الإطار القانوني المناسب لمواجهة هذه الانتهاكات، وهو ما أصبح ضرورة لحماية السلم والأمن الدوليين.

وما يستحق الإشارة إلية في هذا الشأن، هو تقدم روسيا وأوزباكستان والصين وطاجيكستان في عام 2011 للجمعية العامة للأمم المتحدة بمقترح إصدار مدونة قواعد سلوك دولية لأمن المعلومات، [42] ورغم أهمية هذه المدونة إلا أنها لا تمثل وثيقة ملزمة يمكن الاعتماد عليها لمواجهة الانتهاكات السيبرانية للقانون الدولي.

الوثيقة الأخرى التي اكتسبت أهمية عالمية في مجال مواجهة الانتهاكات السيبرانية للقانون الدولي هي دليل تالين، وهو دليل أعده مجموعة خبراء القانون الدولي وخبراء تكنولوجيا المعلومات برعاية حلف الناتو، واحتوى أهم المبادئ التي تنظم استخدام الفضاء السيبراني في النزاعات المسلحة، [43] ومن خلال مطالعة هذا الدليل والمواد التي احتواها يمكن التأكيد على أن التوصل لصيغة اتفاق دولي لتنظيم سلوك الدول في الفضاء السيبراني ليس بالأمر المستحيل، بل إن اسقاط قواعد القانون الدولي ومبادئه على العمليات السيبرانية هي أمر ممكن.

ومما سبق يمكننا استخلاص أن عدم وجود اتفاق دولي يحدد مشروعية سلوك الدول في الفضاء السيبراني يرجع في الأساس لعدم رغبة الدول في تقييد حريتها في هذا المجال الجديد وليس لعدم إمكانية التوافق على قواعد دولية تنظم سلوكياتها في الفضاء السيبراني.

المبحث الثاني

التسلح السيبراني وحق الدول في الدفاع عن نفسها ضد الهجمات السيبرانية

رغم تعدد صور الانتهاكات السيبرانية للقانون الدولي، إلا أن اعتماد الدول على البيانات الرقمية يتزايد يوما بعد يوم، مثل تنامي الاعتماد على بيانات الضمان الاجتماعي

---

[41]) أنظر وثائق الأمم المتحدة رقم (A/70/174)

[42]) نصت هذه المدونة على تعهد الدول التي تنضم إليها طواعية بعدم استخدام الفضاء السيبراني في تنفيذ أنشطة تتعارض مع صون السلام والأمن الدولي، أو استخدامه للتدخل في الشئون الداخلية للدول الأخرى أو لزعزعة استقرارها السياسي والاقتصادي والاجتماعي، والتعاون لمكافحة الأنشطة الإجرامية والإرهابية التي تتم باستخدام الفضاء السيبراني، والعمل على تأمين سلاسل الإمداد المستخدمة لخدمة تكنولوجيا المعلومات والاتصالات، والإقرار بضرورة تمتع الأفراد داخل الفضاء السيبراني بالحقوق المقررة لهم خارج هذا الفضاء

أنظر الرسالة الموجهة من المندوبين الدائمين للاتحاد الروسي وأوزبكستان والصين وطاجيكستان وقيرغيزستان وكازاخستان لدى الأمم المتحدة، في يناير 2015، وثائق الأمم المتحدة رقم (A/69/723).

[43]) https://www.onlinelibrary.iihl.org/wp-content/uploads/2021/05/2017-Tallinn-Manual-2.0.pdf

والحسابات المصرفية والبيانات الطبية وملفات عملاء الشركات وقوائم وسجلات الانتخابات والبيانات البيومترية، [44] وأصبحت هذه البيانات ضرورية لسير الحياة في أي دولة. [45]

ووفقاً للجنة الدولية للصليب الأحمر فأن اعتبار هذه البيانات من الأعيان المدنية التي يجب حماتيها بموجب القانون الدولي هو أمر مثار خلاف وجدل لم يستقر بعد، ولا يوجد اتفاق دولي واضح ينص على اعتبار البيانات المدنية من الأعيان المدنية الخاضعة لحماية القانون الدولي، هذا على الرغم من أهمية هذه البيانات التي ترتقي لمستوى يفوق بعض الأعيان المدنية المنصوص على حمايتها دولياً، حيث أن حذف أو تدمير أو العبث بهذه البيانات يمكن أن يؤدي لشلل العمل في المرافق الحكومية والقطاع الخاص بشكل يؤدي لسرعة انهيار الدولة وانتشار الفوضى. [46]

وقد أدت هذه المقدمات لنتيجتين،

النتيجة الأولى: نشأة مجال جديد لسباق التسلح بين الدول بهدف حماية هذه البيانات، وهو مجال التسلح السيبراني[47]، فلم يعد سباق التسلح مصطلح يقصد به تطوير الطائرات والمدرعات والسفن الحربية وأسلحة الدمار الشامل فقط، بل اتسع هذا المفهوم ليتضمن تطوير البرامج التكنولوجية التي تستطيع حماية بيانات الدولة من الهجمات التي قد تستهدفها والنفاذ إلى معلومات الخصم ونسخها أو تدميرها أو تغيير محتواها. [48]

والنتيجة الثانية: نظراً لطبيعة الفضاء السيبراني فأن سباق التسلح السيبراني لم يقتصر على الدول بمؤسساتها الوطنية، بل تتسابق فيه العديد من القوى الإقليمية وشركات البرمجيات والأشخاص التي تسعى لتطوير البرامج التكنولوجية الخبيثة لاستخدامها لتحقيق أغراض خاصة أو لبيعها للدول. [49]

وقد أشارت تقديرات مكتب مدير الاستخبارات القومية الأمريكية في عام 2017 إلى أن أكثر من ثلاثين دولة قامت بتطوير برامج عمليات إلكترونية هجومية، كما أشار لأن هذه

---

[44]) البيانات البيومترية يقصد بها البيانات التي تتيح التعرف الآلي على الأفراد استناداً على سماتهم البيولوجية والسلوكية مثل بصمة الأصبع والقرنية والوجه.

[45]) Micheal Gervais, "Cyber Attacks and the law of warfare'' O. P p.526

[46]) موقف اللجنة الدولية للصليب الأحمر: القانون الدولي الإنساني والعمليات السيبرانية خلال النزاعات المسلحة، نوفمبر ٢٠١٩. ورقة مقدمة من اللجنة الدولية للصليب الأحمر إلى فريق العمل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، وإلى فريق الخبراء الحكوميين المعني بالارتقاء بسلوك الدول المسؤول في ميدان الأمن السيبراني.

[47] أحمد عبيس الفتلاوي، الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء قواعد التنظيم الدولي المعاصر، مجلة المحقق الحلبي القانونية والسياسية، العدد الرابع، السنة العاشرة، 2016، ص 611.

[48]) حسن فياض، الهجمات السيبرانية من منظور القانون الدولي الإنساني، الموقع الرسمي للجيش اللبناني، 2020، ص 1

[49]) Philip Hemen Fage The Implications of transnational cyber threats in international humanitarian law: analyzing the distinction between cybercrime, cyber-attack, and cyber warfare in the 21st century. Baltic Journal of law & Politics, 2017, vol (10) , p. 27

التكنولوجيا أصبحت متاحة لدى الكثير من العناصر الإجرامية والجهات الفاعلة غير الحكومية، بما يمثل تهديداً حقيقياً للسلام والأمن الدولي والاقتصاد العالمي. [50]

وسوف اتعرض من خلال هذا المبحث لإلقاء الضوء على التسلح السيبراني للدول وانتشار القوة السيبرانية غير المنظمة في مطلب أول، ثم اتعرض لحق الدول في الدفاع عن نفسها ضد الهجمات السيبراني وما عرف بالردع السيبراني في مطلب ثاني.

المطلب الأول

التسلح السيبراني للدول وانتشار القوى السيبرانية غير المنظمة

لا جرم في توجه الدول إلى تطوير قواتها السيبرانية بغرض حماية أمن معلوماتها وتعزيز قوتها السيبرانية في مواجهة الخصوم، حيث فرضت الهجمات السيبرانية المتزايدة على الدول اتخاذ الإجراءات الازمة لحماية أمن معلوماتها والدفاع عن نفسها حال تعرضها للهجمات السيبرانية، إضافة إلى توجه الدول إلى إعداد كوادرها البشرية المؤهلة لخوض غمار هذه الحروب الجديدة. [51]

فامتلاك القوة السيبرانية لا يمثل في ذاته انتهاك للقانون الدولي، وذلك انطلاقاً من أن الهجمات السيبرانية غير محظورة ولا محرمه دولياً إذا تمت في إطار استهداف المنشآت والمواقع التي أباح القانون الدولي مهاجمتها وفقاً لقواعد القانون الدولي المنظمة لاستخدام القوة. [52]

ومن خلال هذا المطلب سأحاول إلقاء الضوء على إنشاء الوحدات السيبرانية التابعة للقوات المسلحة للدول، وبيان مفهوم الأسلحة السيبرانية، ثم ألقى الضوء على مفاهيم الجنود السيبرانيون والمحاربون السيبرانيون التابعين للدول والقوات السيبرانية غير التابعة للدول.

أولاً: إنشاء الوحدات السيبرانية التابعة للقوات المسلحة الوطنية

أفادت تقارير فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، زيادة عدد الدول التي تقوم بتطوير تكنولوجيا المعلومات والاتصالات كأدوات للحرب والاستخبارات، وللأغراض السياسية، [53] حيث شهد العقدين الماضيين سباق تسلح سيبراني بين الدول الكبرى التي تسعى للحفاظ على مكانتها وقوتها وسيطرتها على الساحة الدولة في ظل ما أفرزه عصر تكنولوجيا

---

[50]) تهديدات مجهولة المصدر: نحو مساءلة دولية في الفضاء الإلكتروني، مجموعة باحثين، مؤسسة RAND، 2017، ص 1

[51]) لمزيد من التفصيل بشأن مخاوف الدول من مخاطر استخدام الفضاء السيبراني، راجع: تقرير فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي وثائق الأمم المتحدة (A/68/98) ص7

[52]) The fact that a computer network attack during an armed conflict is not kinetic, physical or violent in itself, does not put it beyond the remit of IHL As with other means and methods of warfare, computer network attacks against combatants and military objectives are legal as long as they are consistent with humanitarian law. www.icrc.org/eng/war-law/conduct-hostilities/information-warfare/overview-information-warfare.htm

[53]) أنظر تقاري فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، وثائق الأمم المتحدة، A/65/201، الصادر في 2010/7/30، ص 2، التقرير (A/68/98) الصادر في 2013/7/13ص9

المعلومات من تحديات وانعكاساته على ميادين الحروب، وقد أنشأت الكثير من الدول وحدات سيبرانية تابعة لقواتها المسلحة. [54]

فالولايات المتحدة الأمريكية أنشأت "مركز الاستخبارات المتكامل للتهديدات السيبرانية" في عام 2015. ليباشر مهام الدفاع السيبراني، ويطبق استراتيجية عمل الولايات المتحدة في الفضاء السيبراني، والتي تبلورت خلال ثلاث عقود، حيث وضعت الولايات المتحدة أول سياسة قومية لأمن الاتصالات وأنظمة المعلومات الأوتوماتيكية في عام 1984، وكانت هذه الوثيقة تتسم بدرجه كبيرة من السرية، وكلفت وكالة الأمن القومي الأمريكية بحماية شبكات الحاسوب من الاختراقات. وعلى الرغم من ذلك، ظل التسلح السيبراني في مؤخرة اهتمامات الولايات المتحدة، وحدثت النقلة النوعية في هذا المجال في عهد الرئيس السابق باراك أوباما. [55] وفي عام 2010 أعلن نائب وزير الدفاع الأمريكي ويليان لين أن الفضاء السيبراني أصبح مجال عمل جديد للقوات المسلحة الأمريكية، وأطلقت الولايات المتحدة الأمريكية أكبر قيادة سيبرانية دفاعية في العالم، وفي 2011 أصدرت وزارة الدفاع الأمريكية "استراتيجية العمل في الفضاء السيبراني" والتي تضمنت استخدام الولايات المتحدة لأحدث الطرق الدفاعية لحماية أمنها السيبراني ومواجهة الاعتداءات السيبرانية. [56]

أما روسيا فكانت من أول الدول التي استشعرت مخاطر استخدام الفضاء السيبراني، ولذا قدمت مقترح للأمم المتحدة بشأن إبرام اتفاقية دولية للأمن السيبراني في عام 1998، إلا أن هذا المقترح لم يلقى قبول الدول. وفي 2010 شكلت روسيا قيادة مستقلة للأمن السيبراني وأشارت في عقيدتها العسكرية التي أعلنتها في هذا التوقيت لأن حرب المعلومات أصبحت تلعب دوراً بالغ الأهمية سواء في الصراعات المسلحة أو غير المسلحة، كما أنشأت روسيا إدارة سيبرانية داخل جيشها. [57]

---

[54]) عمر حمد شاكر، المجال الخامس – الفضاء الإلكتروني، دراسات استراتيجية، المعهد المصري للدراسات، ٢٠١٩، ص ١.

[55]) في عام 1983 شاهد الرئيس الأمريكي الأسبق رونالد ريجان فيلم أسمه (ألعاب الحرب) وعرض الفيلم قصة شاب اخترق "قيادة الفضاء الجوي لأمريكا الشمالية" دون قصد، وظنا منه أنه يلعب لعبة حاسوبية جديدة كاد أن يشعل حرباً عالمية ثالثة دون أن يدري، وتساءل الريس وقتها عن مدى إمكانية حدوث ذلك في الواقع، وعندما عاد للبيت الأبيض سأل رئيس الهيئة المشتركة لرؤساء الأركان وهو أكبر ضباط القوات المسلحة الأمريكية: هل يمكن أن يحدث ذلك؟ رد رئيس الأركان بأنه سينظر في الأمر، وبعد أسبوع، عاد وأجاب على الرئيس قائلا أن الأمر أخطر من ذلك بكثير. ولذلك طلقت الولايات المتحدة الأمريكية في العام التالي سياستها القومية لأمن الاتصالات ولكن فاعلية تطبيق هذه السياسة واجهت تحديات لأن النظام الأمريكي ذاك الوقت كان يحظر على وكالة الأمن القومي التجسس أو اعتراضات الاتصالات الداخلية للأمريكيين، كما أن مخاطر الفضاء السيبراني لم تكن واضحة بالشكل الكافي للمسؤولين عن تنفيذ السياسية بالوكالة، ومع بدايات القرن العشرين بدأ صراع التسلح الأمريكي الروسي يتخذ شكلاً أكثر جدية، واصبح التسلح السيبراني أحد أوليات الرئيس الأمريكي جورج بوش الأمن، والنقلة النوعية الحقيقية في هذا المجال حدث في عهد الرئيس باراك أوباما الذي ضاعف ميزانية التسلح السيبراني ثلاث أضعاف كما ضاعف أعداد العاملين في هذا المجال في القوات المسلحة الأمريكية لأربع أضعاف.
أنظر، فرد كابلان، المنطقة المعتمة: التاريخ السري للحرب السيبرانية، سلسلة عالم المعرفة، المجلس الوطني للثقافة والفنون والآداب، الكويت، مارس ٢٠١٩، ترجمة لؤي عبد المجيد، ص ١١وما بعدها.

[56]) سارة عبد العزيز، الحرب السيبرانية، مرجع سابق، 6

[57]) عمر حمد شاكر، المجال الخامس – الفضاء الإلكتروني، دراسات استراتيجية، المعهد المصري للدراسات، 2019، ص 7

وعلى نفس النهج الأمريكي والروسي كان توجه الصين، حيث ذكرت في الورقة البيضاء التي اطلقتها عام 2006 أن الهدف الرئيسي من بناء جيش حديث هو جعله قادر على الفوز في حرب المعلومات بحلول القرن الحادي والعشرين، وفي 2012 أعلنت استراتيجيتها العسكرية ووضعت أحد محاورها الرئيسية استراتيجية الأمن الإلكتروني، وفي 2015 صرحت بأن الفضاء السيبراني أصبح أحد أهم المجالات التنافسية الاستراتيجية الجديدة بين الدول، وعملت الصين طوال تلك الفترة - وإلى الأن - على تطوير قدارتها السيبرانية الهجومية والدفاعية، وتبادلت الهجمات السيبرانية مع الولايات المتحدة لدرجة وصف هذه المرحل ب "الحرب الإلكترونية الباردة". [58]

كما أنشأت إسرائيل منظومة دفاع سيبراني تابعة لجهاز الأمن الإسرائيلي (الشباك) وهي المسؤولة عن توفير الحماية والدفاع عن المعلومات الإلكترونية وتوجيه الهجمات المضادة والتي اعتبرتها إسرائيل أخطر التهديدات التي سوف تواجهها في المستقبل، ففي عام 2014، وخلال المؤتمر الدولي الأول "سايبر تك" المنعقد في تل أبيب، طالب بنيامين نتنياهو بإنشاء منظمة أمم متحدة للسايبر يكون هدفها تحويل الانترنت من (نعمه إلى نقمة). وفي نفس التوقيت ذكر رئيس هيئة الأركان الإسرائيلي بني غانتس "أن الحرب المقبلة قد تبدأ بصاروخ يستهدف هيئة الأركان العامة للجيش الإسرائيلي أو بهجوم سيبراني واسع على أجهزة الكمبيوتر المدنية والعسكرية، وذكر أن الفضاء الإلكتروني يشهد حروباً بين دولاً لم تعلن الحرب فيما بينها [59]" وذكر إيرز كرينز مؤسس منظومة الدفاع الإسرائيلي، إنه في أي حرب قادمة تخوضها الدولة العبرية، ستتعرض لهجمات سيبرانية متعددة، وأنهم سيتمكنون من ضرب أكثر المواقع الإسرائيلية أهمية وحساسية ... وستمس هذه الأعمال بالأمن القومي الإسرائيلي مساً سافراً. [60]

ثانياً: الأسلحة السيبرانية

إذا كان من الصعب تعريف الأسلحة السيبرانية وتحديد مفهومها بشكل واضح في الوقت الحالي، فإنه – وبشكل مبدئي – يجب الاعتراف بأن البرامج الخبيثة التي تصمم بغرض الإضرار بالدولة الخصم هي بالتأكيد أسلحة سيبرانية مثل البرامج المصممة بغرض استطلاع قواعد معلومات الخصم الإلكترونية، وتحديد نقاط ضعفها والتسلل إليها واستنساخها أو إتلافها أو تغييرها، أو التشويش على الاتصالات السلكية واللاسلكية لنظم تشغيل مرافق الدولة وتوفير المعلومات اللازمة لتوجيه العمليات العسكرية وتعقب الأهداف المتنوعة. [61] وقد تتخذ الأسلحة السيبرانية شكل ديدان إلكترونية مثل دودة ستوكسنت أو

---

[58]) سارة عبد العزيز، الحرب السيبرانية، مرجع سابق، 7

[59]) حلمي موسى، "حرب السايبر" تشعل إسرائيل: البحث في تحويل النقمة إلى نعمه، صحيفة السفير اللبنانية في 2014/1/31.

[60]) د. محمد المجذوب، الوسيط في القانون الدولي العام، مرجع سابق، ص 818

[61]) د. محمد المجذوب، الوسيط في القانون الدولي العام، مرجع سابق، ص 826

فيروسات مثل حصان طروادة، [62] أو القنابل المنطقية، [63] وتتفاوت درجة مخاطر هذه الأسلحة من سلاح لأخر على أساس قوة تدميرها للبيانات التي تتضمنها الشبكات. [64]

ثالثاً: الجنود السيبرانيون والمحاربون السيبراني التابعين للدول

في ظل نمو مخاطر الحروب السيبرانية تسعى الدول لتأهيل كوادر بشرية قادرة على خوض غمار هذه الحرب، وهو ما انعكس على المفهوم القانوني للجنود المقاتلين، والقواعد التي وضعها القانون الدولي للتمييز بينهم وبين المدنيين، بغرض توفير الحماية لمن لا يشاركون الحروب.

والمقاتلون السيبرانيون لا يشبهون هؤلاء المقاتلون التقليديون الذين يشاركون في المعارك مرتدين زياً عسكرياً أو حاملين أسلحتهم لمهاجمة العدو، ولكنهم في الغالب شباب على درجه عالية من الذكاء جالسين أمام شاشات الكمبيوتر في منازل غالباً ما تكون مدنية في أماكن تبعد عشرات الالف من الكيلومترات عن مكان تنفيذ الهجوم السيبراني، وسلاحهم جاز كمبيوتر، وكلمه خاصة للمرور تدخل برامج متطورة معده خصيصاً لتنفيذ الهجمات السيبرانية. [65]

ويميز البعض بين مفهومي الجنود السيبرانيون والمحاربون السيبرانيون، فالجنود السيبرانيون هم العاملون في الأجهزة التابعة للقوات المسلحة للدول، ويكونون متخصصين في مجالات الشبكات وتكنولوجيا المعلومات، ويتبعون الفصائل العسكرية والتسلسل الهرمي العسكري، بشكل واضح، وعادة ما يكون عملهم من مواقع القوات المسلحة لضمان أمن وسرية المعلومات والأجهزة، ويشكلون وحدات داخل الجيوش النظامية للدول، ويتمثل عملهم في صد الهجمات السيبرانية التي توجه للدولة وتوجيه الهجمات السيبرانية للجهات المعادية إذا تطلب الأمر ذلك، وعلى سبيل المثال أعلنت وزارة الدفاع البريطانية في سبتمبر 2013 عن تشكيل وحدة جديدة للحماية السيبرانية وأعلنت عن حاجتها لمتخصصين للالتحاق بهذه الوحدات. أما المحاربون السيبرانيون فهم عملاء سريون تستعين بهم الدول لتطوير قدراتها السيبرانية وتنفيذ الهجمات وفقاً لتوجيهاتها دون أن ينتمون لقواتها المسلحة، ولذا تمنحهم درجة من الاستقلالية ولا تطلعهم على نظم علمها السيبرانية، وفي حال كشفهم تنفي الدولة صلتها بهم. [٦٦]

رابعاً: انتشار القوات السيبرانية غير المنظمة

---

[62]) فيروس حصان طروادة هو جزء صغير من الكود يضاف للبرمجيات يؤدي إلي تحريب عمل النظام الإلكتروني الذي يعمل فيه هذا الكود، وتكمن خطورته في أن النظام الإلكتروني لا يشعر به إلا عندما تحين اللحظة المحددة للقيام بدورة التخريبي.

[63]) القنبلة المنطقية هي أحد أنواع الفيروسات التي تدمر شبكات الكمبيوتر حال تحقق شرط معين يحدده مصمم القنبلة، مثل عدد بلوغ عدد موظفين شركة معينة لرقم محدد، ففي هذه الحالة ينشط الفيروس ويدمر النظام.

[64]) لمزيد من المعلومات عن الأسلحة السيبرانية، راجع بيتر سينجر، الحرب عن بعد: دور التكنولوجيا في الحرب، مركز الإمارات للبحوث والدراسات الاستراتيجية، ٢٠١٠

[65]) د. محمد المجذوب، الوسيط في القانون الدولي العام، مرجع سابق، ص 824

[66]) سارة عبد العزيز، الحرب السيبرانية، مرجع سابق.

اتاحة طبيعة الفضاء السيبراني انتشار قوات سيبرانية غير منظمة ولا تتبع الدول، سواء كانت أفراد أو مجموعات تحركهم دوافع مختلفة، إما مشاعر قومية أو عقائدية أو الرغبة في الحصول على المال، وتوصف القوات السيبرانية غير المنظمة بأوصاف عده منها الهاكر، والمرتزقة السيبرانيون، والقراصنة السيبرانيون. [67] ورغم الصعوبة التي تواجه تقسيمهم لفئات محددة إلا أن النوايا التي تُحركم والهدف من العمليات السيبرانية التي يقومون بها يمكن أن تمثل أساس منطقي لتصنيفهم. [68]

فالهاكرز يكونوا مواطنون مدنيين تدفعهم مشاعرهم القومية أو الأيديولوجية ومهارتهم في استخدام أجهزة الكمبيوتر للمشاركة في الهجمات الإلكتروني، ويسهل الفضاء الإلكتروني المفتوح للكافة القيام بذلك من أي مكان في العالم، [69] حيث يعمل الهاكرز على ابتكار وتطوير برامج اختراق المواقع والشبكات وينفذون هجماتهم دون توجيه حكوماتهم. وقد تلجأ بعض الدول أو المؤسسات غير الحكومية للاستعانة بهؤلاء الأفراد أو المجموعات لتنفيذ مهام بشكل رسمي أو بشكل غير رسمي، والشكل الرسمي يكون من خلال ضمهم للوحدات العسكرية أو الاستخباراتية كما حدث في حالة الوحدة 8200 في إسرائيل وجيش التحرير الشعبي في الصين، أما الشكل غير الرسمي فيكون من خلال تكليفهم بأداء مهام معينة أو شراء برامج التسلل والاختراق منهم، ويطلق أحياناً على هذه الفئة أسم القراصنة الوطنيون، ومن أبرز امثلتهم شباب ناشي في روسيا وتحالف الهاكر الأحمر في الصين والجيش الالكتروني السوري. [70]

ومن أمثلة العمليات التي قاموا بتنفيذها في 2007 الهجوم على القطع الموزع لخدمة الاتصالات في استونيا خلال فترة التوترات مع روسيا، واتهمت الحكومة الإستونية جهات فاعلة حكومية روسية، وألقت روسيا باللائمة على حركة شبابية مؤيدة للكرملين وليس على جهات فاعلة ترعاها الدولة، وعزت روسيا ذلك بسبب غضب الشباب المؤيدين للكرملين من نقل السلطات الإستونية للنصب التذكاري الذي يخلد الجيش الروسي من العاصمة تالين إلى مكان مجهول. [71]

وهنا يجب الإشارة لأن الهاكرز أو القراصنة الوطنيون يختلفون عن المرتزقة السيبرانيون في أن المرتزقة يحركهم دافع المادة أو المصلحة المالية التي تعود عليهم بالربح من العلميات التي يقومون بها ويمكن القول إن المرتزقة يبيعون خبرتهم ومهارتهم المتفوقة

---

[67]) Philip Hemen Fage The Implications of transnational cyber threats in international humanitarian law: analyzing the distinction between cybercrime, cyber-attack, and cyber warfare in the 21st century. OP , p. (1-34)

[68]) Jonathan A.OPHARD, "Cyber warfare and the crime of aggression: the Need for individual Accountability on tomorrow Battlefield, Duke law and technology" O.P, p No6

[69]) Micheal Gervais, "Cyber Attacks and the law of warfare'', O.P, p.546

[70]) سارة عبد العزيز، الحرب السيبرانية، مرجع سابق

[71]) Scott J.Shackelford, Änalogizind Cyber: from Nuclear War to Net war Attacks in international law", university of Cambridge, Dept of politicos and international Studies, Cambridge,UK, 2008, p205

في المجال السيبراني لمن يدفع لهم، [72] وتستعين الدول بهؤلاء الأشخاص لثلاث أسباب رئيسية:

السبب الأول: عدم وجود الخبرات الكافية داخل الكثير من الدولة في مجال مكافحة الهجمات السيبرانية.

السبب الثاني: تنفيذ الهجمات من دون أن يكون للدولة أو الجهة المستفيدة أي علاقة بذلك أو حتى الربط بينها وبين مكان إطلاق الهجوم، حيث توفر تلك الجماعات نوعاً من الغموض والتشويش.

السبب الثالث: قلة تكلفة الاعتماد على هذه المجموعات لأداء مهام محددة إذا قورنت بإنشاء وحدات من المحاربون السيبرانيون داخل المؤسسة العسكرية، والذي يتطلب إلى جانب التكلفة المالية تطوير قدراتهم بشكل مستمر. [73]

ويثير الوضع القانوني لهؤلاء المجموعات غير المنظمة إشكاليات بالغة التعقيد بشأن تمتعهم بالحماية المقررة للمدنيين، ومدى اعتبارهم من المدنيين أو المقاتلين، خاصة وأنهم ينفذون الاعتداءات السيبرانية في غير زمن النزاعات المسلحة، لذلك لا يطبق القانون الدولي الإنساني على أفعالهم، وحتى في حالات النزاعات المسلحة التي يطبق فيها القانون الدولي الإنساني، فإن معظم الهاكرز يكونون من المدنيين لذلك فأنهم محميين من الهجوم المباشر بموجب القانون الدولي الإنساني، ويصبحون عرضه للملاحقة الجنائية وفقاً للقوانين الوطنية على أفعالهم في هذه الحالات، أما إذا شارك الهاكرز بشكل مباشر في الأعمال العدائية، ونفذوا هجومًا إلكترونيًا لدعم جانب واحد في نزاع مسلح، فإنهم يفقدون حمايتهم من الهجوم المباشر أثناء تنفيذ هجوم إلكتروني.

المطلب الثاني

الردع السيبراني وحق الدول في الدفاع عن نفسها في مواجهة الهجمات السيبرانية

يمثل أمن المعلومات أهمية خاصة لكافة الدول في ظل تصاعد مخاطر الهجمات السيبرانية، [74] ولذا تتخذ الدول إجراءات إلكترونية وأخرى مادية لحماية وتأمين معلوماتها، إضافة لاتخاذ الإجراءات التشريعية والإدارية اللازمة لهذه الحماية، وتتضمن الإجراءات المادية توفير الصيانة اللازمة للهياكل المادية لحماية الوثائق والموظفين وأجهزة الكمبيوتر من السرقة، أما الإجراءات التشريعية فتتمثل في سن القوانين التي تجرم محاولات اختراق معلومات الدولة، واللوائح المنظمة للتعامل مع الملفات السرية الحساسة للدولة، كما تضم هذه الإجراءات أمن الموظفين وطريقة تعاملهم مع الملفات السرية، وطرق تشفير البيانات، أما

---

[72]) Jonathan A.OPHARD, "Cyber warfare and the crime of aggression: the Need for individual Accountability on tomorrow Battlefield, Duke law and technology" O.P, p No4

[73]) سارة عبد العزيز، الحرب السيبرانية، مرجع سابق

[74]) مفهوم الأمن السيبراني cyber security يقصد به مجموعة الوسائل التقنية والتنظيمية والإدارية التي يتم استخدامها لمنع الاستخدام غير المصرح به وسوء الاستغلال واستعادة المعلومات الإلكترونية ونظم المعلومات التي تحتويها وذلك بهدف ضمان توافر واستمرار نظم المعلومات وتعزيز حماية وسرية وخصوصية البيانات الشخصية وحماية المواطنين والمستهلكين من مخاطر الفضاء السيبراني. راجع: عمر حمد شاكر، المجال الخامس – الفضاء الإلكتروني، دراسات استراتيجية، المعهد المصري للدراسات، ٢٠١٩، ص 14

الإجراءات الالكترونية فتتمثل في تطوير برامج الحماية التي تقاوم عمل الفيروسات الخبيثة، وتعمل الدول على تطوير هذه البرامج لمحاولة الكشف عن الفيروسات الخبيثة حال محاولة اختراق النظم الالكترونية المؤمنة، وتحديد مصادر الهجمات. [75]

وفي ظل طبيعة الفضاء السيبراني، فإن كافة إجراءات أمن المعلومات لن تحول دون تعرض الدول لهجمات إلكترونية تتسبب في تدمير بياناتها أو تشفيرها أو غير ذلك من الأهداف، ولذا نشأت فكرة الردع السيبراني، وهو توجيه الدولة التي تعرضت للاعتداء السيبراني لهجمات سيبرانية للجهة التي قامت بالاعتداء السيبراني بما يفيد أنها قد حددت الدولة أو الجهة التي نفذت الاعتداء وأنها قادرة على الرد.

والردع السيبراني قد لا يكون مفيداً في الكثير من حالات الاعتداءات السيبرانية، ذلك لصعوبة تحديد مصدر الهجمة الإلكترونية بشكل سريع، وعلى الرغم من ذلك، نجد أن معظم الدول ضمنت استراتيجياتها العسكرية المعلنة حقها عن الدفاع عن النفس ضد الهجمات الإلكترونية التي تتعرض لها، المثال على ذلك، ما تضمنته الاستراتيجية الأمريكية للفضاء السيبراني والتي نصت صراحة على حق الولايات المتحدة الأمريكية في الرد على أي أعمال عدائية سيبرانية في الفضاء السيبراني أسوة بما تقوم به في حال أي تهديد أخر للبلاد. [76]

ولا شك في أن الدولة التي تواجه اعتداء سيبراني، سيكون لها الحق في الدفاع عن نفسها باستخدام كافة الطرق والوسائل المتاحة بما في ذلك الرد العسكري حال خطورة الهجمة السيبرانية التي توجه إليها، [77] وفي هذا الشأن يقول الدكتور بول روزنفياغ الأستاذ بجامعة جورج واشنطن أن الهجمات السيبرانية التي تؤدى إلى الإضرار بالبنية التحتية للدول مثل انقطاع الكهرباء أو تحطيم مفاعل نووي ستعتبر عمل حربي يبرر الرد العسكري من الدولة المتضررة. [78]

ولكن الإشكالية التي تطرح هنا تكون في حالة عدم ارتقاء مستوى الاعتداء للعمل العسكري، ولم يحدث تأثير في البنية التحتية للدولة أو لم يؤدي لخسائر مادية بالغة، بمعنى أن الاعتداء السيبراني اقتصر على سرقة ملفات أو بيانات من أحد أجهزة الدولة، فهل يكون من حق الدولة الرد بعمل عسكري مثل توجيه طائرة بدون طيار لقصف الموقع الذي صدر منه الهجوم حال تحديده؟

والرد القانوني على هذا التساؤل وفقاً لتفسير مبدأ الدفاع عن النفس، أن الرد يجب أن يكون مناسباً لمقدار الاعتداء، ولا يتعدى هدف الرد إلا إيقاف الاعتداء، وإشكالية التطبيق العملي لهذا المعيار القانوني أن الدولة المعتدى عليها هي التي تقيم خطورة البيانات المخترقة، وبالتي قد ترى أن قصف أو تدمير المكان الذي صدرت منه الهجمة هو الاختيار

---

[75]) بول روبنسون، مركز الإمارات للدراسات والبحوث الاستراتيجية، ٢٠٠٩ قاموس الأمن الدولي، ص١٤٣

[76]) الاستراتيجية الأمريكية للفضاء السيبراني.

[77]) يجوز للدولة التي تكون هدفاً للعمليات السيبرانية التي تصل لمستوى الهجوم المسلح أن تمارس حقها الطبيعي في الدفاع عن النفس، وتعتبر العملية السيبرانية هجوماً مسلحاً بالاعتماد على حجمها وأثارها. القاعدة الثالثة عشر من دليل تالين.

[78]) د. محمد المجذوب، الوسيط في القانون الدولي العام، مرجع سابق، ص 822

الوحيد، في ظل صعوبة توجيه هجمه إلكترونية مضادة تستهدف مسح البيانات التي سرقت من الجهاز الذي وجهت منه الهجمة السيبرانية. [79]

ولو كان الحديث عن دولة بحجم الولايات المتحدة الأمريكية فالأمر يبدو أصعب، خاصة وأنه من المعروف أنها تتبنى تفسيراً موسعاً لحق الدفاع عن النفس، وتسمح لنفسها بالرد بعمليات عسكرية عابرة لحدودها الوطنية مستندة لعدم رغبة الدول التي وجه الهجوم من أرضها أو عدم قدرتها على التعامل مع هذه النوعية من الانتهاكات السيبرانية التي يتطلب الكشف عنها ومواجهتها تقنيات متقدمة لا تملكها أغلب دول العالم، [80] بالإضافة لذلك، أن كشف الهجمات السيبرانية والتعامل معها يتطلب سرعة فائقة لدرجة أن الدولة التي يوجه إليها الاعتداء السيبراني لن تملك رفاهية الوقت لإخطار الدولة التي تنطلق منها الهجمات، إضافة لأن الدولة المعتدى عليها لا تستطيع التحقق مما إذا كانت هذه الهجمات موجهة من أجهزة الدولة المراد إخطارها أم كيانات خاصة موجودة على أرضها دون علمها، في ظل هذه التحديات والصعوبات تجد الدولة المعتدى عليها نفسها في مواجهة موقف يكون الاختيار الآمن فيه هو توجيه ضربات عسكرية إما للمهاجمين أو للبنية التحتية الإلكترونية للدولة التي صدر من أرضها الاعتداء السيبراني. [81]

المبحث الثالث

تحديات مواجهة الانتهاكات السيبرانية للقانون الدولي

لا يعني عدم تنظيم استخدام الفضاء السيبراني تركه لمشيئة المحاربين، فهناك أحكام عامة تفرضها قواعد الأخلاق الدولية والمبادئ الإنسانية المستقرة في القانون الدولي وهي واجبة التطبيق على أي عمليات حربية سواء كانت حركية أو سيبرانية، [82] وحال مخالفتها تنشأ مسؤولية دولية في موجهة الدولة التي تنتهكها، فالقانون الدولي الإنساني يحتوي قواعد مكتوبة تنظم العمليات العسكرية البرية والبحرية والجوية وهي ملاءمة للتطبيق على الحروب السيبرانية، حيث أن الهدف العام لاستخدام القوة في أي نزاع هو إضعاف قوة الخصم وإجباره على التسليم، ولذلك فإن الوسائل التي يمكن استخدامها يجب ألا تتعدى هذا الهدف وتصل لما يعرف بالأعمال الوحشية التي تُنكر الطبيعة الأدمية أو الإنسانية للحرب، والاتفاقيات الدولية بشكل عام وضعت الاطار المحدد لمشروعية استخدام القوة في النزاعات

---

[79]) يشار في هذا الشأن إلى أن الرئيس الأمريكي حذر في 2013 من أن الهجمات السيبرانية تعد شكلاً من أشكال العدوان على بلادة، مما يفسح المجال أمام رد عسكري بالمثل، وذلك في اعقاب نشر النيويورك تايمز لأخبار تفيد توصل التحقيقات الجنائية السيبرانية في الولايات المتحدة إلى أن وحدة المحاربون السيبرانيون في الجيش الصيني هي المسؤولة عن غالبية الهجمات التي تعرضت لها الشركات والوزارات الأمريكية. راجع معمر عطوي، ونزار عبود حول الوحدة "61398" تتخذ من شنغهاي منطلقاً لهجماتها، صحيفة الأخبار اللبنانية في 2013/2/21.

[80] THE WHITE HOUSE, FACT SHEET: U.S. POLICY STANDARDS AND PROCEDURES FOR THE USE OF FORCE IN COUNTERTERRORISM OPERATIONS OUTSIDE THE UNITED STATES AND AREAS OF ACTIVE HOSTILITIES (MAY 23, 2013) http://www.whitehouse.gov/the-press-office/2013/05/23/fact-sheet-us-policy-standards-and-procedures-use-force-counterterrorism;

[81] Michael N.Schmidt, the law of cyber warfare, O.P ,p.288

[٨٢]) سلوان جابر هاشم، حالة الضرورة العسكرية في القانون الدولي الإنساني، ط1، المؤسسة الحديثة للكتب، لبنان، 2013، ص 110

المسلحة، والوسائل التي تخرج عن هذا الإطار ستكون وسائل غير مشروعة وفقاً للقانون الدولي وتستتبع قيام المسؤولية الدولية في مواجهة الدولة التي استخدمتها، ويمكن الاستعانة بهذه الاتفاقيات لتحديد مدى مشروعية استخدام الفضاء السيبراني. [83] ويناقش هذا المبحث التحديات التي تواجه تطبيق القانون الدولي الإنساني على الانتهاكات السيبرانية والتحديات التي تواجه إسناد المسؤولية الدولية عن هذه الانتهاكات.

المطلب الأول

تحديات تطبيق قواعد القانون الدولي الإنساني على الانتهاكات السيبرانية

يواجه تطبيق القانون الدولي الإنساني في الفضاء السيبراني الكثير من التحديات التي يفرضها واقع هذا الفضاء ومعطياته، ومن أهم هذه التحديات نجد الاستخدام العسكري للبنية الأساسية المدنية للفضاء السيبراني، وتحديد مدلول الهجوم في الفضاء السيبراني وما يتطلبه من شروط لتطبيق القانون الدولي الإنساني، وهو ما اتعرض لمناقشته من خلال هذا المطلب بعد التعرض لقواعد القانون الدولي الواجبة التطبيق في الفضاء السيبراني.

أولا: قواعد القانون الدولي الإنساني الواجبة التطبيق في الفضاء السيبراني.

بعد دراسة مستفيضة من جانب اللجنة الدولية للصليب الأحمر لاستخدام القوة في الفضاء السيبراني، تقدمت بورقة توضح فيها رأيها في هذا الشأن إلى فريق العمل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، وإلى فريق الخبراء الحكوميين المعني بالارتقاء بسلوك الدول المسؤول في ميدان الأمن السيبراني، [84] حيث انتهت إلى أن القانون الدولي الإنساني يحظر استخدام القوة السيبرانية في توجيه الهجمات العشوائية، كما يحظر استخدام وسائل أو أساليب الحرب السيبرانية في توجيه الهجمات المباشرة ضد المدنيين أو الأعيان المدنية. [85]

ويحظر القانون الدولي الإنساني أيضاً توجيه الهجمات السيبرانية التي تهدف إلى بث الرعب بين السكان المدنيين[86]، وكذلك يحظر توجيه الهجمات السيبرانية التي من شأنها أن تصيب الأهداف العسكرية والأشخاص المدنيين والأعيان المدنية دون تمييز، أو توجيه الهجمات السيبرانية غير المتناسبة التي يتوقع منها أن تحدث خسائر عرضيه تتجاوز الميزة العسكرية الملموسة والمباشرة المنتظرة منها. [87]

---

[83]) أنظر تقارير فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، وثائق الأمم المتحدة، A/65/201، الصادر في 2010/7/30، ص 6، التقرير (A/68/98) الصادر في 2013/7/13ص 10، التقرير (A/70/174) الصادر في 2015/7/22 ص 7 أنظر أيضاً د. محمد المجذوب، الوسيط في القانون الدولي العام، مرجع سابق، ص 826

[84]) موقف اللجنة الدولية للصليب الأحمر: القانون الدولي الإنساني والعمليات السيبرانية خلال النزاعات المسلحة، نوفمبر ٢٠١٩.

[85]) قرار محكمة العدل الدولية الصادر في يوليو ١٩٩٦، مشروعية التهديد بالأسلحة النووية أو استخدامها، الفقرة ٧٨

[٨٦]) نوال أحمد بسيج، القانون الدولي الإنساني وحماية المدنيين والأعيان المدنية في زمن النزاعات المسلحة، ط1، منشورات الحلبي الحقوقية، 2010.

[87]) www.icrc.org/eng/war-law/conduct-hostilities/information-warfare/overview-information-warfare.htm

كما يحظر القانون الدولي الإنساني الهجمات السيبرانية التي تستهدف مهاجمة أو تدمير أو نقل أو تعطيل الأعيان التي لا غنى عنها لبقاء السكان المدنيين، والهجمات السيبرانية التي تستهدف الوحدات الطبية[88].

ويمكن القول إن المبادئ الأساسية للقانون الدولي الإنساني تطبق في الفضاء السيبراني، ومن أهما مبادئ التمييز والتناسب والضرورات العسكرية. [89]

ثانياً: تحدي الاستخدام العسكري للبنية الأساسية المدنية للفضاء السيبراني

أول التحديات التي تواجه تطبيق قواعد القانون الدولي الإنساني في الفضاء السيبراني، هو صعوبة التمييز بين البنية الأساسية للمواقع العسكرية والبنية الأساسية للمواقع المدنية، فكلاهما يشتركان في بنية أساسية واحد [90]، فالشبكات المدنية والعسكرية مترابطة إلى حد يجعل من الصعب الفصل بينهما، ومن المفترض أن الفضاء السيبراني مُعد في الأساس للاستخدامات المدنية وهو ما يؤدي للاعتقاد بأن الأصل في البنية التحتية لهذا الفضاء هو الطابع المدني، والاستخدامات العسكرية التي آتت بعد ذلك اعتمدت على بنية هذا الفضاء الأساسية. [91]

فالأقمار الصناعية وكابلات الألياف البصرية البحرية وأجهزة التوجيه والمراقبة الجوية جميعها تمثل جزء من البنية الأساسية للفضاء السيبراني. وتعتمد وسائل النقل المدنية والعسكرية على السواء على أنظمة الملاحة بالأقمار الصناعية في تسيير حركة الملاحة البرية والبحرية والجوية. فالسفن المدنية والعسكرية والطائرات بمختلف أنواعها واستخداماتها وكذلك المركبات البرية أصبحت تعتمد بشكل أساسي على هذا التكنولوجيا في حركتها، وقد يؤدي استهداف هذه البنية التحتية وتدمير بياناتها لمقتل الآلاف من راكبي السفن والطائرات المدنية.

كما تستخدم سلاسل الإمدادات اللوجستية المدنية والخدمات المدنية الأساسية شبكة الانترنت للاتصالات التي تُستخدم أيضاً للاتصالات العسكرية.

ومن المستقر في القانون الدولي أن استخدام عين مدنية لأغراض عسكرية لا يؤدي إلى تحويل هذه العين المدنية لهدف عسكري تلقائياً، وعلى الرغم من ذلك، فإن الاستخدام العسكري لأي عين مدنية يفقدها الحماية المقررة بموجب القانون الدولي الإنساني، ويجوز أن توجه إليها الهجمات المسلحة المباشرة، وتثير هذه المسألة إشكالية بالغة التعقيد حيث أن الاستخدام العسكري للفضاء السيبراني سيؤدي إلى استنتاج مفاده أن العديد من الأعيان التي تشكل جزء من هذا الفضاء ستفقد حمايتها بوصفها أعيان مدنية، وفي حال استهدافها سيؤدي

---

[88]) عادل عبد الصادق، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، المركز العربي لأبحاث الفضاء الإلكتروني، مصر، 2018، ص 53.

[89] Anne-laure Chaumette, International Criminal Responsibility of Individuals in case of Cyberattacks. International Criminal Law Review, 2018, p 10-25

[90] Jonathan A.OPHARD, "Cyber warfare and the crime of aggression: the Need for individual Accountability on tomorrow Battlefield, Duke law and technology" O.P , p No9

[91]) أنظر تقرير فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، وثائق الأمم المتحدة، A/65/201، الصادر في 2010/7/30، ص 7

ذلك لتعطيل واسع النطاق للخدمات المدنية السيبرانية التي يُعتمد عليها بشكل متزايد يوماً بعد يوم [92].

وتتعاظم خطورة هذه الإشكالية حال التفكير في كيفية تطبيق مبدأ التمييز، وعدم جواز استهداف المواقع المدنية، فاستخدام الفضاء السيبراني لا يكون مشروعاً في النزاعات المسلحة إلا إذا كانت العمليات الهجومية السيبرانية تتم لاستهداف مواقع عسكرية، وأن يكون إتلاف هذه المواقع العسكرية بشكل كلي أو جزئي محققاً لمصلحة عسكرية واضحة. ونظراً لأن الأهداف المدنية والأهداف العسكرية تتشارك فضاء إلكتروني واحد، فيجب على الدول توخي الحذر الشديد عند استهداف المواقع العسكرية وأن تضمن توفير الحماية للمواقع المدنية، وفي حال فقدان البنية التحية السيبرانية المدنية الحماية المقررة لها بموجب القانون الدولي بوصفها أعيان مدنية لاستخدامها عسكرياً، يبقى الهجوم عليها محكوماً بالحظر المفروض على الهجمات العشوائية، والتزام الطرف الذي يتخذ قرار الهجوم بضوابط قواعد التناسب والاحتياط أثناء الهجوم، ويكون عليه اتخاذ ما يلزم من إجراءات لتقييم الضرر المتوقع أن تسفر عنه أي عملية سيبرانية للتأكد من حجم أثرها على المدنيين. [93]

ثالثاً: تحدي تحديد مدلول الهجوم وما يتطلبه من شروط لتطبيق القانون الدولي الإنساني.

التحدي الثاني الذي يواجه تطبيق القانون الدولي الإنساني على الهجمات السيبرانية أثناء النزاعات المسلحة، هو تحديد مفهوم الهجوم بشكل دقيق للوقوف على ما يتطلبه من شروط لاعتباره هجوم وفقاً للقانون الدولي الإنساني، وفي هذا الشأن يجب الإشارة لضرورة التمييز بين مفهوم الهجوم وفقاً لميثاق الأمم المتحدة ومفهوم الهجوم وفقاً لقواعد القانون الدولي الإنساني. فقد يتحقق مفهوم الهجوم وفقاً للقانون الدولي الإنساني المحدد في المادة ٤٩ من البروتوكول الإضافي الأول، دون تحقق مفهوم الهجوم الوارد في المادة ٥١ من ميثاق الأمم المتحدة. [94]

والإشكالية هنا أن معظم القواعد الخاصة باحترام مبادئ التمييز بين المدنيين والعسكريين والاحتياطات الواجب اتخاذها لعدم إصابة المدنيين أو الأعيان المدنية والتناسب بين الهدف المتوخى والأضرار المتوقعة، تنطبق فقط في حالة تحقق مفهوم الهجوم المحدد في المادة ٤٩ من البرتوكول الإضافي الأول والتي عرفت الهجمات بأنها (أعمال العنف الهجومية والدفاعية ضد الخصم).

وعلية فإن ضيق او اتساع مفهوم الهجمات السيبرانية يمثل أمر غاية في الأهمية لتطبيق القانون الدولي الإنساني من عدمه على هذه الهجمات.

وترى اللجنة الدولية للصليب الأحمر أن العمليات السيبرانية التي يتوقع أن تتسبب في وفاة أو إصابة أو أضرار مادية تشكل هجمات في القانون الدولي الإنساني، سواء كانت الأضرار الناشئة تحققت بشكل مباشر أو غير مباشر للهجمات السيبرانية، فمثلاً وفاة مرضى

---

[92]) موقف اللجنة الدولية للصليب الأحمر: القانون الدولي الإنساني والعمليات السيبرانية خلال النزاعات المسلحة، مرجع سابق ص ٥

[93] The Principle of Proportionality in the Rules Governing the Conduct of Hostilities under International Humanitarian Law 2018 ،
https://www.icrc.org/en/download/file/79184/4358_002_expert_meeting_report_web_1.pdf

[94]) Michael N.Schmidt, the law of cyber warfare, O.P ,p.293

العناية المركزة في أحد المستشفيات نتيجة لهجمه سيبرانية استهدفت شبكة الكهرباء مما نتج عنه انقطاع الكهرباء في المستشفى لعدة ساعات يمثل هجوم سيبراني يمثل هجوم سيبراني غير مشروع ويجب محاسبة من ارتكبه.

وهناك اختلاف فقهي في الرأي بشأن العمليات السيبرانية التي تؤدي إلى تعطيل للخدمات دون أن تتسبب في أضرار مادية، فهل يمكن تصنيف هذه العمليات السيبرانية باعتبارها هجوم وفقاً للقانون الدولي الإنساني؟ [95]

الرأي الأول يرى أن العمليات السيبرانية التي تمثل هجمه عسكرية هي التي تؤدي لحدوث أضرار وإصابات واضحة لأشخاص أو منشآت تتمتع بالحماية بموجب القانون الدولي الإنسان، أما الرأي الثاني فيرى أن الهجوم السيبراني العسكري يتحقق بدون وجود أضرار أو إصابات مباشره، مثل الهجمات التي تستهدف تعطيل محطات الطاقة والكهرباء أو تعطيل شبكات الاتصالات والمصارف. [96]

ولكلا الاتجاهين جوانب من القوة وجوانب من الضعف، ولكن فريق خبراء القانون الدولي وخبراء تقنية المعلومات الذين شاركوا في وضع دليل تالين يروا أن العمليات السيبرانية تعتبر هجوم في حالة أنها "من المتوقع بشكل معقول أن تسبب إصابة أو وفاة للأشخاص أو إلحاق أضرار مادية أو تدمير الأشياء" وبالطبع أن الحد الأدنى من الأضرار لا يفي بالدرجة المطلوبة وفقاً لهذا المفهوم. [97]

بينما اعتبرت اللجنة الدولية للصليب الأحمر أن العملية التي تهدف إلى تعطيل أجهزة الكمبيوتر أو شبكة حاسوبية خلال النزاعات المسلحة تمثل هجوماً بموجب القانون الدولي الإنساني، سواء أن تم ذلك عن طريق وسائل حركية أو سيبرانية، وحذرت اللجنة من أن تقييد مفهوم الهجوم ليشمل العمليات التي تتسبب في الوفاة أو الإصابة أو الضرر المادي فقط، من شأنه أن يجعل أي عملية سيبرانية تهدف إلى تعطيل شبكات الكهرباء أو المصارف أو الاتصالات أو من المتوقع أن تتسبب في التأثير على هذه الشبكات بصورة عرضية غير مشمولة بقواعد القانون الدولي الإنساني، وقالت اللجنة أن هذا الفهم المقيد لفكره الهجوم سوف يُفقد القانون الدولي الإنساني غايته المتمثلة في حماية المدنيين والأعيان المدنية. [98]

ويتفق الباحث مع الرأي القائل بأن مفهوم الهجوم يتحقق بمجرد توجيه الهجمات التي تستهدف تعطيل البنية التحتية للدولة المستهدفة، حيث أن نتائج الهجمة السيبرانية هنا تكون ذات طبيعة احتمالية، ولا يجب أن تقتصر محاسبة الدولة التي وجهت الهجمة السيبرانية على

---

[95]) Michael N. Schmitt, Wired Warfare: Computer Network Attack and International Law, 365-99 (2002)
https://www.icrc.org/en/doc/assets/files/other/365_400_schmitt.pdf

[96]) Knut Dörmann, Applicability of the Additional Protocols to Computer Network Attacks, INT'L COMM. OF THE RED CROSS (Nov. 19,2004)
https://www.icrc.org/en/doc/assets/files/other/applicabilityofihltocna.pdf

[97]) Michael N.Schmidt, the law of cyber warfare, O.P ,p.295
https://law.stanford.edu/wp-content/uploads/2018/03/schmitt.pdf

[98]) موقف اللجنة الدولية للصليب الأحمر: القانون الدولي الإنساني والعمليات السيبرانية خلال النزاعات المسلحة، مرجع سابق ص ٦

ما تحقق فعلياً من نتائج بسبب فعلها، بل يجب أن تكون المحاسبة على قيام الدولة بعمل سيبراني كان من المحتمل أن يؤدي للإضرار بالمدنيين.

المطلب الثاني

تحدي إسناد المسؤولية الدولية في الفضاء السيبراني وسبل مواجهته

أدى اشتراك الدول والأفراد والمؤسسات في فضاء سيبراني واحد لوجود شبكة من العلاقات المتداخلة استغلتها الدول للتهرب من مسؤوليتها الدولية عن الكثير من الانتهاكات السيبرانية بدعوى أن التصرفات السيبرانية المنسوبة إليها والتي يثبت إجراءاها من سيرفرات موجودة في إقليمها، لم تصدر عن أحد مؤسساتها الحكومية أو الأجهزة التابعة لها ولكنها صدرت من أشخاص طبيعيين مقيمين على أرضها دون علم الدولة.

ولعرض هذه الإشكالية سأبدأ بتوضيح الإطار القانوني الضابط لمسؤولية الدول عن الانتهاكات السيربانية للقانون الدولي، ثم أوضح إشكالية صعوبة إسناد المسؤولية للدول في الفضاء السيرباني.

أولاً: الإطار القانوني الضابط لمسؤولية الدول عن الانتهاكات السيبرانية.

تتحقق المسؤولية الدولية بوجود ضرر أصاب أحد الدول نتيجة لفعل غير مشروع دولياً ارتكبته دولة أخرى، كما يمكن أن تتحقق هذه المسؤولية مع عدم وجود الفعل غير المشروع وفقاً لنظرية المخاطر التي اعترف بها في عدد من الاتفاقيات الدولية مثل اتفاقية التلوث الناتج عن استغلال الموارد المعدنية في قاع البحار لعام 1969، واتفاقية الاضرار الناشئة عن الأجسام التي تدور في الفضاء لعام 1972، وتمثل نظرية المخاطر أهمية خاصة فيما يتعلق بالمسؤولية الدولية التي تنشأ بسبب تصرفات سيبرانية، حيث أن استخدام الفضاء السيبراني لا يمثل عملاً غير مشروع، ومن الممكن أن يؤدي هذا الاستخدام للإضرار بدول أخرى دون وجود خطأ أو عمل غير مشروع من جانب الدولة التي قامت بالتصرف السيبراني. [99]

وبتطبيق القواعد العامة للمسؤولية الدولية فإن اسنادها للدولة التي تنفذ العمليات السيبرانية أو تديرها أو تتحكم فيها لا يثير أي مشكلة، ذلك انطلاقاً من أن الإطار القانوني الدولي المحدد لهذه المسؤولية واضح بشكل كافي لأن تعرف الدول الالتزامات الواجب عليها احترامها، حيث تسأل الدولة عن تصرف أي جهة من الجهات التالية سواء كان تصرف سيبراني أو بأي وسيلة أخرى: [100]

- أجهزة الدولة بما فيها قواتها المسلحة أو أجهزتها الاستخباراتية؛
- أي أشخاص أو كيانات تم تفويضها من قبل الدولة للقيام بقدر من سلطات الحكومة، مثل الشركات الخاصة؛
- أي أشخاص أو مجموعات تعمل في الواقع بناء على تعليمات الدولة أو تحت إشرافها أو سيطرتها مثل الميلشيات أو مجموعات المتسللين؛

---

[99]) د. محمد المجذوب، الوسيط في القانون الدولي العام، مرجع سابق، ص 833

[100]) راجع ورقة موقف اللجنة الدولية للصليب الأحمر (القانون الدولي الإنساني والعمليات السيبرانية خلال النزاعات المسلحة) أنظر القاعدة ١٤٩، دراسة القانون الدولي الإنساني العرفي الصادرة عن اللجنة الدولية للصليب الأحمر، أنظر أيضا لجنة القانون الدولي، مسؤولية الدول عن الأفعال غير المشروعة دولياً ٢٠٠١، (من المادة الرابعة وحتى المادة التاسعة).

- أي أشخاص أو مجموعات خاصة، والتي تعترف بها الدولة وتتبناها كتصرفات صادرة عنها.

ويتطلب إسناد المسؤولية الدولية في الفضاء السيبراني توفر ثلاث عناصر، الأول هو تحديد الكمبيوتر أو الخادم الذي نفذت من خلاله العملية، والثاني هو تحديد الشخص الذي قام بتنفيذ الهجوم، والثالث هو إثبات أن الفرد تصرف نيابة عن دولة ما ينسب إليها المسؤولية. [101]

ثانياً: تحدي إسناد المسؤولية الدولية في الفضاء السيبراني

العقبة الكؤود التي تواجه إسناد المسؤولية في الفضاء السيبراني هي أن التقنيات التكنولوجية المتقدمة تتيح للقائم بالتصرف السيبراني وسائل متعددة لإخفاء هويته أو تزويرها، حيث تضمن العمليات الرقمية التي بُني عليها الفضاء السيبراني صعوبة التعرف على منفذ الهجمات، وبالتالي يكون من الصعب تحديد المسؤولية عنه بشكل قانوني، [102] فالفضاء السيبراني أدى لمشكلة حقيقية فيما يتعلق بمبدأ الإقليمية الذي يقوم علية القانون وتنسب على أساسة المسؤولية. [103]

ولا تمثل صعوبة تحديد الجهة المنفذة للهجوم إشكالية في مجال تحديد المسؤولية الدولية فقط، بل تمثل إشكالية أيضاً فيما إذا كان القانون الدولي الإنساني سيطبق على هذا النزاع من عدمه، وما إذا كان القانون المطبق على النزاع هو قانون النزاعات المسلحة الدولية، أم قانون النزاعات المسلحة الداخلية. [104] كذا تنعكس صعوبة تحديد مكان الهجوم على تطبيق القانون الدولي الجنائي حال التفكير في اختصاص المحكمة الجنائية الدولية بمعاقبة مرتكبي العمليات السيبرانية عند وصفها بأنها جرائم حرب. [105]

وسبب صعوبة تحديد مصدر الهجمات الإلكتروني، أن تحديد هذا المصدر يتطلب فحص الأدلة الإلكترونية المتاحة على غرار دور اختصاص الأدلة الجنائية في نظم العدالة الجنائية الوطنية، كما يتطلب إجراء تحقيقات مع الكثير من الأطراف، وإجراء تحليلات دقيقة جداً للبيانات التقنية وفهم الدوافع السياسية أو الاقتصادية وتحليل المعلومات الاستخباراتية الشاملة ذات الصلة في حال توافرها. [106]

---

[101]) Marco Roscini, Cyber Operations and the Use of Force in International Law, Oxford University Press, USA, 2014, See also, Jens David, kevin Govern, Claire Finkelstein, Cyberwar War: Law and Ethics for Virtual Conflicts, OXFORD UNIVERSITY PRESS, (2015), P 220

[102]) Jonathan A.OPHARD, "Cyber warfare and the crime of aggression: the Need for individual Accountability on tomorrow Battlefield, Duke law and technology"O.P, p No2

[103]) Anne-laure Chaumette, International Criminal Responsibility of Individuals in case of Cyberattacks. International Criminal Law Review, O.P , p10

[104]) Anne-laure Chaumette, International Criminal Responsibility of Individuals in case of Cyberattacks. International Criminal Law Review, O.P, p 15

[105]القانون الدولي الإنساني وتحديات النزاعات المسلحة ٢٠١١، اللجنة الدولية للصليب الأحمر. ص ٤٢

[106]) أنظر تقرير فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، وثائق الأمم المتحدة، A/65/201، الصادر في 2010/7/30، ص 2

ونظراً للطبيعة الفنية المتخصصة والمعقدة والمتعددة الجوانب لهذه الهجمات فإن كثيراً من التحقيقات لا تصل للفاعل بشكل دقيق وهو ما يؤدي لسهولة التشكيك في نتائجها وبالتالي يضعف إمكانية المساءلة القانونية الدولية، وعندما تعلن نتائج التحقيقات غالباً ما تتهم بالتسييس وإنها ترتكز على أدلة محدودة وغير واضحة بالشكل الكافي لقيام المسؤولية القانونية. [107]

بالإضافة لذلك، أن تعقب مصدر الهجوم والوصول لأجهزة كمبيوتر موجودة في إقليم دولة ما، لن يكون دليلاً كافياً لاتهامها بأنها مسؤولة عن هذا الهجوم الإلكتروني، فقد لا يكون لدى أجهزة هذه الدولة علم بالهجوم، فعلى سبيل المثال بعض الهجمات التي وجهت في السنوات السابقة، وعند فحصها، تبين أنها مخترقة من ملايين أجهزة الكمبيوتر من مختلف أرجاء العالم، وهو ما يعني أن الجاني استطاع عمل إجراء الكتروني ما لإخفاء هويته، [108] وما يزيد الأمر تعقيداً أن علاقة الدولة التي نفذت الهجوم من ارضها في الغالب لا تكون واضحة، فكيف يمكن اثبات أن الدولة شجعت ضمنياً على هذا الهجوم أو أن أجهزة الدولة علمت بالهجوم وغضت الطرف عنه؟ ولذا فأن خبراء الأمن السيبراني يقولون إن تحديد مصدر الهجوم في الغالب يكون على نحو تقديري ومن الصعب تحديده بشكل قاطع. [109]

وما يزيد الأمر صعوبة أن فلسفة المسؤولية الدولية بشكل عام تستند على سيطرة الدولة على إقليمها بشكل كامل، وامتلاكها الأدوات التشريعية والتنفيذية والقضائية التي تمكنها من فرض هذه السيطرة، ومنع أي نشاط من شأنه الإضرار بالدول الأخرى والقبض على من يدبروه ومحاكمتهم، وإن كان ذلك ممكناً فيما يتعلق بالتصرفات الحركية التي يقوم بها الأشخاص، فإن إمكانية ذلك تبدو أكثر صعوبة فيما يتعلق بالتصرفات السيبرانية، فكيف للدولة أن تتعرف على الأنشطة التي تتم من إقليمها في الفضاء السيبراني، وفي ظل سيل المعلومات المنهمر الذي تتضمنه الشبكة العنكبوتية، فلو قام أحد الأجانب بتنفيذ هجمه إلكترونية من أرض الدولة المقيم فيها على دولة أخرى، وأثبتت التحقيقات السيبرانية أن تلك الهجمة نُفذت من على ارض الدولة التي يقيم فيها هذا الأجنبي، فلا يمكن اثبات أن هذا الشخص تصرف بناء على تعليمات دولة إقامته.

وما يزيد الأمر سوء ويؤدي لشيوع المسؤولية الدولية بشكل أكبر أن الطبيعة الفنية الدقيقة للفضاء السيبراني، والتي لا تملكها الكثير من الدول، أجبرت الحكومات على التعاون مع شركات متخصصة من أجل فك شفرات هذا الفضاء والتمكن من التعامل معه للدفاع عن أمنها السيبراني. فقديما كانت أجهزة الدولة فقط هي التي تملك حق استخدام الأدوات العسكرية للدفاع عن أرضها، ولكن مع التطور التكنولوجي وظهور الحروب السيبرانية تبددت هذه القاعدة، وأجبرت الدول على التعاون مع الشركات العالمية المتخصصة في مجال تكنولوجيا المعلومات، وهو ما جعل من تلك الشركات العالمية شريكاً مع الأجهزة الرسمية للدولة في الإجراءات التي تتم في الفضاء الإلكتروني، سواء برامج الحماية والدفاع أو

---

[107]) تهديدات مجهولة المصدر: نحو مساءلة دولية في الفضاء الإلكتروني، مرجع سابق، ص 2

[108]) يمكن للمهاجمين أن ينشؤوا ما يعرف بالشبكات الروبوتية التي تضم عشرات أجهزة الكمبيوتر في دول مختلفة من العالم، وعند توجيه الهجمة يتضح أشتراك عشرات بل مئات الأجهزة في تنفيذ الهجوم.
Jonathan A. Ophardt, Cyber Warfare and crime of Aggression: the Need for Individual Accountability on Tomorrow's Battlefield, O.P, p 18

[109]) تهديدات مجهولة المصدر: نحو مساءلة دولية في الفضاء الإلكتروني، مرجع سابق، 2017 ص ٢٧

البرامج المصممة للهجوم الإلكتروني التي تسعى الدول إلى امتلاكها لتنفيذ الهجمات المضادة في حال التعرض لأي اعتداء الكتروني.

والواقع أن القانون الدولي بوضعه الحالي لا يفرض على الدول التزامات باتخاذ إجراءات احترازية لمنع حدوث انتهاكات سيبرانية من إقليمها، والخشية الحقيقية من المطالبة باتخاذ الدول لهذه الإجراءات الاحترازية أنها سوف تسمح ضمنياً للدول باختراق خصوصية وسائل الاتصال الإلكترونية للشركات والأشخاص الطبيعيين.

ولمعالجة هذه الإشكالية طرحت فكرة اتخاذ العناية الواجبة للوقاية من الهجمات الإلكترونية التي تشن من على إقليمها، والحقيقة أن مفهوم العناية الواجبة يتضمن معنى مطاط لا يمكن ضبطه، ولا تحديد معايير الالتزام به من جانب الدول.

وأمام هذه التحديات نمى سوق الأمن السيبراني الخاص بشكل ملحوظ خلال السنوات السابقة، فضحايا الحوادث الإلكترونية حاولوا معرفة مصادر الهجمات السيبرانية منذ نشأة الانترنت، والمثال الأشهر على ذلك، في عام 1986 عندما اكتشف كليف ستول - وهو مدير مختبر لورنس بيركلي الوطني الأمريكي - عمليات اختراق متعددة وأنشطة استخراج البيانات من أنظمة المختبر، ولمعرفة الفاعل تعاون ستول مع شركات الاتصالات وموظفي إنفاذ القانون في الولايات المتحدة الأمريكية وألمانيا الغربية وأجري تحقيق تقني امتد طوال أشهر وأسفر عن تحديد هوية المهاجمين واعتقالهم. وخلال العقود الثلاث الماضية تطورت نظم كشف مصدر الهجمات الالكترونية، وحقق سوق الأمن الإلكتروني الخاص بعض النجاحات في كشف المهاجمين وظهرت العديد من الشركات في مجال أمن الشبكات والأجهزة والاستخبارات وجمع البيانات وقياسها وتحليلها. [110] وتقدم هذه الشركات خدمات تحديد مصدر الهجمات الالكترونية، وقد سعت الدول إلى تحسين قدراتها في تحديد مصدر الهجمات الالكترونية بعدما تبين أن تحديد هذا المصدر يمثل عنصراً أساسياً للردع الفعال، فمثلاً تفيد وزارة الدفاع الأمريكية في استراتيجية الأمن القومي لعام 2015 أنها تستثمر في مجال كشف مصدر الهجمات الإلكترونية لاعتبارها أن ذلك يمثل أهم وسائل مكافحة هذه الهجمات. [111]

وما يجب الإشارة إلية في هذا الصدد، هو التوجه نحو التنظيم غير الحكومي للكشف عن مصادر الهجمات السيبرانية، حيث اقترح عدد من الخبراء إنشاء منظمة غير حكومية يكون هدفها تحديد مصدر الهجمات الالكترونية، وتضم هذه المنظمة عدد من الخبراء من مختلف دول العالم الذين يتمتعون بخبرات عالية في هذا المجال، وتعمل على فحص الأدلة التي تقدمها الجهات التي تعرضت للهجوم، ولا يكون في هذه المنظمة أي تمثيل رسمي حكومي للدولة، ويرى أصحاب الفكرة عدم الحاجة لتمثيل الدول في المنظمة المقترحة للأسباب التالية: [112]

1 .غالباً ما ترتكز ادعاءات الدول في تحديد مصدر الهجمات الإلكترونية على أدلة ومعلومات واردة من مصادر سرية (استخباراتية)، وترفض الدول الإعلان عن هذه

---

[110]) من هذه الشركات، شركة فاير أي، وشركة كراودستريك، وشركة كاسبيرسكي لاب، وشركة نوفيتا، وشركة سيمانتك، وشركة تراند مايكرو

[111]) المرجع السابق نفسه، ص 5

[112]) المرجع السابق نفسه، ص ٢٩

المصادر علناً بدعوى سريتها وارتباطها بأمنها القومي، ويثير ذلك تساؤلات مستمرة حول كيفية توصلها إلى هذه النتائج وحول مدى مصداقيتها.

2. غالباً ما تنشر الدول ادعاءات تحديد مصدر الهجمات الإلكترونية لأغراض سياسية، وبالتالي فإن قبول عضويتهم في المنظمة المقترح إنشاءها سيمكنهم من توجيه نتائج التحقيقات التي تجرى لتحديد مصادر الهجمات الإلكترونية بطريقة تخدم مصالحها الوطنية.

3. انضمام الدول لعضوية المنظمة المقترحة سيؤثر على نزاهة قرارات قبول المنظمة للتحقيقات في الهجمات الإلكترونية، فمن الممكن أن تكون دولة من الأعضاء طرف فاعل في هجوم ما، وبالتالي سوف تبذل ما في وسعها من أجل الحيلولة دون قبول المنظمة التحقيق في هذا الهجوم.

وبذلك يعتقد أصحاب الفكرة أن هذه المنظمة ستكون أكثر شفافية، وإن كنت اتفق مع الأسباب المذكورة إلا أنني اعتقد انها ليست مقنعه ولا كافية لاستبعاد التمثيل الحكومي من المنظمة المقترحة، فإذا كانت الدوافع السياسية تتحكم في توجهات الدول وهي حقيقية لا يمكن إنكارها، فأن هذه الدوافع السياسية تمثل أيضاً أهم محركات قرارات الشركات الخاصة التي تنصاع لرغبات دولة جنسيتها، ولذا فأنني أرى أن وجود كيان دولي لمكافحة الانتهاكات السيبرانية هو أمر ضروري، ويجب أن يضم هذا الكيان سواء كان اتحاد أو منظمة تمثيل رسمي لحكومات الدول ولا ضرر في أن يعمل هذا الاتحاد من خلال الاستعانة بالشركات المتخصصة صاحبة الخبرة المشهود لها في مجال تقنية المعلومات.

الخاتمة

مثلت تكنولوجيا المعلومات والاتصالات عبر الفضاء السيبراني واحدة من أكبر النعم على البشرية لما تحققه من دفع لعجلة التقدم الاقتصاد، وانتشار لوسائل التواصل الاجتماعي بين البشر، وتعزيز لسبل الاندماج الثقافي بين الشعوب، كما ساهمت تلك التكنولوجيا في تقديم الخدمات الحكومية بشكل أكثر سهولة ويسراً، وجميعها عوامل تسهم بأشكال مختلفة في استقرار الأمن الدولي، وبالتالي يمكن القول إنها بمثابة درع لحماية السلام العالمي.

ولكن على الجانب الأخر، حملت هذه التكنولوجيا بين طياتها نقمه قد تؤدي لكارثة إنسانية في أي لحظة، فهي بلا شك سلاح جديد من أسلحة الحروب المعاصرة يُمكن مستخدمة من الهجوم على أي مؤسسة في أي دولة، دون الاعتراف بحدود إقليمية.

ويتوقف كونها درع للسلم أو أداة للحرب على نية مستخدمها ورغبته، ورغم وجود الكثير من التهديدات التي تعكر صفو السلام والأمن الدولي إلا أن هذه التكنولوجيا أشدها خطورة، ذلك لأن امتلاكها لا يقتصر على الجيوش أو المؤسسات الرسمية للدول فقط، بل أصبح متاحا لكل فرد يحيا على هذا الكوكب.

كما وجه استخدام الفضاء السيبراني في النزاعات المسلحة ضربات قاسمة لقواعد القانون الدولي الإنساني الذي اعتمدت في مجملها على التمييز بين ما هو مدني وما هو عسكري سواء في الأشخاص أو في المنشآت، وطبيعة هذا الفضاء لا هي بالمدنية ولا هي بالعسكرية.

وقد تعددت صور انتهاكات القانون الدولي في الفضاء السيبراني فمنها ما ارتكب بغرض سرقة المعلومات أو تدمير البيانات أو تحقيق أهداف سياسية أو الانتقام لمعتقدات وأفكار مذهبية، وأخطر ما في هذه الانتهاكات أن الكثير منها لا يحدث في زمن الحرب وبالتالي لا يطبق علية القانون الدولي الإنساني، ولا يطبق عليها القواعد العامة لاستخدام القوة في العلاقات الدولية لأنها لا ترتقي لمستوى العنف المطلوب لوصفها بالعدوان الذي يجرمه القانون الدولي.

بالإضافة إلى ذلك فأن الفضاء السيبراني أضحى شبيه بالغرفة المظلمة التي تحوي ملايين البشر، ومحاولة الكشف عن هوية من ينتهك أحكام القانون في هذه الغرفة تتطلب قدر من التعاون والشفافية والإفصاح بين الدول تفتقر إلية العلاقات الدولية بوضعها الراهن.

وأمام كل هذه التحديات تبين من خلال البحث أن التقدم الذي أحرز في مجال مكافحة الانتهاكات السيبرانية للقانون الدولي يكاد لا يذكر أمام تعدد صور هذه الانتهاكات وتطور وسائل ارتكابها فلم تتوصل الدول لاتفاقية دولية لمكافحة هذه الانتهاكات ولا توجد هيئة دولية معنية بمكافحتها.

النتائج

- قلة تكلفة الحرب السيبرانية باعتبارها حربً لا متماثلة تتيح لأي دولة أو أي شخص مهاجمة الدول الأخرى مهما بلغت قوتها العسكرية دون الحاجة للإنفاق على معدات عسكرية أو سفن أو طائرات حربية متطورة.
- لم يعد للمفهوم التقليدي للردع وجود في الفضاء السيبراني حيث أن طبيعة هذا الفضاء تتيح تحديات بالغة التعقيد أمام تحديد هوية منفذي الانتهاكات السيبرانية للقانون الدولي.

- أن عدم وجود اتفاق دولي ملزم لتنظم سلوكيات الدول في الفضاء السيبراني يرجع لعدم توفر الإرادة السياسية لها وعدم رغبتها في تقييد حريتها فيه.
- لن تنجح مكافحة الانتهاكات السيبرانية للقانون الدولي إلا بتعزيز التعاون بين الدول ومشاركة كبرى الشركات المتخصصة في تكنولوجيا الاتصالات وأمن المعلومات.

التوصيات

- رعاية الأمم المتحدة لتوقيع اتفاقية دولية لمكافحة الانتهاكات السيبرانية للقانون الدولي.
- إنشاء اتحاد دولي لمكافحة الانتهاكات السيبرانية للقانون الدولي على أن يضم في عضويته ممثلين حكوميين للدول ويعمل من خلال التعاون مع الشركات العالمية التي تمتلك خبرات واسعة في مجال الأمن السيبراني.
- تعزيز الدول العربية لقدراتها السيبرانية التي تمكنها من الدفاع عن نفسها حال مواجهة اعتداء سيبراني.

قائمة المراجع

المراجع العربية

١. أحمد عبيس الفتلاوي، الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء قواعد التنظيم الدولي المعاصر، مجلة المحقق الحلبي القانونية والسياسية، العدد الرابع، السنة العاشرة، 2016.

٢. بيتر سينجر، الحرب عن بعد: دور التكنولوجيا في الحرب، مركز الإمارات للبحوث والدراسات الاستراتيجية، ٢٠١٠

٣. بول روبنسون، قاموس الأمن الدولي، مركز الإمارات للدراسات والبحوث الاستراتيجية، الإمارات العربية المتحدة، 2009.

٤. حسن فياض، الهجمات السيبرانية من منظور القانون الدولي الإنساني، الموقع الرسمي للجيش اللبناني، 2020

٥. حلمي موسى، "حرب السايبر" تشعل إسرائيل: البحث في تحويل النقمة إلى نعمه، صحيفة السفير اللبنانية في 2014/1/31

٦. سارة عبد العزيز، الحرب السيبرانية، التداعيات المحتملة لتصاعد الهجمات الإلكترونية على الساحة الدولية، مركز المستقبل للأبحاث والدراسات المتقدمة، 2017

٧. سلوان جابر هاشم، حالة الضرورة العسكرية في القانون الدولي الإنساني، ط1، المؤسسة الحديثة للكتب، لبنان، 2013

٨. شادي عبد الوهاب منصور، حروب الجيل الخامس، أساليب "التفجير من الداخل" على الساحة الدولية، الطبعة الأولى، العربي للنشر والتوزيع، القاهرة – مصر، 2019

٩. صلاح الدين عامر، مقدمة لدراسة القانون الدولي العام، دار النهضة العربية، الطبعة الحادية والعشرون، 2020

١٠. على صادق أبو هيف، القانون الدولي العام، منشأة المعارف، الإسكندرية

١١. عمر حمد شاكر، المجال الخامس – الفضاء الإلكتروني، دراسات استراتيجية، المعهد المصري للدراسات، 2019

١٢. علم الدين بانقا، مخاطر الهجمات الإلكترونية، السيبرانية، دراسات تنموية، المعهد العربي للتخطيط، الكويت، العدد 63، 2019

١٣. عادل عبد الصادق، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، المركز العربي لأبحاث الفضاء الإلكتروني، مصر، 2018

١٤. د. محمد المجذوب، الوسيط في القانون الدولي العام، الطبعة السابعة، ٢٠١٨، منشورات الحلبي الحقوقية

١٥. منزر رابح، درويش سعيد، الطبيعة القانونية للهجمات السيبرانية التي تقع بين الدول، مجلة صوت القانون، المجلد الثامن، 2021.

١٦. نوال أحمد بسيح، القانون الدولي الإنساني وحماية المدنيين والأعيان المدنية في زمن النزاعات المسلحة، ط1، منشورات الحلبي الحقوقية، 2010.

١٧. تهديدات مجهولة المصدر: نحو مساءلة دولية في الفضاء الإلكتروني، مجموعة باحثين، مؤسسة RAND، 2017

المراجع الأجنبية

1. Albi Kociblli, Aggression, from Cyber-Attacks TO ISIS: Why International law Struggles to Adapt,2017 vol39
2. Anne-laure Chaumette, International Criminal Responsibility of Individuals in case of Cyberattacks. International Criminal Law Review, 2018
3. Philip Hemen Fage The Implications of transnational cyber threats in international humanitarian law: analyzing the distinction between cybercrime, cyber-attack, and cyber warfare in the 21st century. Baltic Journal of law & Politics, 2017
4. Gianpiero Greco, Cyber-attacks as aggression crimes in cyberspace in the context of international criminal law, European Journal of Political science studies, volume 4, Issue 1, 2020
5. John Arquilla and David Ronfeldt, In Athena's Camp: Preparing for Conflict in the Information Age, Santa Monica, RAND, 1997
6. Jens David, kevin Govern, Claire Finkelstein, Cyberwar War: Law and Ethics for Virtual Conflicts, OXFORD UNIVERSITY PRESS, 2015
7. Jonathan A.OPHARD, "Cyber warfare and the crime of aggression: the Need for individual Accountability on tomorrow Battlefield, Duke law and technology" DUKE LAW & TECHNOLOGY REVIEW, 2010.
8. Kevin L. Miller, The Kampala Compromise and Cyberattacks: Can there Be an international Crime of Cyber-Aggression? Southern California Interdisciplinary law Journal, 2014.
9. Micheal Gervais, "Cyber Attacks and the law of warfare'', Berkeley Journal of international law, vol:30. Issue.2 article 6, 2012
10. Michael N.Schmidt, the law of cyber warfare, STANFORD LAW & POLICY REVIEW, 2014

11. Marco Roscini, Cyber Operations and the Use of Force in International Law, Oxford University Press, USA, 2014
12. Solce, The Battlefield of Cyberspace: The Inevitable New Military Branch - The Cyber Force, 18 ALB. L.J. SCI. & TECH. 293, 301 (2008).
13. Scott J.Shackelford, Änalogizind Cyber: from Nuclear War to Net war Attacks in international law", university of Cambridge, Dept of politicos and international Studies, Cambridge, 2008
14. Scott Shackelford, From Nuclear War to War: Analogizing Cyber Attacks in International law, Berkley Journal of International Law (BJIL), VOL.25, NO.3, 2009.
15. Thomas Rid and peter McBurney, cyber – weapons, Routledge publisher, The RUSI Journal, February 2012
16. THE WHITE HOUSE, FACT SHEET: U.S. POLICY STANDARDS AND PROCEDURES FOR THE USE OF FORCE IN COUNTERTERRORISM OPERATIONS OUTSIDE THE UNITED STATES AND AREAS OF ACTIVE HOSTILITIES, 2013

قرارات الجمعية العامة للأمم المتحدة

١. قرار الجمعية العامة للأمم المتحدة رقم (A/RES/45/49)
٢. قرار الجمعية العامة للأمم المتحدة رقم (A/RES/56/19)
٣. قرار الجمعية العامة للأمم المتحدة رقم (A/RES/28/32)
٤. قرار الجمعية العامة للأمم المتحدة رقم (A/RES/60/45)
٥. قرار الجمعية العامة للأمم المتحدة رقم (A/RES/62/17)
٦. قرار الجمعية العامة للأمم المتحدة رقم (A/RES/64/25)
٧. قرار الجمعية العامة للأمم المتحدة رقم (A/RES/66/24)
٨. قرار الجمعية العامة للأمم المتحدة رقم (A/RES/66/24)
٩. قرار الجمعية العامة للأمم المتحدة رقم (A/65/201)
١٠. قرار الجمعية العامة للأمم المتحدة رقم (A/68/98)
١١. قرار الجمعية العامة للأمم المتحدة رقم (A/70/174)
١٢. قرار الجمعية العامة للأمم المتحدة رقم (A/69/723)

الوثائق الصادرة عن اللجنة الدولية للصليب الأحمر

- **القانون الدولي الإنساني والعمليات السيبرانية خلال النزاعات المسلحة**، ورقة موقف اللجنة الدولية للصليب الأحمر مقدمة إلى فريق العمل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق

الأمن الدولي، وإلى فريق الخبراء الحكوميين المعني بالارتقاء بسلوك الدول المسؤول في ميدان الفضاء السيبراني. نوفمبر 2019

- **القانون الدولي الإنساني وتحديات النزاعات المسلحة،** اصدار اللجنة الدولية للصليب الأحمر، 2019