الجوانب القانونية للحرب السيبرانية

دراسة في إطار القانون الدولي الإنساني

إعداد

الدكتور/ ناجي محمد أسامة الشاذلي

المدرس بالأكاديمية الحديثة بالمعادي

بريد الكترونى : nagimohammedelshazly@gmail.com

ملخص البحث

يلعب التقدم العلمي دوراً بارزاً في تقدم ورفاهية الشعوب في وقت السلم ووقت الحرب معاً. وتغيرت بدورها أشكال الحروب. فبعد الحروب التقليدية ظهرت في الآفق صور أخرى من الحروب، كان أخرها الحرب السيبرانية، والتي تعتمد على أحدث أنواع التكنولوجيا في المجتمع الافتراضي لتعطيل واختراق الشبكات الإليكترونية في دولة ما وإلحاق ضرر شامل بها سواء على مستوى الأشخاص أو الممتلكات.

ولم يقف القانون الدولي الإنساني والفقه الدولي إزاء هذا التطور مكتوف الأيدي، وإنما تناول السبل القانونية المتاحة أمام الدولة لتقرير المسئولية الدولية والإجراءات التي قد تتخذها للرد والدفاع عن النفس إذا تجاوز النشاط السيبراني حد معين لأي هجوم مسلح.

ويناشد المجتمع الدولي الالتزام بأحكام ميثاق الأمم المتحدة والاستجابة لمبادئه وتطويعها على الفضاء السيبراني.

ويمثل دليل تالين، آليه لتكييف المبادئ الأساسية للقانون الدولي الإنساني للتطبيق في مجال الحرب السيبرانية، وتنظيم قواعد الأمن السيبراني، والقواعد الحاكمة للنزاعات المسلحة السيبرانية.

الكلمات المفتاحية بالبحث:

الحرب السيبرانية ، الفضاء السيبراني ، الاختراقات الإليكترونية ، دليل تالين ، المجتمع الافتراضي ، الأمن السيبراني.

Summary Research

Scientific progress also plays an important role in the progress and prosperity of the peoples. It also plays an important role in the progress and change of images of war. After traditional wars, scientific progress has caused other forms of wars, the most recent of these wars was the cyber war, in which the latest types of technology are used. Despite the novelty of this type of war, it has tremendous results, tension and congestion between peoples. It also used between Russia and United States of America during the US elections, in which the United States of America claimed that Russia used cyber warfare to influence the course of those elections, which were between Trump and Hillary Clinton.

International law intervened to limit and prevent these types of wars in several ways, including the Tallinn guide, which was used to adapt the basic principles of international law to cyber wars, in addition to addressing international jurisprudence to establish controls regarding international responsibility for the damages of cyber war.

Keywords: Cyber war, Cybernetics, E. penetration, Tallinn Manual, Virtual Community.

مقدمة

لازالت الحروب بين الدول – رغم التقدم العلمي في كافة المجالات – هي المسيطرة حتى وقتنا الراهن. وبدلا من استخدام هذا التطور في خدمة البشرية، فقد استعملت في دمارها بما يسمى الحرب السيبرانية حيث تصدر الهجمات السيبرانية عن الدولة أو إحدى مؤسساتها بهدف إضعاف الوظيفة التي تقوم بها أجهزة الحاسوب المستهدفة، كما أن القواعد التي تنظم من خلالها الهجمات هي قواعد القانون الدولي العام[١].

وغني عن البيان أن الباعث على الهجمات السيبرانية يتمثل في إضعاف وتعطيل شبكات الحاسوب في دولة أخرى لتحقيق هدف سياسي أو عسكري، وبالتالي إلحاق ضرر شامل سواء للأشخاص أو الممتلكات في الدولة الأخرى[٢].

تغير مفهوم الردع في الحروب السيبرانية:

توجد صعوبة في تطبيق سياسات الردع بصورتها التقليدية في الحروب السيبرانية، نظرا لاستحالة التيقن من هوية الطرف القائم بالهجوم، ولذلك تلجأ الدول عادة إلى استهداف الطرف الذي تعتقد أنه قام بشن هجمات سيبرانية ضدها، وذلك لتأكد قدرتها على اختراقه، وإمكانية الإضرار به، وذلك لردعه عن محاولة إعادة تنفيذ أي هجمات جديدة، وبالتالي فإن جوهر الردع في المجال السيبراني قد تغير عن مفهومة التقليدي إبان الحرب الباردة، فأصبح الردع هو نتاج امتلاك القدرة على الهجوم، فضلا عن امتلاك القدرة على الدفاع[٣].

---

(١) أحمد عبيس الفتلاوي، الهجمات السيبرانية، مفهومها والمسئولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق المحلي، كلية القانون، جامعة بابل، ٢٠١٥، ص ١٨.

(٢) Michael N. Schmitt (ed.), Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press, 2013, P. 106.

(٣) Tim Stevens, Acyber War of Ideas? Deterrence and Norms in Syber Space, Contemporary Security Policy, Vol. 33, No 1, April 2012, P.150.

ويستفاد مما تقدم أنه لم يعد الردع بالمعايير التقليدية ملائما للتصدي لكافة التهديدات الأمنية غير التقليدية.

ولنا أن نتخيل إقدام دولة ما على هجوم سيبراني لتخترق من خلاله نظام الطيران العسكري أو محطة نووية أو كهربائية أو أنظمة السدود لدى دولة معينة، ففي كل هذه الفروض يتسبب هذا الاختراق بأضرار للدولة "المعتدى عليها" قد تكون خارجة عن نطاق التصور، ولا يعلم مداها إلا الله.

مشكلة البحث:

هناك عدة إشكاليات تتصل بطبيعة الفضاء السيبراني، وهى الإشكاليات التي يمكن الوقوف عليها تفصيلاً على النحو التالي:

(١) تعقد المجال السيبراني: يعتبر المجتمع الدولي الفضاء السيبراني مجالاً للعمليات المعلوماتية، وهو ما يعني بالضرورة تعامله مع بيئة يسهل اختراقها، وتسمح بالانتشار السريع للمعلومات، مما يمثل انعكاسات عميقة على الأمن الدولي، ويغير طبيعة المفاهيم التقليدية للحروب.

(٢) على الرغم من اتفاق العديد من الدول على صياغة سياسة أمنية تمنع الأنشطة السيبرانية الضارة من خلال تحديد العقبات، ووضع إطار لتنظيم الفضاء السيبراني بما يتجاوز النهج الأمني التقليدي، من شأن هذا التعقد

أن يقوض الاستجابة في الوقت المناسب، وستتزايد تلك المشكلة تعقيداً مع توسيع البنية التحتية السيبرانية، وزيادة عدد المستخدمين.

(٣) لازال هناك خلاف بين أعضاء المجتمع الدولي حول تكييف الهجمات السيبرانية، حيث لا يتضح على وجه التحديد متى تتذرع دولة عضو بالمادة (٥١) من ميثاق الأمم المتحدة رداً على هجوم سيبراني وحقها في الدفاع عن النفس إزاء هذا الهجوم من بعض الدول الأعضاء. وكيف تعمل الدولة المعتدى عليها في حالة نشوب حرب سيبرانية إلى جانب استراتيجيات الحرب غير المتماثلة، وكل ذلك يمثل إشكالية على صعيد العمليات المستقبلية.

ولعل أبرز هذه الأسئلة يتمثل في الطرق القانونية المتاحة أمام الدولة للتعامل مع الحالة التي تتعرض فيها إلى حرب سيبرانية منشؤها دولة أخرى، وتكمن أهمية هذه الإشكالية في أن العدوان السيبراني له طبيعة مميزة ويتصف بعدم الحركة (كما في الحروب التقليدية) وهو ما كان خارجاً عن تصور الدول عند توقيعها على الاتفاقيات الدولية خاصة ميثاق الأمم المتحدة.

ويسعى البحث إلى إلقاء الضوء على هذه الإشكاليات المحورية، ابتغاء للوصول إلى تمهيد الطريق للباحثين في مجال القانون الدولي، وإعداد دراسات أكثر تعمقاً في هذا الموضوع.

الهدف من البحث:

يهدف البحث إلى إلقاء الضوء على الطبيعة القانونية للهجمات السيبرانية التي تقع بين الدول من حيث كونها إما جريمة سيبرانية تحكمها اتفاقية بودابست لعام ٢٠٠١ المتعلقة بالجريمة السيبرانية، أم حرب سيبرانية تخضع لأحكام دليل تالين لعام ٢٠١٣ الخاص بقواعد القانون الدولي المطبقة على الحروب السيبرانية التي تتم في إطار نزاع مسلح أو هي جريمة دولية ذات طابع خاص تطبق عليها قواعد القانون الدولي الإنساني، ومن ثم يمكن إثارة المسئولة الدولية للدولة المعتدية أم هذا السلوك يعد صورة من صور العدوان الذي يحظره القانون الدولي.

منهج البحث:

سوف يتبع الباحث في تناول موضوع "الجوانب القانونية للحروب السيبرانية دراسة في إطار القانون الدولي الإنساني". المنهج التحليلي والمنهج المقارن، وذلك بطرح النصوص القانونية الدولية الخاصة باستخدام القوة والدفاع عن النفس ومقارنتها مع المبادئ التي قررها القانون الدولي الإنساني، ومدى انطباقها على الهجمات السيبرانية وكذلك تناول آراء الفقه الدولي وأحكام المحاكم الدولية بهذا الخصوص.

خطة البحث

الجوانب القانونية للحرب السيبرانية

دراسة في إطار القانون الدولي الإنساني

- مبحث تمهيدي: تأثيرات الحرب السيبرانية على العلاقات الدولية
- الفصل الأول: ماهية الحرب السيبرانية وأنواعها
- المبحث الأول: مدلول الحرب السيبرانية
- المبحث الثاني: أنواع الحرب السيبرانية والتمييز بينها وبين غيرها
- الفصل الثاني: الجهود الدولية في تنظيم الحرب السيبرانية وتقرير المسئولية الدولية
- المبحث الأول: دور المنظمات الدولية في تنظيم الحرب السيبرانية
- المبحث الثاني: دليل تالين
- المبحث الثالث: المسئولية الدولية عن أضرار الحرب السيبرانية
- النتائج والتوصيات التي توصل إليها البحث

مبحث تمهيدي

تأثيرات الحرب السيبرانية على العلاقات الدولية

تمهيد:

لا شك أن الصراع في الفضاء السيبراني سوف يُحدث بمرور الوقت تأثيرات على طبيعة العلاقات الدولية، وذلك ناتجا عن عدة عوامل، لعل أبرزها:

١- استخدام الهجمات السيبرانية كأداة جديدة للصراع بين بعض الدول، وصعود أدوار الفاعلين من الدول الصغيرة وغير الدول على الساحة الدولية.

٢- حدوث توتر واحتقان دبلوماسي ينتج عن اتهام دولة لأخرى بالتدخل في شئونها الداخلية عبر الفضاء الالكتروني.

٣- إطلاق سباق تسلح سيبراني بين بعض الدول يتم فيها استخدام وحدات هجوم سيبرانية نظامية أو غير نظامية للدفاع والردع، وأيضاً الرد الدبلوماسي.

وكشف التوظيف العالمي لشبكات الانترنت عن الوجه الحقيقي لممارسات بعض الفاعلين من غير الدول في مجتمع العالم الافتراضي[١]، حيث خضع إلى

(١) يرجع مفهوم العالم الافتراضي إلى هاورد رينجولد Rhingold الذي ألف الكتاب الأول والرائد في هذا السياق بعنوان "المجتمع الافتراضي Virual Community"، والذي عرفه بأنه "تجمعات اجتماعية تشكلت من أماكن متفرقة في أنحاء العالم، يتقاربون ويتواصلون فيما بينهم عبر شاشات الكمبيوتر، والبريد الإلكتروني، ويتبادلون المعارف فيما بينهم ويكونون صداقات".

عمليات أيديولوجية غايتها تكريس هيمنة بعض الدول الأطراف على آخرين، مما اضطر بعض المؤسسات العالمية إلى تطوير مواثيق واتفاقيات أضحت تشكل بدورها نوعاً جديداً من القواعد الخاصة بها.

والحرب في الوقت الراهن هي حرب من نوع خاص، وذات تأثيرات متنوعة على الخصم في أسرع وقت ممكن وباقل جهد وتكلفة، وبدون إراقة دماء أو مواجهة مباشرة مع الخصم، كما أن أسلحة هذه الحرب غير تقليدية، كما كانت في حروب الأجيال السابقة (كالطائرات والمدافع والصواريخ والأسلحة الكيميائية أو النووية) بل أسلحة ترتبط باستخدام التكنولوجيا في جميع مراحل عمليات الهجوم والدفاع والحماية والوقاية[١].

كان لثورة المعلومات والاتصالات انعكاساتها في ربط المصالح القومية للدول بالبنية التحتية لها، ومع زيادة الترابط بين الواقع الافتراضي والواقع الحركي للنظام الدولي، ودفع الفواعل سواء من الدول أو غيرها ممن يمتلكون القوة للتوجه نحو الاستقطاب السيبراني.

ولا ريب في أن القوة السيبرانية تمثل سلاحا ذو حدين، حيث يمكن استخدامها للمصالح القومية للدول أو لهلاكها، فطبيعة الأسلحة المتطورة للقوة السيبرانية وأثرها يتوقف على الهدف الذي تبتغيه كل دولة من وراء ذلك الاستخدام.

للمزيد حول العالم الافتراضي راجع:

د. عبد العال الديربي، ملامح شبكات التواصل الاجتماعي: الخصائص والأنماط / مجلة رؤى مصرية، السنة الثالثة، العدد (٣١)، أغسطس ٢٠١٧، ص ٤.

(١) محمود الرشيدي، حرب المعلومات: حروب ذكية بأسلحة غير مرئية، مجلة رؤى مصرية، مرجع سابق، ص٢٢.

فالفيروسات التي تصيب الحواسب المرتبطة بشبكات الانترنت لها آثار تدميرية تسبب خسائر اقتصادية هائلة عند شن إحدى الفواعل الدولية هجوماً سيبرانياً على بنية تحتية حيوية لدولة ما.

(١) أثر السيبرانية على تطوير مفهوم القوة:

تعد القوة هي المحدد الرئيس لأداء الدولة ونفوذها على الصعيد الدولي، حيث ترسم دورها في الوقت الحالي وفي المستقبل.

ومنذ نهاية الحرب الباردة بين الولايات المتحدة الأمريكية وروسيا (الاتحاد السوفيتي سابقا) في مطلع تسعينات القرن المنصرم، شهد مفهوم القوة جملة تغييرات لمواكبة التطور الحادث في حقل العلاقات الدولية، ويمكن التفرقة بين مستويين للتغيير الذي طرأ على مفهوم القوة، مستوى خاص بالفاعل الذي يمتلك القوة، خاصة مع امتلاك فاعلين من غير الدول[١] بعض مصادر القوة. وأما المستوى الآخر، فيتعلق بالعناصر المكونة للقوة والأشكال المختلفة التي تتخذها هذه القوة[٢]. ولم يعد مستساغاً أن تكون القوة العسكرية التقليدية فقط هي العنصر الحاكم في العلاقات الدولية في ظل التطور العلمي والتكنولوجي، وطغيان استخدام الإنترنت في كافة مناحي الحياة. وبدأ الحديث عن تطور الأسلحة السيبرانية ونشر منظومات الأقمار الصناعية، كما دخلت الحروب السيبرانية حيزها بين الدول مثل الولايات المتحدة وروسيا والصين وكوريا الشمالية وإيران وأضحى الفضاء السيبراني ساحة قتال، برزت فيه العديد من الأنماط الجديدة والعديدة على كافة الأصعدة للاستخدامات العسكرية، وبات جلياً أن من يمتلك آليات

(١) مثل المنظمات الحكومية وغير الحكومية والجماعات والميلشيات والأفراد.

(٢) تغريد صفاء. لبنى خميس مهدي، أثر السيبرانية في تطور القوة، مجلة حمورابي، العدد (٣٣) ، (٣٤) – السنة الثامنة – شتاء، ربيع ٢٠٢٠، ص ١٤٥.

توظيف القوة السيبرانية يصبح أكثر قدرة على تحقيق أهدافه والتأثير في المجتمع الدولي.

(٢) دور السيبرانية في تصعيد الصراعات بين الدول الكبرى:

يتصاعد التنافس الفضائي والسيبراني بين موسكو وواشنطن في ضوء اتجاه القوى الكبرى إلى عسكرة الفضاء وجعله ساحة النزال المستقبلية بينهما، ومجال استعراض القوة وفرض الهيمنة، وذلك مع إعلان الرئيس الأمريكي "ترامب" في ١٨ يونيو ٢٠١٨ إنشاء قوات فضائية كفرع سادس ضمن القوات المسلحة للولايات المتحدة مشددا على أن مجرد الوجود في المجال الفضائي لا يكفي لحماية أمريكا من التحديات، بل تحتاج إلى الهيمنة على الفضاء، وباعتبار ذلك الأمر مسألة أمن قومي، وستكون هذه بمثابة قوة فضاء بلا حدود.

ومن ناحية أخرى تزداد حدة المواجهة السيبرانية بين موسكو وواشنطن في ضوء الاتهامات المتبادلة بتوجيه هجمات إلكترونية على أهداف حيوية، كان من أبرزها اتهام روسيا بالتدخل في الانتخابات الأمريكية لعام ٢٠١٦، ومحاولة الهجوم السيبراني[١] على منظمة حظر الأسلحة الكيماوية، واتهامات وزارة العدل الأمريكية

---

(١) يعرف البعض الهجمات السيبرانية على أنها (فعلاً يقوض من قدرات ووظائف شبكة الكمبيوتر لغرض قومي أو سياسي من خلال استغلال نقطة ضعف معينة تمكن المهاجم من التلاعب بالنظام).

راجع :

“Cyber – Attacks and the use of force : Malthew C. Waxman the yale Journal of International, Back to the future of Article 2 (4)”, Vol. 36, 2011, P. 423.

ضد سبعة من عملاء الاستخبارات الروسية بالقرصنة على منظمات مكافحة المنشطات الدولية. ونفت روسيا في أكثر من مناسبة هذه الاتهامات.

ولا شك في تسابق الدول الكبرى لشن هجمات سيبرانية، وأن الولايات المتحدة تحتل المركز الأول التي تشكل مصدرا للتهديدات السيبرانية، ومواجهة أي هجمات محتملة من الطرف الآخر المعتدي، ولهذا تعزز الولايات المتحدة دفاعاتها السيبرانية حيث أنشأت القيادة الإلكترونية الأمريكية (مجموعة عمل خاصة لمواجهة أنشطة روسيا في الفضاء السيبراني)[١].

الحروب السيبرانية والجماعات الإرهابية:

نجحت العديد من التنظيمات الإرهابية، في السنوات الأخيرة في استغلال شبكات الإنترنت للترويج للأفكار المتطرفة، لأنها تمثل وسيلة لجذب أكبر عدد من الأفراد، وتمنح قدرا كبيرا من السرية، وسيبقى المحتوى الالكتروني هو القضية الأكثر أهمية نظرا لوضوح تكثيف توظيف الجماعات المتطرفة لتقنيات الإنترنت الاتصالية والبرمجية ومن ناحية أخرى توفر مواقع الإنترنت إمكانية تنسيق وترتيب وشن عمليات إرهابية دون تكلفة كبيرة، وفي الوقت نفسه إحداث خسائر كبرى لدى خصوم هذه الجماعات المتطرفة[٢].

ومع هذا الانتشار، ظهرت في الأفق إجراءات مضادة تبنتها الولايات المتحدة الأمريكية، والاتحاد الأوروبي بالتنسيق مع مؤسسي المواقع على شبكة الانترنت والشركات الكبرى العاملة في هذا المجال لشن حملات لمواجهة انتشار وتمدد تلك

(١) د. نورهان الشيخ، روسيا وإعادة التعددية القطبية، مجلة رؤى مصرية، السنة الخامسة، العدد (٥٨)، نوفمبر ٢٠١٩، ص ١٠.

(٢) حسين علي، شبكات التواصل الاجتماعي والتنظيمات الإرهابية، مجلة رؤى مصرية، السنة الثالثة، العدد (٣١)، أغسطس ٢٠١٧، ص ٢٥ ، ٢٦.

التنظيمات الكترونياً وكانت أولى هذه الإجراءات، القيام بإغلاق أكثر من نصف الحسابات التابعة لتنظيم داعش، كما أعلنت الولايات المتحدة الأمريكية في بداية عام ٢٠١٦ عن إنشاء جهاز "فرقة محاربة التطرف المرتبط بالعنف في الولايات المتحدة، وتم إنشاء مركز هداية لمكافحة داعش إلكترونياً وذلك في أبو ظبي بدولة الإمارات العربية المتحدة[١].

(١) سامي الريامي، جيش داعش الالكتروني، موقع الإمارات اليوم، ١٢ يوليو ٢٠١٥.

الفصل الأول
ماهية الحرب السيبرانية وأنواعها

تمهيد وتقسيم:

وسع البعض من تعريف الحرب السيبرانية بأنها "استخدام القدرات الشبكية للدولة أو الفاعلين من غير الدول لتعطيل أو حرمان أو تقليل كفاءة أو التحكم أو حتى تدمير البيانات والمعلومات الموجودة في أجهزة أو شبكات أجهزة الحاسبات للفاعلين الآخرين أو حتى تدمير تلك الأجهزة والشبكات ذاتها".(١)

فالحرب السيبرانية هي "الهجمات التي تطلقها الدول أو مجموعات من الدول، أو الجماعات السياسية المنظمة، ضد البنية التحتية السيبرانية لدولة أخرى، وذلك بالتزامن مع هجمة عسكرية".(٢)

ولعل هذا الاختلاف في تعريف الحرب السيبرانية يرجع إلى تنوع أشكال هذه الحرب، وارتباطها بالجرائم الإلكترونية والهجمات السيبرانية والأمن السيبراني والفضاء السيبراني.

وسوف نلقي الضوء على الموضوعات السابقة من خلال مبحثين:

---

(١) (craig B. Greathouse, Cyber War and Strategic thought: Do the classic theorists still matter? In J.F Kremer and B. Muller, Eds., Cyberspace and international Relations, (Verlag Berlin Heidelberg: Springer), 2014, P. 24.

(٢) (keir Giles and William Hagestad li, “Divided by Acommon Language: cyber Definitions in Chinese, Russian and English” in K.Podins, J. Stinissen and M. Maybaum (Eds.), 2013 5th International Conference on cyber conflict, Tallinn, Nato Publications, 2013, PP. 4 – 5.

المبحث الأول: مفهوم الحرب السيبرانية

المبحث الثاني: أنواع الحرب السيبرانية والتمييز بينها وبين غيرها

المبحث الأول

مفهوم الحرب السيبرانية

تمهيد:

بدأت الإرهاصات الأولى لإطلاق مفهوم الحرب السيبرانية عام ١٩٩٣، عندما كتب John Arquilla and David Ranfeldt مقالا تحت عنوان الحرب السيبرانية قادمة، والتي توقع فيها العديد من التحديات التي سيواجهها الأمن الغربي خلال السنوات القادمة ومدى تغير المفاهيم المرتبطة بالفضاء السيبراني ودورها في إحداث تغييرات جذرية بجيوش الدول وآليات عملها أو ما يعرف بالضربات من غير هجوم Hitting Without Holding وقد يبدو من الأهمية بمكان تناول مفهوم الأمن السيبراني، والفضاء السيبراني كمدخل أساسي لدراسة الحرب السيبرانية[1].

أولاً: مفهوم السيبرانية

ثانياً: مفهوم الأمن السيبراني

ثالثاً: مفهوم الفضاء السيبراني

(1) السيبرانية في اللغة: إن كلمة سيبرانية أو سايبر أو سيبراني ترجمة حرفية (Cyber) والمشتقة من (Cybernetics) وقد استخدم هذا المصطلح أكاديميا من حلال كتاب "علم التحكم الآلي" لعالم الرياضيات الأمريكي نوربرت وينر عام ١٩٤٨ وذلك للإشارة إلى آليات التنظيم الذاتي. كما ورد معنى Cybernetics بأنه علم التحكم الأوتوماتيكي". وتعدد استخدام المصطلح في العديد من الوثائق الصادرة عن الأمم المتحدة، واللجنة الدولية للصليب الأحمر بمعنى علم الضبط أو التحكم الافتراضي عن طريق الإنترنت.

أولاً – مفهوم السيبرانية:

اشتق مصطلح السيبرانية Cybernetic من المصطلح الإغريقي Kybernetes ويعني الطيار أو قائد الدفة أو الحاكم، ويفيد الاشتقاق الحديث بأن كلمة سيبرانية تتضمن آليات تعقيب تتيح وظائف القيادة والتحكم في الأنظمة المغلقة[١].

والسيبرانية مأخوذة من كلمة (سيبر Cyber) وتعني صفة لأي شيء مرتبط بثقافة الحواسيب أو تقنية المعلومات أو الواقع الافتراضي[٢].

ومصطلح (Cyber) الإنجليزي متأصل في كثير من الكلمات التي يشيع استخدامها في مجال تكنولوجيات المعلومات والاتصالات مثل الفضاء السيبراني Cyber Space والخيال العلمي Cyber Punk [٣].

ويشير قاموس "المورد" إلى السيبرانية بأنها علم الضبط ومصدرها (Cybernetics) وهو مصدر يتطابق مع مفهوم الهجمات السيبرانية أي ضبط الأشياء عن بعد والسيطرة عليها[٤].

أما قاموس مصطلحات الأمن المعلوماتي فعرف السيبرانية بأنها هجوم عبر الفضاء الإلكتروني يهدف إلى السيطرة على مواقع الكترونية أو بنية محمية الكترونيا لتعطيلها أو تدميرها أو الإضرار بها.

---

(١) بيتر بي سيل، الكون الرقمي الثورة العالمية في الاتصالات، ترجمة ضياء وارد، مؤسسة هنداوي CIC، إنجلترا، ٢٠١٧، ص ٢٢.

(٢) صالح بن علي بن عبد الرحمن، الأمن الرقمي وحماية المستخدم من مخاطر الانترنت، رؤية ٢٠٣٠، هيئة الاتصالات بالسعودية، ٢٠١٧، ص ٦.

(٣) بيتر بي سيل، الكون الرقمي الثورة العالمية في الاتصالات، مرجع سابق، ص ٢٢.

(٤) منير البعلبكي، قاموس المورد دار العلم للملايين، بيروت، ٢٠٠٤، ص ٢٤٣.

وعرف قاموس المصطلحات العسكرية الأمريكية السيبرانية بأنها "أي فعل يُستَخدَم عن طريق شبكات إلكترونية بهدف السيطرة أو التعطيل لبرامج إلكترونية أخرى"[١].

ويعرفها البعض بأنها (مفهوم يشير إلى أي نزاع يحدث في الفضاء الإليكتروني ويكون له طابع دولي)[٢].

الحرب السيبرانية هي "استخدام الطيف الإلكتروني أو الكهرومغناطيسي لتخزين وتعديل وتبادل البيانات وجها لوجه مع أنظمة تحكم في بنىً تحتية مرتبطة بها".

أو هي "مجموعة من الإجراءات التي تتخذها الدولة للهجوم على نظم المعلومات بهدف الإضرار بها، وفي الوقت نفسه للدفاع عن نظم المعلومات الخاصة بالدولة المهاجمة".

وعرفها البعض[٣] بأنها "أعمال تقوم بها دولة ما تحاول من خلالها اختراق أجهزة الكمبيوتر والشبكات التابعة لدولة أخرى بهدف تحقيق أضرار بالغة أو تعطيلها".

---

(١) أحمد عبيس الفتلاوي، الهجمات السيبرانية مفهومها والمسئولية الدولية الناتجة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية والسياسية، المجلد ٨، العدد ٤، جامعة بابل، ٢٠١٦، ص ٦١٣.

(٢) (A look, the challenge of unrestricted warfare, Kevin Coleman.com. direction smag. www//:http, Back and look Ahead Articles.

(٣) (The spectrum of conflict from Hacking, Bonnie N. Adkkins A, to Information Warfare : what is Law Enforcement's Role? Research Report submitted to the faculty in partial fuldillment of the Alabama, April, Maxx well Air force Base, Graduation, Requirements, 2001.

ويرى الأستاذ (Marco Roscini) أن الحرب السيبرانية عبارة عن "تطويع الإمكانيات الإلكترونية العسكرية لأجل التأثير في مواقع إلكترونية أخرى وتعطيلها أو تدميرها سواء أكانت خدمات عسكرية أو مدنية".

وهناك من يذهب إلى اعتبار الحرب السيبرانية امتداد للحروب التقليدية والمادية، إذ يتألف جندها من المدنيين والعسكريين في آن واحد، كما أنها حرب عقول بالدرجة الأولى، لكونها تستهدف في المقام الأول تدمير البنية العلمية والمعلوماتية للهدف، وتأخذ اشكالاً عدة. كشكل الاتصالات بين الجيوش وقياداتها، واضعاف شبكات النقل والإمدادات اللوجستية، وضرب الاقتصاد، والعبث بالمحتوى التقني والرقمي وغيرها[١].

ويرجع البعض تعدد التعريفات المطروحة للحرب السيبرانية دون وجود تعريف جامع لها نتيجة لحداثة نشأتها، وعدم وجود إطار يحكم الأنشطة التي تتم ممارستها من خلالها. ويبدو الاختلاف في أغلب الأحيان حول محورين أساسيين:

المحور الأول: اقتصار الحرب السيبرانية على الدول فحسب، من حيث كون الأخيرة هي الفاعل الرئيسي في هذه الحرب، بينما ترى وجهات نظر أخرى ضرورة تضمين الفاعلين من غير الدول في تعريف تلك الحرب نتيجة لدورهم في إطلاق الهجمات السيبرانية سواء بشكل منفرد أو بالنيابة عن الدول.

ووفقا لما تقدم، فإن الحرب السيبرانية هي "إجراء من دولة ضد دولة أخرى بما يعادل الهجوم المسلح أو استخدام القوة في الفضاء السيبراني، والذي قد يؤدي إلى رد فعل عسكري باستخدام القوة التقليدية المناسبة".

(١) أحمد عبيس الفتلاوي، الهجمات السيبرانية، مرجع سابق، ص ٥ ، ٦.

أما المحور الثاني فيظهر بسبب طبيعة الأضرار والآثار التي تخلفها هذه النوعية من الحروب؛ وذلك نظرا لحجم الضرر وطبيعة الآثار المتعددة المباشرة وغير المباشرة على الدولة المعتدى عليها.

ثانياً – مفهوم الأمن السيبراني:

يقصد به أمن الشبكات والأنظمة المعلوماتية، والبيانات والمعلومات والأجهزة المتصلة بالإنترنت[١].

فالاعتماد على المعلومة كحقيقة لا لبس فيها تفرض اعتمادا أكثر على الأنظمة الإلكترونية التي تعالجها والحديث عن الحروب السيبرانية يستدعي تعريف الخطر، أي التهديد الذي يتعرض له نظام المعلومات في دولة ما، إضافة إلى نقاط الضعف، أو الثغرات التي تعتريه، ومن ثم الإجراءات الواجب اتخاذها لدفع خطر الهجمات السيبرانية[٢].

فالأمن السيبراني – كما يعرفه البعض – هو النشاط الذي يؤمن حماية الموارد البشرية والمالية المرتبطة بتقنيات الاتصالات والمعلومات، ويضمن إمكانات الحد من الخسائر والأضرار التي تترتب في حال تحقق المخاطر والتهديدات، كما يتيح إعادة الوضع إلى ما كان عليه بأسرع وقت ممكن، بحيث لا تتوقف عجلة الإنتاج، وبحيث لا تتحول الأضرار إلى خسائر دائمة[٣].

---

(١) حنين جميل أبو حسين، الإطار القانوني لخدمات الأمن السيبراني، رسالة ماجستير، كلية الحقوق، جامعة الشرق الأوسط، عمان، الأردن، ٢٠٢١، ص ١٨.

(٢) هشام محمد خليل رستم، الجوانب الإجرامية للجوانب المعلوماتية، مجلة الأمن والقانون، أكاديمية شرطة دبي، العدد (٢)، ٢٠١٧، ص ٢٠.

(٣) سعيد عبد اللطيف حسن، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت، دار النهضة العربية، ٢٠١٧، ص ٢١٤.

العلاقة بين الأمن السيبراني والأمن القومي:

إن الناظر بعينٍ ثاقبة فيما يدور حولنا، يلاحظ الخشية التي تبديها معظم الدول حاليا، من تعرض أمنها القومي، نتيجة الاعتداءات السيبرانية، لاسيما وأن تقنية المعلومات والاتصالات، قد رفعت منسوب الخطر عبر إتاحتها مصادر جديدة متشعبة، ومتعددة، وإمكانات هائلة لتحقيقه، مقابل انخفاض نسبة المخاطر وإمكانية كشفها كدولة معتدية، وهذا ما دفع العديد من الدول إلى القيام بالتنسيق بين إدارات الأمن والاقتصاد والمعلومات والمرافق العسكرية. إضافة إلى الترابط بين الأمن السيبراني والأمن القومي، فالتقنيات التي وسعت الآفاق، وامتدت إلى كافة مناحي الحياة، وإلى كل أرجاء العالم، باتت تهدد الهوية الوطنية والقومية، حيث تبدو الهوية وكأنها خاضعة لعملية إعادة تشكيل من خلال تكنولوجيا المعلومات وحرص الغالبية العظمى من الأفراد وإقبالهم على تلقي المعلومات من خلالها. إن التهديد الآتي من الأمن السيبراني، من أخطر المسائل التي تطرح على المستويين القومي والاقتصادي.

وفي هذا الإطار، نبهت توصية المجلس الأوروبي الصادرة عام ٢٠٠٢ بأن الأمن القومي يشمل كافة الإجراءات القانونية والإدارية والعسكرية والأمنية التي تهدف إلى حماية بلد معين ضد أي نوع من التهديدات والأخطار التي يمكن أن تعرض سلامة مواطنيها أو أراضيها أو سيادتها بما فيها سلامة مرافقها والبنية التحتية للاتصالات والمعلومات.[١]

(١) دليل الأمن السيبراني للبلدان النامية الصادر عن الاتحاد الدولي للاتصالات، ٢٠١٠، ص ٤٤١.

ثالثاً – مفهوم الفضاء السيبراني:

تعريف الفضاء السيبراني:

يقرر الاتحاد الدولي للاتصالات والوكالة المتحدة المتخصصة في مجال تكنولوجيا المعلومات والاتصالات بأن الفضاء السيبراني هو "الحيز المادي وغير المادي الذي ينشأ أو يتكون من جزء أو من كل العناصر التالية: حواسيب أجهزة ممكنة وشيكات ومعلومات محوسبة وبرامج ومضامين ومعطيات مرور ورقابة والذين يستخدمون كل ذلك"(١).

والفضاء السيبراني هو مجال عالمي داخل بيئة المعلومات تم تشكيلة من خلال استخدام الالكترونيات واستغلال المعلومات عبر الشبكات المترابطة والمرتبطة باستخدام تكنولوجيا المعلومات والاتصالات(٢).

(١) خالد وليد محمود، الهجمات عبر الإنترنت، ساحة الصراع الإلكتروني الجديدة، سلسلة دراسات ودراسة السياسات، المركز العربي للأبحاث، قطر، ٢٠١٣، ص ٤.

(٢) Daniel T-Kuehl, From cyber space to cyber power, defining the problem in cyber power and national security, washing ton, D.C. national Defence up, 2009, P. 12.

المبحث الثاني

أنواع الحرب السيبرانية والتمييز بينها وبين غيرها

تمهيد:

إن الحروب التقليدية لها عدة أشكال، فإن الحروب السيبرانية لا تقتصر على نوع واحد كذلك. ويرجع ذلك عادة إلى الهدف من وراء هذه الحرب، وما إذا كان الهدف من وراء القيام بها سياسيا أم عسكريا أم معلوماتيا أم اقتصاديا.

ومن ناحية أخرى لابد أن نميز بين الحرب السيبرانية والهجمات السيبرانية والجرائم السيبرانية، لتوضيح أيٍّ من هذه الأشكال يخضع لأحكام القانون الدولي الإنساني.

وسوف نتناول كافة هذه الأمور على النحو التالي:

أولا: أنواع الحروب السيبرانية

ثانيا: التمييز بين الحرب السيبرانية عن غيرها

أولا – أنواع الحروب السيبرانية:

تتعدد وتتنوع الحروب السيبرانية بحسب أهدافها وتأثيراتها، ولكنها لا تخرج عما يأتي:

١) حرب سيبرانية هجومية:

تستهدف هذه النوعية من الحروب إفساد وتخريب أو التشكيك في دقة المعلومات ومن أمثلة ذلك عمليات التنصت الإلكتروني، والقرصنة الالكترونية والهجمات الإرهابية الإلكترونية، ومن أهم أسلحة هذه الحرب الفيروسات بأنواعها Logic Doors و Back Doors وعمليات الـ Chipping وكذلك الاختراقات الالكترونية (E. Penitration).

٢) حرب سيبرانية دفاعية:

وتشمل استخدام كافة التقنيات، والوسائل التكنولوجية الوقائية لتجنب أو التقليل من مخاطر وتهديد الحروب السيبرانية الهجومية من الدول أو (الفاعلين من غير الدول) المعادية.

فالحروب السيبرانية حروب حقيقية مسرحها المباشر الشبكات والتقنيات الرقمية، وأهدافها الأساسية نفسية معنوية للتأثير على الخصوم في كافة المجالات[١].

([١]) تعرضت أكثر من مائتي دولة حول العالم لهجمات سيبرانية معقدة اطلق عليها هجمات الفدية الخبيثة، حيث تم خلالها حدوث حالات ابتزاز مالي وتشفير ملفات إلكترونية على أجهزة حاسبات مؤسسات ومرافق هذه الدول وتسبب ذلك في أضرار مادية ومعنوية جسيمة لهذه الدول، وقد نُسب تنفيذها إلى مجموعة هاكرز، كما كانت هناك هجمات بيتيا حيث لم تقتصر على تشفير الملفات، بل قامت بتشفير وحدة (MRC) بالهارد ديسك كله، واتُّهِمت أوكرانيا روسيا بأنها المتسببة في هجمات بيتيا الأخيرة.

ثانيا – التمييز بين الحرب السيبرانية عن غيرها:

لبيان الحرب السيبرانية بشكل جلي، ينبغي التمييز بينها وبين الهجمات السيبرانية، والجرائم السيبرانية، وذلك على النحو التالي:

١) التمييز بين الحرب السيبرانية والهجمات السيبرانية:

الحرب السيبرانية هي نوع من الهجمات السيبرانية التي تحدث أثناء نزاع مسلح حركي أو التي تنتج آثار مادية تشبه وتعادل في آثارها الهجمات المسلحة التقليدية، بينما الهجمات السيبرانية هي كل نشاط سيبراني ضار بالدول الأخرى سواء كان في وقت السلم أو في سياق نزاع مسلح حركي وسواء نتجت عنه آثار مادية جسيمة في الأرواح أو الأعيان المادية أو تشويش أنظمة الكمبيوتر بها، ما دام كان ذلك لأغراض عسكرية وأمنية.[١]

وغني عن البيان أن الحرب السيبرانية يمكن أن تشكل هجوما وجرائم سيبرانية في ذات الوقت[٢].

حاصل القول: إن الهجمات السيبرانية هي عمليات تقوم بها الدولة أو جهات حكومية أو غير حكومية سواء كانت هجومية أو دفاعية، تهدف من ورائها إلى إحداث إصابة أو وفاة الأشخاص أو الأضرار وتدمير الأعيان لخصم معين، وذلك عن طريق

للمزيد حول هذا:

اللواء محمود الرشيدي، حروب المعلومات – حروب ذكية بأسلحة غير مرئية، مرجع سابق ص٢٤.

(١) أحمد عبيس نعمه الفتلاوي، الهجمات السيبرانية (دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر)

(٢) زهراء عماد محمد كلنتر، المسئولية الدولية الناشئة عن الهجمات السيبرانية، رسالة ماجستير، كلية القانون، جامعة الكوفة، ٢٠١٦، ص ١٩ ، ٢٠.

الدخول قصدا وبطريقة غير مشروعة إلى منظومة معلوماتية أو موقع إلكتروني على الإنترنت، دون أن يكون لها الحق في القيام بذلك[١]. أما الحرب السيبرانية وتبعا للظروف نزاعا مسلحا وفقا لقواعد القانون الدولي الإنساني[٢].

وقد يحدث تداخل بين الهجمات والحروب السيبرانية كما حدث لدولة إستونيا في ٢٧ أبريل ٢٠٠٧ من هجوم سيبراني شامل استهدف المواقع الإلكترونية الحكومية والبرلمان وحسابات البنوك والصحف، وتسبب هذا الهجوم في عزل الدولة عن العالم وانقطاع الخدمات عن تلك المواقع.

٢) التمييز بين الجرائم السيبرانية والحروب السيبراني:

ذهب مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين المنعقد في فيينا عام ٢٠٠٠ إلى تعريف الجريمة السيبرانية بانها "أي جريمة يمكن ارتكابها على نظام حاسوبي أو شبكة حاسوبية، وتشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إليكترونية".[٣]

والجريمة السيبرانية هي "كل فعل أو امتناع عن فعل باستعمال نظام معلوماتي معين للإضرار بمصلحة أو حق يحميه القانون من خلال جزاء جنائي، سواء كانت هذه المصالح أو الحقوق المحمية جنائياً تمثل نماذج معلوماتية مستحدثة او كانت تدخل

(١) نور أمير الموصلي، الهجمات السيبرانية في ضوء القانون الدولي الإنساني، رسالة ماجستير، الجامعة الافتراضية السورية، سوريا، ٢٠٢١، ص ١٠.

(٢) Philip Levitz, the law of cyber – attack, 2012, Vol, 100, Issue, 4, P. 833.

(٣) مشار إليه لدى د. أميرة عبد العظيم عبد الجواد، المخاطر السيبرانية وسبل مواجهتها في القانوون الدولي العام، مجلة الشريعة والقانون، العدد (٣٥)، الجزء الثالث، ٢٠٢٠، ص ٣٩٣.

في نطاق المصالح أو الحقوق المحمية جنائياً فيها سبق بالطرق التقليدية وسواء كان الاعتداء واقعاً داخل حدود الدولة أو يتجاوزها إلى مجموعة من الدول".[١]

إن القاسم المشترك بين الجرائم السيبرانية والتي تعني ارتكاب أفراد أو جهة غير حكومية عملا غير قانوني عن طريق الانترنت، وبين الحروب السيبرانية متمثلة في مجالها الذي يحدث فيه أي الفضاء السيبراني، إلا أنهما يختلفان في الآتي:

أ- من حيث الأشخاص، فغالبا ما يكون مرتكبي الجرائم السيبرانية هم الأفراد وتوجه ضد مؤسسات مالية أو شركات أو حتى أفراد. وسواء تمت داخل أو خارج إقليم الدولة بخلاف الحروب السيبرانية والتي تتم من قبل دول أو كيانات حكومية أو فاعلين من غير الدول ضد دولة أخرى[٢].

ب- من حيث الأهداف، ترمي الجرائم السيبرانية إلى إثبات مهارة الفاعل تقنيا وقدرته على اختراق أجهزة الكمبيوتر أو تحقيق مكاسب مالية شخصية أو سرقة الملكية الفكرية عن طريق شبكة الإنترنت أو التسلل إلى أنظمة البنوك والتلاعب بأرقام الحسابات وتحويل الأموال دون الحاجة إلى تدمير أو تعطيل شبكة المعلومات لدى الجهة المعتدى عليها، وتكون مجرمة بموجب القانون الوطني. بينما الحرب

(١) د. هلالي عبد اللاه أحمد، جرائم الحاسب والإنترنت بين التجريم الجنائي وآليات المواجهة، دار النهضة العربية، ١٩٩٧، ص ١١٧.

(٢) د. طارق جمعة، تحديات إثبات الجرائم الالكترونية عبر وسائل التواصل الاجتماعي، مجلة رؤى مصرية، السنة الثالثة، العدد (٣١)، أغسطس ٢٠١٧، ص ٣٤.

السيبرانية تهدف إلى المساس بالأمن القومي والسياسي للدولة المعتدى عليها، وذلك من خلال تخريب شبكة المعلومات التي تتحكم في البنية التحتية للدولة وتدميرها، بقصد زعزعة النظام فيها وتحقيق مآرب أمنية أو عسكرية أو سياسية[١].

(١) زهراء عماد محمد كلنتر، المسئولية الدولية الناشئة عن الهجمات السيبرانية، مرجع سابق، ص ١٧.

الفصل الثاني
الجهود الدولية في تنظيم الحرب السيبرانية

تمهيد:

يثور التساؤل حول مدى اعتبار الحرب السيبرانية من الحروب التقليدية التي تنطوي على استخدام القوة، ومن ثم إمكانية تطبيق معايير القانون الدولي عليها، أم أنها مجرد صراعات في الفضاء السيبراني فحسب، ولم تبلغ أقصى درجة لها على نحو يعد إعلانا للحرب؟

يقرر البعض أن الجهود المبذولة من الدول والمنظمات الدولية تتركز على تطوير قواعد القانون الدولي، ومن الممكن أن تُسهم في احتواء الهجمات السيبرانية وتضمينها من بين الأعمال العدائية التي تنطوي على استعمال القوة، ووضع المعايير وتدابير لبناء الثقة للتطبيق على المستوى الدولي. وترتب على هذه الجهود ظهور ما يعرف بنظام الأمن السيبراني Cybersecurity Regime، ويشمل كافة القواعد والمؤسسات والإجراءات الرسمية وغير الرسمية، والتي تعمل على تطوير القواعد الحاكمة للأنشطة السيبرانية، كما أنها تشمل المنظمات العالمية والإقليمية التي تلعب دوراً بارزاً في صياغة سياسات الأمن والدفاع السيبراني وحقوق الإنسان وحماية الملكية الفكرية.

وسوف نتطرق إلى جهود المجتمع الدولي في تنظيم الحرب السيبرانية من خلال دور المنظمات الدولية (ميثاق الأمم المتحدة – الجهود الدبلوماسية)، ودليل تالين، ثم نتناول تقرير المسئولية الدولية عن أضرار الحرب السيبرانية وذلك على النحو التالي:

المبحث الأول: دور المنظمات الدولية في الحرب السيبرانية

المبحث الثاني: دليل تالين

المبحث الثالث: المسئولية الدولية عن أضرار الحرب السيبرانية

المبحث الأول

دور المنظمات الدولية في تنظيم الحرب السيبرانية

تمهيد:

لعبت الأمم المتحدة دورا بناءً في الدبلوماسية السيبرانية، حيث أنشأت فريقا من الخبراء الحكوميين "Group Of Government Experts" لتحقيق التعاون الدولي في دراسة قضايا الأمن السيبراني وتقديم توصيات بشأن التدابير الرامية إلى تقليل التهديدات والمخاطر السيبرانية وزيادة الاستقرار.

وفي عام ٢٠١٣ نادى فريق الخبراء الحكوميين من خلال الجهود الدبلوماسية على أن مبدأ السيادة الوطنية ينطبق على الفضاء السيبراني بدرجة انطباقه على الأرض نفسها، كما تم الاتفاق على قائمة مطولة من قواعد وإجراءات بناء الثقة في الفضاء السيبراني(١).

- **الدبلوماسية السيبرانية:**

غالبا ما تسفر الهجمات السيبرانية عن إحداث نوع من التوتر والاحتقان في العلاقات الدبلوماسية بين الدول، ولعل أهم هذه الهجمات هو تصاعد ذروة الحرب السيبرانية بين كل من روسيا والولايات المتحدة الأمريكية على خلفية اتهامات وُجهت لروسيا

(١) (James A. Lewis, Statement Before the House Committee on Foreign Affairs, Cyber War: Definitions, Deterrence and Foreign Policy, September 30, 2015, PP. 6-7.

بالتدخل في الانتخابات الرئاسية الأمريكية لصالح دعم "ترامب" واختراق البريد الإلكتروني لحملة المنافس، مما أحدث اهتزازا في شرعية الانتخابات الأمريكية[١].

وعادة ما تلجأ الدول لوسائل تنطوي على استخدام الأدوات الدبلوماسية التقليدية مع الاستفادة من الفضاء السيبراني، وبالشكل الذي يعمل على احتواء التهديدات والهجمات السيبرانية.

وظهرت بعض الأمثلة على تصاعد دور الدبلوماسية في احتواء الصراعات السيبرانية كاتفاق الأمن السيبراني بين الولايات المتحدة الأمريكية والصين عام ٢٠١٥[٢].

الاتفاقيات الدولية وقواعد الحروب السيبرانية:

باستقراء قواعد القانون الدولي، نجد أن هناك مجموعة من الاتفاقيات الدولية أبرمت لكي تنظم حالة الحرب[٣]، سواء قواعد اللجوء إلى استخدام القوة أو خلال إدارة

---

(١) اتهمت الولايات المتحدة الأمريكية روسيا بالتدخل في الانتخابات الرئاسية الأولى لصالح دعم فوز ترامب "المرشح الجمهوري" على حساب "هيلاري كلينتون" المرشحة الديمقراطية من خلال اختراق شبكة لجنة الحزب الديمقراطي، وتسريب رسائل البريد الإلكتروني لحملة هيلاري، الأمر الذي كان له أثر داخلي تمثل في إحداث نوع – ولو ضئيل – من اهتزاز شرعية الانتخابات الأمريكية، وأما على الجانب الدولي فقد زاد من حدة التوتر بين الولايات المتحدة وروسيا، وفرض مزيد من العقوبات على الكيانات الروسية المشاركة في عملية القرصنة وطرد ٣٥ دبلوماسي روسي من الولايات المتحدة الأمريكية.

راجع: د. أحمد عبيس الفتلاوي، الهجمات السيبرانية، مجلة المحقق المحلي، مرجع سابق، ص ٢٥.

(٢) تم التوقيع على الاتفاق في ٢٥ سبتمبر ٢٠١٥.

(٣) من أمثلة هذه الاتفاقيات: اتفاقية لاهاي لعام ١٨٩٩، ١٩٠٧، واتفاقيات جنيف الأربعة لعام ١٩٤٩.

الحرب، وتعاملت تلك الاتفاقيات مع النطاق المكاني والمتمثل في اليابسة، والبحر، والجو والفضاء. فضلا عن النطاق الزمني لقيام الحرب.

وفي ظل التقدم التكنولوجي وثورة الإنترنت والاتصالات، ظهر نطاق مكاني جديد لم يكن متصورا عند التوقيع على هذه الاتفاقات، يتمثل في الفضاء الإلكتروني (Cyber Space) كوسط يُستخدم لأجل استخدام القوة أو إدارة المعارك بدون نقل لقطع عسكرية من مكان إلى آخر، ولا يمكن التنبؤ بالفترة الزمنية التي سيستخدم فيها هذا الوسط من أجل إحداث خلل وظيفي أو تركيبي.

ويذهب البعض[١] من الفقه إلى أن الفضاء الإلكتروني لا يعتبر مجالا متميزا، بل إنه في حقيقة الواقع – أسلوب مستحدث لإدارة المعارك واستخدام القوة – على ذات نسق الأسلحة النووية، وذلك على أساس أنه ينطلق من واحدة من المجالات الأربعة (اليابسة والبحر والجو الفضاء) ويحدث أثرا في واحدة منها، وبالتالي يعد تطورا في الأسلوب فحسب.

مبدأ حظر استخدام القوة أو التهديد باستخدامها بين الدول:

تقرر المادة (٤/٢) من ميثاق الأمم المتحدة مبدأ رئيسيا من مبادئ القانون الدولي العام بأنه "على جميع الأعضاء في علاقاتهم أن يتخلصوا من التهديد باستخدام أو استخدام القوة ضد سلامة الإقليم أو الاستقلال السياسي لأي دولة، أو في أي حالة أخرى تتعارض مع مبادئ الأمم المتحدة".

)١(Thomas Rid, Cyber War Will Not Take Place, Oxford University Press, 2013, PP. 165 – 166.

ولا ريب أن موقع هذه المادة من الميثاق، والتركيبة اللغوية التي صيغت بها، تشير إلى مركزيتها والوصول إلى رؤية شاملة لمنظمة الأمم المتحدة في تحقيق الأمن والسلم الدوليين، من خلال عدم التهديد أو استخدام القوة[١].

وعليه باتت وجهة النظر بشأن هذه المادة، كونها خلقت حظرا عاما على استعمال القوة أو التهديد بها في سياق العلاقات بين الدول.

وقد تطور هذا المبدأ ليصبح عرفا دوليا، كما أشارت بذلك محكمة العدل الدولية في قضية "الأنشطة العسكرية وشبه العسكرية ضد نيكاراجوا عام ١٩٨٦"[٢].

وتنص المادة (٥١) على أنه "لا يوجد في هذا الميثاق ما ينقص أو يضعف الحق الطبيعي للدول بشكل فردي أو جماعي، في الدفاع عن النفس في الحالة التي تتعرض بها إلى اعتداء مسلح.....".

ويرى البعض أن هناك اختلافا حول المصطلح المستخدم في المادة (٥١) وهو شرط الاعتداء المسلح لتفعيل الحق في الدفاع عن النفس، ومصطلح استخدام القوة أو التهديد بها وفقا للمادة (٤/٢). ولا ريب أن هاتين المادتين استخدمتا صياغات مختلفة كل منها يؤدي إلى خيارات قانونية متباينة أمام الدول المعتدى عليها. فالاعتداء

---

(١) رزق أحمد سمودي، حق الدفاع عن النفس نتيجة الهجمات الإلكترونية في ضوء قواعد القانون الدولي العام، مجلة جامعة الشارقة، المجلد ١٥، العدد (٢)، ديسمبر ٢٠١٨، ص ٣٣٩.

(٢) (Judgment of the international court of justice in Military and Paramilitary Activities in and against Nicaragua (Nicaragua V. United States), 1986, I.C.J. 14, 96 – 97.

Malcolm Shaw, International Law, (7th edition, 2014).

وفي التعليق على الحكم أنظر Cambridge University Press: Yoram Dinstein, War, Aggression and Self – defence (3ed edition 2011).

المسلح يضع الدولة المعتدى عليها أمام خيار استخدام القوة، وذلك في سياق الدفاع عن النفس سواء على المستوى الفردي أو الجماعي وفقا للمادة (٥١) من ميثاق الأمم المتحدة.

أما استخدام القوة أو التهديد بها "والذي لا يرقى إلى كونه اعتداءً مسلحا، فيضع الدولة المعتدى عليها أمام خيارات قانونية أخرى. وتأتي في مقدمتها الإجراء المضاد والذي يعطي الدولة المتضررة القدرة على الرد ضد الاعتداء بوسائل أخرى دون استخدام القوة[١].

ومن ناحية أخرى فإن فكرة الإجراء المضاد كخيار أمام الدولة المعتدى عليها المقررة في المادة (٢٢) من مشروع مواد مسئولية الدول عن الأفعال غير المشروعة لعام ٢٠٠١جاء مقيدا بمجموعة من الشروط أهمها شرط التناسب بين الخرق والخرق المقابل، وهذا ما أكدت عليه محكمة العدل الدولية في قضية كوسوفو عام ١٩٩٧[٢].

بينما المناوشات المسلحة على الحدود – مثلا – لا ترقى إلى مرتبة الاعتداء المسلح الذي من شأنه تفعيل خيار الدفاع عن النفس وفقا للمادة (٥١)، كما بينت ذلك محكمة العدل الدولية في قضية نيكاراجوا[٣].

وجاء تعريف الجمعية العامة للأمم المتحدة للعدوان مشترطا الخطورة الكافية كأحد متطلبات الهجوم العسكري[١].

)١(Omer Elegab; the Legality of Non-forcible counter-measures in International Law, Oxford Monographs in International Law, 1988, P. 29.

)٢(ICJ, Case Concerning Gabcikovo – Nagymaros Project (Hungay Islovakia), 1997, Paragraph 71.

)٣(ICJ, Case Concerning Military and Poramilitary Activities in and Against Nicaragua (Nicaragua V. United States), Reports, 1986, Para, 191.

ويستفاد من جملة ما سبق أن كل اعتداء مسلح في ضوء المادة (٥١) يعد في الوقت ذاته استخداما للقوة، ولكن العكس غير صحيح، فالهجوم بالأسلحة الفتاكة كالنووي والدمار الشامل مثلا يعد استخداما للقوة وهجوما مسلحا في آن واحد، وبالتالي يتم تطبيق المادة (٥١) لأنها حققت الشرط الوارد بها.

ولا يفوتنا أن نشير إلى أن تفعيل المادة (٥١) واللجوء إلى الدفاع عن النفس في مواجهة هجوم مسلح لا يعني – في حقيقة الواقع – أن الدولة المدافعة في حِلٍّ من القيود، فهذا الفهم يناقض قواعد العرف الدولي[٢]، كما يناقض المادة (٥١) من ميثاق الأمم المتحدة التي تتطلب مجموعة من الشروط الواجب توافرها حتى يبقى التصرف متوافقا مع أحكامها وتتمثل في **أولا – الضرورة:** ويقصد بها توافر الحالة التي تجبر فيها الدولة على اللجوء للدفاع عن نفسها باستخدام القوة، حيث لم يعد اللجوء إلى خيار "الوسائل والطرق السلمية لفض النزاع وفقا للمادة (٣٣) من الفصل السادس من ميثاق الأمم المتحدة، كالمفاوضات والتحقيق والوساطة والتوفيق والتحكيم"، أو أن هذه الطرق الأخيرة قد تم اللجوء إليها ولكنها أثبتت عدم فعاليتها في مواجهة الدولة المعتدية[٣].

---

(١) قرار الجمعية العامة للأمم المتحدة رقم ٣٣١٤ لعام ١٩٧٤

انظر UN. General Assembly Res. 3313 (XXIX), Definition of Aggression, Adopted 14 December 1974.

(٢) للمزيد حول هذه الشروك راجع الرأي الاستشاري لمحكمة العدل الدولية في موضوع الأسلحة النووية عام ١٩٩٦.

(٣) Lee Stuesser, Active Defense; state Military Response to International Terrorism, 17, California Western International La Journal, 1987, P. 31.

ثانيا – التناسب: ويعني اتخاذ الإجراءات اللازمة والضرورية لرد الاعتداء وعدم تجاوزها، وبعبارة أخرى ألا تتجاوز الإجراءات المتخذة الهدف العام وهو تحقيق الأمن والسلم الدوليين[١].

مدى انطباق قواعد القانون الدولي على الهجمات السيبرانية:

في ظل عدم وضوح المعنى الدقيق لمصطلح "استخدام القوة" الوارد في المادة (٤/٢) من ميثاق الأمم المتحدة، فضلا عن خلو الاتفاقيات الدولية أو العرف الدولي من هذا التحديد.

وبالرجوع إلى دليل تالين "Tallinn Manual" نجد أنه يقرر أن: "الاعتداء على الدولة – بأي شكل كان بما في ذلك الهجمات السيبرانية – يشكل انتهاكا لسيادتها ما يعطي الحق للدولة المعتدى عليها رد هذا الاعتداء ضمن شرط جوهري، مفاده أن يكون حجم وتأثير هذا الهجوم على الدولة المعتدى عليها ضمن مستوى معين" وهو ما عملت لجنة الخبراء جهدا استثنائيا لتحديده من خلال مجموعة من الصفات التي يجب أن تتسم بها الحروب أو الهجمات السيبرانية حتى ترقى إلى درجة الهجوم المسلح، وبالتالي تعطي الدولة المعتدى عليها فرصة تفعيل المادة (٥١) من ميثاق الأمم المتحدة.

---

(١) (Micheal Newton & Larry May; Proportionality in International Law, Oxford University Press, 2014: Arbitral Award in the Naulilaa Case 1928, 2 Reports of the International Arbitral Awards 1011 – 1028.

- **الشروط الواجب توافرها وفقا لدليل تالين:**

١) **الجسامة أو الخطورة:** اعتبرت لجنة الخبراء أن أهم شرط يجب الاستناد إليه في تحديد مدى وصول الهجمات السيبرانية إلى درجة الهجوم المسلح يتمثل في جسامة وحدة هذه الهجمات، ومدى تأثيرها على الدولة المعتدى عليها[١].

ولاريب أن جوهر هذا الشرط يتمثل في الضرر المادي على الممتلكات والأفراد بالدولة المعتدى عليها بهجوم سيبراني، حيث ترقى إلى مستوى الهجوم المسلح الوارد في المادة (٥١) من ميثاق الأمم المتحدة فقط في الحالة التي تعكس فيها هذه العمليات ضررا ماديا حالا بالممتلكات والأفراد بالدولة المعتدى عليها. ولبيان ذلك قامت اللجنة بالقياس بين أثر الهجمات العسكرية التقليدية والهجمات السيبرانية. ولاريب أنه يمكن للأخيرة أن تنتج مثل هذا الضرر المتصور في الهجمات العسكرية التقليدية إن لم يكن يفوقها. ومثال ذلك الهجمات السيبرانية على مرافق الدولة التي تقدم خدماتها للأفراد، والاعتداء على شبكات الكمبيوتر الخاصة بمطارات الدولة بما قد يؤدي إلى تصادم الطائرات وتعرض العديد من الركاب للموت أو تسبب خسائر مادية ومالية أو الاضرار بمصلحة وطنية أو أمنية دون أن تصل إلى ضرر مادي محسوس بالدولة المعتدى عليها.

(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)، ديسمبر ٢٠١٨، ص ٣٥١.

٢) **الضرر الحال:** أي أن الخطر الحال هو الذي سوف يقع لا محالة دون أي قدرة للدولة المعتدى عليها لرده، ولا بأي وسيلة كانت. وقد تبنت لجنة الخبراء شرط الضرر الآتي أو الحال والذي يتحقق في حالتين:

الأولى، عندما يقع الضرر فعلا على الدولة المعتدى عليها. والثانية، عندما لا يكون الضرر قد وقع فعلا وإنما هو ضرر وشيك الوقوع، وهو – وفقا لرأي اللجنة – مُنتِج للحق في الدفاع عن النفس. كما استندت اللجنة إلى معيار "الفترة الزمنية الكافية" التي يمكن أن تستغلها الدولة "المعتدى عليها" لتجنب وقوع الضرر من خلال تواصلها بالدولة مصدر الاعتداء للتراجع عن هذا التصرف، ولا يمكن لهذا الأخير أن يرقى إلى كونه استخداما للقوة إذا ثبت أن الدولة المستهدَفة في هذا الهجوم قد فرطت بأي فترة زمنية كان يمكن لها استغلالها لدرء الضرر[١].

ويضرب البعض[٢] مثالا واقعيا لشرط الضرر الحال (الآنية) بحادثة كارولاين بين الولايات المتحدة الأمريكية وإنجلترا، حيث تقرر عرفا دوليا مفاده أن "للدولة الحق في الدفاع عن نفسها حيال أي هجوم عسكري لم يقع بعد ولكنه وشيك ولا يترك أي خيار أو وقت للمداولات".

وبالتالي ينبغي أن يُقرأ شرط الآنية في سياق الخطر المحتمل المعروف في القانون الدولي.

)١(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, 2012, P. 769.

)٢(Larry May; War Crimes and Just War, Cambridge University Press, 2007, P. 206.

٣) أن يكون أثر الهجوم السيبراني مباشرا:

لاريب في أن أهم ما يميز الهجمات العسكرية التقليدية عن الهجمات السيبرانية يكمن في أن نتائج الأخيرة قد تكون غير مباشرة، بمعنى أن الفضاء وعدم الوضوح هو الأساس فيها وبالتالي عدم القدرة على تحديد علاقة السببية بين الفعل والضرر، وذلك ناجم عن الانفصال الزمني بين التصرف الذي يعد مخالفة والنتائج التي يمكن أن يرتبها هذا التصرف، وهذه خاصية ملازمة للهجمات السيبرانية[١].

فمثلا الهجمات السيبرانية على البورصة في دولة ما، سوف تؤثر سلبا وإن كان على مدى زمني طويل – في أدائها بشكل عام، وينجم عن ذلك انكماش أو انهيار للنظام الاقتصادي في هذه الدولة. فالأحوال المتردية للاقتصاد تعد نتيجة مباشرة للهجمات السيبرانية خاصة إذا كان اقتصاد تلك الدولة في الأساس ضعيفا.

٤) **الفورية:** وتعني ألا تترك الدولة المعتدى عليها فترة زمنية طويلة على الاعتداء قبل أن تقوم باتخاذ إجراءات الدفاع عن النفس، لأنه في هذه الحالة سوف ينتفي المقتضى من إعطاء الدولة الحق في الدفاع عن نفسها دون اللجوء إلى مجلس الأمن صاحب الاختصاص الأصيل في حفظ الأمن والسلم الدوليين[٢].

)١(Haitao Du and Shanchieh Jay Yaung, Temporal and Spatial Analyses for Large scale Cyber Attacks, Handbook of Computational Approaches to Counter Terrorism 2012, PP. 559 – 578.

)٢(Yoram Dinstein; Computer Network attacks and Self-Defense, 76 U.S. Naval War College of International Law Studies, 2002, P. 14.

وغني عن البيان أن شرط الفورية يجب أن يُنظَر إليه بنوع من الجدية في سياق الهجمات السيبرانية والتي تكمن في مدى التعقيد الذي يكتنف التحقق من مصدر الاعتداء[١].

٥) الاعتداء:

يعتبر شرط الاعتداء أحد الشروط ذات الصلة بحالة الدفاع عن النفس، وهو ما جاءت به المادة (٥١) من ميثاق الأمم المتحدة، حيث اعتبرت أن الاعتداء من دولة باتجاه دولة أخرى هو المحرك الأساسي لتفعيل حالة الدفاع عن النفس بالنسبة للدولة المعتدي عليها، وهو يعكس الرابطة المباشرة بين السلوك ونية الاعتداء لدى الدولة المعتدية في إحداث ضرر بالدولة الأخرى أو إحدى مصالحها[٢].

ويُستفاد مما تقدم أن شرط الاعتداء يتمثل في سوء النية الكامن خلف الهجمات السيبرانية، والتي ترتقي إلى مصاف الهجوم المسلح. ومتى كانت الدولة المعتدى عليها قادرة على إثبات أن هذا التصرف يرمي – في حقيقته – إلى تحقيق أهداف عدائية بها كإضعاف القدرة العسكرية من خلال التأثير على شبكات الاتصال في مرفق الدفاع.

وغني عن البيان أن إثبات النية وراء القيام بتصرف ما، هي من الأمور بالغة الصعوبة، ولا يتم الوصول إليها إلا من خلال عرض المسألة على القضاء للبت فيها. وهذا غير متصور في حالة الحروب السيبرانية نظرا لعدم وجود اختصاص قضائي

---

(١) رزق أحمد سمودي، حق الدفاع عن النفس نتيجة الهجمات الإلكترونية في ضوء قواعد القانون الدولي العام، مرجع سابق، ص ٣٤٣.

(٢) ICJ, Oil Plat Forms Case, (Islamic Republic of Iran V. United States of America), Reports, 2003, P. 161.

دولي ملزم للدول كافة، حتى وإن وجد فإن اللجوء إلى القضاء يصطدم مع تطلب السرعة في رد الهجوم والذي يعد المقتضى لمباشرة الدولة المعتدى عليها في حقها في الدفاع عن نفسها[١].

٦) اتصال التصرف بالدولة:

من الأمور المسلم بها لنهوض المسئولية الدولية، تعلق الهجمات السيبرانية بالدولة، بمعنى أن يكون التصرف صادرا عن أي جهة يعهد إليها مهمة القيام بعمل معين بالنيابة عن الدولة. ومع هذا فإن تطلب هذا الشرط يعد في غاية الصعوبة، ومرجع ذلك هو صعوبة تحديد ما إذا كان هذا التصرف منسوبا للدولة فعلا، وهذا مرتبط بالقدرة التكنولوجية فائقة التطور، والتي قد تكون عاملا رئيسيا في طمس هوية الفاعل الحقيقي، فضلا عن صعوبة أخرى في الأحوال التي لا تكون الشبكة الإلكترونية هي الوسط الذي تمت من خلاله الهجمات السيبرانية، كإرسال فيروسات تُنقَل مباشرة في أجهزة الحاسوب بالدولة المستهدفة، أو استخدام إقليم دولة أخرى لتنفيذ هذه الهجمات.

ولا يفوتنا أن نشير إلى قيام لجنة الخبراء بوضع شروط أخرى – بالإضافة إلى ما سبق – مثل ضرورة وضوح أثر الهجمات السيبرانية أو القدرة على قياسها، وهو ما يطلق عليه القدرة على تحديد الضرر الناجم عن الهجمات السيبرانية، وغلبة الطابع العسكري على الهجمات السيبرانية.

وهذا الشرط أكدت عليه ديباجة ميثاق الأمم المتحدة والتي تفرض على كافة الدول واجب "عدم استخدام القوة العسكرية إلا لتحقيق مصالح مشتركة".

---

(١) رزق أحمد سمودي، حق الدفاع عن النفس نتيجة الهجمات الإلكترونية في ضوء قواعد القانون الدولي العام، مرجع سابق، ص ٣٥٦.

رأي الباحث:

يرجع الفضل للجنة الخبراء على الجهود المضنية فيما بذلوه لتحديد مجموعة من الشروط التي يجب أن تتحقق في الهجمات السيبرانية حتى ترقى إلى درجة الهجوم المسلح، وبالتالي تُعطي الدولة المعتدى عليها فرصة تطبيق المادة (٥١) من ميثاق الأمم المتحدة. إلا أنه يؤخذ عليها تأثرها بالفكرة التقليدية لاستخدام القوة على اعتبار أنها مكافئة للقوة العسكرية، وغلبة النظرة النمطية للدول حول مدلول استخدام القوة، وإنما ينبغي النظر في إطار تطور الوسائل السيبرانية لتنفيذ الهجوم، وتغير غايات الدول في الوقت الراهن ، حيث أضحت كل دولة ترى في هذه الهجمات السيبرانية تفوقا خارج إطار التفوق التقليدي العسكري كما هو الحال في مجالات الاتصالات وسوق المال والبيئة والمحطات النووية والسدود وغيرها.

المبحث الثاني

دليل تالين (Tallinn Manual)

تمهيد:

يمثل دليل تالين[١] آلية لملاءمة المبادئ الأساسية للقانون الدولي مع الحروب السيبرانية، ويقرر الدليل – من حيث المبدأ – أن أحكام ميثاق الأمم المتحدة قابلة للتطبيق على الهجمات والحروب السيبرانية، ويناشد الدول ألا تعامل الفضاء السيبراني على أنه فراغ قانوني لا تنطبق عليه المبادئ القانونية المطبقة في الفضاءات المادية، وينبغي على المجتمع الدولي الاستجابة والاستعداد للهجمات السيبرانية، والالتزام بمتطلبات القانون الدولي.

---

(١) دليل (Tallinn Manual) صدرت النسخة الأولى منه في مارس ٢٠١٣، وقد تمثل هدفه الرئيسي في التحقيق في القضايا وتطبيق القانون الدولي في مجال الحرب السيبرانية. ويتكون الدليل من قسمين رئيسيين هما: قانون الأمن السيبراني الدولي، وقانون النزاعات المسلحة السيبرانية وذلك في سبعة فصول. كما يتضمن (٩٥) قاعدة قانونية صاغتها لجنة الخبراء في القانون الدولي البارزين في تالين باستونيا على نحو يحدد الخطوط الحمراء التي تستوجب التدخل العسكري، وطرق مشاركة مختلف الأطراف.

وفى عام ٢٠١٦ تم إصدار النسخة المحدثة لدليل تالين (القانون الدولي المطبق على عمليات الإنترنت) ليشمل القواعد التي حقق فيها الإصدار الأول، ويضم أربعة أجزاء رئيسية، وبلغت عدد القواعد التي يمكن تطبيقها على العمليات السيبرانية (١٥٤) قاعدة من قواعد القانون الدولي.

للمزيد حول الدليل راجع:

Laszlo Kovacs, “cyper security policy and strategy in the European union and NATO”, Revista Academiei Fortelor Terestre, Vol. 1. No. 89, 2018.

ومن ناحية أخرى يحدد الدليل الإجراءات التي قد تتخذها الدول للرد، حيث تؤكد القاعدة (١٣) منه على أنه "إذا تجاوز النشاط السيبراني سقف أي هجوم مسلح بالمعنى المقصود في المادة (٥١) من ميثاق الأمم المتحدة، فينبغي أن يكون للدولة الحق في ممارسة حقها الأصيل في الدفاع عن النفس.

ويقرر أيضا مبدأ مفاده "أن العمليات السيبرانية – ان أسفرت عن أضرار جسيمة ووفيات يمكن الرد عليها بأسلحة الحرب الحقيقية"[١].

وغني عن البيان أن التجسس السيبراني الخالص لا يعتبر عملا حربيا – وفقا لقواعد تالين – فإن هجمات التجسس التي يمكن اعتبارها تحضيراً لهجوم مدمر قد تتطلب الرد عليها بضربة وقائية. وقد تطالب الدول بحقها في الدفاع عن النفس إذا كان المهاجم دولة، أو جماعة منظمة. أما في حال كون المهاجم فردا، فلا يحق للدولة المعتدى عليها، اللجوء لضربة وقائية. وترتيبا على ذلك، لا يمكن – من حيث المبدأ – الرد على التسريبات والأخبار المتداولة عن هجوم ما – قبل حدوثه من خلال الأداة العسكرية إلا إذا كانت الإصابات والخسائر المحتملة وشيكة الحدوث[٢].

(١) د. رغدة البهي، مجال حرب: كيف استجاب حلفي شمال الأطلسي للدفاع السيبراني، كراسات استراتيجية، مركز الأهرام للدراسات السياسية والاستراتيجية، العدد (٣٣٤) المجلد (٣١) – مارس ٢٠٢٢، ص ٢٧.

(٢) Annegret Bendiek, Tests of partnership transatlantic cooperation in syber security" Internet governance and data protection, Berlin, SWP research paper, RR 5, March 2014, pp. 10 – 11.

المبحث الثالث

المسئولية الدولية عن أضرار الحرب السيبرانية

تمهيد:

نتناول أولاً تعريف المسئولية الدولية، وعناصرها ثم التعويض عنها على النحو التالي:

أولاً ـ تعريف المسئولية الدولية:

يعرف البعض المسئولية الدولية بأنها: "الالتزام الذي يفرضه القانون الدولي على الشخص بإصلاح الضرر لصالح من كان ضحية سواء كان تصرف أو امتناع وتحمل العقاب جزاء هذه المخالفة"[١].

وعرفت لجنة القانون الدولي في مشروعها بخصوص المسئولية الدولية لعام ١٩٥٧ بأنها: "إسناد فعل غير مشروع دوليا لأحد أشخاص القانون الدولي العام، مما يترتب التزامه بدفع التعويض أو جبر الضرر الذي حدث نتيجة هذا الفعل غير المشروع دوليا".[٢]

ويرى البعض أن المسئولية الدولية هي "عملية إسناد فعل إلى أحد أشخاص القانون الدولي سواء كان هذا الفعل يحظره القانون الدولي أو لا يحظره، ما دام قد ترتب عليه

---

(١) د. محمد طلعت الغنيمي، الوسيط في القانون الدولي للسلام، منشأة المعارف، الإسكندرية، ١٩٨٢، ص ٣٤٩.

(٢) مشار إليه لدى د. أحمد أبو الوفا، شروط المسئولية الدولية، مجلة الدبلوماسي، العدد (١٣)، ٢٠٠٠، معهد الدراسات الدبلوماسية، المملكة العربية السعودية، ص ٤٠ وما بعدها.

ضرر لأحد أشخاص القانون الدولي، الأمر الذي يقتضي توقيع جزاء دولي معين، سواء أكان هذا الجزاء ذات طبيعة عقابية أم كان ذات طبيعة غير عقابية"[١].

أي أن المسئولية الدولية هي علاقة بين شخصين من اشخاص القانون الدولي يلتزم إحداهما بتعويض الضرر الذي سببه للآخر.[٢]

وساهم الفقه والقضاء الدوليان في تطوير قواعد المسئولية الدولية على نحو يكفل ضمان المشروعية الدولية، لا سيما القواعد الدولية الآمرة التي تنظم المصالح الأساسية والضرورية للإنسانية[٣]. ونتناول تعريف المسئولية الدولية على النحو التالي:

يعرف البعض المسئولية الدولية بأنها: "نظام قانوني يترتب بموجبه على الدولة التي ارتكبت عملاً يجرمه القانون الدولي تعويض عن الضرر الذي لحق بالدولة المعتدى عليها".

---

(١) السيد أبو عيطة، الجزاءات الدولية بين النظرية والتطبيق، مؤسسة الثقافة الجامعية، الإسكندرية، ٢٠١١، ص ٢٥٠.

(٢) للمزيد حول المسئولية الدولية راجع:

د. مفيد محمود شهاب، دراسات في القانون الدولي الإنساني، دار المستقبل العربي، ٢٠٠٥، ص ٢٣٩ وما بعدها.

د. مصطفى أحمد فؤاد، القانون الدولي الإنساني، دار المطبوعات الجامعية، ٢٠١٨، ص ٢٧٥ وما بعدها.

(٣) جدير بالذكر أن المذاهب السياسية والاقتصادية كان لها أثر كبير في تطوير وتغيير المفاهيم التقليدية للمسئولية الدولية، ونجم عن هذا التطور مفهوم واضح لمعالم المسئولية الدولية. للمزيد حول هذا الموضوع راجع:

السيد أبو عيطة، الجزاءات الدولية بين النظرية والتطبيق، مرجع سابق، ص ٢٤٤.

فالمسئولية الدولية وفقا للمفهوم القديم مسئولية ضيقة، بحيث تقوم على ثلاث ركائز هي: ١- أشخاص القانون الدولي العام والمتمثل في الدولة فقط.

٢- اقتصار المسئولية المدنية التي تتحملها الدولة في صورة التعويضات.

٣- تقف حدود المسئولية عند أضرار الدولة الناجمة عن أعمال يعاقب عليها القانون الدولي.

وقامت لجنة القانون الدولي العام لعام ٢٠٠١ بتعريف المسئولية الدولية بأنها "كل فعل غير مشروع دوليا تقوم به الدولة، يستتبع مسئوليتها الدولية".

كما أشارت محكمة العدل الدولية للمسئولية الدولية بأنها "من مبادئ القانون الدولي أن مخالفة التزام دولي يستتبع الالتزام بالتعويض عن ذلك بطريقة كافية وأن هذا الالتزام بالتعويض هو النتيجة الحتمية لأي إخلال في تطبيق أية اتفاقية دولية ولا ضرورة للإشارة إليه في كل اتفاقية على حدة".

وفي قضية مصنع شاروز أكدت على أن "هناك مبدأً في القانون الدولي العام مفاده أن انتهاك أي قاعدة يؤدي إلى واجب إصلاح مناسب والتعويض هو النتيجة الجوهرية لانتهاك معاهدة"[١].

رأي الباحث:

يجب أن يكون التعريف لأي مصطلح قانوني جامع مانع، جامع لكل العناصر التي تدخل في نطاقه، ومانع من دخول أي مصطلح يشتبه به، أو يدخل عليه ما ليس منه؛

(١) مشار إليها في غسان الجندي، المسئولية الدولية، ط ١، مطبعة التوفيق، عجمان، ١٩٩٠، ص ٤.

وعليه ينبغي أن يكون التعريف للمسئولية الدولية جامع لنوعي المسئولية المدنية والجنائية، سواء كانت هذه المسئولية ناتجة عن فعل مشروع لا يحظره القانون الدولي لكن يترتب عليه ضرر لأحد الأشخاص الدولية أو التابعين لها، أو نتيجة فعل يعد انتهاكا لأحد الالتزامات الدولية، والنتيجة المترتبة على توافر هذه المسئولية ودور المجتمع في توقيع العقاب المناسب.

ثانياً ـ عناصر المسئولية الدولية:

وفقاً للفقه الدولي يجب توافر ثلاثة عناصر حتى نكون بصدد المسئولية الدولية وهى الفعل والضرر وعلاقة السببية :

(١) الفعل:

ويقصد بذلك الفعل غير المشروع دوليا، أو حتى التصرف المشروع لكنه يسبب ضررا لأي شخص من أشخاص القانون الدولي، كما يعبر عنه البعض بالعنصر الموضوعي للمسئولية الدولية، ويمكن أن يكون هذا الفعل جريمة دولية كالانتهاكات الجسيمة لأحكام ومبادئ القانون الدولي الإنساني[١].

(٢) علاقة السببية:

ويقصد بذلك ضرورة إسناد أو نسبة الواقعة المنشئة للمسئولية الدولية إلى أحد أشخاص القانون الدولي العام سواء كانت دولة أو منظمة دولية. أما الأعمال التي تنسب إلى أفراد عاديين، فإن الدولة تكون مسئولة عنها بشروط وضوابط وأحوال

(١) السيد أبو عيطة، الجزاءات الدولية بين النظرية والتطبيق، مرجع سابق، ص ٢٥٤.
وكذلك د. مصطفى أحمد فؤاد، القانون الدولي الإنساني، مرجع سابق، ص ٢٧٧.

معينة، لأن القاعدة العامة هي عدم مسئولية الدولة عن تصرفاتهم والاستثناء أن تنعقد مسئوليتها في حالتين[١]:

الحالة الأولى: تصرف الفرد بناء على تعليمات من الدولة وبتوجيه منها وتمت تحت رقابتها.

الحالة الثانية: عدم بذل الدولة العناية الواجبة لمنع هذه الأعمال التي يترتب عليها ضرر للآخرين[٢].

وغني عن البيان أنه يمكن أن تشترك في المسئولية الدولية أكثر من دولة، إذا تم الفعل غير المشروع بمساهمة مشتركة، كما تسأل الدولة إذا سمحت بالتصرف الضار أن يمر
عبر الفضاء السيبراني لها، أو ساعدت على ذلك. ومن ناحية أخرى يمكن أن تشترك المسئولية بين الدولة والأفراد، كما في جرائم الحرب السيبرانية فيتحمل الأفراد المسئولية الدولية الجنائية، وتتحمل الدولة المسئولية المدنية أو التعويض، كما تسأل المنظمات الدولية
عن الأعمال غير المشروعة التي يرتكبها موظفوها وعن الأجهزة التابعة لها وتتصرف باسمها[٣].

أي أن الفعل أو التصرف غير المشروع، صدر من شخص دولي، ونجم عنه ضرر بإحدى الأشخاص الدولية الأخرى.

---

(١) د. مصطفى أحمد فؤاد، القانون الدولي الجنائي، دار المطبوعات الجامعية، ٢٠١٨، ص ٢٩١.

(٢) د. صلاح الدين عامر، مقدمة لدراسة القانون الدولي العام، دار النهضة العربية، ٢٠٠٢، ص ٧٣٩.

(٣) د. وائل أحمد علام، مركز الفرد من النظام القانوني للمسئولية الدولية، دار النهضة العربية، ٢٠٠١، ص ٢٥.

(٣) الضرر:

يقصد بالضرر كشرط من شروط المسئولية الدولية "كل ضرر يلحق مصلحة أو حق مشروع لأحد أشخاص القانون الدولي العام". وهذا الضرر قد يكون ماديا أو معنويا[١].

ثالثاً ـ التعويض عن الهجمات السيبرانية:

نتناول مدلول التعويض في القانون، ثم أساس التعويض في القانون الدولي الإنساني وأشكاله، وذلك على الوجه التالي:

(١) مدلول التعويض:

يقصد بالتعويض[٢] "التزام يُلقى على عاتق دولة ما في أعقاب حرب بتقديم تعويضات كافية عن الأضرار التي أصابت دولة أخرى أو رعاياها بسبب الحرب"[٣].

(٢) أساس التعويض في القانون الدولي الإنساني:

(١) يذهب البعض إلى عدم اعتبار الضرر من شروط المسئولية الدولية مبررا ذلك بأن معظم الاتفاقيات الدولية تتناول مجموعة من الالتزامات الدولية دون أن تشير إلى الأضرار المادية التي تترتب على انتهاك هذه الالتزامات ومع ذلك تقوم المسئولية الدولية بمجرد انتهاك الالتزامات الواردة بالاتفاقية إذ أن الضرر إن كان نتيجة محتملة لفعل أو تصرف دولي غير مشروع إلا أنه لا يعد أحد عناصره.

د. حسام عبد الخالق، المسئولية والعقاب على جرائم الحرب مع دراسة تطبيقه على جرائم الحرب في البوسنة والهرسك، دار الجامعة الجديدة للنشر، الإسكندرية، ٢٠٠٤، ص ٢٨ ، ٢٩.

(٢) التعويض لغة: أصل العوض، البدل، يقال عاضه وعاوضته، وعوضته، أعطيته البدل ما ذهب منه واستعاضه وتعويضه، سأله العوض، وهو البدل والخلق في الاستقبال.

راجع لسان العرب، لابن منظور، ج ٧، دار ابن جرير للنشر، بيروت، ١٩٨٤، ص ١٩٢.

(٣) د. صلاح الدين عامر، مقدمة لدراسة القانون الدولي العام، مرجع سابق، ص ٧٤٥.

ألزمت المبادئ العامة لاتفاقيات لاهاي الأربعة لعام ١٩٠٧، احترام قوانين وأعراف الحرب البرية، وأوجبت على المحارب الذي يخل بأحكامها دفع تعويض إذا اقتضت الحاجة، كما يكون مسئولا عن جميع الأعمال التي يرتكبها أشخاص ينتمون إلى قواته المسلحة[١].

وأشارت فتوى محكمة العدل الدولية لانتهاكات القانون الإنساني وحقوق الإنسان في الأراضي الفلسطينية المحتلة عن التزام إسرائيل بتقديم تعويضات لجميع الأشخاص الطبيعية (الأفراد) والمعنوية جراء ما لحق بهم من أضرار، وذلك بالنظر إلى أن تشييد الجدار والنظام المرتبط به، قد ترتب عليه الاستيلاء على المنازل ومشاريع تجارية، وأراضي زراعية وتدميرها، وألزمت المحكمة إسرائيل بجبر الضرر الذي لحق بجميع الأشخاص الطبيعيين والاعتباريين المعنيين".

(٣) أشكال التعويض عن المسئولية الدولية:

يترتب على المسئولية الدولية عدة آثار قانونية يأتي في مقدمتها التزام الدولة المسئولة بجبر الضرر الذي نشأ عن التصرف غير المشروع، وأكد ذلك القضاء الدولي في العديد من أحكامه، ويتخذ التعويض عدة أشكال منها التعويض العيني ويقصد به إعادة الأمور إلى ما كانت عليه قبل صدور التصرف أو على الأقل إزالة الأعمال الحربية.

وهذا ما أكدته محكمة العدل الدولية بأنه "يقع على إسرائيل التزام بأن توقف فورا أعمال تشييد الجدار الجاري بنائه في الأراضي الفلسطينية المحتلة، والقيام فورا بإزالة

---

(١) راجع الفقرة (١٥٢) من فتوى محكمة العدل الدولية بشأن الآثار القانونية الناشئة عن تشييد جدار في الأراضي الفلسطينية المحتلة الصادر في ٢٠٠٤/٧/١٣، ص ٧٣.
راجع ملخصات أحكام وفتاوى محكمة العدل الدولية على الموقع lcJ-cij.org

أجزاء ذلك البناء الواقعة داخل الأراضي الفلسطينية بما فيها القدس الشرقية وما حولها"[١].

وقد يتم التعويض ماليا عن الضرر الناتج عن الفعل غير المشروع، وهذا هو الغالب واقعيا، وأشارت للتعويض المالي محكمة التحكيم الدائمة بأنه "ليس بين مختلف مسئوليات الدول فروق أساسية، ويمكن تسويتها جميعا بدفع مبلغ من المال"[٢]. وقد يتم الاتفاق على التعويض نتيجة لمفاوضات تتم بين الأطراف المعنية ويعقبها اتفاق على مقدار ونوع التعويض.

وأخيرا قد يتخذ التعويض صورة الترضية، كأن تصدر الدولة اعتذارها وأسفها على ما يصدر من أخطاء صادرة عن جنودها أو موظفيها أثناء قيامهم بواجبهم الرسمي، وعادة يتم ذلك بالطرق الدبلوماسية[٣].

(١) راجع الرأي الاستشاري لمحكمة العدل الدولية، المرجع السابق، الفقرة ١٤٥، ص ٧١.

(٢) د. محمد عبد العزيز أبو سخيلة، النظرية العامة للمسئولية الدولية، مرجع سابق، ص ٣٦٠.

(٣) د. محمد عبد العزيز أبو سخيلة، النظرية العامة للمسئولية الدولية، مرجع سابق، ص ٣٦٣.

النتائج والتوصيات التي توصل إليها البحث

انتهى البحث في موضوع "الجوانب القانونية للحرب السيبرانية". دراسة في إطار القانون الدولي الإنساني إلى جملة من النتائج والتوصيات تتمثل في الآتي:

أولاً – النتائج:

- أكد البحث على أن الحروب السيبرانية من المفاهيم الحديثة التي لا يوجد اتفاق دولي على تعريفها، وأن الفضاء الإلكتروني بما يتمتع به من مزايا قد فرض نفسه كبعد استراتيجي جديد في النزاعات والحروب الدولية، ولم يعد مجرد مجال لجمع المعلومات، وإنما هو فضاء مثالي لتوجيه أقوى الضربات العسكرية.
- هناك من القواعد الدولية ما يمكن الاستناد إليها في تنظيم الحروب السيبرانية، مثل ميثاق الأمم المتحدة، البروتوكول الإضافي الأول لعام ١٩٧٧، وأحكام محكمة العدل الدولية، ودليل تالين.
- أشار البحث إلى أن القانون الدولي الإنساني أقر بالمسئولية الدولية عن الأضرار الناشئة عن الهجمات السيبرانية، وأن أساس هذه المسئولية هو الالتزام بجبر الأضرار التي أحدثها التصرف غير المشروع.
- أكد البحث إمكانية خضوع الحروب السيبرانية التي تحدث في سياق النزاع المسلح الحركي للقانون الدولي الإنساني، إلا أن التحدي الأكبر هو تلك الهجمات التي تحدث خارج سياق النزاع المسلح الحركي ومدى إمكانية عدها نزاع مسلح وإثبات نسبة الهجوم لدولة معينة ومن ثم إمكانية تطبيق القانون الدولي الإنساني عليها.

ثانياً – التوصيات:

- ضرورة وجود إطار قانوني لحماية الأمن السيبراني، والذي من خلاله يمكن حماية المواقع الاقتصادية، والعسكرية، والمرافق السيادية من أي اختراق أو هجمات سيبرانية، نظرا لما تمثله هذه المرافق من أهمية كبيرة في الدولة.
- بات من الضروري استعداد أجهزة الدولة في كافة المجالات الاستعداد التكنولوجي الفني والأمني لمواجهة تحديات المستقبل المتمثلة في الحروب السيبرانية، والعمل على خلق ثقافة معرفية اجتماعية عامة فيما يتعلق بالمفهوم العام لهذه النوعية من الحروب، وتطوراتها التقنية للحد من خطورتها الحالية والمستقبلية، وإضعاف قدرات الخصوم على استخدام قدراته التكنولوجية كسلاح أساسي في حروب.

قائمة المراجع

أولا - المعاجم اللغوية:

قاموس المورد لمنير البعلبكي، دار العلم للملايين، بيروت، ٢٠٠٤.

ثانيا - المراجع العربية:

أ) الكتب القانونية العامة:

- صلاح الدين عامر، مقدمة لدراسة القانون الدولي العام، دار النهضة العربية، ٢٠٠٧.
- مفيد محمود شهاب، دراسات في القانون الدولي الإنساني، دار المستقبل العربي، ٢٠٠٥.
- مصطفى أحمد فؤاد، القانون الدولي الجنائي، دار المطبوعات الجامعية، ٢٠١٨.
- مصطفى أحمد فؤاد، القانون الدولي الإنساني، دار المطبوعات الجامعية، ٢٠١٨.

ب) الكتب القانونية المتخصصة:

سعيد عبداللطيف حسن، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت، دار النهضة العربية، ٢٠١٧.

ج) الرسائل العلمية:

١- حنين جميل أبو حسين، الإطار القانوني لخدمات الأمن السيبراني، رسالة ماجستير، كلية الحقوق، جامعة الشرق الأوسط، ٢٠٢١.

٢- زهراء عماد محمد كلنتر، المسئولية الدولية الناشئة عن الهجمات السيبرانية، رسالة ماجستير، كلية القانون، جامعة الكوفة، ٢٠١٦.

٣- نور أمير الموصلي، الهجمات السيبرانية في ضوء القانون الدولي الإنساني، رسالة ماجستير، الجامعة الافتراضية بسوريا، ٢٠٢١.

د) المجلات والدوريات العلمية:

١- أحمد عبيس الفتلاوي، الهجمات السيبرانية – مفهومها والمسئولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي، كلية القانون، جامعة بابل، ٢٠١٥.

٢- أميرة عبد العظيم محمد عبد الجواد، المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام، مجلة الشريعة والقانون، العدد ٣٥، الجزء الثالث، ٢٠٢٠.

٣- تغريد صفاء، لنبى خميس مهدي، أثر السيبرانية في تطور القوة، مجلة حمورابي، العراق، العدد (٣٣ ، ٣٤) – السنة الثامنة – شتاء / ربيع ٢٠٢٠.

٤- خالد وليد محمود، الهجمات عبر الانترنت. ساحة الصراع الإلكتروني الجديدة، سلسلة دراسات ودراسة السياسات، المركز العربي للأبحاث، قطر، ٢٠١٣.

٥- رزق أحمد سمودي، حق الدفاع عن النفس نتيجة الهجمات الإلكترونية في ضوء قواعد القانون الدولي العام، مجلة جامعة الشارقة، المجلد ١٥، العدد (٢)، ديسمبر ٢٠١٨.

٦- رغدة البهي، مجال حرب: كيف استجاب حلف شمال الأطلسي للدفاع السيبراني، كراسات استراتيجية، مركز الأهرام للدراسات السياسية والاستراتيجية، العدد (٣٣٤)، المجلد (٣١) مارس ٢٠٢٢.

٧- طارق جمعة، تحديات إثبات الجرائم الإلكترونية، مجلة رؤى مصرية، السنة ٣، العدد (٣١) أغسطس ٢٠١٧.

٨- عبد العال الديربي، ملامح شبكات التواصل الاجتماعي: الخصائص والأنماط، مجلة رؤى مصرية، السنة الثالثة، العدد (٣١)، أغسطس ٢٠١٧.

٩- محمود الرشيدي، حرب المعلومات: حروب ذكية بأسلحة غير مرئية، مجلة رؤى مصرية، السنة الثالثة، العدد (٣١) أغسطس ٢٠١٧.

١٠- نورهان الشيخ، روسيا وإعادة التعددية القطبية، مجلة رؤى مصرية، السنة الخامسة، العدد (١٥٨)، نوفمبر ٢٠١٩.

١١- هشام محمد خليل رستم، الجوانب الإجرامية للجوانب المعلوماتية، مجلة الأمن والقانون، أكاديمية شرطة دبي، العدد (٢)، ٢٠١٧.

ثانياً: المراجع باللغة الأجنبية

1- ICJ Oil Platforms Case (Islamic public of Iran V. united states of America) Reports, 2003.

2- Craig B. Greathouse, cyberwar and strategic thought, Verlag Berlin Heidelberg: Springer, 2014.

3- Keir Giles and William Hagestad li, Divid by A common language (Edsl, 2013; 5th International conference on cyber conflict Tallinn, Nato publications, 2013.

4- Daniel T. Kuehl, from cyber space to cyber power defining the problem in cyber power and national security. Washington, Doc national Defence up, 2009.

5- Micheal N. sch mitt (ed.), Tallinn Manual on the International Law Applicable to cyber war fore, Cambridge University press, 2013.

6- James A. Lewis, Statement Before the House, September 30, 2015.

7- Tim Stevens, A cyberwar of Ideas? Delerrence and Norm Sin syber space, contemporary Security policy, Vol. 33, no. 1, April, 2012.

8- Cyber – Attacks and the use of force : Malthew C. Waxman the yale journal of international, Back to the future of Article 2 (4), vol, 26, 2011, P. 423.

9- A look, the challenge of unrestricted war fare, Kevin Coleman .com direction smag. www//: http Back and look Ahead Articles.