الهجمات السيبرانية واستخدام القوة في القانون الدولي المعاصر

Cyber-attacks and the Use of Force in contemporary International Law

إعـــداد الدكتور

محمد ربيع أحمد حسين محمد

دكتوراه في القانون

كلية الحقوق - جامعة بنها

المقدمة

لقد شهد القرن الحادي والعشرون، تطورا كبيرا في وسائل الاتصالات. وذلك بفعل تنامي ظاهرة العولمة، وبخاصة عولمة وسائل الاتصالات.[١] إذ أصبحت التكنولوجيا الحديثة، تمثل جوهر وجود الجنس البشري. فبينما تسعى الدول، إلى نشر مفاهيم التحول الرقمي، وتبني مفاهيم الحكومات الذكية؛ إذ أصبحت الهجمات الإلكترونية، عبر الإنترنت أكثر تواترا وعالمية. مما أدى إلى تحويل الفضاء الإلكتروني، إلى ساحة حرب جديدة في القرن الحادي والعشرين. في الواقع، كان العديد من الدول والأفراد، هدفا للعديد من الهجمات الإلكترونية، نظرا لاعتمادهم على أجهزة الحاسب الآلي، والشبكات، والإنترنت. وبينما تتولى التشريعات الوطنية للدول، محاولة توفير الحماية القانونية، للأفراد والشركات الخاصة، التي تتعرض للجرائم الإلكترونية، مثل: جرائم التجسس والاحتيال الإلكتروني؛ فإن الهجمات الإلكترونية التي تستهدف الدول، تخضع للقانون الدولي بشكل عام، وتخضع لقانون الحرب بشكل خاص.

يقدم هذا البحث، وجهة نظر مختلفة، حول نطاق تطبيق المادة (٤/٢) من ميثاق الأمم المتحدة، في مجال الفضاء الإلكتروني. الافتراض القانوني السائد هو أن المادة (٤/٢) تنطبق على الهجوم السيبراني، الذي يشبه في تأثيره الهجوم الحركي. ومع ذلك، فإن هذه الفرضية تخلق ثغرة قانونية، مفادها أن الهجمات السيبرانية، التي تستهدف بيانات المستشفيات، أو الأنظمة المصرفية، أو غيرها من الشبكات الخاضعة

[١] لقد أدى بزوغ ظاهرة العولمة، إلى التأثير على الكثير من مبادئ القانون الدولي العام، فضلا عن التأثير على الدول والأفراد. وللمزيد راجع: حسين، محمد ربيع أحمد (٢٠٢٢)، الجذور التاريخية لمبدأ التدخل الدولي الإنساني وتطبيقاته المعاصرة، رسالة دكتوراه، كلية الحقوق، جامعة بنها، ص ٥٦ وما بعدها.

لسلطات الدولة، ليست بمثابة استخدام للقوة. الأمر الذي يحرم الدولة، من حقها في استخدام مبدأ الدفاع الشرعي، بل وينكر على الدول استخدام مثل هذا الحق.

كما يقدم هذا البحث، محاولة لسد الفجوة القانونية، في تطبيق قاعدة حظر استخدام القوة، بين الهجمات القتالية الحركية – بشكلها التقليدي المعروف– وبين الهجمات السيبرانية، التي تنشأ في الفضاء السيبراني. لقد تطورت قاعدة حظر استخدام القوة على مر السنين، وتم تعديلها وتطويرها، وفقا للتطورات والتغيرات القانونية، في الحياة الحديثة. لقد شكلت الأحداث التاريخية مثل: الحرب الباردة، والإرهاب، والاحتلال الحربي، تحديات قانونية أعادت صياغة قاعدة حظر استخدام القوة. ويشكل الفضاء السيبراني تحديا جديدا، حيث يقدم منظورا جديدا، في مجالات استخدام القوة بالعلاقات الدولية، ولكن هذه المرة في العالم الافتراضي. ونظرا لكون قاعدة حظر استخدام القوة في العلاقات الدولية، تشكل واحدة من أهم الركائز القانونية الصلبة، في مجال العلاقات الدولية؛ فإنه يلزم أن تكون مستوحاة من عالمنا المتغير باستمرار، ومتواكبة مع تطوره.

كما يتناول البحث، أحكام المسؤولية الدولية، عن الهجمات السيبرانية. وذلك باعتبار أن تنفيذ تلك الهجمات السيبرانية، قد يمثل فعلا دوليا غير مشروع، بل ويمثل خرقا لقواعد القانون الدولي. وعليه نبحث مدى انطباق أحكام المسؤولية الدولية، في مجال الهجمات السيبرانية، لأشخاص القانون الدولي، حال ارتكاب التصرفات غير المشروعة دوليا، والتي تشكل خرقا للالتزامات الدولية النافذة.

١. أسباب اختيار موضوع البحث:

لقد شكل الاهتمام العالمي المتزايد، بالتحول إلى النمط الرقمي، في كافة التعاملات، سواء المدنية أو العسكرية، مجالا خصبا لتزايد الانتهاكات السيبرانية. إذ تلاحظ اتساع دائرة الهجمات السيبرانية، كما تلاحظ مدى جسامة الأضرار، التي تنجم

عن تلك الهجمات السيبرانية، سواء استهدفت تلك الهجمات، مواقع مدنية، أو مواقع عسكرية، مما يهدد الأمن والسلم الدوليين. فضلا عن وجود فراغ تشريعي دولي، ينظم ويعالج موضوع الهجمات السيبرانية.

٢. منهج البحث:

يسعى الباحث للإلمام بجوانب هذا الموضوع، نظرا لأهميته العلمية والعملية، وذلك من خلال تقديم دراسة قانونية موجزة، بالاعتماد على ما يخدم البحث، من مناهج البحث العلمي. وتعتمد الدراسة على "المنهج التاريخي"، لبيان نشأة وتطور الهجمات السيبرانية. كما اعتمد البحث على "المنهج التحليلي" وذلك عند الحاجة إلي الاستعانة، بالنصوص القانونية الدولية، والآراء الفقهية، وأحكام القضاء الدولي.

٣. خطة البحث:

ينقسم هذا البحث إلى ثلاث مطالب:

المطلب الأول: لمحة عن ماهية ونشأة الهجمات السيبرانية

المطلب الثاني: التكييف القانوني للهجمات السيبرانية في ضوء التنظيم الدولي المعاصر

المطلب الثالث: المسؤولية الدولية الناشئة عن الهجمات السيبرانية

المطلب الأول

لمحة عن ماهية ونشأة الهجمات السيبرانية

مصطلح الهجمات السيبرانية، هو مصطلح حديث، ظهر في العقود الأخيرة؛ نتيجة لثورة تكنولوجيا المعلومات، ولم تكن الهجمات السيبرانية معروفة إلا منذ وقت قريب. مما يشكل أحد أهم التحديات الراهنة، التي يواجهها المختصون في القانون الدولي العام، فيما يخص تحديد طبيعتها، أو تعريفها، أو الكشف عن عناصرها. وللوقوف على مفهوم هذا المصطلح حديث النشأة, سيتم التطرق إلى تعريف الهجمات السيبرانية لغويا في ضوء المعاجم اللغوية، بالإضافة إلى التطرق لتعريف الهجمات السيبرانية اصطلاحا، في ضوء الاجتهادات الفقهية، والممارسات الدولية. فضلا عن الوقوف على نشأة الهجمات السيبرانية، وأشهر النماذج المعاصرة لها، وذلك على النحو التالي:

أولا: مصطلح "السيبرانية" في اللغة:

يرجع أصل كلمة (Cyber) في المعاجم اللغوية، إلى المصطلح اليوناني (Kybernetes) ويعني: القيادة أو التحكم عن بعد.[١] وتعرف السيبرانية: بعلم الضبط، ومصدرها (Cybernetics).[٢] بينما تتم الإشارة إلى عالم الرياضيات (Norbert Wiener) باعتباره أول من استخدم مصطلح السيبرانية وذلك في عام ١٩٤٨م، في أثناء دراسته لموضوع القيادة والسيطرة والاتصال في عالم الحيوان.[٣]

---

[١] Julia Cresswell (٢٠١٠), "Oxford Dictionary of word Origins: Cybernetics", Oxford Reference Online, Oxford University Press.

[٢] البعلبكي، منير (٢٠٠٤)، المورد: قاموس انكليزي – عربي، دار العلم للملايين، بيروت، ص ٢٤٣.

[٣] Norbert Wiener (١٩٤٨), "Cybernetic or control communication in the animal and the machine, M.I.T, Press, Second Edition, Cambridge, Massachusetts.

ثانيا: مصطلح "السيبرانية" في الاصطلاح:

تعددت التعاريف التي تناولت، مصطلح الهجمات السيبرانية، على ضوء الاجتهادات الفقهية، والممارسات الدولية العملية.

ومن تلك التعاريف، ما جاء به خبراء القانون الدولي الإنساني، ومنهم (Schmitt) إذ يرى الهجوم السيبراني بأنه: "مجموعة من الإجراءات، التي تتخذها الدولة، من أجل الهجوم على نظم المعلومات للعدو، بهدف التأثير والإضرار بها. وفي الوقت نفسه، للدفاع عن نظم المعلومات، الخاصة بالدولة المهاجمة".[١]

بينما عرفها (Zimet & Barry) بأنها: "مجموعة من العمليات القائمة على الحرب الإلكترونية، والخداع النفسي، فضلا عن استهداف شبكة تواصل العدو العسكرية، وعملياته الأمنية الإلكترونية".[٢]

ويذهب (Roscini) إلى تعريفها أنها: "تطويع الإمكانيات الإلكترونية العسكرية، لأجل التأثير في مواقع إلكترونية أخرى، وتعطيلها أو تدميرها، سواء أكانت تقدم خدمات مدنية أو عسكرية".[٣]

ونرى من خلال إمعان النظر – في التعاريف السابقة – أن الهجمات السيبرانية قد تشكل وسيلة قتالية بذاتها، أو تشكل طريقة من طرق الحرب، وذلك بالنظر إلى الهدف من استخدامها. بحيث عندما تسهم في توجيه العمليات العسكرية، لتحديد أهداف عسكرية منتقاه وتدميرها، أو لتعطيل أجهزة الكشف المبكر للهجمات،

---

[١] Michael N. Schmitt (١٩٩٩), 'Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework', Columbia Journal of Transnational Law, Vol. ٣٧, P.٨٩٠.

[٢] Elihu Zimet, Charles L. Barry (٢٠٠٩), "Military services Overview, Cyber power and National Security, National Defense University Press, Washington DC, USA, P. ٢٩١.

[٣] Marco Roscini (٢٠١٠), World Wide Warfare: Jus ad bellum and the use of cyber force, Max Planck Yearbook of United Nations Law, Vol. ١٤, P. ٩١.

التي يقوم بها العدو، أو تشويش وقطع عمليات الاتصال في المطارات العسكرية أو المدنية. وفي هذه الحالات يعتبر الهجوم السيبراني طريقة قتالية مساعدة، إذ يدخل من ضمن الخطط العسكرية. ونسوق مثالا على ذلك، الهجوم الذي قام به الاحتلال الصهيوني، عام ٢٠٠٧م، ضد مواقع سورية، زعمت إسرائيل أنها منشآت نووية. حيث تم رصد توقف عمل أجهزة الرادار، ومنظومة الاتصال في المطارات العسكرية والمدنية، أثناء الهجوم الجوي الصهيوني.[١]

كذلك قد تكون الهجمات السيبرانية وسيلة قتالية بذاتها، من خلال استخدامها للتسلل إلى الأنظمة الإلكترونية، الخاصة بحماية وتنظيم عمل المنشآت الحيوية. كمحطات الكهرباء والمياه، ومحطات الطاقة النووية، أو السدود، أو وسائل النقل، بهدف السيطرة والتحكم بها، مما قد يؤدي إلى تعرضها للتعطيل الكلي أو الجزئي، أو الانفجار، أو تأخير أداء مهامها المعتادة. ومن أشهر الأمثلة على ذلك، ما تعرضت له المحطة النووية الإيرانية، من هجوم سيبراني، أدى إلى تعطل بعض العمليات الفنية، وألحق أضرارا جزئية بعمليات تخصيب اليورانيوم. ويعتبر هذا الهجوم من أبرز السوابق، في حقل الهجمات السيبرانية.[٢]

ويذهب جانب من الفقه الدولي، إلى القول بعدم صحة تصنيف الهجمات السيبرانية، كوسيلة قتالية بذاتها. ويدلل على ذلك بأن الأدوات المستخدمة في الهجمات السيبرانية، لا تحتوي على الطاقة الحركية (Kinetic) والتي تعتبر أهم صفات الأسلحة التقليدية. حيث لا يمكن – في رأيهم – تحسس الهجوم السيبراني على نحو مادي،

---

[١] Thomas Rid and Peter Mcburney (٢٠١٢), "Cyber – Weapons", Routledge publisher, The RUSI Journal, Vol.١٥٧, NO.١.P. ٦.

[٢] Micheal Gervais (٢٠١٢),"Cyber Attacks and the Laws of War", Berkeley Journal of International Law, Vol: ٣٠, Issue .٢, Article ٦, p.٤٦.

بالإضافة إلى عدم احتواء أدوات الهجوم السيبراني، على مواد شديدة الانفجار، ولذلك يرى أنصار هذا الرأي استبعاد الهجمات السيبرانية من طائفة الأسلحة.[١]

وفي هذا الشأن، نرى أن استبعاد الهجمات السيبرانية، من فئة الأسلحة، هو اجتهاد فقهي غير صائب. إذ لا يشترط في الأسلحة عموما، احتوائها على الطاقة الحركية. فعلى سبيل المثال، فإن الأسلحة البيولوجية لا يشترط احتوائها على طاقة حركية، أو مواد شديدة الانفجار. كما أنه يمكن استخدامها دون الحاجة إلى قذائف أو صواريخ.

وبذلك يكون المعيار الأنسب – من وجهة نظرنا – للتمييز بين وسائل وطرق القتال، هو الهدف والنتيجة من الاستخدام. فكلما تسببت سواء بشكل مباشر أو غير مباشر، في قتل أو جرح أو تدمير أو تعطيل (كلي أو جزئي)؛ فإنها تعد وسيلة قتالية. أما إذا استخدمت كجزء من مخطط عسكري؛ فإنها تعتبر من طرق القتال. والهجمات السيبرانية تتصف بالوصفين معا.

ثالثا: نشأة الهجمات السيبرانية

ترتبط الهجمات السيبرانية بحدثين هامين. الحدث الأول: هو استحداث أجهزة الحاسب الألي، في منتصف الخمسينيات من القرن الماضي، كأداة لمعالجة وحفظ المعلومات بشكل رقمي (Digital). وقد تطور ذلك بصورة كبيرة، خلال العقود اللاحقة، حتى أصبح الحاسب الآلي، يمثل حجر الأساس في عمل أغلب المؤسسات العامة والخاصة، بالإضافة إلى تدخل التكنولوجيا في الحياة اليومية للأفراد. أما الحدث الثاني: فهو ظهور الشبكة العنكبوتية (Internet)، والتي أحدثت اختلافا كبيرا، في حياة البشرية، من خلال القدرة على التواصل، ونقل المعلومات بسرعة فائقة. كما تبنت

[١] Nils Melzer (٢٠١١),"Cyber warfare and International Law: IDEAS for Peace and Security", UNIDIR Researches, P. ٥.

الدول نهجا إلكترونيا، لتحقيق قفزات نوعية في المجال الأمني والعسكري، وذلك منذ مطلع التسعينيات من القرن الماضي.[١]

وفي بادئ الأمر، لم تكن للهجمات السيبرانية صدى على المستوى الدولي. إذ نشأت الهجمات السيبرانية، على هيئة جرائم تقوم بها أفراد، أو مؤسسات خاصة، ضد المؤسسات المالية والمصرفية، والشركات الخاصة بتطوير برامج الحاسب الألي، لأغراض تحقيق مكاسب مالية. ولقد عالجت الكثير من الدول، هذه الطائفة من الجرائم عن طريق، سن التشريعات التي تجرم الدخول غير المشروع، إلى المواقع الإلكترونية والأنظمة المعلوماتية المملوكة للغير. وأما فيما يخص الدول، فغالبا ما تلجأ الدول لاستخدام التكنولوجيا المتقدمة في أهدافها العسكرية، لغرض تحقيق الهيمنة العسكرية على الخصوم.

بيد أن الأمر لم يقف عند ذلك الحد، حيث اتسع نطاق استخدام الهجمات السيبرانية، ليشمل تهديد المصالح العسكرية والسياسية والاقتصادية للدول. فضلا عن التهديدات الإجرامية، الناشئة عن الكيانات الإرهابية. ويسجل لنا التاريخ المعاصر، العديد من النماذج عن الهجمات السيبرانية، نذكر منها على سبيل المثال:

١. الهجوم السيبراني الذي نفذته الولايات المتحدة الأمريكية، ضد منظومة التحكم في أنبوب النفط التابع للاتحاد السوفيتي السابق (Chelyabinsk)، والذي أدى لانفجار كبير، وخسائر بالغة. علما بأن الاتحاد السوفيتي قد نفى هذا الهجوم آنذاك.[٢]

---

[١] Peter Sommer & Ian Brown (٢٠١١),"Reducing Systemic Cyber security Risk", OCED, PP.١٣-١٦.

[٢] Diego Rafael Canabarro and Thiago Borne (٢٠١٣),"Reflection on the fog of Cyber War", National Center for Digital Government, Policy working Paper No.١٣:٠٠١, March ١, ٢٠١٣, footnote ١١, p.١٠.

٢. الهجوم السيبراني الذي تعرضت له أنظمة الاتصال الإلكترونية، التابعة لوزارة الدفاع الأمريكية (Pentagon)، ووكالة الفضاء الأمريكية (NASA)، ووكالة الطاقة الأمريكية بين الأعوام ١٩٩٨ – ٢٠٠٠، والذي أدى إلى الاستحواذ على ملفات سرية. وقد وجهت الولايات المتحدة الأمريكية، اتهام رسمي إلى روسيا الاتحادية. في حين أنكرت روسيا مسؤوليتها عن الهجوم.[١]

٣. الهجوم السيبراني الذي تعرضت له (Estonia) عام ٢٠٠٧، بعد أن قررت الحكومة نقل تمثال الجندي البرونزي، والذي يمثل التضحية السوفيتية، من العاصمة (Tallinn) إلى مكان آخر بجانب المقابر العسكرية. والذي أدى إلى تعطيل كلي لمواقع حيوية، تشمل الموقع الرسمي لرئيس الوزراء، والبرلمان، والبنوك، والصحف. ولقد تم توجيه الاتهام إلى روسيا الاتحادية، واعتبرتها استونيا هجمات انتقامية ردا على نقل التمثال.[٢]

٤. الهجوم السيبراني خلال عام ٢٠١٠ على منشأة خاصة بتخصيب اليورانيوم، بالقرب من مدينة (Natanz) الإيرانية. عن طريق استخدام البرمجيات الخبيثة، والتي أطلق عليها (Stuxnet). ويعد هذا الهجوم هو الأخطر على صعيد الهجمات السيبرانية، لمنشآت مدنية أو عسكرية على الإطلاق، وذلك لاستهداف أجهزة الطرد المركزية

[١] Scott J. Shackelford (٢٠٠٩),"From Nuclear War to Net War: Analogizing Cyber Attacks in International Law", Berkeley Journal of International Law, Vol. ٢٧:١, P. ٢٠٤.

[٢] Janne Valo (٢٠١٤), Cyber Attacks and the Use of Force in International Law, Master's Thesis, Faculty of law, University of Helsinki, P. ١٣.

وخروجها عن السيطرة، ولقيامة بالتحايل على أجهزة التحكم، والايحاء لها أنها تعمل بصورة طبيعية.[١]

المطلب الثاني

التكييف القانوني للهجمات السيبرانية في ضوء التنظيم الدولي المعاصر

يشكل ظهور الإنترنت، وسرعة انتشاره على الصعيد العالمي، سببا في حدوث أسرع وأقوى ثورة تكنولوجية، في تاريخ البشرية. وبفعل تلك الثورة الهائلة، أصبحت الدول، والمؤسسات العامة، والكيانات الخاصة، والأفراد في حالة ترابط لم يحدث من قبل. وفي ذات الوقت، فقد ازداد الاعتماد العسكري، على أنظمة الحاسب الآلي، مما فتح المجال "**الخامس**" من القتال إلى جانب المجالات التقليدية: الأرض، والبحر، والجو، والفضاء الخارجي، فيما يعرف بحروب الجيل الخامس.

لقد واجه العالم في الفترة الأخيرة، نوعا جديدا من الهجمات الدولية، والتي تعرف بالهجمات السيبرانية. والتي تبدو مختلفة عن الحروب العسكرية، وتختلف كذلك عن الجرائم الإلكترونية، والتي يكون هدفها في الغالب ماليا. فالهجمات السيبرانية لها أهداف سياسية، وخير دليل على ذلك، الهجوم السيبراني بفيروس **(Stuxnet)**. والذي غير مسار التاريخ السيبراني, حيث كان ذلك البرنامج الخبيث، أكبر مثال على الهجمات السيبرانية في الفترة الأخيرة، حيث ضرب المنشأة النووية الإيرانية. إضافة إلى ذلك, فإن الجماعات الإرهابية، لم تغفل عن الفضاء السيبراني، فقد استغلوه كوسيلة سهلة للتواصل مع الأفراد والجماعات الأخرى حول العالم. وهذا التطور الذي أحدثه الفضاء السيبراني، على الساحة الدولية يثير التساؤل: إلى أي مدى يمكن أن تطبق قواعد القانون الدولي الإنساني على المجال السيبراني؟ فإذا كان الأصل أن القانون

[١] Ibid, P. ١٤.

الدولي القائم، يحكم أنشطة الدولة أينما كانت، بما في ذلك الفضاء السيبراني. بيد أن تطبيق القواعد والمفاهيم القانونية الموجودة مسبقا، إلى تكنولوجيا جديدة قد ينطوي على بعض الصعوبات، في ضوء الخصائص المتميزة للفضاء السيبراني.

إن البحث في إمكانية، تطبيق قواعد القانون الدولي الإنساني، على الهجمات السيبرانية، قد يستلزم بحث مسألة مدى شرعية الهجمات السيبرانية، في ضوء حظر استخدام القوة في العلاقات الدولية. فالقانون الدولي المعاصر، قائم على مبدأ حظر استخدام القوة أو التهديد باستخدامها في العلاقات الدولية. ويستثنى من ذلك حق الدول فرادى أو جماعات، في الدفاع عن نفسها بموجب حق الدفاع الشرعي، المقرر بنص المادة (٥١) من ميثاق الأمم المتحدة. أو بموجب التدابير التي يتخذها، مجلس الأمن وفقا لصلاحياته، في الحفاظ على السلم والأمن الدوليين، والمقررة بالفصل السابع من ميثاق الأمم المتحدة. وأما بخلاف ما سبق فإن استخدام القوة في العلاقات الدولية، يعتبر عملا غير مشروع، وفقا لقواعد القانون الدولي المعاصر. وتثور هنا إشكالية تفسير كلمة "**القوة**"، الواردة بنص المادة (٤/٢) من ميثاق الأمم المتحدة. إذ تحظر المادة (٤/٢) من ميثاق الأمم المتحدة، على الدول استخدام القوة أو التهديد بها، لكن لا يوجد تعريف صريح لما يشكل القوة.[١]

لقد انقسمت آراء الفقه الدولي، حول تفسير لفظ "القوة" الوارد في نص المادة (٤/٢). وذلك من حيث أن الحظر يشمل استخدام القوة العسكرية، أو التهديد باستخدامها. أم أن اللفظ الوارد يتسع ليشمل، الضغوط الاقتصادية والسياسية والتهديد بها أيضا، وذلك إلى ثلاث اتجاهات:[٢]

---

[١] Janne Valo (٢٠١٤), op. cit., P. ٣٠.

[٢] الموسى، محمد خليل (٢٠٠٤)، استخدام القوة في القانون الدولي المعاصر، الأردن: دار وائل للنشر، الطبعة الأولى، ص ١٥. حسين، محمد ربيع أحمد (٢٠٢٢)، مرجع سابق، ص ٢٢٠ – ٢٢٥.

الاتجاه الأول: المذهب الموسع لحظر استخدام القوة

يذهب أنصار هذا الاتجاه، إلى القول بأن النص يحظر كل الأشكال، التي يمكن أن تأخذها القوة المستعملة. سواء أكانت القوة مباشرة، كاستخدام القوة العسكرية أو غير مباشرة، كالضغوط السياسية، والاقتصادية. ويرى الفقه المؤيد لهذا الاتجاه، أن مصطلح القوة إنما يشتمل على استعمال القوة بأنواعها، وحتى تلك التي لا تصل لدرجة استعمال القوة المسلحة، كالتهديد باستخدامها.

الاتجاه الثاني: المذهب المضيق لحظر استخدام القوة

يذهب أنصار هذا الاتجاه، إلى أن هذا النص، يحظر فقط استخدام القوة المسلحة أو التهديد بها، دون إمكانية إدراج الضغوط الأخرى، للحظر المنصوص عليه. وعليه فإن هذا الاتجاه الفقهي، يرى أن لفظ القوة الوارد في الميثاق، ينصرف إلى القوة العسكرية، ولذلك لا يجوز اعتبار التهديدات السياسية والاقتصادية، فعلا من أفعال القوة، التي تستوجب الدفاع الشرعي.

الاتجاه الثالث: المذهب التوفيقي

يرى أنصار هذا الاتجاه، أن الضغوط الاقتصادية وغيرها، إذا تمت ممارستها بدرجة كبيرة، فإنها تدخل في نطاق حظر استخدام القوة. وحجتهم في ذلك، أن العبارات التي تضمنها الميثاق، في الفقرة (٤) من المادة (٢)، جاءت عامة بحيث لا تنصرف إلى القوة العسكرية وحدها. فضلا عن كون استهداف الوحدة الترابية للدولة، واستقلالها السياسي، يمكن الوصول إليه، من خلال ممارسة الضغوط الاقتصادية وغيرها.

هذا، ونرى، أن الاتجاه الثالث، هو الأقرب إلى الواقع الدولي المعاصر. إذ أن قصر لفظ "**القوة**" على استعمال القوة العسكرية فقط. دون باقي وسائل الضغط – التي يمكن اتباعها من جانب الدول ضد بعضها البعض – يؤدى إلى إبقاء الدول المستهدفة بالتصرف، عاجزة عن الدفاع الشرعي عن نفسها. لاسيما وأن الضغوط السياسية

والاقتصادية، إذا تمت ممارستها بدرجة كبيرة على الدولة، قد تؤدى إلى فشل الدولة، وانقسامها، واشتعال الثورات فيها. وهذا يؤدى – بلا شك– إلى الإضرار بالوحدة الإقليمية للدولة، واستقلالها السياسي.

وبناء على تأييدنا للاتجاه الثالث، وبتطبيق ذاك على الهجمات السيبرانية، يتبين أن الهجمات السيبرانية شأنها شأن الحروب البيولوجية أو الجرثومية، لا يتوافر لها العنصر الحركي، المتوافر في الحروب التقليدية. غير أنها مازالت تشكل تهديدا للاستقلال السياسي للدول، وتضر بالوحدة الإقليمية لها، إذا تمت ممارستها على نطاق واسع، ومن ثم، فإنها تدخل من ضمن الأفعال المحظورة بموجب الميثاق.

إن قواعد القانون الدولي، رغم كونها قواعد آمرة، إلا أنها ليست جامدة. بمعنى أنها يجب أن تتطور، لمواكبة التطور الحاصل على الصعيد الدولي. هذا الأمر الذي يستدعي بالضرورة النظر في تغيير مفهوم "القوة" لتصبح: "مجموعة من الوسائل والطاقات والامكانيات المادية وغير المادية، المنظورة وغير المنظورة، التي بحوزة الدولة، ويستخدمها صانع القرار، في فعل مؤثر، يحقق مصالح الدولة، وتؤثر في سلوك الوحدات السياسية الأخرى".[١]

ومن ثم، فإن عناصر القوة وفقا للمنظور السابق، تتمثل في التناغم بين القدرات التكنولوجية، والسكانية، والاقتصادية، والصناعية، والقوة العسكرية، التي تحوزها الدولة. مما يسهم في دعم امكاناتها على ممارسة الإكراه، أو الإقناع، أو ممارسة التأثير السياسي، في أعمال الدول الأخرى، بغرض الوصول للأهداف. سواء أكانت تلك الأهداف مشروعة – متى ما توافقت مع القواعد القانونية، ومنها القواعد القانونية الدولية – أو غير مشروعة. وبالتالي فإن التغير في مفهوم القوة يؤدي

[١] جوزيف ناي، ترجمة أحمد أمين الجمل، ومجدي كامل (١٩٩٧)، المنازعات الدولية– مقدمة للنظرية والتاريخ، الجمعية المصرية لنشر المعرفة والثقافة العالمية، القاهرة، ص ٨٢.

بالضرورة إلى تغير في منظور الحرب، حيث انتقلت من نسق الحروب التقليدية القائمة على تدمير الخصم أو احتلال أرضه أو الاستيلاء على موارده، إلى حروب تعمل للاستحواذ على سباق التقدم التكنولوجي، وسرقة الأسرار الاقتصادية والعلمية، والتحكم بالمعلومات، والعمل على اختراق الأمن القومي، بدون طائرات أو متفجرات، أو حتى انتهاك الحدود، والتي قد يكون لها تأثير يفوق الحرب التقليدية، لما تشكله من آثار مدمرة على الاقتصاد والبنية التحتية.

لم يكن اختلاف الآراء الفقهية، حول تفسير مفهوم لفظ "القوة"، الواردة في ميثاق الأمم المتحدة، هو الاختلاف الوحيد، الذي يثيره بحث التكييف القانوني للهجمات السيبرانية. إذ أن الآراء الفقهية قد اختلفت، في شأن تحديد القانون الواجب التطبيق، على الهجمات السيبرانية، إلى اتجاهين:

يرى **الاتجاه الأول:** أن الهجمات السيبرانية ليست مقننة أو منظمة، وفقا للقواعد الدولية المتعارف عليها. ويدلل أنصار هذا الاتجاه على ذلك، بأن المدة التي جرى فيها سن القواعد القانونية، ذات الصلة باستخدام وسائل وطرق القتال.[١] تسبق نشأة استخدام الأنظمة الإلكترونية، في الأغراض العسكرية، وعليه ينتهى أنصار هذا الاتجاه، إلى القول بأن الهجمات السيبرانية، ليس لها أي أساس قانوني، في أغلب قواعد القانون الدولي.[٢] ويرى أنصار هذا الاتجاه، أن قواعد القانون الدولي الإنساني، ليست كافية لتنظيم وتكييف الهجمات السيبرانية، مما يشير وبقوة إلى ضرورة إعادة

---

[١] يشير أنصار هذا الاتجاه إلى الفترة الزمنية، التي تم فيها سن القواعد الدولية، المنظمة للحرب، والتي أبرمت في منتصف القرن الثامن عشر، والتي تتمثل في اتفاقيات لاهاي لعام (١٨٩٩ – ١٩٠٧). واتفاقيات جنيف لعام ١٩٤٩، واللحقين الإضافيين لعام ١٩٧٧، تلك القواعد القانونية التي تشكل في جملتها قواعد القانون الدولي الإنساني.

[٢] Rwx HUGES (٢٠١٠),"A treaty for Cyberspace", International Affairs journal, Vol.٨٦.No.٢, P.٥٣٣.

النظر بتلك القواعد القانونية، حتى تستوعب دخول أنماط جديدة وغير تقليدية على وسائل وطرق القتال.[١]

ويرى **الاتجاه الثاني:** أن الهجمات السيبرانية، يمكن أن ترتكب في أثناء النزاعات المسلحة، سواء النزاعات المسلحة الدولية أو الداخلية، كما يمكن أن ترتكب في أوقات السلم كذلك. وعليه، فإن الهجمات السيبرانية لا تخضع لقواعد القانون الدولي الإنساني والجنائي فحسب، بل هي تخضع – في رأي أنصار هذا الاتجاه – إلى قواعد ومبادئ القانون الدولي العام في مجملها. وينتهي أنصار هذا الاتجاه إلى القول، بأن المبادئ والقواعد المكونة للقانون الدولي الإنساني، تنطبق على الهجمات السيبرانية.[٢]

هذا، ونرى، أن الاتجاه الأول قد جانبه الصواب، وذلك بالنظر إلى عاملين أساسيين:

العامل الأول: يتعلق بكون القواعد القانونية ليست مرتبطة بالوقت التي أبرمت فيه، وبعبارة أخرى فإن القواعد القانونية ليست قوالب جامدة. كما أنها ليست نصوصا مقدسة، بل هي نتيجة للاجتهادات الفقهية، في وقت معين، وفي ظروف معينة، وبالتالي فهي تقبل التطور، حال اختلاف الوقت، وتغير الظروف التي أنشأتها.

العامل الثاني: فيتمثل في (Martens Principle)

ترجع نشأة هذا المبدأ إلى: (Fyodor Fyodorovich Martens).[٣] أحد مندوبي روسيا في مؤتمر السلام عام ١٨٩٩. إذ صرح: "أنه في الحالات غير

---

[١] Davis Brown (٢٠٠٦), "Proposal for an international convention to regulate the use of information System in Armed Conflict", Harvard International Law review, Vol. ٤٧, P.١٧٩.

[٢] See Rwx HUGES (٢٠١٠), op. cit., P. ٥٣٣.

[٣] He is a Russian jurist and diplomat, international arbitrator and historian of European colonial ventures in Asia and Africa. Born: August ٢٧, ١٨٤٥ in Livonia. And Died: June ٢٠, ١٩٠٩ (aged ٦٣) in St. Petersburg. https://www.britannica.com/biography/Fyodor-Fyodorovich-Martens

المشمولة بالأحكام، يظل السكان المتحاربون، تحت حماية وسلطان مبادئ قانون الأمم، كما جاءت به من تقاليد، والتي استقر عليها الحال بين الشعوب المتمدنة، وقوانين الإنسانية، ومقتضيات الضمير العام".[١] ولقد تكرر مضمون هذا المبدأ، عند صياغة ديباجة اتفاقية لاهاي الثانية، المتعلقة بقوانين وأعراف الحرب البرية ١٨٩٩، حيث نصت: "**حتى تصدر مدونة بقوانين الحرب أكثر اكتمالا، ترى الأطراف المتعاقدة، من المناسب أن تعلن، أنه في الحالات، التي لا تشملها، هذه اللائحة التي اعتمدتها، يظل السكان المدنيون والمقاتلون، تحت حماية مبادئ الأمم، الناتجة عن العادات الراسخة، بين الشعوب المتحضرة، وقوانين الإنسانية، وما يمليه الضمير العام**".[٢]

ولقد أشار بعض الفقه الدولي، أن مبدأ مارتينيز، يعتبر الأكثر قربا، للتطبيق على الهجمات السيبرانية. وذلك كونه يغطي أوضاعا، غير منظمة في الاتفاقيات الدولية. ولا يكون ذلك ممكنا، إلا باللجوء للقانون الدولي العرفي، ذلك المصدر الذي أشارت إليه المادة (٣٨) من النظام الأساسي لمحكمة العدل الدولية.[٣] وكذلك يرى آخر، أن مسألة الفراغ القانوني، لموضوع الهجمات السيبرانية، لا يعتبر سوى حجة

---

[١] Antonio Gessese (٢٠٠٠),"The Martens Clouse: Half a loaf or simply pie in the sky?", EJIL, Vol. III, No. ١, PP. ١٩٣ - ١٩٤.

[٢] بالإضافة إلى اتفاقية لاهاي الثانية لعام ١٨٩٩، فقد تم الإشارة إلى هذا المبدأ في العديد من الصكوك الدولية منها: اتفاقيات جنيف الأربعة لعام ١٩٤٩، حيث ورد النص بالمادة ٦٣ بالاتفاقية الأولى. والمادة ٦٢ من الاتفاقية الثانية. والمادة ١٤٢ من الاتفاقية الثالثة. والمادة ١٥٨ من الاتفاقية الرابعة. كما أشار اللحق الإضافي الأول لعام ١٩٧٧ لهذا المبدأ بالمادة ٢/١. وكذلك تمت الإشارة لهذا المبدأ بديباجة اللحق الإضافي الثاني لعام ١٩٧٧. بما يفيد تواتر العمل بهذا المبدأ في قواعد القانون الدولي.

[٣] Micheal N. Schmmitt (٢٠٠٢),"Wired warfare: Computer network attack and jus in Bello", IRRC, Vol.٨٤, No.٨٤٦, P.٣٦٩

مصطنعة للبعض، ويسوق تأييدا لرأيه القول: "بأن مبدأ مارتينيز يشير إلى أنه حال عدم وجود نص واضح، في الاتفاقيات الدولية المعاصرة، أو الأعراف الدولية المستقرة؛ فإن المبادئ التي تضمنها قانون النزاعات المسلحة [سواء أكانت نزاعات مسلحة دولية أو داخلية] تكون هي المبادئ واجبة التطبيق في هذه الحالة".[١]

دليل تالين (Tallinn Manual):[٢]

يشكل دليل تالين، أول محاولة دولية، للبحث في التكييف القانوني، للهجمات السيبرانية، بإصدارية الأول عام ٢٠١٣، والثاني عام ٢٠١٧. حيث أكدت قواعده، على أن بعض أحكام القانون الدولي المعاصر، يمكن تطبيقها في مجال الفضاء السيبراني. أو اعتبارها نقطة انطلاق مناسبة، لكيفية التعامل مع هذا التطور

---

[١] Erki Kodar (٢٠١٢),"Applying the law of armed conflicts to Cyber-attacks: from the Martens Clouse to Additional Protocol I", ENDC Proceeding, Volume ١٥, P.١١٠

[٢] وهو عبارة عن دراسة غير ملزمة للدول، أعدها (٢٠) أكاديميا ومتخصصا في القانون الدولي، ويشار إليهم بفريق الخبراء (IGE)، وتبنى الإشراف على إعداده حلف شمال الأطلسي (NATO)، ويبين الدليل مدى ملاءمة القانون الدولي للتطبيق على الهجمات السيبرانية. بدء إعداد هذا الدليل خلال عام ٢٠٠٩، داخل مركز للدفاع السيبراني التابع لحلف الناتو، في مدينة "تالين" عاصمة "استونيا". وظهر أول إصدار له عام ٢٠١٣، تحت اسم "تالين ١"، وتضمن (٩٥) قاعدة توجيهية لسلوك الدول، في سياق الحروب السيبرانية، مع تعليقات على كل قاعدة. وفي عام ٢٠١٧ ظهر الإصدار الثاني، تحت اسم "تالين ٢"، وتضمن (١٥٤) قاعدة، ليشكل مستوى أكثر اتساعا لمعالجة الهجمات السيبرانية، مع التعليق على كل قاعدة. وترجع تسمية الدليل بهذا الاسم، نسبة إلى "تالين"، عاصمة "استونيا"، التي تعرضت لسلسلة هجمات سيبرانية من جانب "روسيا" عام ٢٠٠٧. وللمزيد:
E. T. Jensen (٢٠١٧), The Tallinn Manual ٢.٠: Highlights and Insights, Research Paper, No. ١٧, Georgetown Journal of International Law, P. ١.
R. Buchan (٢٠١٩), Cyber Espionage and International Law, HART Publishing, Oxford, PP. ٦ - ١٩.

التكنولوجي. لقد ساهم هذا الدليل، بشكل فعال، في النقاش بين الدول، حول المواضيع المثيرة للتحديات. وكيفية تفسير القانون الدولي عامة، والقانون الدولي الإنساني خاصة، وكيفية تطبيقه على أنشطة الدول، والأطراف من غير الدول، في الفضاء السيبراني.

يناقش هذا الدليل، مسألة الهجمات السيبرانية، ويقر أن تلك الهجمات قد تشكل، نزاعات مسلحة، لاسيما بالنظر إلى الآثار المدمرة لتلك الهجمات السيبرانية. ويتناول الدليل تعريف الهجوم السيبراني، في ضوء القانون الدولي الإنساني، كما ورد بالقاعدة (٣٠) من "تالين ١"، بأنه: **"كل عملية سيبرانية، سواء أكانت هجومية أو دفاعية، يتوقع أن تتسبب في إيقاع إصابة أو قتل أشخاص، أو إلحاق أضرار بأعيان أو تدميرها".**

وفي الختام نرى، أن السبب الحقيقي وراء تأخر الدول، في الوصول إلى اتفاقية دولية، معنية بالهجمات السيبرانية، إنما يرجع إلى مصالح الدول الكبرى، الرائدة في مجال الفضاء والأمن السيبراني. الأمر الذي يتطلب ضرورة الضغط على المجتمع الدولي، لإنجاز اتفاقية دولية ملزمة، تنظم مسألة الهجمات السيبرانية، من حيث تكييفها القانوني، وعناصرها، وآلياتها، والمسؤولية الدولية عن الأضرار الناشئة عنها.

المطلب الثالث

المسؤولية الدولية الناشئة عن الهجمات السيبرانية

تناولنا فيما سبق، بيان ماهية الهجمات السيبرانية، ولمحة عن نشأتها، وبعض النماذج المعاصرة، التي ترتب عليها أضرارا كبيرة. ثم تناولنا بحث مسألة التكييف القانوني، للهجمات السيبرانية، من خلال استعراض مختلف الآراء الفقهية، التي تناولت بحث تلك المسألة. وانتهينا إلى ضرورة تفسير قواعد القانون الدولي عامة، والقانون

الدولي الإنساني خاصة، بشكل يسمح بمواكبة التطورات التكنولوجية، المتسارعة في وقتنا الراهن.

لقد ثبت من خلال البحث، في موضوع الهجمات السيبرانية، أنها حال ارتكابها سواء في أثناء النزاعات المسلحة، أو في أوقات السلم؛ فإنها – دون أدني شك – تمثل انتهاكا صريحا، لأحكام القانون الدولي. فضلا عما تخلفه وراءها من أضرار، سواء أكانت أضرار مادية، أو معنوية.

ونتناول في هذا المطلب بحث مدى إمكانية، تحريك المسؤولية الدولية ضد أشخاص القانون الدولي، أو إلى مجموعات من غير الدول (Non-State Actors)، حال ارتكاب الهجمات السيبرانية.

المسؤولية الدولية هي عبارة عن جزاء قانوني، يرتبه القانون الدولي العام، كنتيجة لعدم وفاء أحد أشخاصه، بالتزاماته الدولية. ولقد صاغت لجنة القانون الدولي، مشروعا بشأن مسؤولية الدول، عن الأفعال غير المشروعة دوليا.[١] واستقرت اللجنة على ضرورة توافر شرطين، لتحريك دعوى المسؤولية الدولية، بين أشخاص القانون الدولي. ولقد صاغت اللجنة الشروط على النحو التالي:

١. ارتكاب فعل غير مشروع دوليا.

٢. أن ينسب هذا الفعل لشخص دولي.

أما في مجال الهجمات السيبرانية، تثور إشكالية تقرير المسؤولية الدولية، نظرا لطبيعة تلك الهجمات، وتضمنها لبعض الممارسات، التي لم يتحدد وضعها القانوني حتى الآن، كهجمات التجسس السيبراني. كذلك لارتكاب غالبية تلك الهجمات، بواسطة

---

[١] مشروع مواد لجنة القانون الدولي بشأن مسؤولية الدول عن الأفعال غير المشروعة دوليا لعام ٢٠٠١، وثيقة رقم:
(GA Res. ٥٦/٨٣ annex, UN Doc. A/RES/٦٥/٨٣, December ١٢, ٢٠٠١)

أفراد أو كيانات خاصة، مما يتطلب بحث مدى إمكانية إسناد أفعال هؤلاء إلى الدول، أو إلى المنظمات الدولية.[١] وكذلك لقد تولى دليل "تالين" إيضاح، أن مصطلح الدولة المسؤولة، ينصرف إلى تلك الدولة، التي تنتهك التزاما دوليا، تجاه دولة أخرى. ويشار إلى الأخيرة بمصطلح "الدولة المضرورة"، وتتحمل الدولة المسؤولية الدولية، عن الهجمات السيبرانية، التي تنسب إليها، وتشكل خرقا لالتزام دولي.[٢] ويعتبر إسناد أو نسبة الفعل غير المشروع إلى الدول، هو جوهر تقرير المسؤولية، وفق ما أوضحته المادة الأولى، من مشروع لجنة القانون الدولي، بشأن تحمل الدولة المسؤولية عن أفعالها، غير المشروعة دوليا، والتي تشكل خرقا لالتزام قانوني دولي ساري، مع نسبته إليها وفقا للقانون الدولي.

أولا: الفعل غير المشروع دوليا في مجال الهجمات السيبرانية

ترتكب الدولة فعلا غير مشروع دوليا، عندما يشكل التصرف المنسوب إلى الدولة، خرقا لالتزام دولي مقررا على تلك الدولة. ومصطلح خرق التزام دولي على الدولة، متعارف عليه منذ زمن طويل، ويستخدم ليشمل كلا من الالتزامات التعاهدية وغير التعاهدية. ولا يشكل مصدر الالتزام، الذي تم خرقه، أي فارق عند تقرير

---

[١] لقد امتد مفهوم المسؤولية الدولية ليشمل المنظمات الدولية بجانب الدول، حيث انتهت لجنة القانون الدولي عام ٢٠٠٨، من اعتماد مشروع هذه المواد، راجع تقرير لجنة القانون الدولي، الدورة (٥٣)، ملحق رقم (١٠) وثيقة رقم (A/٥٦/١٠).

[٢] انظر القاعدة رقم (٦) من دليل تالين ١، والقاعدة رقم (١٤) من تالين ٢، بعنوان المسؤولية القانونية للدول:

Rule No. (١٤) of the Tallinn Manual ٢: "Internationally wrongful cyber acts a State bears international responsibility for a cyber-related act that is attributable to the State and that constitutes a breach of an international legal obligation".

مسؤولية الدولة.[١] كما أن وصف فعل الدولة، بأنه غير مشروع دوليا، هو أمر يحكمه القانون الدولي. ولا يتأثر هذا الوصف، بكون الفعل ذاته، يعد فعلا مشروعا في القانون الداخلي.

ويتمثل الفعل غير المشروع، في مجال الهجمات السيبرانية، حال شن هجمات سيبرانية على أهداف مدنية، أثناء نزاع مسلح. أو قيام سفينة بهجوم سيبراني، ضد دولة ساحلية، من داخل بحرها الإقليمي، بالمخالفة لقواعد المرور البريء. أو إتاحة دولة ما بنيتها الإلكترونية لدول أو كيانات خاصة أو أفراد، مما يتسبب في الإضرار بدول أخرى، حال فشل الدولة الراعية، في بذل الجهد اللازم لإنهاء هذا الهجوم السيبراني، الصادر من بنيتها الإلكترونية.[٢] وقد تكون العملية السيبرانية، مشروعة دوليا، غير أن وسائل تنفيذها، تنتهك التزامات دولية. إذ على سبيل المثال: عند قيام تبادل تجاري إلكتروني بين دولتين، فتقوم إحداهما باستغلال معلومات تحصلت عليها، عن طريق التجسس السيبراني، ضد الدولة الأخرى، لتعظيم منافعها المالية، وهو فعل يخرق التزام دولي، بحماية حق الإنسان في الخصوصية.[٣]

ومن المعلوم أن الهجمات السيبرانية، قد تبدأ وتنطلق من أي مكان، وعلى ذلك، فإنه لا يوجد شروط تتعلق بالموقع الجغرافي، الذي انطلق منه الهجوم السيبراني،

---

[١] أبو الوفا، أحمد (٢٠٠٣)، المسئولية الدولية للدول واضعة الألغام في الأراضي المصرية: دراسة في إطار القواعد المنظمة للمسئولية الدولية وللألغام البرية، دار النهضة العربية، القاهرة، ص ٢١ – ٢٢.

[٢] M. J. Sklerov (٢٠٠٩), Solving the Dilemma of State Responses to Cyber-attacks: A Justification for the Use of Active Defenses against States Which Neglect Their Duty to Prevent, Mil. L. Rev. ٢٠١, PP. ٣٨ - ٣٩.

[٣] Micheal N. Schmmitt, L. Vihul (٢٠١٩), Tallinn Manual ٢.٠ on the International Law Applicable to Cyber Operations, Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Center of Excellence, Cambridge University Press, P. ١٧٠.

غير المشروع دوليا. إذ قد يبدأ الهجوم من داخل إقليم الدولة المستهدفة، أو إقليم أي دولة أخرى، أو من أعالي البحار، أو من المجال الجوي الدولي، أو من الفضاء الخارجي. ويستثنى من ذلك حالة المرور البريء، حيث يشترط أن تقوم السفينة، بالهجوم السيبراني، من داخل البحر الإقليمي للدولة الساحلية.[١]

ثانيا: تنسيب الفعل غير المشروع دوليا في مجال الهجمات السيبرانية إلى أشخاص القانون الدولي

انتهت لجنة القانون الدولي، إلى أن الشرط الثاني لتقرير المسؤولية الدولية، عقب تحقق الفعل غير المشروع دوليا، هو تنسيب هذا الفعل إلى دولة، وذلك وفقا للمواد (٤ : ١١) من المشروع. ويتحقق ذلك بصدور الفعل، من أي جهاز من أجهزة الدولة، سواء أكان الجهاز يمارس وظائف تشريعية، أو تنفيذية، أو قضائية، أو أية وظائف أخرى. أو من أفراد عاديين، أو أفعال الثوار، وحركات التمرد والعصيان، باعتبار أن هذه الفئات، تمثل أجهزة الدولة، أو تتصرف نيابة عنها، حتى لو تجاوزت تصرفاتها وخالفت، أحكام القانون الداخلي.[٢]

وفي مجال الهجمات السيبرانية، فإن كثير من تلك الهجمات، يتم تنفيذه من جانب، كيانات خاصة أو أفراد، من الممكن أن تستخدمهم الدول أو المنظمات الدولية لهذه الأغراض. وبالتالي، فإن تنسيب هذه الهجمات يواجه العديد من الإشكاليات، من

---

[١] عسكر، محمد عادل (٢٠٢١)، وضع العمليات السيبرانية في القانون الدولي مع التطبيق على ممارسة التجسس وقت السلم–دراسة على ضوء دليل تالين بشأن القانون الدولي المطبق على العمليات السيبرانية ٢٠١٣–٢٠١٧، ص ٤٢٣.

[٢] تسأل الدولة عن الخطأ الذي يرتكبه موظفوها، خلال ممارستهم لأعمالهم، إذا كانوا مخولين سلطة تنفيذ أوامرها. كما تفترض مسئوليتها إذا كانت مذنبة في اختيارهم، وفي الرقابة على أعمالهم، وفي التعليمات الصادرة إليهم. أنظر: أبو الوفا، أحمد (٢٠٠٦)، القانون الدولي والعلاقات الدولية، دار النهضة العربية، القاهرة، ص ٥٠٨ – ٥٠٩.

جراء صعوبة الاعتماد على المعايير التقليدية، لمحاولة إثبات الصلة، بين تلك الفئات وبين أشخاص القانون الدولي. وذلك من حيث بحث مدى انطباق، وصف أجهزة الدولة أو وكلاء الدولة عليهم. أو كونهم مخولين بموجب القانون الداخلي، بممارسة سلطة حكومية بطبيعتها، وبالتالي اعتبارهم كأجهزة الدولة.[١] أو كونهم خاضعين لسيطرة الدولة أو لرقابتها.[٢]

ولمحاولة دراسة هذه الإشكاليات، وبيان احتمالات تنسيب الهجمات السيبرانية، إلى أشخاص القانون الدولي [الدول والمنظمات الدولية]، والقواعد الدولية التي تحكم كل حالة، نفرد النقاط التالية:

أ- مسؤولية الدولة عن قيام أجهزة تابعة لها بهجمات سيبرانية غير مشروعة

أوضحنا سابقا، أن تصرف أي جهاز تابع للدولة، ينسب إلى الدولة، أيا كانت الوظيفة التي يضطلع بها، وأيا كان مكانه في الهيكل التنظيمي للدولة. ونلاحظ هنا، أن اللجنة قد توسعت في مفهوم "أجهزة الدولة"، وهو ذات الاتجاه الذي أقره دليل "تالين ٢" في القاعدة رقم (١٥)، والتي أشارت إلى تنسيب الهجمات السيبرانية، التي تجريها أجهزة الدولة، إلى تلك الدولة. مع اجماع فريق الخبراء، على أنه لا يمكن للدولة، أن تتجنب المسؤولية عن تصرف جهاز تابع لها، بحرمانه من هذا الوضع بموجب تشريع

---

[١] تنص المادة (٥) من مشروع مواد لجنة القانون الدولي على أن: "يعتبر فعلا صادرا عن الدولة، بمقتضى القانون الدولي، تصرف شخص أو كيان، لا يشكل جهازا من أجهزة الدولة، ولكن يخوله قانون تلك الدولة، صلاحية ممارسة بعض اختصاصات السلطة الحكومية، بشرط أن يكون الشخص أو الكيان، قد تصرف بهذه الصفة، في الحالة المعنية".

[٢] تنص المادة (٨) من مشروع مواد لجنة القانون الدولي على أنه: "يعتبر فعلا صادرا عن الدولة، بمقتضى القانون الدولي، تصرف شخص أو مجموعة أشخاص، إذا كان الشخص أو مجموعة الأشخاص يتصرفون في الواقع، بناء على تعليمات تلك الدولة، أو بتوجيهات منها أو تحت رقابتها لدى القيام بذلك التصرف".

خاص.[١] وبشكل عام، يمثل استخدام أصول حكومية – وبخاصة الأصول العسكرية والأمنية – مؤشرا لا يمكن إنكاره، بشأن التنسيب؛ نظرا لعدم إمكان استخدام تلك الأصول إلا من جانب الدولة. أما في مجال الهجمات السيبرانية، فإنه لا يمكن تطبيق تلك الفرضية بسهولة. إذ قد تسيطر دولة أو كيان خاص أو حتى فرد، على البنية الإلكترونية حكومية، ويتم استغلال تلك البنية بهجمات سيبرانية. ولذلك نلاحظ أن دليل "تالين"، لم يكتفي بانطلاق الهجوم السيبراني، من بنية إلكترونية حكومية لدولة، كدليل لتنسيب ذلك الهجوم إلى هذه الدولة. وإنما اعتبر ذلك مجرد قرينة أو إشارة قوية، بأن تلك الدولة، قد تكون مرتبطة بذلك الهجوم.[٢]

أما فيما يتعلق بوضع جهاز تابع لدولة، تحت تصرف دولة أخرى، فإنه في هذه الحالة، إذا كان الجهاز يمارس اختصاصات السلطة الحكومية، للدولة التي يوضع تحت تصرفها؛ فإن التصرفات الصادرة عن هذا الجهاز تنسب إلى الدولة، التي هو تحت تصرفها.[٣] وبذات المعنى قضت القاعدة رقم (١٦) من دليل "تالين ٢"، وذلك بالنسبة للعمليات السيبرانية. ولكن مع توافر شرطين: السيطرة الحصرية على الجهاز.

---

[١] Rule No. (١٥): **Attribution of cyber operations by state organs**
"Cyber operations conducted by organs of a state, or by persons or entities empowered by domestic law to exercise elements of governmental authority, are attributable to the State".

[٢] نصت القاعدة (٧) من دليل تالين: تحت عنوان: العمليات السيبرانية التي انطلقت من البنية التحتية الإلكترونية الحكومية
"بأنه مجرد انطلاق عملية سيبرانية من البنية الإلكترونية لدولة، لا يكون دليلا كافيا، لإسناد تلك العملية إلى الدولة، وإنما يمكن اعتبارها إشارة إلى وجود ثمة ارتباط بين العملية، وبين الدولة المعنية".

[٣] تنص المادة (٦) من مشروع لجنة القانون الدولي على أنه: " يعتبر فعلاً صادراً عن الدولة بمقتضى القانون الدولي تصرف جهاز يوضع تحت تصرف هذه الدولة من قبل دولة أخرى إذا كان هذا الجهاز يتصرف ممارسة لبعض اختصاصات السلطة الحكومية للدولة التي يوضع الجهاز تحت تصرفها."

وأن يتعلق الفعل غير المشروع، بالأعمال التي أناطتها الدولة للجهاز، ليباشرها نيابة عنها.[١]

ونلاحظ أن استمرار التمويل، أو توفير الموارد للجهاز، من جانب الدولة المرسلة، لا ينفي مسؤولية الدولة المستقبلة للجهاز، طالما مازالت تمارس سلطتها الحصرية عليه. بحيث لا تملك الدولة المرسلة، أي سلطة في استدعاء جهازها، أو توجيهه، بشأن الأنشطة التي يباشرها، في الدولة المستقبلة.

ب- مسؤولية الدولة عن قيام كيانات أو أشخاص بخلاف أجهزتها بهجمات سيبرانية غير مشروعة

لقد أوردت لجنة القانون الدولي، المعنية بمسؤولية الدول عن الأفعال غير المشروعة دوليا، حالتين بالنسبة لتنسيب الأفعال غير المشروعة دوليا، التي يباشرها أشخاص أو كيانات، لا تعتبر من أجهزة الدولة.

الحالة الأولى: وهي الحالة الواردة بالمادة (٥) من مشروع لجنة القانون الدولي، والتي تنسب إلى الدولة، التصرفات غير المشروعة دوليا، الصادرة عن أي كيان، ليس من أجهزة الدولة، ولكنه يمارس بعض اختصاصات السلطة الحكومية، بموجب تشريع داخلي، على شرط أن يكون هذا الكيان قد تصرف، بهذه الصفة، حال ارتكابه الفعل غير المشروع. وفي مجال الهجمات السيبرانية، نلاحظ أن فريق الخبراء، قد أخذ ذات القاعدة، وأقرها دليل "تالين ٢" بالقاعدة (١٥)، إذ نصت على: "**أن**

[١] Rule No (١٦): **Attribution of cyber operations by organs of other States** "Cyber operations conducted by an organ of a State that has been placed at the disposal of another State are attributable to the latter when the organ is acting in the exercise of elements of governmental authority of the State at the disposal of which it is placed".

العمليات السيبرانية التي يضطلع بها، أشخاص أو كيانات، مخولة بموجب القانون الداخلي، لممارسة اختصاصات السلطة الحكومية، تعزى إلى الدولة".

الحالة الثانية: وهي الحالة الواردة بالمادة (٩) من المشروع، والتي تنص على أنه: "**يعتبر فعلاً صادراً عن الدولة بمقتضى القانون الدولي تصرف شخص أو مجموعة أشخاص إذا كان الشخص أو مجموعة الأشخاص يمارسون في الواقع بعض اختصاصات السلطة الحكومية في غياب السلطات الرسمية أو في حالة عدم قيامها بمهامها وفي ظروف تستدعي ممارسة تلك الاختصاصات**". وتتناول هذه المادة تنظيم الحالة الاستثنائية، والتي لا تنشأ إلا نادرا، كما في حالة الثورة، أو النزاع المسلح، أو الاحتلال الأجنبي، حيث تنحل السلطات العادية، أو تقمع، أو تتعطل عن العمل في حينه. وتحدد المادة السابقة ثلاثة شروط، ينبغي الوفاء بها لنسب التصرف إلى الدولة: **الأول**، ينبغي للتصرف أن يتصل فعلياً بممارسة بعض اختصاصات السلطات الحكومية. **والثاني**، يجب أن يكون التصرف قد صدر في غياب السلطات الرسمية أو في حالة تعطلها. **والثالث**، يجب أن تستدعي الظروف القائمة ممارسة اختصاصات السلطة تلك. وفي مجال الهجمات السيبرانية، تشير هذه القاعدة، إلى الحالات التي يبادر فيها شخص أو مجموعة أشخاص، بشكل طوعي، لمساعدة الدولة، في مواجهة أخطار تكنولوجية، قد عجزت الدولة عن التعامل معها. ولذلك تقبل تطوع الأفراد أو الكيانات الخاصة، للمساعدة على تجاوز تلك الظروف الطارئة، مع اعتبار الدولة مسؤولة عن التصرفات غير المشروعة دوليا، والتي قد تصدر عنهم.[١]

[١] عسكر، محمد عادل (٢٠٢٠)، وضع العمليات السيبرانية في القانون الدولي مع التطبيق على ممارسة التجسس وقت السلم–دراسة على ضوء دليل تالين بشأن القانون الدولي المطبق على العمليات السيبرانية ٢٠١٣–٢٠١٧، مرجع سابق، ص ٤٢٧.

لقد تحدثنا فيما سبق عن قواعد مسؤولية الدول، في مجال الهجمات السيبرانية. أما فيما يتعلق بمسؤولية المنظمات الدولية، باعتبارها أحد أشخاص القانون الدولي، فإن الفقه والقضاء الدولي، قد استقر على التزام المنظمات الدولية، بقواعد القانون الدولي، وبأنها مسؤولة عن أفعالها، التي تمثل خرقا لهذه القواعد، كما أنها مسؤولة عن تصرفات من يمثلها، أو ينفذ المهام تحت سيطرتها ورقابتها.[١]

وترتيبا على ذلك؛ فإن المنظمات الدولية، تكون مسؤولة عن تصرفاتها غير المشروعة دوليا، سواء صدر التصرف عن المنظمة، أو عن جهاز أو وكيل تابع للمنظمة، بغض النظر عن مركز الوكيل التنظيمي والإداري، بالنسبة للمنظمة، وإنما العبرة بطبيعة المهام الموكلة إليه.[٢] وعلى ذلك تنعقد مسؤولية المنظمات الدولية، عن تصرفات الأشخاص الطبيعيين، أو الكيانات التي تستخدمها، لأداء وظائف معينة لها، أو لجهاز من أجهزتها، حال قيامهم بأي هجمات سيبرانية غير مشروعة، وذلك باعتبار أنهم يعملون كوكلاء تابعين للمنظمة.

وغني عن البيان، أن الهدف من بحث ودراسة المسؤولية الدولية، إنما يتعلق ببحث آثارها وبمحاولة تطبيق تلك المسؤولية. والتي تتعلق – في الغالب – بجبر كامل

---

[١] بالنسبة للقضاء الدولي فلقد استقر رأى محكمة العدل الدولية، على تبني هذا النهج، ونذكر على سبيل المثال: الرأي الاستشاري بشأن تفسير الاتفاق المبرم في ٢٥ مارس ١٩٥١م، بين منظمة الصحة العالمية ومصر، إلى أن "المنظمات الدولية ملزمة بأي التزامات تفرض عليها بموجب القواعد العامة للقانون الدولي، أو بموجب دساتيرها، أو الاتفاقات الدولية التي تكون طرفا فيها، وتنتهك المنظمة القانون الدولي، عندما تخرق أي من هذه الالتزامات الدولية. أما بالنسبة للفقه الدولي، فلقد أكدت لجنة القانون الدولي، في مشروعها الخاص، بمسؤولية المنظمات الدولية لعام ٢٠٠٩، على مسؤولية المنظمات الدولية عن أفعالها التي تشكل خرقا لقواعد القانون الدولي. وللمزيد راجع:
تقرير لجنة القانون الدولي (٢٠٠٩)، وثيقة رقم (A/٦٤/١٠)، دورة الجمعية العامة رقم (٦٤)، التعليق على المادة (٤)، ص ٤٨.

[٢] راجع تقرير محكمة العدل الدولية، لعام ١٩٨٩، الفقرتين ٤٧، ٤٨.

الخسارة، التي لحقت بالمضرور، وذلك باستخدام كافة الطرق القانونية الممكنة. كالرد، أو التعويض، أو الترضية، أو بالجمع بينها.[١] كما تتعلق بضرورة متابعة الدولة، لواجبها بالوفاء بالالتزام الدولي، الذي تم خرقه، والكف عن الفعل غير المشروع، وتقديم الضمانات والتأكيدات الملائمة لعدم تكراره.[٢]

الخـــاتمة

استعرضنا في هذه الدراسة، الجوانب القانونية المختلفة، لموضوع الهجمات السيبرانية، بداية من التعرف على ماهية الهجمات السيبرانية، وبحث نشأتها وعرض لبعض النماذج، التي أثرت بشكل كبير على المجتمع الدولي. ومرورا ببحث التكييف القانوني للهجمات السيبرانية، لغرض تحديد مدى انطباق القواعد القانونية الدولية عليها. وانتهينا بدارسة قواعد المسؤولية الدولية، في مجال الهجمات السيبرانية. ويمكن أن نجمل فيما يلي أهم النتائج، والتوصيات التي توصلت إليها الدراسة:

أولا: نتائج الدراسة

١) لايزال المجتمع الدولي غير متفق، على مفهوم واحد للهجمات السيبرانية، وطبيعتها القانونية.

---

[١] والرد: هو أول أشكال الجبر المتاحة للدولة المضرورة، ويشمل الرد إعادة الحالة قدر الإمكان، إلى ما كانت عليه قبل ارتكاب الفعل غير المشروع دوليا. والرد قد يستلزم في الغالب استكماله بالتعويض، لضمان جبر كامل للضرر المتسبب فيه. وأما التعويض فهو يشمل أي ضرر يكون قابلا للتقييم، من الناحية المالية، بما في ذلك ما فات من الكسب، بقدر ما يكون هذا الكسب مؤكدا في الحالة المعنية. ونلاحظ أن التعويض في هذه الحالة، لا يشمل الأضرار المعنوية، التي تلحق بالدولة المضرورة. أما الترضية: وهي الشكل الثالث من أشكال الجبر، والترضية يتم اللجوء إليها إذا ما تعذر إصلاح الخسارة عن طريق الرد أو التعويض. وللمزيد راجع:
المواد أرقام (٣١، ٣٤، ٣٥، ٣٦، ٣٧) من مشروع لجنة القانون الدولي.

٢ راجع المادة (٢٩، ٣٠) من مشروع لجنة القانون الدولي.

٢) لاتزال القوى المهيمنة على المجتمع الدولي، تعمد إلى عرقلة الجهود الدولية، لوضع تنظيم قانوني دولي ملزم، يهدف إلى تنظيم استخدام الفضاء السيبراني، لمحاولة منع الهجمات السيبرانية غير المشروعة.

٣) إن التشريعات الداخلية للدول، مازالت تقف عند حد وضع العقوبات على الجرائم السيبرانية، دون وضع تنظيم قانوني، يحكم الهجمات السيبرانية.

٤) عدم كفاية الجهود الفقهية الدولية، المعنية ببحث ودراسة الهجمات السيبرانية.

٥) إن التطور التقني السريع، أصبح له جوانب سلبية على الأمن القومي للدول.

٦) رغم اتجاه أغلب الدول العربية، إلى تبني مفاهيم التحول الرقمي، في كافة المجالات، غير أنه يلاحظ عدم بذل أي جهد، لتشكيل منظومة عربية دفاعية، للحد من الهجمات السيبرانية.

ثانيا: توصيات الدراسة

١. نوصي المؤسسات الأكاديمية بضرورة الاهتمام بدراسة موضوع الهجمات السيبرانية وعلى الأخص من الناحية الفنية والقانونية. كما نوصي بضرورة العمل على تطوير المحتوي العلمي، الخاص بدراسة القانون الدولي العام، داخل كليات الحقوق المصرية بشكل خاص، وكليات القانون العربية بشكل عام، لتسمح بدراسة الموضوعات المستحدثة، ومن أبرزها موضوع الهجمات السيبرانية.

٢. نوصي بضرورة وضع تصور عربي بشكل عام، ومصري بشكل خاص، يشمل الإجراءات اللازمة لحماية المنظومة الإلكترونية العربية عموما، والمصرية خصوصا، لدرء الهجمات السيبرانية العابرة للحدود.

٣. ضرورة الاهتمام بتأهيل كوادر متخصصة، ومدربة على مستوى مناسب، لرصد وصد أي هجوم سيبراني.

٤. ضرورة الاهتمام بالالتزامات الدولية المعنية بحقوق الإنسان، لاسيما الخاصة بحق الإنسان في الخصوصية، وتداول المعلومات، حال وضع تشريعات وطنية، تهدف إلى رصد وصد الهجمات السيبرانية.

٥. ضرورة التكاتف الدولي، لوضع تنظيم قانوني دولي ملزم، أو إعادة النظر في صياغة القواعد السارية، لتسري على المستجدات الدولية، ومنها مسائل الهجمات السيبرانية.

قائمة المراجع

المراجع باللغة العربية:

أولا: الكتب والمراجع العامة

١. أبو الوفا، أحمد (٢٠٠٣)، المسئولية الدولية للدول واضعة الألغام في الأراضي المصرية: دراسة في إطار القواعد المنظمة للمسئولية الدولية وللألغام البرية، دار النهضة العربية، القاهرة.

٢. أبو الوفا، أحمد (٢٠٠٦)، القانون الدولي والعلاقات الدولية، دار النهضة العربية، القاهرة.

٣. البعلبكي، منير (٢٠٠٤)، المورد: قاموس انكليزي – عربي، دار العلم للملايين، بيروت.

٤. جوزيف ناي، ترجمة/ أحمد أمين الجمل ومجدي كامل (١٩٩٧)، المنازعات الدولية– مقدمة للنظرية والتاريخ، الجمعية المصرية لنشر المعرفة والثقافة العالمية، القاهرة.

٥. الموسى، محمد خليل (٢٠٠٤)، استخدام القوة في القانون الدولي المعاصر، الطبعة الأولى، الأردن: دار وائل للنشر.

ثانيا: الرسائل العلمية

١. حسين، محمد ربيع أحمد (٢٠٢٢)، الجذور التاريخية لمبدأ التدخل الدولي الإنساني وتطبيقاته المعاصرة، رسالة دكتوراه، كلية الحقوق، جامعة بنها.

ثالثا: المقالات والمجلات والدوريات العلمية

١. عسكر، محمد عادل (٢٠٢١)، وضع العمليات السيبرانية في القانون الدولي مع التطبيق على ممارسة التجسس وقت السلم–دراسة على ضوء دليل تالين بشأن القانون الدولي المطبق على العمليات السيبرانية ٢٠١٣–٢٠١٧، مجلة البحوث القانونية والاقتصادية، كلية الحقوق، جامعة بني سويف، المجلد (٣٣)، العدد (١).

رابعا: اتفاقيات دولية

١. اتفاقيات جنيف الأربع لعام ١٩٤٩.
٢. اتفاقية لاهاي الثانية لعام ١٨٩٩.
٣. اتفاقية لاهاي الرابعة لعام ١٩٠٧.
٤. اللحقين الإضافيين باتفاقيات جنيف لعام ١٩٧٧.

خامسا: قرارات المنظمات الدولية

١. مشروع مواد لجنة القانون الدولي بشأن مسؤولية الدول عن الأفعال غير المشروعة دوليا لعام ٢٠٠١، وثيقة رقم:
(GA Res. ٥٦/٨٣ annex, UN Doc. A/RES/٦٥/٨٣, December ١٢, ٢٠٠١)
٢. تقرير لجنة القانون الدولي، الدورة (٥٣)، ملحق رقم (١٠) وثيقة رقم (A/٥٦/١٠).
٣. تقرير لجنة القانون الدولي (٢٠٠٩)، وثيقة رقم (A/٦٤/١٠)، دورة الجمعية العامة رقم (٦٤).

المراجع الأجنبية:

First: Books and General References

١. Elihu Zimet, Charles L. Barry (٢٠٠٩), "Military services Overview, Cyber power and National Security, National Defense University Press, Washington DC, USA.
٢. Julia Cresswell (٢٠١٠), "Oxford Dictionary of word Origins: Cybernetics", Oxford Reference Online, Oxford University Press.
٣. Norbert Wiener (١٩٤٨), "Cybernetic or control communication in the animal and the machine, M.I.T, Press, Second Edition, Cambridge, Massachusetts.
٤. Peter Sommer & Ian Brown (٢٠١١),"Reducing Systemic Cyber security Risk", OCED.
٥. R. Buchan (٢٠١٩), Cyber Espionage and International Law, HART Publishing, Oxford.

Second: Articles and Researches

١. Antonio Gessese (٢٠٠٠),"The Martens Clouse: Half a loaf or simply pie in the sky?", EJIL, Vol. III, No. ١.

٢. Davis Brown (٢٠٠٦), "Proposal for an international convention to regulate the use of information System in Armed Conflict", Harvard International Law review, Vol. ٤٧.

٣. Diego Rafael Canabarro and Thiago Borne (٢٠١٣),"Reflection on the fog of Cyber War", National Center for Digital Government, Policy working Paper No.١٣:٠٠١, March ١, ٢٠١٣, footnote ١١.

٤. E. T. Jensen (٢٠١٧), The Tallinn Manual ٢.٠: Highlights and Insights, Research Paper, No. ١٧, Georgetown Journal of International Law.

٥. Erki Kodar (٢٠١٢),"Applying the law of armed conflicts to Cyber-attacks: from the Martens Clouse to Additional Protocol I", ENDC Proceeding, Volume ١٥.

٦. M. J. Sklerov (٢٠٠٩), Solving the Dilemma of State Responses to Cyber-attacks: A Justification for the Use of Active Defenses against States Which Neglect Their Duty to Prevent, Mil. L. Rev. ٢٠١.

٧. Marco Roscini (٢٠١٠), World Wide Warfare: Jus ad bellum and the use of cyber force, Max Planck Yearbook of United Nations Law, Vol. ١٤.

٨. Michael N. Schmitt (١٩٩٩), 'Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework, Columbia Journal of Transnational Law, Vol. ٣٧.

٩. Micheal Gervais (٢٠١٢),"Cyber Attacks and the Laws of War", Berkeley Journal of International Law, Vol: ٣٠, Issue .٢, Article ٦.
١٠. Micheal N. Schmmitt (٢٠٠٢),"Wired warfare: Computer network attack and jus in Bello", IRRC, Vol.٨٤, No.٨٤٦.
١١. Micheal N. Schmmitt, L. Vihul (٢٠١٩), Tallinn Manual ٢.٠ on the International Law Applicable to Cyber Operations, Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Center of Excellence, Cambridge University Press.
١٢. Nils Melzer (٢٠١١),"Cyber warfare and International Law: IDEAS for Peace and Security", UNIDIR Researches.
١٣. Rwx HUGES (٢٠١٠),"A treaty for Cyberspace", International Affairs journal, Vol.٨٦.No.٢.
١٤. Scott J. Shackelford (٢٠٠٩),"From Nuclear War to Net War: Analogizing Cyber Attacks in International Law", Berkeley Journal of International Law, Vol. ٢٧:١.
١٥. Thomas Rid and Peter Mcburney (٢٠١٢), "Cyber – Weapons", Routledge publisher, The RUSI Journal, Vol.١٥٧, NO.١.

Third: Thesis

١. Janne Valo (٢٠١٤), Cyber Attacks and the Use of Force in International Law, Master's Thesis, Faculty of law, University of Helsinki.