الدفاع الشرعى ضد الهجمات السيبرانية

دكتور

سامي محمد عبد العال

أستاذ القانون الدولى العام المساعد

كلية الحقوق – جامعة طنطا

الملخص

يسعى القانون الدولي بشتي الطرق ليحكم الحاضر ويشكل المستقبل، حيث تغير شكل الصراع الدولي – فضلًا عن شكل الحرب – بشكل أساسى من خلال ظهور العمليات السيبرانية، فمستقبل الحروب والصراعات ليس كما كان عليه من قبل، وهذه هى المعضلة. فالحرب السيبرانية حرب حديثة لم تكن ظاهرة من قبل، ولم يتصورها واضعي القانون الدولي، بل إنها تضرب وتهاجم عناصر مثل الاتصالات التى لم تكن معلومة هي الأخرى من قبل.

وهذا ما جعلنا نحاول سرد مصطلح الهجوم السيبراني لمعرفة وتحديد حق الدول فى الدفاع عن نفسها ضد تلك الهجمات، استنادًا إلي قواعد قانونية دولية تصبح سندًا قانونيًا لها فى حالة الدفاع الشرعى عن النفس.

Abstract:

International law seeks in various ways to govern the present and shape the future, as the form of international conflict - as well as the form of war - has changed mainly through the emergence of cyber operations. The future of wars and conflicts is not what it used to be, and this is the dilemma. Cyber warfare is a modern war that was not apparent before, and was not imagined by the makers of international law. Rather, it strikes and attacks elements such as communications that were also not known before.

This is what made us try to list the term cyber attack to know and define the right of countries to defend themselves against these attacks, based on international legal rules that become a legal basis for them in the case of legitimate self-defense.

قائمة المختصرات

List des principales abbreviations

Term	Def
AIJ	An International Journal
AUILR	American University International Law Review
BJIL	Berkeley Journal of International Law
CJTL	Colombia Journal of Transitional Law
CILJ	Cornell International Law Journal
HILJ	Harvard International Law Journal
ILS	International Law Studies
JC&SL	Journal of Conflict and Security Law
JNAALJ	Journal of the National Association of Administrative Law Judiciary
JNSL&P	Journal of National Security Law & Policy
JTL	Journal Of transnational Law
NWCILS	Naval War College International Law Studies
MPYUNL	Max Planck Yearbook of United Nations Law
ORIL	Oregono Reviear Of International Law
PPSY	Polish Political Science Yearbook
RCRDDF	Revue du Centre de Recherches et D'études Sur les Droits Fondamentaux
SJIL	Stanford Journal of International Law
SLR	Southwestern Law Review
SL&PR	Stanford law and policy Review
VJIL	Virginia Journal of International law
YJIL	Yale Journal Of International Law

مقدمة

أثرت الثورة التكنولوجية بشكل كبير فى حقل العلاقات الدولية خاصة مع تطور المجال السيبراني، وكان لهذا التطور تأثير فى ظهور نوع جديد من التهديدات الأمنية أطلق عليها " التهديدات الهجين". كما أثرت على مصادر القوة ووسائلهاعلى الساحة الدولية، فضلًا عن التغير فى أنماط الصراع والحروب، مما أدى إلى إثارة مشكلة الدفاع الشرعى ضد الهجمات السيبرانية.

إشكالية البحث:

يسعى القانون الدولي بشتي الطرق ليحكم الحاضر ويشكل المستقبل، حيث تغير شكل الصراع الدولي – فضلًا عن شكل الحرب – بشكل أساسى من خلال ظهور العمليات السيبرانية، والتى أضافت بُعدًا جديدًا للعلاقات الدولية.

فمستقبل الحروب والصراعات ليس كما كان عليه من قبل، وهذه هى المعضلة. فالحرب السيبرانية حرب حديثة لم تكن ظاهرة من قبل، ولم يتصورها واضعو القانون الدولي، بل أنها تضرب وتهاجم عناصر مهمة؛ مثل الاتصالات التى لم تكن معلومة هي الأخرى من قبل.

فقد ألغي الفضاء السيبراني الحدود الجغرافية التقليدية، وأصبح الأفراد والمنظمات مرتبطون اليوم بشبكات واسعة تعمل على نشر المعلومات والبيانات بمعدل أسرع، فأصبحت هذه العمليات تسيطر على التعامل اليومي بين الأفراد والدول، مما ينشأ خطر كبير يتمثل فى: أن تصبح هذه الأنظمة والشبكات المرتبطة والبيانات الواردة فيها هدفًا لأفعال كيدية متعمدة من قبل الدول، والجهات الفاعلة من غير الدول، فلم يعد غريبًا أن يصبح الفضاء السيبراني جبهة جديدة للهجوم، نظرًا لسهولة الاتصال السيبراني والاستيعاب العالمى له.

كل ذلك خلق قلق عالمي حول طبيعة ونطاق الهجمات السيبرانية، حيث يمكن أن تسبب عواقب بعيدة المدى ومدمرة، خاصة التأثير المحتمل على المدنيين وقت النزاعات المسلحة، وهو ما دفع القانون الدولى إلى تغير بعض أحكامه المتعلقة بالحرب التقليدية، ليتكيف مع حروب وهجمات الجيل الجديد بمنحها حماية، وتفصيل أكثر مما كانت عليه من قبل، وذلك بفرض التزامات دولية على الدول إزاء الجهة الفاعلة، بالإضافة إلى حق الرد عن طريق القوة على بعض الهجمات السيبرانية.

ففي منتصف التسعينات كانت ضربة البداية، حيث بدأ متخصصو الشؤون الأمنية الدولية فى النظر فى إمكانية أن تصبح الحرب السيبرانية عنصر من عناصر النزاع المسلح التقليدى، بما يحمل نفس خطورة الهجوم المسلح التقليدي، ومع ذلك فقد تلاشي الموضوع من الأجندة الأمنية أعقاب هجمات ١١ سبتمبر ٢٠٠١.

وفي عام ٢٠٠٧ ظهرت مجددًا الهجمات السيبرانية، حيث عانت دولة إستونيا- الدولة العضو فى الناتو- من هجمات سيبرانية واسعة النطاق، من جهات فاعلة من غير الدول من أصل روسى.

وفى عام ٢٠٠٨ احتلت العمليات السيبرانية مكانة بارزة فى النزاع المسلح الدولى بين روسيا وجورجيا، حيث أمضى العديد من الأكاديميين والممارسين القانونيين في المجال الدولى ثلاث سنوات متتالية لصياغة دليل " تالين " بشأن القانون الدولي المنطبق على الحرب السيبرانية.

أهمية البحث:

ينصرف هذا البحث إلي الوقوف على مدي مشروعية الدفاع الشرعي عن النفس ضد الهجمات السيبرانية في ضوء قواعد القانون الدولي، وتتمثل الأهمية الرئيسية في أن الجدل لايزال قائمًا حول مدى اعتبار الهجوم السيبراني هجومًا مسلحًا من عدمه، كذلك ما مدى تطبيق نص المادة (٥١) من ميثاق الأمم المتحدة

على الهجوم السيبراني. كما ترجع أهمية هذا البحث إلى أن الهجمات السيبرانية تُعد استغلالًا متعمدًا لأنظمة الحاسب الآلي، والشبكات، والجهات التي يعتمد عملها على تقنية المعلومات والاتصالات الرقمية؛ بهدف إحداث الإضرار بالدول الأخرى.

أسباب اختيار البحث:

الذى دفعنى للبحث فى هذا الموضوع السعى الحثيث من قبل الدول نحو محاولة تحديث أسلوب الحرب التقليدي المعروف منذ بداية الخليقة، وبالتالي الالتفاف حول قواعد القوانين الدولى التى تجرم الحرب، ومن ثم الهروب من العقاب الدولى.

فالمخاوف كبيرة وكثيرة مما قد يحدث، إذا تطور أسلوب الحرب دون وجود قواعد تحكم هذا التطور فى عالم يسوده التوتر والخلافات الدائمة، فهذا التطور يبقى بعيدًا عن مصطلح استخدام القوة، وبالتالي ينحصر حق الدول فى الدفاع عن نفسها استنادًا إلي حق الدفاع الشرعى عن النفس ضد أى هجوم مسلح.

فالتطور التقنى الرهيب فى وسائل القتال والهجمات على الدول، بعيدًا عن الأسلوب التقليدي للهجوم، يجعل الدول المعتدى عليها فى مأزق، بسبب عدم قدرتها الدفاع الشرعي عن نفسها ضد هجوم بدون أسلحة تقليدية.

وهذا ما جعلنا نحاول سرد مصطلح الهجوم السيبراني لمعرفة وتحديد حق الدول فى الدفاع عن نفسها ضد تلك الهجمات، استنادًا إلي قواعد قانونية دولية تصبح سندًا قانونيًا لها فى حالة الدفاع الشرعى عن النفس.

منهج البحث:

يعتمد البحث على مجموعة متداخلة من مناهج البحث، حيث اعتمد البحث على استخدام المنهج الاستنباطى، والذى يعرف فى المجال القانونى بالمنهج التحليلى الذى يقوم على القواعد العامة الموجودة سلفًا، فنقطة الانطلاق فى هذا

المنهج هى انتقال الباحث من العام إلى الخاص، أو من الكل إلى الجزء.

كما استخدم البحث المنهج الاستقرائى، والذى يعرف فى المجال القانونى بالمنهج التأصيلى، ويُقصد به المنهج الذى يعتمد فيه الباحث على عدد من الظواهر المتشابهة، بصدد موضوع معين، ويقوم بدراستها وتحليلها، ومعرفة أسباب التشابه بينها، ثم يصل إلى قاعدة عامة تحكم هذه الظاهرة أو تلك.

خطة البحث:

لقد قمنا بتقسيم هذه الدراسة الى ثلاث مباحث على النحو التالي:

المبحث الأول: ماهية الهجمات السيبرانية.

المبحث الثاني: الإطار القانوني لحق الدفاع الشرعي ضد الهجمات السيبرانية.

المبحث الثالث: الجهود الدولية إزاء حق الدفاع الشرعى ضد الهجمات السيبرانية.

المبحث الأول
ماهية الهجمات السيبرانية

من الجدير بالذكر أن ما يسمى بالعالم " الافتراضي " عالم الإنترنت وشبكات الكمبيوتر والفضاء الإلكتروني بشكل عام، أصبح الآن جزءًا راسخًا من " العالم الحقيقي" لا سيما فى مجالات الأمن القومى والاستراتيجية العسكرية(١). حيث تتيح التطورات الثورية في التكنولوجيا الأن للجيوش والمدنيين – على حد سواء – الانخراط فى النشاط السيبراني، لتحقيق الأهداف المرجوة، سواء كانت تتعلق بالاحتجاج، الثورة، الجريمة، الإرهاب، التجسس أو العمليات العسكرية(٢). وبناء عليه نقوم بتوضيح لبعض المصطلحات السيبرانية فى مطلب أول، على أن نخصص المطلب الثانى لمفهوم الهجوم السيبرانى بالتفصيل، وذلك على النحو الآتي:

المطلب الأول
المفهوم القانونى لبعض المصطلحات السيبرانية

غالبًا ما يستخدم الفقه الدولي مصطلحات إلكترونية أو سيبرانية متشابهة مثل: الفضاء الإلكتروني، العمليات الإلكترونية، الحرب الإلكترونية، والهجمات الإلكترونية. فقد استحوذت كلمة cyber على اهتمام العالم بأسرة على مدار السنوات العديدة الماضية(٣).

---

(١) **د. يحيى مفرح الزهرانى:** الأبعاد الاستراتيجية والقانونية للحرب السيبرانية، مجلة البحوث والدراسات، كلية العلوم الاستراتيجية، جامعة نايف للعلوم الأمنية، المملكة العربية السعودية، العدد (٢٣)، السنة (١٤)، ٢٠١٧، ص ٢٣٥ وما بعدها.

(2) **Tim Jordan:** Cyberpower the culture and politics of cyberspace and the internet, London, 1999, p. 12.

(3) **Laurie R. Blank:** International Law and Cyber Threats from Non-State Actors, ILS, vol. 89, 2013, p. 406.

والتساؤل المثار هنا هل تختلف المصطلحات السابق ذكرها من حيث المعنى والمضمون أم لا ؟ سوف نوضح ذلك على النحو التالى:

أولاً: الفضاء الالكتروني:

أدى ظهور الإنترنت، وكذلك الاستخدام المتزايد لأنظمة المعلومات، إلى تغييرات غير عادية في حياة الإنسان(١)، فقد أدى ذلك إلى إزالة الحواجز التنموية بين المجتمعات، والسماح للبشر فى جميع أنحاء العالم بالتواصل، وتبادل الأفكار، بغض النظر عن الحواجز التقليدية، وهو ما أدى بدوره إلى ظهور ما يسمى بالفضاء السيبراني(٢).

ولا يخفي عن الفطنة أن العالم بصفة عامة، والاقتصاد العالمى بصفة خاصة، يعتمد بشكل كبير – فى الوقت الراهن – على البنية التحتية للفضاء الإلكتروني، حيث إن معظم جوانب الوجود البشرى تعتمد فى أدائها الفعال والسليم على الفضاء الإلكترونى(٣).

والحقيقة أن مصطلح الفضاء السيبراني لا يزال بحاجة إلي تعريف مقبول عالميًا، على الرغم إنه فى بعض الأحيان يرقى إلى مفهوم الإنترنت أو عالم افتراضى رقمى، وقد ظهرت عدة تعريفات لهذا المصطلح، مثل تعريف وكالة الاستخبارات الأمريكية التي عرفته بأنه: "مجالًا عالميًا داخل بيئة المعلومات يتكون من شبكة مترابطة من البنية التحتية لتكنولوجيا المعلومات، بما في ذلك الإنترنت وشبكات الاتصالات وأنظمة الكمبيوتر والمعالجات وأجهزة التحكم المدمجة". ووصفت القمة

(1) **Michael N. Schmitt:** Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework, CJTL, vol. 37, 1999, p. 885.

(2) **Sabu M. Th, Bharat B, Pradeep K. A:** Managing trust in cyberspace, A Chapman & Hall Book, New York, 2014, p. 10.

(3) **Annette Froehlich:** Outer space and cyber, European space policy institute, Vienna, Austria, 2021, p. 56.

الروسية الأمريكية للأمن السيبراني، الفضاء الإلكتروني بأنه: "وسيط إلكتروني يتم من خلاله إنشاء المعلومات ونقلها وتخزينها ومعالجتها وحذفها"(١).

ثانياً: الحرب السيبرانية (الإلكترونية):

يجب التنويه بداية إلى أن الساحة السيبرانية العالمية تحولت إلي أرض معارك حقيقية، فى عالم افتراضى تقنى يعتمد على كل ما هو جديد من صيحات التكنولوجيا الرقمية والاتصالات الحديثة، وهذا ما دفع القوات المسلحة للدول، وأجهزة الاستخبارات إلى وضع الأمن المعلوماتي على رأس أولوياتها، للسيطرة على الفضاء السيبراني باعتباره ساحة حرب جديدة على المستوي الدولي(٢).

وقد تم تعريف الحرب السيبرانية بأنها " أفعال تقوم بها دولة قومية لاختراق أجهزة الكمبيوتر أو الشبكات الخاصة بدولة أخرى للإضرار بهذه الدولة "(٣).

كما عرفها البعض بأنها " حرب افتراضية أو تخيلية ذات طبيعة غير ملموسة تحاكي الواقع بشكل شبه تام، وهي حرب بلا دماء، بحيث تتلخص أدوات الصراع فيها بالمواجهات الإلكترونية، والبرمجيات التقنية، وجنود من برامج التخريب المحوسبة"(٤).

---

(1) **U. M. Mbanaso:** The Cyberspace: Redefining A New World, IOSR Journal of Computer Engineering, Vol. 17, 2015, p 15.

(2) **Steven F., Nalhan C:** Human aspects of information security and assurance, University of Nottingham, Nottingham U K, 2021, p. p. 63.

(٣) حيث ذهب Petr Hruza إلى القول:

«Cyberwarfare has been defined as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption».

راجع مؤلفه بعنوان:

Cyberwarfar, International Conference Knowldege -based organization, Vol. XXIII, No. 1 , 2017, p. 162.

(٤) أ. **وليد غشان جلعود:** دور الحرب الإلكترونية في الصراع العربي الإسرائيلي، رسالة ماجستير، جامعة النجاح الوطنية ، ٢٠١٣، ص٨١.

والحرب السيبرانية لا تتوقف علي الدول فحسب، فتنسب وتقوم بها جهات غير حكومية([1]) مثل الجماعات الإرهابية، والشركات السياسية أو الأيديولوجية، وكذلك المنظمات الإجرامية.

وتشمل الحرب الإلكترونية العديد من الأدوات والوسائل التى يتم توظيفها فى الصراعات التى تنشب فى الفضاء السيبراني ومنها:

التجسس المعلوماتي([2]): التجسس نمط من أنماط اليلوك الإنسانى، رافق نشوء المجتمعات منذ القدم، وتطور بتطورها، فهو قديم قدم البشرية. فهذه الوسيلة أحد أشهر وأقدم أسلحة الحرب السيبرانية، فقد تم استخدام هذا السلاح منذ بداية الاستعمال الإنسانى لوسائل الاتصال والتواصل([3]).

ولم تزدهر الجاسوسية إلا مع بداية الحرب العالمية الثانية، فلم يُعد التجسس قاصرًا على الأسرار بل تعداه إلى المعلومات الصناعية والعلمية، وفي منتصف التسعينات، بدأ متخصصو الشؤون الأمنية الدولية في التفكير في نشوب حرب إلكترونية، كعنصر من عناصر النزاع المسلح التقليدى.

وفى نهاية القرن العشرين تغيرت أدوات وأساليب التجسس وذلك للثورة التكنولوجية والمعلوماتية فى مجال الإتصالات، فأصبح العالم قرية صغيرة، وأصبحت كل المعلومات السياسية والاقتصادية وأحيانًا العسكرية معلومة للكافة.

زرع الفيروسات التقنية في البيئات المعلوماتية: وهي عبارة عن برامج

(1) **Ashley S. Deeks:** "Unwilling or Unable": Toward a Normative Framework for Extraterritorial Self-Defense, VJIL, vol. 52, 2012, p. 483.

(2) **Inaki N., Russell B.:** Peacetime Espionage, International Law and the Existence of Customary Exceptions, CILJ, vol. 51, 2019, p. 898.

(٣) **د. جعفر جاسم:** حرب المعلومات بين إرث الماضي وديناميكية المستقبل، دار البداية للنشر، ٢٠١٠ ص ١٧١.

إلكترونية مدمرة، تعمل ضمن آلية معينة يحددها صانع هذه البرامج، ولها أشكال متعددة تهدف إلى إحداث فوضى في نظام تشغيل الضحية، وتلويث بيئته المعلوماتية([1]).

إن الأمن المعلوماتي يرتبط أرتباطا وثيقًا بأمن الحاسوب، فلا يوجد أمن للمعلومات إذا لم يراعى أمن الحاسوب، وفي ظل التطورات المتسارعة في العالم والتي أثرت على الامكانات التقنية المتقدمة المتاحة والرامية الى خرق منظومات الحاسوب بهدف السرقة او تخريب المعلومات أو تدمير أجهزة الحاسوب، كان لا بد من التفكير الجدي لتحديد الإجراءات الدفاعية والوقائية وحسب الامكانات المتوفرة لحمايتها من اي اختراق او تخريب.

القرصنة الإلكترونية: تعتبر القرصنة من أضخم وأشمل الأسلحة الإلكترونية المستخدمة عبر الفضاء السيبراني، ويشتمل هذا السلاح التقني علي غالبية وسائل الصراع الإلكتروني الآن، وذلك لشمولية مفهومه ومضمونه، حيث تقوم آلية عمله على تجنيد العديد من الأشخاص المؤهلين والقادرين على التعامل مع الحاسوب بخبرة ودراية تمكنهم من اقتحام مختلف الوسائل الاتصالية والنظم التكنولوجية، من حواسيب وهواتف وألياف ضوئية([2]).

ثالثاً: العمليات السيبرانية:

تُعرف العمليات السيبرانية بأنها " عمليات ضد أو عبر جهاز كمبيوتر أو نظام كامل من خلال تدفق البيانات، وذلك بهدف التسلل إلي النظام وجمع البيانات وتصديرها أو اتلافها أو تغييرها أو تشفيرها أو التلاعب بها بأي طريقة أخرى مما

---

(١) **د. فاروق حسين:** فيروسات الحاسب الألي: دار هلا للنشر القاهرة، الطبعة الأولي، ١٩٩٩، ص٧.

(٢) **د. رأفت علوه:** قرصنة الإنترنت، مكتبة التجمع العربي للنشر عمان، الطبعة الأولي، ٢٠٠٦، ص ٢٣-٢٤.

يسبب ضرر لهذا النظام"([1]).

وعرفت وزارة الدفاع الأمريكية العمليات السيبرانية بأنها " العمليات التي تنطوى علي توظيف قدرات الفضاء الإلكتروني، حيث يكون الغرض الأساسى هو تحقيق أهداف في أو من خلال الفضاء السيبراني أو الإلكتروني، بما في ذلك تعطيل أجهزة الكمبيوتر أو إضعاف أو إتلاف المعلومات الموجودة علي أجهزة الكمبيوتر. ووسعت وزارة الدفاع من مفهوم العمليات السيبرانية، فقد أكدت أنها غير مرتبطة بالعمليات العسكرية فقط، بل تشمل حصول الأجانب علي معلومات استخباراتية غير مرتبطة بأهداف عسكرية محددة، مثل فهم طريقة الحصول علي التطورات التكنولوجية، أو الحصول على معلومات حول القدرات العسكرية للخصم([2]).

رابعاً: الهجوم السيبراني:

يُعد مصطلح الهجوم السيبراني الأكثر شيوعًا في النقاشات حول العمليات السيبرانية، فقد تم استخدام مصطلح "هجوم" لوصف تشوية المواقع الإلكترونية أو اختراق الشبكات أو سرقة المعلومات، أو تعطيل خدمة الإنترنت بشكل كامل، والتى لها أهمية قانونية فى إطار قانون الحرب، مما يمنح حق الدفاع الشرعي ضد هذه الهجمات([3]).

(1) **Matthew C. Waxman:** Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4), YJIL, vol. 36, 2011, p. 421.

(٢) راجع:

Peter Z. Stockburger: Known Unknowns: State Cyber Operations, Cyber Warfare, and the Jus Ad Bellum, AUILR, 2016, Vol.16 ,p 552.

(3) **Ben Buchanan:** The cybersecurity dilemma hacking trust , and fear between nations, Oxford University press, 2017, p. 65.

المطلب الثاني
مفهوم الهجوم السيبراني

تُعد الهجمات السيبرانية حديثة العهد نسبيًا، وهو ما يشكل إحدى أهم التحديات الراهنة التى يواجهها المختصون فى القانون الدولي العام، وبالخصوص فى تحديد طبيعتها أو عناصرها، فضلاً عن نطاق هذه الهجمات، وما يترتب عليها من تبعات المسؤولية الدولية، وما يزيد في اتساع التحدى الذى يواجهه المختصون فى القانون الدولي العام، إنما يتجسد فى الغموض التى اكتنف مفهوم الهجمات السيبرانية، وعدم الاتفاق على تعريف محدد يمكن الاستدلال في ضوئه لتنظيم استخدامها بالحظر، أو التقييد لمواجهة عواقبها الخطرة على الصعيد الدولى([1]).

كما أن التقدم التكنولوجي سلاح ذو حدين، حيث إن أنظمة الكمبيوتر التي تراقب وتتحكم في البنية التحتية لمختلف المجالات تجلب الكفاءة، ولكن فى نفس الوقت تجلب تحديات أمنية، وبسبب هذه التعقيد اقترحت بعض الدول استخدام القوة العسكرية ردًا علي الهجمات السيبرانية عبر الإنترنت، الأمر الذى أحدث بدوره مشكلة قانونية على صعيد المجتمع الدولى، بسبب عدم توافر آليات محددة لتطبيق قانون الحرب، والدفاع الشرعي عن النفس ضد الهجمات السيبرانية([2]).

ومن أجل الوقوف على مفهوم الهجمات السيبرانية، سنبحث فى نطاق تعريفها لغة واصطلاحًا في ضوء المعاجم اللغوية، وما درج عليها المختصون فى القانون الدولي العام، وخبراء تكنولوجيا المعلومات، فضلاً عن الأحكام الواردة فى الاتفاقيات الدولية والقوانين الداخلية ذات الصلة.

---

(1) **James A. G:** Cyber warfare, London and New York, 2015, p. 96 et ss.

(2) **Denis Goulet:** Technology, the Two Edged Sword, East-West Technology and Development Institute, East-West Center, 1976, p. 19.

أولًا: المفهوم اللغوي للسيبرانية:

تجدر الإشارة إلي أن أول من استخدم مصطلح السيبرانية هو عالم الرياضيات، "Norbert wiener" وذلك في عام ١٩٤٨، أثناء دراسته لموضوع القيادة والسيطرة والاتصال في عالم الحيوان، فضلا عن حقل الهندسة الميكانيكية(١). أما مصدر كلمة "Cyber" في المعاجم اللغوية، فيتضح أنها يونانية الأصل وترجع إلي مصطلح "kybernetes" الذي ظهر في مؤلفات الخيال العلمي، ويعني القيادة أو التحكم عن بعد(٢).

وبالرجوع إلي قواميس اللغة العربية، فنجدها لم تشر فى الغالب إلى مصدر كلمة Cyber، سوي في قاموس (المورد) إذ يعرفها بالقول أن السيبرانية هى " علم الضبط ومصدرها (Cybernetics) "(٣). وهو مصدر يتطابق مع مفهوم الهجمات السيبرانية، أي ضبط الأشياء عن بُعد والسيطرة عليها.

أما قاموس مصطلحات الأمن المعلوماتي، فعرف السيبرانية بأنها " هجوم عبر الفضاء الإلكتروني، يهدف إلى السيطرة على مواقع الكترونية، أو بنية محمية الكترونيًا لتعطيلها أو تدميرها أو الإضرار بها ". كما عرف قاموس المصطلحات العسكرية الأمريكية السيبرانية بأنها " أي فعل يستخدم عن طريق شبكات إلكترونية بهدف السيطرة أو التعطيل لبرامج إلكترونية أخرى"(٤).

---

(1) **Norbert Wiener:** "Cybernetics or control communication in the animal and the machine, M.I.T, Press, Second Edition, Cambridge, Massachusetts, 1948.

(2) **Julia Cresswell:** "Oxford Dictionary of word Origins: Cybernetics", Oxford Reference Online, Oxford University Press, 2010.

(٣) منير البعلبكي:" المورد : قاموس إنجليزي –عربي"، دار العلم للملايين، بيروت، ٢٠٠٤،ص، ٢٤٣.

(٤) مشار إليه لدى د.أحمد عبيس الفتلاوي: الهجمات السيبرانية مفهومها والمسئولية الدولية الناتجة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية والسياسية، المجلد =

ثانياً: المفهوم الاصطلاحي للسيبرانية:

في هذه الدراسة استخدمنا مصطلح الهجمات السيبرانية "Cyber Attack" على عكس ما درج عليه البعض من المختصين، فمنهم من تبنى مصطلح الفضاء السيبراني "Cyber Space" بالاستناد إلي المحيط الذي تجري فيه العمليات السيبرانية الناشئة عن أداء أنظمة إلكترونية، مهمتها متابعة وجمع المعلومات التي تعمل إلكترونيًا وتحليلها، ومن ثم اتخاذ إجراءات ووسائل محددة لمهاجمتها عن طريق أنظمة إلكترونية أخرى مخصصة لهذا الغرض(١).

وتبنى آخرون مصطلح الحرب السيبرانية "Cyber Warfare" استنادًا إلى أيديولوجية أمنية أو عسكرية تضع منهاجًا لتحقيق أهداف على الصعيد الأمني، أو العسكري تجاه العدو المفترض(٢). أما البعض الأخر فقد تبنى مصطلح الهجمات السيبرانية كوصف واقعي(٣)، فهو تصرف يدور فى عالم افتراضي قائم على استخدام البيانات الرقمية، ووسائل اتصال تعمل إلكترونيًا، ومن ثم تطور ليتضمن مفهومًا أوسع يقوم على تحقيق أهداف عسكرية أو أمنية ملموسة ومباشرة، جراء اختراق مواقع إلكترونية حساسة، كأنظمة حماية محطات الطاقة النووية أو الكهربائية أو المطارات(٤).

=

(٨)، العدد (٤)، جامعة بابل، العراق، ٢٠١٦، ص ٦١٤.

(١) للمزيد راجع: د. يحيى مفرح الزهرانى: الأبعاد الاستراتيجية والقانونية للحرب السيبرانية، مرجع سابق، ص ٢٣٥ وما بعدها.

(2) **Shin Beom chul:"** The Cyber Warfare and the Right of Self –Defense: Legal Perspectives and the Case of the United States, IFANS,Vol. 19, no. 1, 2011, p. 104.

(3) **Scoot j. Shckelford:** " State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem", University of Cambridge, dept of politicos and International STUDIES, Cambridge, UK, 2009. P. 194.

(4) **K. Saalbach:** " Cyber War, Methods and Practice", University of Osnabruck, Jun 2014, p. 6.

ثالثاً: المفهوم القانوني للهجوم السيبراني:

اختلف الفقه حول وضع تعريف للهجوم السيبراني من قبل الدول، بل أطلق عليه البعض الحرب الإلكترونية(١). ورغم الاختلاف اللفظي بين كلا المصطلحين إلا انهما يتقابلان فى مضمونهما.

حيث ذهب البعض(٢) الى أن المقصود بالهجوم السيبراني " استخدام أنشطة متعمدة للتأثير على شبكات الحاسوب للخصم، عبر اتلافها، اضعافها، تدميرها، تعطيلها، التحكم في الأجهزة والآلات المرتبطة بها، منع مستخدميها من الولوج الى

(١) ويلاحظ أن السلوك السبراني يتشابه مع السلوك التقليدي من حيث القائم بهذا الهجوم فهناك مجرم له دافع للقيام بالهجوم، وضحية قد تكون شخص طبيعي أو معنوي. اما الاختلاف الحقيقي فيظهر في أداة الهجوم ومكان الهجوم، ففي الهجوم السيبراني الأداة تكون ذات تقنية عالية، وأيضًا المكان الذي انطلق منه الهجوم لا يتطلب انتقال فاعله انتقال جسمانيًا، لأنه يتم عن بُعد، بواسطة خطوط وشبكات الاتصال بين المهاجم ومكان الهجوم.

كما تتميز الحرب السيبرانية عن الحرب التقليدية، فى أن المفهوم التقليدي للحرب، ينطوي على استخدام الجيوش النظامية، ويسبقها اعلان واضح لحالة الحرب وميدان قتال محدد، بينما تبدو هجمات الفضاء الالكتروني غير محددة المجال وغامضة الأهداف، كونها تتحرك عبر شبكات المعلومات والاتصالات المتعدية للحدود الدولية، إضافة إلى اعتمادها ما يمكن وصفه بأسلحة الكترونية جديدة تلائم طبيعة السباق الالكتروني لعصر المعلومات، حيث يتم توجيهها ضد المنشئات الحيوية أو دسها عن طريق عملاء لأجهزة الاستخبارات، وعليه فإن احد معايير التمييز بين الحرب السيبرانية والحرب التقليدية يمكن أن يكون بالاستناد إلى طبيعة السلاح المستخدم، وبالتالي يمكن القول أن الحرب السيبرانية، هي الحرب التي تستخدم فيها الاسلحة غير التقليدية، وفقاً للآثار المترتبة على استخدام هذا النوع من الاسلحة، والمتمثل بالتدمير واسع النطاق.

للمزيد راجع:

Martin C. Libicki: Conquest in Cyberspace: National Security and Information Warfare, New York: Cambridge University Press, 2007,p. 1-14.

(٢) هربرت لين: النزاع السبراني والقانون الدولي الإنساني، المجلة الدولية للصليب الأحمر، مجلد ٩٤، ٢٠١٢، ص٥١٨.

خدمة المعلومات أو الحاسوب اتلاف بيانات ذات أهمية استراتيجية". وقد عرف جانب فقهى الهجوم السيبراني بأنه" أفعال تقوم بها دولة لاختراق أجهزة الكمبيوتر أو الشبكات الخاصة بدولة أخري بهدف إحداث ضرر أو اضطراب(١).

كما عرفه Hayden المدير السابق لوكالة الأمن القومي ووكالة المخابرات المركزية بأنه " محاولة متعمدة من دولة لتعطيل شبكات الكمبيوتر الخاصة بدولة أخري أو تدميرها"(٢).

وعرفه "Schmitt" بأنه" مجموعة من الإجراءات التي تتخذها الدولة للهجوم علي نظم المعلومات المعادية بهدف التأثير والإضرار بها، وفي ذات الوقت للدفاع عن نظم المعلومات الخاصة بالدولة المهاجمة(٣).

---

(١) حيث ذهب Oona A. Hathaway إلى القول :

« Actions by a nation state to penetrate another nation's computers or networks for the purposes of causing damage or disruption».

راجع مؤلفه بعنوان:

The Law of Cyber-Attack, Yale Law School, vol. 100, 2012, P.8.

كما أكد Matthew C. Waxman على أن الهجوم السيبراني هو:

«Use of malicious computer code or electronic signals to alter, disrupt, degrade or destroy computer systems or networks or the information or programs on them».

راجع مؤلفه بعنوان:

Self-defensive Force against Cyber Attacks: Legal, Strategic and Political Dimensions, ILS, 2013, v. 89, p. 109.

(٢) حيث أكد Tom Gjelten حول الهجوم السيبراني:

«Deliberate attempt to disable or destroy another country's computer networks».

راجع مؤلفه بالتفصيل بعنوان:

Extending the Law of War to Cyberspace, (Sept. 22, 2010), p. 29.

(3) **Schmitt, M.N**," Computer Network Attack and the Use of Force in International Law through on a Normative", CJTL, 1999, v.27, n.885 p.937.

وذهب "Roscini" إلي القول بأن الهجمات السيبرانية هي " تطويع الإمكانيات الإلكترونية العسكرية للتأثير على مواقع إلكترونية أخرى لتعطيلها أو تدميرها سواء كانت تقدم خدمات مدنية أو عسكرية(١).

كما عرف "Noam Lubell " الهجمات السيبرانية بأنها " عمليات تسعي إلى تحقيق مجموعة واسعة من الأثار، مثل: تدمير البيانات علي شبكة أو نظام متصل بالشبكة، أو تغيير البيانات المخزنة على الشبكة أو إبطال أو رفض الخدمة على الشبكة(٢).

فيما عرفها البعض(٣) بأنه " هجوم عبر الانترنت يقوم على التسلل إلى مواقع الكترونية غير مرخص بالدخول إليها، بهدف تعطيل أو إتلاف البيانات المتوفرة فيها أو الاستحواذ عليها، وهى عبارة عن سلسلة هجمات الكترونية تقوم بها دولة ضد أخرى".

ومن جانبنا يمكننا أن نعرف الهجوم السيبراني بأنه " أي عملية إلكترونية تقوم بها دولة ضد دولة أخرى، يكون هدفها تعطيل المعلومات الموجودة على شبكات

---

(1) **Marco Roscini**:" World Wide Warfare – Jus ad bellum and the use of Cyber Force", MPYUNL, vol. 14,2010, p. 91.

(٢) أكد **Noam Lubell** على أن:

«Cyber attacks are described as operations seeking to accomplish a wide range of effects, including "destroy data on a network or a system connected to the network" e an active member of a network and generate bogus traffic clandestinely alter data in a database stored on the network" and degrade or deny service on a network».

راجع مؤلفه بعنوان:

Lawful targets in cyber operations: Does the principle of distinction apply? IlS, 2013, v.89, p. 254.

(٣) د.أحمد عبيس الفتلاوي، الهجمات السيبرانية مفهومها والمسئولية الدولية الناتجة عنها في ضوء التنظيم الدولي المعاصر، مرجع سابق، ص٦١٦.

الكمبيوتر، أو إتلافها، لتعريض الدولة لخطر ما، أو السيطرة علي بعض المجالات داخل الدولة".

ويتضح من هذا التعريف جملة خصائص تتسم بها الهجمات السيبرانية، أهمها(١):

- **إن الهجمات السيبرانية تقنية متطورة، تعكس التطور الحاصل فى مجال البرمجيات والحواسيب والاتصالات.**
- **التكلفة المتدنية – نسبيًا – مقارنة مع الميزانيات الضخمة التى تخصص لإنتاج أسلحة تقليدية، كالغواصات والمقاتلات المتطورة.**
- **هجمات خاطفة وسريعة تحدث فى زمن السلم والحرب، وفى مدة قصيرة تعطي أفضلية للمهاجم.**
- **صعوبة تحديد هوية منفذيها ومصدرها، كما تتطلب مهارات وامكانيات فنية لاكتشافها.**
- **عدم محدودية الهجمات السيبرانية من حيث النطاق الجغرافي، ومن حيث الأهداف والنتيجة، فقد تتعدى الهدف المرصود الى مواقع سيادية وحساسة.**

وبالتالي فإن هذه الهجمات تتم بواسطة استخدام الكمبيوتر أو الشبكات، وتهدف إلي تعطيل أو تدمير أنظمة الإنترنت أو الممتلكات أو الوظائف الحاسوبية الخاصة بالخصم، فهذه الهجمات تشكل تهديدًا ضد سلامة الأراضي أو الاستقلال السياسي لأية دولة، أو التي لا تتفق مع مقاصد الأمم المتحدة(٢).

---

(١) د. بوطلاعة وداد، الهجمات السبرانية على البنية التحتية الحرجة دراسة في ضوء القانون الدولي العام، مجلة حقوق الإنسان والحريات العامة، المجلد (٧)، عدد (٢)، ٢٠٢٢، ص٣٢٦.

(2) **Marco Roscini:** World wide warfare jus ad bellum and the of cyber force, Op, Cit, p.91.

كذلك فإن هذه العمليات والهجمات لا يقتصر أثارها علي الحصول علي بيانات ومعلومات فقط من أجل استخدامها ضد الدولة(١)، بل تهدف دائمًا إلي التأثير على مقدرات الأمور داخل الدول المخترقة، مثل اختراق أنظمة الكمبيوتر للسيطرة علي الحركة الجوية وخطوط أنابيب النفط، ومحطات الطاقة النووية، ومراقبة الحركة الجوية والبرية والبحرية، لذلك فإن أثر هذه العمليات يكون على درجة كبيرة من الخطورة، والذى قد يؤدى إلي حدوث كوارث داخل الدولة(٢).

رابعاً: طبيعة الهجمات السيبرانية وسماتها:

مما لا شك فيه أن المخاطر فى حد ذاتها لا تتغير، ولكن سماتها هى التى تتغير مع تطور الأدوار والوسائل المستخدمة، فقد أصبحت الدول تهتم بتكنولوجيا المعلومات ودورها فى الصراعات والحروب المستقبلية، وذلك استعدادًا لمواجهة ما قد ينشأ عنها من مخاطر، والتى يتوقع الكثير حدوثها فى الفضاء السيبراني، ولذا نجد أن هناك مناورات يتم إجراؤها للتدريب على هذا النوع الجديد من الصراع، وكيف يمكن مواجهته والاستعداد له. ولذا بات من الصعب تخيل صراع عسكري اليوم دون أن يكون لهذا الصراع أبعاد سيبرانية، وأصبحت فى صلب اهتمامات الأنظمة الدفاعية لأٍي صراع يمكن أن يحدث في المستقبل، فالحرب التي تم شنها ما بين روسيا وإستونيا عام ٢٠٠٧(٣)، وبين جورجيا وروسيا عام ٢٠٠٨(١)، دفع العديد من

---

(١) من أشهر الهجمات السيبرانية هجمات titan Rain عام ٢٠٠٣ عندما تم اختراق منشآت وزارة الدفاع الأمريكية ومختبرات ناسا ولوكهيد مارتن (يزعم أن الصين كانت وراء هذه العملية). هجمات فيروس Stuxnet ضد المنشآت النووية الإيرانية.

Tim Jordan: Hacking: Digital Media and Technological Determinism polity press, Cambridge, 2008, p. 78.

(2) **Sirohi M. N:** Cyber Terrorism and Information Warfare, 2015, p. 106.

(٣) ففي عام ٢٠٠٧ تعرضت استونيا، – إحدى جمهوريات الاتحاد السوفيتي السابق – إلى هجمات سيبرانية متلاحقة أدت إلى تعطيل كامل لشبكات الاتصال الالكترونية فيها، وبالذات المواقع =

الدول مثل الولايات المتحدة الأمريكية وغيرها من الدول الأخرى مثل الصين – على الرغم من التقدم التكنولوجي لها – ببناء وحدات إلكترونية على شبكات الإنترنت للحماية من مئات وآلاف القراصنة المحترفين(٢).

فالحرب السيبرانية أصبحت بديلاً لتلك الحروب التقليدية التي كانت تعتمد على جيوش عسكرية وأسلحة قتالية، فعلى الرغم من أن الحرب السيبرانية تكون بدون نار أو قصف، إلا أن لها جانبًا عنيفًا من حيث الاختراقات والقرصنة ونشر الفيروسات وغيرها من الأساليب، وبالرغم من فداحة الخسائر، فإن الأسلحة بسيطة لا تتعدى فى أغلب الأحوال « الكيلو بايتس » والتي تتمثل فى فيروسات إلكترونية تخترق شبكة الحاسب الآلي، وتنتشر بسرعة بين الأجهزة، وتبدأ عملها فى سرية تامة وبكفاءة

=

الرسمية الحساسة لرئيس الوزراء ورئيس البرلمان، فضلاً عن المواقع الرسمية الأخرى لمكاتب الوزراء الاستونيين، وقد وجه الاتهام رسميًا إلى روسيا الاتحادية، إذ عدتها استونيا هجمات انتقامية بسبب قيامها بنقل نصب تذكاري يخلد الجيش الروسي من العاصمة (تالين) إلى مكان آخر مجهول.

- **Allen D. Walker:** Applying International Law to the CyberAttacks in Estonia, Air Command and Staff College, 2008, p. 5.
- **Dieter Fleck**: **Searching** for International Rules Applicable to Cyber Warfare: A Critical First Assessment of the New Tallinn Manual' JC&SL, vol. 18, no. 2, 2013, p. 331-335.

(١) حيث أنه قبل بدء العمليات القتالية بين الدولتين وبالتحديد بيوم واحد ، تعطل نظام الاتصال الالكتروني(IT) للقوات الجورجية بالكامل، ولاسيما في إقليم اوسيتيا الجنوبية الذي شهد حالة من التوتر بسبب إعلانه الانفصال عن جورجيا، ولقد أسهم الهجوم السيبراني في حدوث إرباك اضعف قدرة وسائل الدفاع الجوي الجورجية، فضلاً عن تعرض مواقع الكترونية أخرى لهجمات سيبرانية مماثلة، طالت مواقع حساسة كوسائل الإعلام والبني التحتية وأهمها قطاع المواصلات.
Mark Galeotti: Russia's Five-Day War: The invasion of Georgia, August 2008, 2023, p.7.

(٢) د. عباس بدران، الحرب السيبرانية، الاشتباك في عالم المعلومات، مركز دراسات الحكومة السيبرانية، بيروت، ٢٠١٠، ص١١٠.

عالية. وتتميز هذه الحروب بالسرعة والدقة فى تنفيذ العمليات العسكرية، وتُعتبر من أدوات الحرب الشاملة(١).

ويتميَّز الهجوم السيبراني بأنه من الهجمات الخفية(٢) التى لا يلاحظها الضحية رغم أنها تقع أثناء وجوده على الشبكة، والسبب في ذلك تمتع فاعل الهجوم بقدرات فنية عالية تجعله ينفذ هجومه بدقه، كما في حالة إرسال الفيروسات وسرقة الاموال والبيانات الخاصة أو إتلافها والتجسس وسرقة المكالمات وغيرها من الهجمات. كما تتميز الهجمات السبرانية بأنها عابرة للحدود(٣)، اذ لم تعد هناك حدود مرئية أو ملموسة تقف أمام نقل المعلومات بين الدول، وذلك لما تتمتع به الحواسيب وشبكاتها في نقل كميات كبيرة من المعلومات، وبالتالي فان أماكن متعددة في دول مختلفة قد تتأثر بهجمة الكترونية، فقد يكون الفاعل في دولة والهجوم يقع في دولة أخرى(٤).

وبالتالي يمكن القول أن هذه الهجمات تُعد تدميرًا لا يصاحبه دماء وأشلاء بالضرورة، بل يتضمن التجسس والتسلل ثم النسف، لكن لا دخان ولا أنقاض، ويتميز أطرافه بعدم الوضوح، وتكون تداعياته خطيرة، سواء عن طريق تدمير المواقع على

---

(١) د. هاني محمد خليل العزازي: النظام القانوني الدولي لمكافحة المخاطر السيبرانية، مجلة مصر المعاصرة، عدد (٥٤٩)، يناير ٢٠٢٣ ، ص٤٧٦.

(2) **Gary Brown, Colonel, Keira Poellet, Major:** The Customary International Law of Cyberspace, Strategic Studies Quarterly, 2012, p. 139.

(3) **Johann-Christoph Woltag:** Cyber Warfare: Military Cross-border Computer Network Operations Under International Law, Intersentia, 2014, p. 112.

(٤) د. رعد فجر الراوي: القصور التشريعي في مواجهة الهجمات السيربانية، مجلة كلية القانون للعلوم القانونية والسياسية، المجلد (١٠)، العدد (٣٩)، ٢٠٢١، ص١٩٤.

الإنترنت ونسفها وقصفها بوابل من الفيروسات، أو العمل على استخدام أسلحة الفضاء السيبراني المتعددة للنيل من سلامة تلك المواقع، وهي أسلحة يسهل الحصول عليها من خلال مواقع الإنترنت وتعلم كيفية استخدامها، كما أن انتشار الفضاء السيبراني وسهولة الدخول إليه يمكن أن يوسع دائرة استهداف المواقع، بالإضافة إلى زيادة عدد المهاجمين(١).

خامساً: القطاعات التي تستهدفها الهجمات السيبرانية(٢):

ظهرت العلاقة بين الفضاء السيبراني والنزاع كبعد جديد يشمل الجميع شبكات الاتصالات ومصادر المعلومات التي يتم تبادلها إلكترونيًا، والصراع الإلكتروني في حالة التضارب في المصالح والقيم يتم حلها وتسويتها من خلال الفضاء السيبراني، واتجه الصراع الدولي حول الموارد والمصالح نحو الاعتماد على تكنولوجيا الاتصالات والمعلومات فيما يعرف بـ "عصر المعلومات" والتنافس فى ساحة الإنجازات المادية، وصراع أخر على الأفكار والقيم والموارد(٣).

ويتميز " الصراع السيبراني" بأنه تدمير لا يصاحبه دماء أو أشلاء بالضرورة. فهو يشمل التجسس والتسلل ثم النسف، ولكن لا دخان ولا أنقاض ولا غبار. ويتميز أطرافه بعدم الوضوح، وتداعياته خطيرة، سواء بتدمير مواقع على شبكة الإنترنت

---

(1) **Oona A. Hathaway:** The Law of Cyber-Attack, Op, Cit, p. 9.

(٢) الجدير بالذكر أنه قد أنشات دول كثيرة منظمات حكومية للأمن السيبراني للحماية ضد تهديد الهجمات السيبرانية، حيث قدرت شركة مكافي العالمية للأمن أن ١٢٠ دولة قد طورت بالفعل طرقًا لاستخدام الإنترنت لاستهداف الأسواق وأنظمة الكمبيوتر الحكومية والمرافق.

Miranda Grange: Cyber warfare and the law of armed conflict, University of Wellington, 2014, p.9.

(٣) للمزيد راجع:

Michael Schmitt: Classification of Cyber Conflict, JC&SL, vol. 17, no. 2, 2012, p. 245-260.

ونسفها بقصفها بوابل من الفيروسات، أو العمل على استخدام أسلحة فضائية إلكترونية للنيل من سلامة هذه المواقع(١). لذلك تستهدف الهجمات السيبرانية قطاعات عديدة بهدف السيطرة علي مقاليد الأمور في الدول والتى منها:

١. **القطاع العسكري والحربي:**

مما لا شك فيه أن التسليح يلعب أهمية استراتيجية في توازن القوى وبسط النفوذ، وتمكين الدول من ممارسة العديد من الأدوار، والضغوط والتكتلات في ظل بيئة أمنية يسيطر عليها الشك وعدم اليقين، ومصالح استراتيجية قابلة للتدمير في ثواني معدودة، وهو ما يحمل خطورة عسكرة الفضاء السيبراني أو الإلكتروني دون الأخذ بعين الاعتبار كونه يختلف عن ظروف التقدم في امتلاك الأسلحة النووية أو البيولوجية ودون الأخذ بالاعتبار حجم التدمير المنتظر وقوعه حال التعرض لهجوم سيبراني(٢).

والقطاعات العسكرية والحربية شهدت تطورات عديدة في الآونة الأخيرة واعتمدت بشكل كبير علي عنصر المعلوماتية والرقمية، وأصبحت بناءات تتسلح بأجيال جديدة من الأسلحة التكنولوجية، ولكن هذا التطور العسكري يقابله تهديدات أمنية كشفت ثغرات هذا التحول، مما جعلها أهدافًا للهجمات السيبرانية، فالقطاع العسكري نفسه الذي ينتج جزءًا من هذه النيران الإلكترونية هو نفسه الذي يكون

---

(١) للمزيد راجع بالتفصيل:

Myriam Dunn: "The Cyberspace Dimension in Armed Conflict: Approaching a Complex Issue with Assistance of the Morphological Method", Information and Security: AIJ, vol. 7 2001, p. 145- 158.

(2) **Neil Robinson :** Stocktaking Study of Military Cyber Defense Capabilities in the European Union (milCyberCAP): Unclassified Summary. RAND Research Report 286 (Santa Monica, CA: RAND, 2013): p.7.

مرشحًا لأن يتلقى ضربات من هذه الوسائل الرقمية.

لذلك ذهبت العديد من دول العالم إلي إضفاء أهمية خاصة على التكنولوجيا العسكرية ومحاولة تأمينها من أى هجوم معلوماتي أو سيبراني، حيث إن الأسلحة السيبرانية المستخدمة في الهجوم يمكن صناعتها بقدر تكلفة دبابة حربية، بالإضافة إلي أن مصدرها يمكن أن يبقي مجهولاً، ويمكن إنجاز الهجوم في زمن قياسي، كذلك تدخل هجمات الأسلحة السيبرانية في إطار الحروب غير المتكافئة، كون الطرف الذي يتمتع بقوة هجومية ويبادر باستخدامها هو الطرف الأقوى، بغض النظر عن حجم قدراته العسكرية التقليدية(١).

وهذا ما ذهب إليه الجيش الإسرائيلي فى ٢٠٠٣، حيث أسست هيئة الأركان العامة في الجيش الإسرائيلي شعبة تحمل اسم " شعبة المعالجة عن بُعد" بهدف توفير استجابة فورية لحالات التعرض لهجمات سيبرانية معادية، فضلاً عن الربط بين نظم الحواسيب العسكرية بالجيش الإسرائيلي(٢).

٢. **قطاع الأعمال والأنظمة الحكومية وغير الحكومية:**

كما هو الحال في جميع القطاعات الإلكترونية، والتي تعتبر هدفًا مباشرًا لنيران الهجمات السيبرانية، فإن القطاعات الحكومية بشكل عام، والتي تتعلق أعمالها بالعمل المدني والإداري وتقديم كافة الخدمات للجمهور بشكل خاص معرضة لتلقي ضربات سيبرانية أو إلكترونية، كونها أحد أهداف صراعات التقنية في عالمنا اليوم،

---

(١) **د. عادل عبد الصادق:** أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، وحدة الدراسات المستقبلية، مكتبة الإسكندرية، ٢٠١٦، ص ٥٨.

(٢) **د. ربيع محمد يحيي:** إسرائيل وخطوات الهيمنة علي ساحة الفضاء السيبراني في الشرط الأوسط، دراسة حول استعدادات ومحاور عمل الدولة العبرية في عصر الإنترنت، مركز الإمارات للدراسات والبحوث الاستراتيجية، ٢٠١٣ ، ص٧٠.

خاصة بين الحكومات التي تتسابق إلى الدخول فى تطبيق منظومات الحوكة الإلكترونية، أو تلك الشركات التى تعيش القالب التنافسي الرقمي(١).

لذلك تلجأ كافة الحكومات الإلكترونية في العصر الحديث إلي معاينة كافة التحركات التى تتم عبر فضائها الإلكتروني، ورصد كافة العمليات والبيانات التي تخرج عن سياق عملها الحكومي من قبل روداها، ولم يتوقف الأمر عند الحكومات فقط بل امتد إلي القطاع الخاص، حيث تقوم شركات القطاع الخاص بحماية كافة المعلومات الخاصة بها وضبط وتحليل تدفق المعلومات إليها، وكذلك التنسيق مع القطاع الحكومي في كيفية توريد المعلومات بين الطرفين، وعلي الأخص فى الدول الرقمية.

ومن نماذج الهجوم السيبراني في التاريخ المعاصر، الهجوم السيبراني الذي قامت به الولايات المتحدة الأمريكية عام ١٩٨٢ ضد منظومة التحكم العالية صناعيًا في أنبوب نفط Chelyabinsk التابع للاتحاد السوفيتي السابق، والذي نجم عنه انفجار هائل طال ثلاثة كيلو مترات من الأنبوب، وأدى إلى خسائر بالغة، وهو ما نفاه الاتحاد السوفيتي آنذاك(٢).

---

(١) **كلارك ريتشارد:** حماية الفضاء الإلكتروني في دول مجلس التعاون الخليجي، الطبعة الأولي، مركز الإمارات للدراسات والبحوث الاستراتيجية، ٢٠١١، ص ٣١-٣٢.

(٢) للمزيد راجع:

- **Diego Rafael Canabarro and Thiago Borne**:" Reflection on the fog of Cyber War", National Center for Digital Government, Policy working Paper no. 13, March, 2013, p.10.
- **Arif Sari:** Applying methods of scientific inquiry into intelligence, security and counterterrorism, United States of America, 2019, p. 7.

٣. قطاع الاتصالات والمعلومات:

يشمل هذا القطاع جميع شبكات الاتصال العامة للدولة، وفي مقدمتها الإنترنت، الحاسبات، الشبكات الحكومية والأكاديمية والمدنية والتجارية، ومحطات البث التليفزيوني، وشبكات الخلوي، ومراكز استقبال الموجات السلكية واللاسلكية، والألياف الضوئية، وكل ما يمك إدراجه تحت مظلة هذا القطاع الاتصالي والمعلوماتي(١).

وكما ذكرنا سلفًا أن الهجمات السيبرانية أو الحرب الإلكترونية تستهدف أمن المعلومات الخاصة بكافة القطاعات، لذلك فإن التدمير المصاحب لهذه الهجمات لا تصاحبه في الغالب دماء وأشلاء، فهي تستهدف الفضاء الإلكتروني للنيل من سلامة هذه المواقع.

ونحن نرى أن تلك المتغيرات ساهمت في تغير أساليب الحروب والهجمات، فقد أدت إلي بروز وعي عالمي لزيادة المعرفة في عمليات الإنتاج والابتكار لقطاع الاتصالات والمعلومات، وعدم الاعتماد علي القوة العسكرية فقط، فالصراع السيبراني يتجاوز الحدود التقليدية للدول ضاربًا بسيادتها عرض الحائط، فحرب المعلومات أصبحت تتساوي مع الحروب التقليدية، لذلك كان علي الكيانات الدولية حماية نفسها وامنها المعلوماتي ضد الجيل الجديد من الحروب.

سادساً: خصائص الأسلحة والهجمات السيبرانية:

تُعرف الأسلحة بوجع عام بأنها أجهزة أو ذخائر أو أدوات أو مواد أو قطع من المعدات التي تولد قدرة هجومية يمكن تطبيقها علي شخص أو كائن معاد، أو هي وسيلة حرب تستخدم في العمليات القتالية، سواء بندقية أو صاروخ أو قنبلة، والتي

---

(١) د. **وليد غسان جلعود:** دور الحرب الإلكترونية في الصراع العربي الإسرائيلي، مرجع سابق، ص ٩٠.

يمكن أن تسبب إصابة أو وفاة أو تدمير الأشياء(١).

كما تُعرف وسائل الحرب بأنها" أسلحة أو أنظمة أسلحة أو أشكال منصات تستخدم لأغراض الهجوم، وعليه فإن وسائل الحرب لا تشمل أنظمة الأسلحة فحسب، بل تشمل أيضًا المعدات المستخدمة للتحكم لتسهيل أو توجيه سير الأعمال العدائية(٢).

وبناء عليه فإن السلاح هو كل ما يؤدي إلي الدمار باستخدام القوة الحركية، مثل القنابل والصواريخ والقذائف، إلا أن أنواعًا أخرى من الأسلحة مثل الغازات

---

(1) **william H. Boothby**: weapons and the law of armed conflict, no. 4, 2009, p. 344.

(٢) حيث تتعدد أسلحة الهجوم السيبراني:

- **رفض الخدمة أو الوصول إلي الشبكة:** هذه هي الخطوة الأولي في الهجوم السيبراني، حيث يتمكن المهاجمون من إلي الوصول إلي الشبكة أو جهاز الكمبيوتر، ويمنعون الوصول المباشر لمستخدمي النظام.
- **البرامج الخبيثة:** تعمل البرامج الضارة عادة بواسطة تعطيل وظائف الكمبيوتر العادية أو عن طريق فتح باب خلفي للمهاجم عن بعد للسيطرة علي الكمبيوتر، وأشهر البرامج الضارة الفيروسات، حيث يقوم الفيروس بإرفاق نفسه ببرامج أو ملف كمبيوتر، وينتشر من كمبيوتر لأخر، والشكل الشائع هو الدودة، وينتشر من كمبيوتر إلي أخر ويختلف عن الفيروس فإنه قادر علي الانتقال دون مساعدة من مستخدمي الكمبيوتر الفرديين، وتميل الديدان إلي استهلاك كميات هائلة من الذاكرة.
- **تعديل البيانات أو إتلافها:** هنا يحصل المتسللون علي وصول غير مصرح به إلي الشبكات بقصد إتلاف البيانات أو تغييرها، ويمكن أن يشمل هذا الهجوم شبكات خاصة أو حكومية، وذلك لدوافع إجرامية أو حربية
- **السيطرة الكاملة علي أجهزة الكمبيوتر والشبكات:** وذلك أشرس أنواع الهجوم والهدف النهائي للمتسللين، ويصفه البعض بأنه احتلال رقمي.

- **Miranda Grange:** Cyber warfare and the law of armed conflict, op.cit, p. 5.
- **Bradley Raboin:** Corresponding Evolution: International Law and the Emergence of Cyber Warfare, JNAALJ,vol. 31, 2011, p. 612.

والعوامل الكيميائية والبيولوجية، تؤدى إلى التدمير دون استخدام القوة الحركية، وعليه فإن العامل الحاسم فيما يتعلق بالأسلحة هو تحقيق الدمار والتأثير الضار علي الأشخاص(١).

والسؤال المثار هنا هل الهجوم السيبراني يعتبر سلاح بالمعني المطروح سلفًا؟

أجاب علي هذا التساؤل البروفيسور "Schmitt " حيث قال أنه بالرغم أن القدرة الحركية السيبرانية تتمثل في تحريك أصابع اليد علي مفتاح الكمبيوتر ليبدأ الهجوم السيبراني، إلا أن العواقب العنيفة المترتبة علي الهجوم السيبراني هي الحاسمة في وصف مثل هذا الحدث علي أنه هجوم سيبراني، وقال أن النتائج العنيفة من التسبب في وفاة شخص أو إصابتهم من الهجوم السيبراني تكفي لاعتباره سلاح بالمعني المتعارف عليه في القانون الدولي(٢).

---

(١) حيث أكد **William H. Boothby** ذلك بقوله:

«Weapons as conventionally understood can take a variety of forms. While some weapons, such as bombs, rockets, bullets, artillery shells and the like generate their destructive effect by the use of kinetic force, other kinds of weapons, such as gases, chemical and biological agents achieve their wounding or deadly purpose without necessarily operating kinetically The critical factor in relation to all weapons is the injurious or damaging effect that they have on the persons and/or objects associated with the adverse party to the conflict». **William H. Boothby:** Methods and Means of Cyber Warfare, Naval War College, ILS, 2013, v. 89, P.388.

(٢) حيث أكد **Michael N. Schmitt** على أن:

«It is the violent consequences that are designed or intended to follow the use of the cyber capability that are critical to the characterization of such a cyber event as a cyber attack. The same intended violent consequences are critical to the characterization of a cyber capabil-ity as a cyber weapon.Therefore, a cyber weapon would comprise any computer equipment or computer device that is designed, intended or used, in order to have violent consequences, that is, to cause death or inju-ry to persons or damage or destruction of objects».

راجع مؤلفه بعنوان:

=

وعليه فإن تأثير القدرة السيبرانية علي المنشأة التي يخدمها الحاسب المستهدف من الهجوم، يجعل هذه القدرة سلاحًا سيبرانيًا أو إلكترونيًا، وذلك مثل الهجوم على نظام التحكم الذي يتحكم فى تشغيل منشأة للمرافق العامة، كمعمل لتكرير البترول، فإن الضرر الذي تسببه العملية السيبرانية لمصفاة البترول، يؤدي إلي اعتبار الأداة الإلكترونية سلاحًا إلكترونيًا(١).

وتختلف البنية التحتية لقدرات الأسلحة السيبرانية عن الأسلحة التقليدية، فتتكون من جهاز كمبيوتر أو هاتف محمول متصل بالإنترنت وسلسلة من برمجيات تقليدية، وبرمجيات خبيثة وبرامج تجسس، ولا تحتاج عملية التطوير لمعدات متخصصة أو يمكن حظرها كما هو الحال في الأسلحة النووية، والتي تحتاج إلي عمليات تخصيب اليورانيوم وخدمات لوجستية معقدة، كما تتطلب هذه الأسلحة مهارات نادرة لإنتاجها ولا تحتاج لإطلاقها سوي منصات بسيطة وغير مرئية، تتمثل في موقع إطلاق، كمبيوتر، وموقع علي شبكة الإنترنت ومحرك بحث وخادم افتراضي أو مادي(٢)، كما أن هذه الأسلحة قد يستخدمها العسكريون والمدنيون، بل يتميز فيها المدني علي العسكري علي عكس الأسلحة التقليدية. كما أن هجمات الفضاء السيبراني تكون استباقية دون سابق إنذار، وأنها غير محددة المجال أو المدى وتكون أهدافها غير مأمونة، وذلك بخلاف الحرب التقليدية التى تكون أهدافها محددة ومكانها محددًا، كما أن قوات الحرب السيبرانية غير معروفة وغير مرئية.

=

Cyber Operations and the Jus in Bello: Key Issues, Naval War College International Law Studies, 2011, v. 87, P.93-94.

(1) **William H. Boothby:** Methods and Means of Cyber Warfare, op.cit, P.389.

(٢) **د. عادل عبد الصادق:** أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، مرجع سابق، ص ٥٥ وما بعدها.

سابعاً: تمييز الهجوم السيبراني عن الجريمة السيبرانية:

مما لا شك فيه أن هناك فرق بين مصطلح الهجوم السيبراني والجريمة السيبرانية والذي كثيرًا ما يتم الخلط بينهما من قبل المهتمين في هذا المجال، إذ أن الخلط بين المصطلحين يؤدي بالنتيجة الى خلق مشكلة جديدة قد تؤدي الى خرق القانون الدولي، فيما لو أن الدولة المعتدى عليها قد تصرفت بغض النظر عن تحديد نوع الاعتداء هل هو هجوم سيبراني أم جريمة سيبرانية، باعتبار أن حق الدولة المعتدى عليها في الهجوم السيبراني يكون مختلف عن حقها في الرد عن الجريمة السيبرانية. كما أن الهجوم السيبراني هو فعل يقوض من قدرات ووظائف شبكات الحاسوب من أجل هدف قومي أو سياسي، من خلال استغلال نقاط الضعف لتمكن المهاجم من خرق الأنظمة والعبث بها(١).

إن الهجوم الإلكتروني له القدرة على اغلاق أجهزة الطرد المركزي النووية وأنظمة الدفاع الجوية والشبكات الكهربائية، مما يعد تهديدا خطيرًا للأمن القومي. لذا ينبغي التعامل مع الهجمات السيبرانية بوصفها أعمال حرب لأنها تشبه الهجمات المسلحة التي ينظمها قانون الحرب، ومن ثم يتضح أن الهدف من الهجوم السيبراني يعطي صورة واضحة، إنه جاء من نتاج سياسة الدولة، وليس شخص أو جماعة(٢).

أما الجريمة السيبرانية فهي عبارة عن مخالفة ترتكب ضد الأشخاص أو الجماعات بدافع إجرامي كالدخول غير المصرح به، وإتلاف البيانات المخزونة في

---

(1) **Ian Traynor:** Russia Accused of Unleashing Cyber War to Disable Estonia, Guardian London, May 17, 2007, p. 39.

(2) **Kubo Mačák:** Is the international law of cyber security in crisis?, University of Exeter, United Kingdom, 2016, p.136.

كما أكد على أن:

«Cyberspace is not the first novel phenomenon to have resisted the development of global governance structures for some time after its emergence».

النظم أو الاعتراض غير القانونى لها عن طريق نقلها من جهاز حاسوب لآخر، كإدخال بيانات خاطئة أو العبث بها. كما عُرفت بأنها " سلوك غير مشروع معاقب عليه قانونًا، صادر عن إرادة إجرامية، محله معطيات الحاسوب(١).

وبالتالي فالهجوم السيبراني يكون ضمن اختصاص القانون الدولي العام، لأنه يمثل خرق لسيادة الدولة، بينما تكون الجريمة السيبرانية ضمن اختصاص القانون الوطني وفقًا لمبدأ إقليمية القانون(٢).

ونحن نتفق مع ما ذهب إليه البعض(٣) من أن ما يميز الهجوم السيبراني عن الجريمة السيبرانية هو أن الهجوم السيبراني يهدف إلى إضعاف أو تدمير قدرات الدولة من خلال شبكات الإنترنت لغرض سياسي أو لمقتضيات الأمن القومي، وهذا لا نجده في الجريمة السيبرانية حيث يكون هدفها مقتصرًا على السرقة من أجل الحصول على منافع مالية أو نقدية، وفي كلتا الحالتين تكون الدولة مسؤولة مسؤولية دولية عن اعمال مواطنيها التي تسبب ضررًا بمصالح الدول الأخرى، وهذا يؤدي الى الحد من الهجمات السيبراني.

---

(١) **د.** نائل عبد الرحمن صالح: واقع جرائم الحاسب في التشريع الأردني، مؤتمر القانون والكمبيوتر والأنترنت، كلية الشريعة والقانون، جامعة الامارات العربية المتحدة، الطبعة الثالثة، المجلد الأول، ٢٠٠٤، ص ١٩٢.

(2) **Gary D. Brown:** International law applies to cyber warfare! now what?, SLR, vol. 46, 2017, p. 357.

(3) **Mark Johnson:** Cyber Crime, Security and Digital Intelligence, New York, 2013.

المبحث الثاني
الإطار القانوني لحق الدفاع الشرعي
ضد الهجمات السيبرانية

لقد كان للحرب نصيبها الوافر من التطور التكنولوجي، إذ شهد العالم نوعًا جديدًا من سباق التسلح، الذي تحوّل إلى عنوان في العلاقات الدولية، ومقياس يقاس به توازن الردع بين الدول(١). فلم يعد سباق التسلح اصطلاحًا عسكريًا يقوم على تكديس الطائرات أو المدافع أو الدبابات أو أسلحة الدمار الشامل فقط، بل يقوم على استحداث برامج إلكترونية مُعدة لأغراض عسكرية وتطويرها، تُعرف اختصارًا بـ "Cyber"(٢).

وقد انبثق عن هذا التسليح السيبراني نزاعات مسلحة دولية وغير دولية، مما يعطي للدول الحق في الدفاع الشرعي عن نفسها وعن سيادتها.

ونقسم هذا المبحث إلي مطلبين:

المطلب الأول: ماهية حق الدفاع الشرعي.

المطلب الثانى: شروط ممارسة حق الدفاع الشرعى.

المطلب الثالث: ضوابط الدفاع الشرعي ضد الهجمات السيبرانية.

---

(1) **Hitoshi N., Robert M.:** New Technologies and the Law of Armed Conflict, Australian National Of Law, Australia, 2013, p.3.

(2) **David H. Brandin ،Michael A. Harrison:** The Technology War, Wiley, University California, 1987, p. 26.

المطلب الأول
ماهية حق الدفاع الشرعي

يُعد الدفاع الشرعي احدى الاستثناءات الرئيسية التي تمثل خروجًا علي نص المادة الرابعة من ميثاق الأمم المتحدة، والتي تحظر استخدام القوة في العلاقات الدولية، حيث أن حق الدفاع الشرعي حق طبيعي معترف به للدول. وإن أي استخدام للقوة على الصعيد الدولي يخضع – من الناحية القانونية – للقانون الدولي، بغض النظر عن الطريقة التي يتم بها استخدام القوة وتنفيذها(١).

والدفاع الشرعي يعني " قيام دولة ما يقع عليها عدوان، بالرد المسلح لدفع هذا العدوان الواقع عليها"، وبديهي أن هذا الرد هو عمل غير مشروع في ظل تحريم اللجوء إلى استخدام القوة في العلاقات الدولية، إلا أنه نظراً لأن الرد المسلح اتخذ كدفاع عن النفس فإن الدفاع الشرعي يجعل هذا الرد عملاً مشروعًا(٢).

وبالتالي فلكل دولة الحق الكامل فى أن تقابل أي هجوم على إقليمها أو على رعاياها بالقوة المسلحة عند الاقتضاء، بشرط أن يشكل هذا الاعتداء أعمالاً غير مشروعة أصلاً، بحيث تكون الدولة التى تدافع عن نفسها ضحية لعدوان، ولا يمكن لها أن تدفع هذا العدوان إلا باستخدام القوة، وذلك إلى أن يتخذ مجلس الأمن إجراءً جزائيًا دوليًا يتمثل في تدابير قمعية وفقًا للفصل السابع من ميثاق الأمم المتحدة(٣).

وهو ما نصت عليه المادة (٥١) من ميثاق الأمم المتحدة بقولها أنه " ليس

---

(1) **Terry D. G. and Paul A. L. D.:** Anticipatory Self-Defense in the Cyber Context, ILS, Vol. 89, 2013, p. 439.

(٢) د: وائل أحمد علام: مركز الفرد في النظام القانوني للمسئولية الدولية، دار النهضة العربية، القاهرة، ٢٠٠١، صـ ٢٩.

(٣) د: نبيل بشر: المسئولية الدولية في عالم متغير، ط١، بدون دار نشر، ١٩٩٤، ص٢٤٣.

في هذا الميثاق ما يضعف أو ينقص الحق الطبيعي للدول، فرادي أو جماعات، في الدفاع عن أنفسهم إذا اعتدت قوة مسلحة علي أحد أعضاء الأمم المتحدة وذلك إلي أن يتخذ مجلس الأمن التدابير اللازمة لحفظ السلم والأمن الدوليين، والتدابير التي اتخذها الأعضاء استعمالا لحق الدفاع عن النفس تبلغ إلي المجلس فورًا ولا تؤثر تلك التدابير بأي حال فيما للمجلس- بمقتضي سلطته ومسؤولياته المستمدة من أحكام هذا الميثاق- من الحق أن يتخذ في أي وقت ما يري ضرورة لاتخاذه من الأعمال لحفظ السلم والأمن الدولي أو إعادته إلي نصابه".

وباستقراء المادة السابقة يتضح أن الميثاق قد أجاز للدول استخدام القوة المسلحة كميزة تضفي المشروعية على تصرف يُعد – بحسب الأصل – غير مشروع، إلا أنه قد اتُخذ حماية لحقوق جوهرية، يعتمد عليها أمن الدولة وبقائها، وتطبيقاً لمبدأ أن الضرر يزال. ويشترط حتى يكون التصرف مشروعًا أن يرتبط ارتباط لزوم بمعيار المناسبة، بمعنى تناسب رد الفعل مع الخطر محل المواجهة، وعدم تجاوز الضرر المتطلب لحماية الحق الجوهري المعرض للخطر(١).

وبناء على ما تقدم يمكننا تعريف حق الدفاع الشرعي بأنه " الحق الذي يقرره القانون الدولي لدولة أو مجموعة من الدول باستخدام القوة المسلحة لصد عدوان مسلح حال، يرتكب ضد سلامة إقليمها لدرء ذلك العدوان ومتناسبًا معه، ويتوقف حين يتخذ مجلس الأمن التدابير اللازمة لحفظ السلم والأمن الدوليين "(٢).

---

(١) د. مصطفى أحمد فؤاد، الأمم المتحدة والمنظمات الحكومية وغير الحكومية، مطبعة جامعة طنطا، بدون سنة نشر صـ ٥٨.

(2) **Terry D. Gill and Paul A. L. Ducheine:** Anticipatory Self-Defense in the Cyber Context, Naval War College, ILS, 2013, v.89,p.441.
حيث أكد على أن:
«The right of self-defense under international law is the right of a State to repel or, if necessary, overcome an unlawful use of force amounting to
=

إذا يتمثل حق الدفاع الشرعي فى القانون الدولي، في تمكين دولة تعرضت لاعتداء مسلح من الرد علي هذا الاعتداء بالقوة المسلحة، وهو نتيجة حتمية للحق في البقاء والمحافظة علي النفس، لذلك فمن الطبيعي أن يكون استعمال القوة دفاعًا عن النفس مشروعًا، سواء فى ظل القوانين والتشريعات الداخلية أو الدولية(١).

فحق الدفاع عن النفس حق أصيل للدول بموجب القانون الدولي العرفي(٢) واستثناء لحظر استخدام القوة على النحو المنصوص عليه في المادة (٤/٢) من ميثاق الأمم المتحدة، ولإدراج حق الدفاع الشرعي عن النفس في الميثاق غرضًا مزدوجًا. الأول: الاعتراف بالحق القائم مسبقًا للدول بموجب القانون الدولي العرفي. الثاني: إدماج حق الدفاع الشرعي في نظام الميثاق للأمن الجماعي من أجل توفير أساس لا لبس فيه للدفاع الجماعي عن النفس(٣).

=

an armed attack. That is what characterizes it and sets it apart from other uses of force, whether lawful (e.g., action undertaken by or with the authoriza-tion of the UN Security Council to maintain or restore international peace and security or as a law enforcement measure in the domestic legal context), or unlawful (e.g., uses of force that do not have a recognized legal basis».

(١) ذهب فقه القانون الدولي أثناء اجتماع لجنة القانون الدولى إلي أن الدفاع الشرعي لا يعتبر حقًا، وإنما رخصة تؤدي بالقائم بها إلي انتفاء وصف اللامشروعية، إذ تتحرر الدولة من الالتزام بعدم اللجوء إلي القوة تجاه المعتدي إلي أن يقوم مجلس الأمن بمسؤولياته تجاه الموضوع. راجع حولية لجنة القانون الدولي، المجلد ٢، الجزء الثاني، ١٩٧٠.

(2) **David E. Graham:** Cyber Threats and the Law of War, JNSL&P, vol. 4, 2010, p. 93.

حيث أكد على أن:

«There is firm international consensus on this very fundamental issue a state unmistakably possesses both an inherent and Charter-derived right to engage in an "appropriate" selfdefense response to such an attack».

(3) **Terry D. Gill and Paul A. L. Ducheine:** Anticipatory Self-Defense in

=

ومن جانبنا فإننا نرى أنه على الرغم من أن استخدام القوة العسكرية في العلاقات الدولية محظور بموجب القانون الدولي، إلا أن الدفاع الشرعي يدخل ضمن أسباب إباحة استخدام القوة العسكرية، إذ أن أسباب الإباحة هي الأحوال التي يعتبرها القانون سببًا كافيًا لتجريد الفعل غير المشروع من صفته الإجرامية، وإخراجه من دائرة التجريم وإعادته إلي نطاق المشروعية. فالفعل الذي يقع في إطار أسباب الإباحة لا يحمل في طياته معني العدوان علي المصالح المحمية قانونًا.

=

the Cyber Context, Naval War College, ILS, 2013, v.89,p.442.

حيث قرر:

«The inclusion of the right of self-defense within the Charter had and has a dual purpose: recognition of the preexisting right of States under customary international law and integra-tion of the right of self-defense into the Charter system of collective securi-ty in order to provide an unequivocal basis for collective self-defense».

المطلب الثانى
شروط ممارسة حق الدفاع الشرعي

على الرغم من أن القانون الدولي منح الدول حق الدفاع الشرعي عن النفس، لكنه لم يترك هذا الأمر دون قيد أو شرط، فقد وضع عدة شروط تبيح للدولة الحق في الدفاع عن نفسها، لكن يثور التساؤل هل هذه الشروط أو تلك القيود صالحة للتطبيق على الهجمات السيبرانية، علمًا بأنها لا تطلب استخدام القوة العسكرية؟

الحقيقة أنه لن يكون استخدام القوة من قبل دولة ضحية لهجوم سيبراني ممكنًا قانونًا للدفاع عن النفس، إلا إذا توافرت شروط معينة:

أولًا: الهجوم السيبراني استخدام للقوة:

يجدر التنويه بداية إلى أن اتفاق بريان كيلوج سنة ١٩٢٨ اعتبر ولأول مرة في التاريخ أن اللجوء إلي استخدام القوة العسكرية في العلاقات الدولية يعتبر عملًا غير مشروع(١)، وحذا ميثاق الأمم المتحدة هذا الحذو، من خلال نصه فى الفقرة الرابعة من المادة الثانية(٢) على التزام الدول بالامتناع عن اللجوء إلي استخدام القوة أو التهديد باستخدامها، بغرض المساس بسلامة وأمن واستقلال الدول الأخرى.

وجاء مصطلح القوة فى الفقرة الثانية من المادة الرابعة من الميثاق مختلفًا عما استخدم من أجله في المادة الرابعة من عهد عصبة الأمم، إزاء ذلك فقد اختلف

---

(١) ميثاق Kellogg-Briand هو عن اتفاقية لحظر الحرب تم توقيعها في ٢٧ أغسطس ١٩٢٨. يُطلق على الاتفاقية أحيانًا اسم " ميثاق باريس" وكان هذا الميثاق أحد أهم الجهود الدولية لمنع وقوع حرب عالمية أخرى، ولكن كان له تأثير ضئيل فى وقف النزعة العسكرية المتزايدة فى الثلاثينيات أو منع الحرب العالمية الثانية.

(٢) نصت المادة الثانية في فقرتها الرابعة علي أن " يمتنع أعضاء الهيئة جميعًا في علاقاتهم الدولية عن التهديد باستعمال القوة أو استخدامها ضد سلامة الأراضي أو الاستقلال السياسي لأية دولة أو علي وجه أخر لا يتفق ومقاصد الأمم المتحدة.

فقه القانون الدولى حول المقصود بالقوة، هل القوة المقصودة فى المادة الرابعة هى القوة المباشرة فقط، أم تشمل القوة غير المباشرة ؟

فهناك من يرى أن القوة التى أشارت إليها المادة الثانية، هى القوة المسلحة دون غيرها(١)، ففسر البعض القوة بأنها أعمال الغزو والهجوم والعدوان المسلح، فاستخدام القوة يمثل الصفة المسلحة ولا يشمل باقي الأنماط كالضغط الاقتصادي وغيرها، وهذا ما أكده واضعو ميثاق الأمم المتحدة، حيث رفضوا اقتراحًا بإدراج الإكراه الاقتصادي ضمن معني مصطلح القوة، وبالتالي قيام دولة بإجبار دولة أخري علي الانخراط في مسار معين باستخدام العمليات السيبرانية لا يعتبر استخدامًا للقوة(٢).

ومن ثم يأخذ أنصار هذا الرأي بالتفسير الضيق للمادة ٢ فقرة ٤، وبالتالي فالقوة المقصوده من وجهه نظر هذا الرأي هي القوة العسكرية فقط، ويستند في ذلك الى الحجج التالية(٣):

١. إن تفسير المادة (٤/٢) يجب أن يكون في حدود ديباجة الميثاق ونصوصه الأخرى.

---

(١) وقد تبنت محكمة العدل الدولية تفسيرًا ضيقًا للمادة(٥١)، بالتأكيد على جواز حق الدفاع فقط فى حالة الهجوم المسلح من قبل دولة ضد دولة أخرى، وأوردت المحكمة فى قضية « منصات النفط » عام ٢٠٠٣ أمثلة لهذا الهجوم، حيث اعتبرت أنَ استهداف منصَة عسكرية، أو منشأة عسكرية قد يرقى إلى مستوى الهجوم المسلَّح. راجع: موجز فتاوى واحكام محكمة العدل الدولية، أغسطس ٢٠٠٣، يوليو ٢٠٠٤، الامم المتحدة، نيويورك ٢٠٠٤، ص٣١.

(٢) راجع باستفاضة:

Michael N. Schmitt: the law of cyber warfare: quo vadis? SL&PR,vol. 25, 2014, p.280.

(3) **Joseph N. Madubuike - Ekwe:** Cyberattack and the Use of Force in International Law, Beijing Law Review, 2021,p.631.et.ss.

٢. إن الأعمال التحضيرية للمادة (٤/٢) تدل كلها على أن المقصود بالقوة هي القوة المسلحة فحسب، ومن ذلك الاقتراح الذي قدمته البرازيل في مؤتمر سان فرانسيسكو والتي قالت فيه بأن الضغط الاقتصادي هو استخدام غير مشروع للقوة وقد قوبل بالرفض.

وعلي النقيض ذهب الفقيه "Kelsen" إلي وضع تفسير أكثر شمولًا لمصطلح القوة، حيث قرر أن استخدام القوة يكون بأي شكل من الأشكال دون الاقتصار علي القوة المسلحة دون غيرها، واستند في رأيه إلي الفصل السابع من ميثاق الأمم المتحدة وخصوصًا المواد(٤١- ٤٢) علي وجه التحديد، حيث تضمن نص المادة (٤١) إجراءات وتدابير لقمع العدوان من خلال وسائل لا تضم القوات المسلحة، في حين تضمنت المادة (٤٢) إجراءات وتدابير أخري لقمع العدوان تنطوي علي استخدام القوات المسلحة(١).

كذلك أكد الفقيه "Sahovic" إلي أن المنع من استخدام القوة يشمل كل أشكال القوة، حيث قرر أن هذا المنع يشمل الأشكال غير القانونية للضغط في علاقات الدول مع بعضها البعض، وحتي تلك التي قد تتطور بعد تبني ميثاق الأمم المتحدة بما يستهدف سياستها أو اقتصادها أو أي عنصر من عناصر حضارتها، ولا يقتصر المنع علي الهجوم المسلح بل يشمل أى تعرض أو هجوم بأى صورة(٢).

وكذلك رفضت محكمة العدل الدولية التفسير الضيق لمفهوم القوة، حيث أكدت على " أنه لا يجوز اقتصار مفهوم القوة علي العمليات الحركية أو غير الحركية التي

(1) **Kelsen, Hans:** Principles of International Law, 2 edición, Holt, Rinehart and Winston, New York, 1966, pp. 41,43

(2) **Sahovic, Milan:** Principles of international law concerning friendly relation and cooperation, Institute of international politics and economics, Dobbs Ferry, Oceana,Belgrade, 1972 , p.64.

يترتب عليها تأثيرات مماثلة للعمليات الحركية، فقد قررت المحكمة في قضية " نيكاراغو" أن تسليح الدولة للعصابات المنخرطة في أعمال عدائية ضد دولة أخري تعتبر استخدام للقوة، ولكن مجرد تمويل هذه الجماعات بالأموال فقط لا يرقي إلي استخدام القوة من جانب الدولة"([1]).

وذهب البعض إلي استنتاج مفاده أن العمليات السيبرانية غير المدمرة يمكن أن ترقي أحينًا إلي استخدام القوة، مثل توفير البرامج الضارة لمجموعة متمردة، وتدريب أعضائها علي استخدام تلك البرامج بطريقة مدمرة([2]).

وقد نصت القاعدة (١١) من دليل تالين علي أن " العملية السيبرانية تشكل

---

(١) ذهبت محكمة العدل الدولية في هذا الشأن إلي القول:

«Assistance to the contras in Nicaragua. by "organizing or encouraging the organization of irregular forces or armed bands. for incursion into the territory of another State". and "participating in acts of civil strife . in another State", in the terms of General Assembly resolution 2625 (XXV). According to that resolution, participation of this kind is contrary to the principle of the prohibition of the use of force when the acts of civil strife referred to "involve a threat or use of force". In the view of the Court, while the arming and training of the contras can certainly be said to involve the threat or use of force against Nicaragua, this is not necessarily so in respect of all the assistance given by the United States Government. In particular, the Court considers that the mere supply of funds to the contras, while undoubtedly an act of intervention in the internal affairs of Nicaragua, does not in itself amount to a use of force».

راجع القضية بالتفصيل:

Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S)، 1986 I.C.J. 14, ,para 195- 228.

(٢) أكد Schmitt :

«The logic of the holding leads to the conclusion that non-destructive cyber operations can sometimes amount to a use of force. For example, providing malware to a rebel group and training its members to employ that malware in a destructive manner would seemingly qualify». **Michael N. Schmitt:** The law of cyber warfare: quo vadis? Op.cit. p 280.

استخدامًا للقوة عندما يكون الحجم والأثار قابلة للمقارنة بالعمليات غير السيبرانية التي ترفع إلي مستوي استخدام القوة".

وقد وضع مجموعة من الخبراء الدوليين قائمة غير حصرية بالعوامل التي قد تؤثر علي توصيف العمليات السيبرانية من قبل الدول علي أنها استخدام للقوة، مثل: الخطورة، التوجيه المباشر، الغزو، القابلية للقياس، الطابع العسكري، مشاركة الدولة، والشرعية الافتراضية(١)، بالإضافة إلي البيئة السياسية السائدة، علاقة

(١) **يقصد بالخطورة أو الشدة:** العمليات التي تؤدي إلي ضرر جسدي للأفراد أو الممتلكات، فهذه العمليات تعتبر استخدامًا للقوة، أما تلك التي تسبب مجرد إزعاج أو تهيج لا تعتبر استخدامًا للقوة.

العمليات الموجهة: هي العمليات أو الهجمات التي ينتج عنها ضرر فوري يتساوي بالعمليات الإلكترونية التي تستغرق أسابيع أو شهور لتحقيق الهدف المرجو منها.

العمليات المباشرة: هي العمليات التي يرتبط فيها السبب والتأثيرات الضارة بشكل واضح وصريح.

الغزو: هو اقتحام العمليات الإلكترونية للدولة المستهدفة أو أنظمتها الإلكترونية بطريقة تعرض مصالحها للخطر، بحيث يكون تأثير الغزو الإلكتروني يرقي إلي تأثير الغزو العسكري.

القابلية للقياس: عواقب الهجمات السيبرانية أقل وضوحًا بشكل عام من العواقب الناجمة عن الهجمات الحركية، فالهجمات السيبرانية التي تؤدي إلي مجموعة عواقب قابلة للقياس والتحديد تعتبر استخدامًا للقوة.

الطابع العسكري: هي الهجمات السيبرانية ذات الطابع العسكري.

مشاركة الدولة: تعني مدي ودرجة مشاركة الدولة في الهجمات السيبرانية ضد الدولة الخري، فزيادة مشاركة الدولة في الهجمات يصنف استخدامًا للقوة.

الشرعية الافتراضية: أي أن تكون الهجمات السيبرانية غير محظورة بموجب قانون المعاهدات أو القانون العرفي الدولي، فمن غير المرجح تصنيف الهجمات السيبرانية القانونية علي أنها استخدامًا للقوة.

راجع هذه التعريفات لدى:

Sonia Boulos: Cyberspace Risks and Benefits for Society, Security and Development The tallinn manual and Jus ad Bellum: Some critical notes, =

العملية بالقوة العسكرية المحتملة، هوية المهاجم، سجل المهاجم فيما يتعلق بالعمليات السيبرانية، وطبيعة الهدف، كل هذه العوامل وغيرها تعمل في تناغم وتشابك، حيث تتخذ كل دولة قراراتها علي حدة، باستثناء الخطورة وحدها هي التي يمكن أن تصف العملية الإلكترونية بأنها استخدام للقوة. وعليه فقد وافق الخبراء الدوليين بالإجماع على أن أى عملية إلكترونية تسبب ضررًا، أو إصابة أكبر من الحد الأدنى للضرر، كافية لاعتبارها استخدام للقوة، واكدوا على أن الأضرار التي لحقت بالمنشآت النووية الإيرانية في ٢٠١٠ والناجمة عن فيرس "ستوكسنت" استخدام للقوة(١).

ثانياً: أن يكون الهجوم السيبراني هجوماً مسلحاً:

من الجدير بالذكر أنه لا يكفي لاستخدام حق الدفاع الشرعي ضد الهجوم السيبراني أن يوصف الهجوم بأنه استخدام للقوة، وإنما يلزم أن يوصف الهجوم

=

Springer International Publishing, 2017 p. 233 .

(١) جاء بدليل تالين للعمليات السيبرانية أن:

«The International Group of Experts developed a nonexclusive list of factors that would likely influence the characterization of cyber operations by states as uses of force: severity, immediacy, directness, invasiveness, measurability, military character, state involvement, and presumptive legality. Additional factors found meaningful by the Experts included, inter alia, the prevailing political environment, the nexus of an operation to prospective military force. The attacker's identity, the attacker's track record with respect to cyber operations, and the nature of the target. These and other factors operate in concert as states make case-by-case determinations. Of them, only severity alone can qualify a cyber operation as a use of force. In this regard, the Group unanimously agreed that any cyber operation causing greater than de minimis damage or injury suffices. For instance, they concurred that the damage to Iranian nuclear facilities in 2010 resulting from the Stuxnet virus crossed the threshold». **Michael N. Schmitt:** Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge University press, 2017, p. 42.

السيبراني بأنه هجومًا مسلحًا، أي أن يصل لدرجة عالية من الحدة والخطورة .

ولا يفوتنا أن نلقي الضوء علي الخلاف حول مصطلح" هجوم" حيث جاء بالبروتوكول الإضافي الأول لعام ١٩٧٧ الملحق باتفاقية جنيف علي أنه " أعمال عنف" وهذا التعريف أصبح ملزمًا بشكل عرفي حتي لغير الدول الأطراف في البروتوكول، ونتيجة لذلك أقر الفقيه "**Walker** " بأن عددًا قليلًا جدًا من الأنشطة في الحرب الإلكترونية سترقي إلي مستوي الهجوم(١). وذهب " **Schmitt** " إلي القول بأن الهجوم هو " أي شئ يؤدي إلي الموت أو الضرر أو الدمار أو الإصابة. وقرر البعض بأن أي شئ يستهدف المدنيين يرقي إلي مستوي الهجوم"(٢).

وعليه فإن مصطلح " الهجوم المسلح" يختلف عن " استخدام القوة" وهذا ما أقرته محكمة العدل الدولية في قضية نيكاراجوا، حيث أكدت أنه من الضروري التمييز بين أخطر أشكال استخدام القوة - تلك التي تشكل هجومًا مسلحًا - وبين أشكال استخدام القوة الأقل خطورة(٣)، بناءً علي ما أقرته المحكمة، فإن جميع الهجمات المسلحة هي استخدام للقوة، ولكن ليس كل استخدام للقوة هجوم مسلح.

وخلص جانب فقهي إلي أن" أي استخدام للقوة يتسبب في جرح أو قتل

---

(١) راجع باستفاضة حول مصطلح الهجوم:

Paul A. Walker: Rethinking Computer Network "Attack": Implications for Law and U.S. Doctrine, National security law brief, vol.1, no. 1, 2011, p.33.

(2) **Michael N. Schmitt:** Wired Warfare: Computer Network Attack and Jus in Bello, IRRC, vol. 84, no. 846, 2002, P.374- 379.

(٣) أكدت محكمة العدل الدولية أن:

«As regards certain particular aspects of the principle in question, it will be necessary to distinguish the most grave forms of the use of force (those constituting an armed attack) from other less grave forms». CIJ, Recueil des arrêets, Affaire des activites militares et paramilitaires au Nicarague et contre celui-ci, 27 Juin, 1986, p. 23.

الأشخاص أو يضر أو يدمر الممتلكات يرقي إلي مستوي الهجوم المسلح، ويمنح الدولة الحق في اللجوء إلي القوة دفاعًا عن النفس(١).

ولقيام حق الدفاع الشرعي يجب أن تتعرض الدولة لعدوان مسلَح، وهذا الشرط يُعد من أهم القيود التي وضعتها المادة (٥١) من الميثاق(٢)، ومعنى ذلك أن العدوان المنشئ لحق الدفاع الشرعي يجب أن تتوفر فيه مجموعة شروط وهي:

١. **أن يكون للعدوان صفة عسكرية: يقوم هذا الشرط إذا كان هناك اعتداء مسلَح، غير أن هذا المدلول قد أثار خلافا فقهيا فيما يتعلَّق بتفسير عبارة:" اعتدت قوة مسلَّحة" الواردة في المادة (٥١)، حيث عرف الفقه الدولي العدوان المسلح بأنه " استخدامًا للقوة ينشأ خارج إقليم الدولة المستهدفة، يرتفع فوق مستوي الحادث المسلح أو نشاط إجرامي صغير ومعزول، ويكون موجهًا ضد أراضي الدولة أو سفنها، طائرتها العسكرية في المجال الجوي الدولي، أو الموجودة بشكل قانوني علي أراضي دولة أخري، أو ضد مواطنيها الموجودين فى الخارج(٣).**

ولا يفوتنا التنويه إلى أن الفقه الدولي اختلف حول ما إذا كان الهجوم علي

---

(1) **Michael N. Schmitt**: Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, op.cit, p.55.

حيث ذهب إلى القول:

«Any use of force that injures or kills persons or damages or destroys property" amounted to an armed attack against which a state enjoys the right to resort to force in self-defense».

راجع أيضًا:

Sheng Li: When does internet denial trigger the right of armed self-defence, YJIL, vol. 38, 2013, p. 199.

(2) **Stephen Moore:** Cyber Attacks and the Beginnings of an International Cyber Treaty, International Law; Commercial Law, vol. 39, 2013, p. 236.

(3) **Terry D. Gill and Paul A. L. Ducheine**: Anticipatory Self-Defense in the Cyber Context,op.cit. p. 445.

رعايا دولة فى الخارج يعتبر هجومًا مسلحًا من عدمه؟

فذهب رأي إلي رفض الموقف القائل بأن الهجوم علي رعايا دولة في الخارج يعتبر هجومًا مسلحًا. وذهب رأي أخر إلي اعتبار الهجوم علي الرعايا هجومًا مسلحًا، حيث إن حماية المواطنين تندرج ضمن الحق العرفي للدفاع عن النفس. وذهب رأي وسط إلي أنه إذا كان الرعايا يتعرضون لتهديدات علي حياتهم أو سلامتهم الجسدية من أجل الحصول علي تنازلات أو تغير في سياسية الدولة الأم، فإن ذلك يشكل هجومًا مسلحًا(١).

وبناء عليه فإنه يشترط في العدوان المسلح أن يكون ماسًا بأحد الحقوق الجوهرية للدولة، سواء كان عدوانًا منصبًا علي أملاك الدولة أو مهددًا لها، ويرجع السبب في اشتراط هذه الصورة من العدوان ثبوت حالة القوة القاهرة التي تبيح للدولة اللجوء إلي استخدام القوة المسلحة في إطار من المشروعية الدولية، لأغراض الدفاع عن حقها الطبيعي في الوجود(٢). وإذا قام بالهجوم المسلح جماعة مسلحة منظمة مع حصولها علي دعم مادي أو معنوي أو لوجستي أو دبلوماسي أو أيديولوجي من الدولة، فإن هذا الهجوم يشكل بالمستوي المطلوب مشاركة الدولة في الهجوم، ومن ثم يعتبر هجومًا مسلحًا(٣).

---

(١) راجع الأراء بالتفصيل:

Terry D. Gill & P.A.L. Ducheine: Rescue of Nationals Abroad, in the handbook of the international law of military operation, supra note 4, at 217–219.

(٢) **د. حازم عتلم:** قانون النزاعات المسلحة الدولية– النطاق الزمني، دار النهضة العربية، القاهرة ، ٢٠٠٨، ص ١٠٠.

(3) **Terry D. Gill and Paul A. L. Ducheine:** Anticipatory Self-Defense in the Cyber Context, op.cit. p. 446.

٢. **أن يكون الهجوم المسلح على درجة كبيرة من الجسامة:** يشترط لقيام العدوان أن يكون الفعل من الجسامة بحيث يصلح أن يشكل عدوانا، ومنه يجب استبعاد الحوادث البسيطة كمشاكل الحدود، فعندما تطلق فرق حرس الحدود النار على نظيرتها للدولة المجاورة، هنا لا يجوز اللجوء للدفاع الشرعي لوجود الطرق السلمية لاقتضاء الدولة المعتدي عليها حقها، كحصولها على التعويض أو الاعتذار، ويمكن التحقق من توافر هذا الشرط بتعيين عدد وحجم القوات القائمة بالعدوان ومدى تسليحها وفعالية تلك الأسلحة([1]).

ولكن هل يعتبر الهجوم السيبراني هجوماً مسلحاً؟

على الرغم من أن الرأى الغالب في الفقه الدولي يستلزم في فعل العدوان أن يكون عدوانًا مسلحًا حتى يبرر قيام حق الدفاع الشرعي([2])، إلا أن هناك اتجاه فقهى يرى أن الهجمات الإلكترونية عبر الإنترنت يمكن أن تشكل هجومًا مسلحًا([3])، لا سيما في ضوء قدرتها على الإصابة أو القتل([4])، وذلك لان التطور العلمي ربما يجعل صورًا أكثر خطورة للدولة من مجرد استخدام القوة المسلحة، ومثال ذلك اختراق انظمة الحواسب الآلية المستخدمة فى المجال المالي والاقتصادي والاضرار بها بما يؤدي الى افلاس الدولة وتعرضها لمخاطر كبيرة أو قيام احدى الدول بتزييف عملة

(1) **Davis Brown:** A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict, HILJ, vol. 47, 2006, p. 181-183.

(2) **Clémentines Bories:** Appréhender la cyberguerre en droit international. Quelques réflexions et mises au point, RCRDFR, vol. 6, 2014, p. 3.

(3) **Daniel B. Silver:** Computer Network Attack as a Use of Force Under Article 2(4) of the United Nations charter, ILS, vol. 76 , 2002, p. 92–93.

(4) **Thomas Wingfield:** When is a Cyberattack an "Armed Attack?": Legal Thresholds for Distinguishing military activities in cyberspace, Cyber Conflict Studies Association, 2006, p. 6.

دولة أخرى بكميات كبيرة بما يهز مركزها المالي، ويؤدي الى انهيار الثقة الدولية فيها، وبالتالي يخلص هذا الرأي إلى إنه لا يصح في تقديره حصر شرط العدوان في العمل ذو الصبغة العسكرية وحده، بل ينبغي القول بأن أي فعل يهدد بالخطر الجسيم الحال دولة اخرى يكفي لإجازة الدفاع الشرعي، ولو لم يكن عملًا عسكريًا(١).

وبالتالي يمكننا القول: أن الهجوم السيبراني يعتبر هجومًا مسلحًا شريطة أن يكون موجهًا ضد البنية التحتية الحيوية للدولة، بحيث يكون للهجوم السيبراني القدرة علي شل قدرة الدولة على تنفيذ المهام الأساسية لها(٢)، وكذلك التأثير علي الاستقرار السياسي والاجتماعي لفترة طويلة من الزمن(٣). وقد تبنت بعض الدول هذا الموقف في استراتيجياتها الوطنية للأمن السيبراني، حيث اتفق العديد من خبراء القانون الدولي علي أن الهجوم السيبراني يمكن أن يرقى الى درجة من الخطورة، ويصل إلي مستوى الهجوم المسلح، مما يستوجب معه استخدام القوة(٤).

---

(١) د. محمد يونس الصائغ، حق الدفاع الشرعي وإباحة استخدام القوة في العلاقات الدولية، الرافدين للحقوق، مجلد (٩)، عدد (٣٤)، ٢٠٠٧، ص ١٨٦.

(2) **Ashley S. Deeks:** Toward a Normative Framework for Extraterritorial Self-Defense, VJIL, vol. 52, 2012, p. 483.

(3) **Terry D. Gill and Paul A. L. Ducheine:** Anticipatory Self-Defense in the Cyber Context, op.cit. p. 444.
«An armed attack could arguably include a cyber attack directed against a State's critical infrastructure, provided the cyber attack had the potential to severely cripple a State's ability to carry out and ensure the conducting of essential State functions or severely undermine its economic, political and social stability for a prolonged period of time».

(٤) تعترف الاستراتيجيات السيبرانية للعديد من الدول بإمكانية التعامل مع المسار الذي يؤدي إلي وقوع إصابات بشرية أو أضرار مادية كبيرة باعتباره هجومًا مسلحًا يبرر ممارسة الدفاع عن النفس، وهذا ما أقرته وزارة الدفاع الأمريكية في تقرير سياسة الفضاء الإلكتروني.
See, e.g., U.S. Department of Defense, Cyberspace Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act
=

ولعل الاستناد إلى معيار درجة الخطورة لتصنيف العمليات السيبرانية كهجوم مسلح، يُثير إشكالية تتعلق بكيفية تقدير أو تقييم هذه الخطورة، إلا أنه يمكن الاعتماد على تقييم مدى تأثير العملية على الدولة المضرورة، وعلى سبيل المثال: عند تعطيل أو إعاقة مؤسسات الدولة عن أداء وظائفها، وحدوث أضرار يتعذر تداركها، كتخريب الأجهزة التي تعتمد عليها منشآت طبية، مما ينتج عنه وفيات، فإن مثل هذه العمليات تكافئ استخدام القوة، ويكون للدول حق الرد عليها بموجب المادة (٥١) من الميثاق([1]).

وقد تبنت بعض الدول معيار درجة الخطورة، لتصنيف العمليات السيبرانية

=

for Fiscal Year 2011, Section 934, at 4, 9 (2011), available at http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/NDAASection934Report_Forwebpage

كذلك أصدر المجلس الاستشاري للشؤون الدولية واللجنة المعنية بقضايا القانون الدولي العام في هولندا تقريرًا مشتركًا لعام ٢٠١١ بعنوان الحرب الإلكترونية، حيث تم اعتبار كل الهجوم الإلكتروني الذي يؤثر تأثيرات مماثلة لتلك الخاصة بالهجوم الحركي التقليدي هجومًا مسلحًا ويؤدي بذاته إلي استخدام حق الدفاع عن النفس.

See Advisory council on internationl affaire & advisory committee on issues of public international law, cyber warfare 21 (2011), available at http://www.aiv advies.nl/ContentSuite/upload/aiv/doc/webversie AIV77CAVV22ENG

(1) **Tsagourlas N:** Cyber Attacks, Self-defence and the Problem of Artibution, J.Conflict & Sec L.vol.17, no 2 , 2012, pp.229-244.

وعلى الرغم من ذلك فقد اعترض جانب فقهى على أن الهجوم السيبرانى لا يرقى إلى مرتبة النزاع المسلح.

M. Condron: Getting it Right: Protecting American Critical Infrastructure in Cyberspace, Harvard Journal of International Law, vol. 16, 2007, p. 415.

حيث قرر:

«Cyber-attack alone will almost never constitute an armed attack for the purposes of Article 51».

كهجوم مسلح، ومن ثم ترقى للرد عليها وفقًا للمادة (٥١) من ميثاق الأمم المتحدة، ومنها الولايات المتحدة الأمريكية، التي أكدت فى تقرير قدمته إلى الأمم المتحدة عام ٢٠١١ "إنه فى بعض الظروف تشكل الأنشطة التخريبية فى الفضاء السيبراني هجومًا مسلحًا، ويكون من الملائم ألا يقتصر الرد عليها بشن هجوم إلكتروني مضاد فحسب، وإنما يتطلب هجومًا بالوسائل العسكرية التقليدية"(١).

ولكن التساؤل المثار حول الهجمات السيبرانية غير المدمرة، هل تعتبر هجومًا مسلحًا أم لا؟

اعتبرت اللجنة المعنية بدليل "تالين" أن أهم المعايير التي يجب الاستناد إليها في تحديد المستوى المطلوب لوصول الهجمات السيبرانية إلى مرتبة الهجوم المسلح، يتمثل في جسامة هذا التصرف أو حدته، ومدى تأثيره على الدولة المعتدى عليها، ولكن العقدة الأبرز في هذا الشرط كانت تتمثل في مستوى هذه الحدة، أو الحد المطلوب لتصنف الهجمات السيبرانية على أنها جسيمة، وترقي إلي الهجوم المسلح، وهو ما خلق فجوة في قرار محكمة العدل الدولية في حكمها بقضية نيكاراجوا، لذلك رأت اللجنة ضرورة وضع معيار دقيق يستند إليه لسد هذه الفجوة. في هذا السياق أقرت اللجنة أن جوهر المعيار يتمثل في الضرر المادي على الأفراد أو الممتلكات في الدولة المعتدى عليها بهجوم إلكتروني، حيث إن الهجمات السيبرانية ترقى إلى مستوى الهجوم المسلح الوارد في المادة (٥١) في الحالة التي تعكس فيها هذه العمليات ضررًا ماديًا على الأفراد أو على الممتلكات في الدولة المعتدى عليها(٢).

---

(1) United Nation, General Assembly, Development in the field of information and telecommunications in the context of international security, Report, Sixty-sixh session, 15 July 2011, (UN DOC.A/66/152).

(٢) حول هذا المعني راجع:

Michael N. Schmitt: the law of cyber warfare: quo vadis? Op.cit p. 282-

=

كذلك ذهب جانب فقهي أخر إلي أن طبيعة الأهداف المرجوة من الهجمات السيبرانية أمر حيوي وهام في تحديد ما إذا كانت هذه الهجمات ترقي إلي الهجوم المسلح من عدمه، لذلك يقرر هذا الجانب الفقهي أن أي هجوم علي البنية التحتية للدولة، سواء البنية المعلوماتية أو البنية التحتية للاتصالات اللاسلكية والسلكية والمؤسسات المالية، كذلك التحكم في بوابات السدود المائية وفتحها مما يتسبب في وفيات واسعة النطاق للمدنيين يعتبر هجوم مسلح مما يستوجب الدفاع الشرعي(١). بل أن هذا الاتجاه ذهب إلي أنه بالرغم من أن أعمال التجسس السيبراني مشروعة بموجب القانون الدولي(٢)، إلا أنه من الممكن أن ينتج عنها حق الدفاع الشرعي بشكل استباقي، حيث سمح هذا الاتجاه للضحايا باستنتاج نية العدائية التي تنذر بهجوم مسلح(٣).

وفي عقدنا الشخصي أن الهجوم السيبراني يعتبر هجومًا مسلحًا في حالة ما إذا

=

283.

(1) **Eric Talbot Jensen:** Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense, BYU law digital commons, Brigham young University Law School, SJIL,2002, v. 207, p. 226.

(2) **Ashley Deeks:** An International Legal Framework for Surveillance, VJ IL, vol. 55, 2015, p. 293 .

(٣) أكد Sheng Li على أن:

«The target-based framework ignores the gravity requirement prescribed by the ICJ. Even acts of cyber espionage against critical infrastructure systems, which are legal under international law, can trigger the right to self-defense, as the approach allows victims to infer hostile intent presaging an imminent armed attack, and to lawfully respond in anticipatory self-defense. This is dangerously overinclusive and risks catalyzing retaliation and escalation over minor offenses». **Sheng Li:** When does internet denial trigger the right of armed self-defence, Yjil, op.cit p. 187.

كان تحقيق الضرر الناتج عنه لا يمكن تحقيقه في السابق بدون استخدام القوة المسلحة، فعلي سبيل المثال، تدمير البنية التحتية للكهرباء في دولة ما عن طريق الهجوم السيبراني يعتبر هجومًا مسلحًا، لأنه في السابق قبل التقدم التكنولوجي كان يحتاج الأمر إلي تدخل مسلح عن طريق قصف محطات الكهرباء، فهنا تساوت نتائج الهجوم السيبراني مع الهجوم المسلح.

ثالثاً: أن يكون الهجوم السيبراني غير مشروع:

يشترط في الهجوم الإلكترونى أن يكون غير مشروع، ويترتب علي ذلك ثلاث نتائج:

النتيجة الأولي: لا محل للدفاع الشرعي إذا كان مصدر الخطر مشروعًا، بمعني أنه إذا كان مصدر الخطر بدوره استعمالًا لحق الدفاع الشرعي من قبل، فإنه يكون مباحًا، ولا يجوز الرد عليه تطبيقًا لقاعدة لا دفاع ضد دفاع.

النتيجة الثانية: تتمثل في جواز الاحتجاج بالدفاع الشرعي ضد كل خطر غير مشروع، ومقتضي ذلك أنه إذا قامت دولة ما باستخدام الهجوم السيبرانى استخدامًا غير مشروع، فإن للدولة التى استخدم الهجوم السيبرانى ضدها أن تمارس حقها فى الدفاع الشرعي لدرء الاعتداء الواقع عليها(١).

النتيجة الثالثة: إن الدفاع الشرعى للدول عن النفس لا صلة له إلا بالاستخدامات غير المشروعة للقوة، التي تنشأ خارج إقليم الدولة، والتي ترقى إلى مستوى الهجوم المسلح. وهذا يعني أن أي نوع آخر من النشاط ، سواء كان ينطوي على درجة من القوة أقل من هذا الحد، أو يشكل سلوكًا إجراميًا أو انتهاكًا لقواعد قانونية وطنية أو دولية أخرى لا تتعلق باستخدام القوة، يقع خارج نطاق تلك

(1) **Al chalabi ;H. Abdel Hadi**: la légitime défense en droit international, l'éditions universitaires d'Egypte , la Caire 1952, p 63.

الإجراءات التي قد تستخدمها الدول دفاعًا عن نفسها. لذلك لا تخضع الأنشطة الإجرامية السيبرانية والتجسس السيبراني للشركات، وأشكال أخرى مختلفة من الاختراق غير المصرح به وسرقة البيانات وتخريب أنظمة الكمبيوتر، سواء كانت عامة أو خاصة ، والتي لا تتناسب مع تعريف الهجوم المسلح([1]).

(1) **Jordan J. Paust:** Self-Defense Targetings of Non-State Actors and Permissibility of U.S. Use of Drones in Pakistan, JTL&P, vol. 19, 2010, p. 237.

المطلب الثاني
ضوابط حق الدفاع الشرعي ضد الهجمات السيبرانية

مما لا شك فيه أن استخدام القوة في العلاقات الدولية، وكذلك ظهور الحرب السيبرانية، والتي تبتعد كل البعد عن مفهوم الحرب بالمعني التقليدي، تشكل قلقًا كبيرًا للمجتمع الدولي، لخطورة هذه الهجمات التي فاقت في تدميرها الحروب التقليدية، وإزداد المر صعوبة مع عدم وجود موقف واضح من المجتمع الدولي تجاه هذه الهجمات، ومدي اعتبارها استخدام للقوة من عدمه(١).

وذكرنا سلفًا أن الهجوم السيبراني يعتبر استخدام للقوة في ظروف وأحوال معينة، وبالتالي تكون الدولة التي ينسب إليها الهجمات السيبرانية قد خالفت قاعدة حظر استخدام القوة في العلاقات الدولية، أما حق الدفاع عن النفس يكون في الحالات التي تستخدم فيها الدولة القوة ردًا على العمليات السيبرانية. ولكن استخدام القوة وحدها لا يمنح الحق فى الدفاع عن النفس إلا إذا كان الهجوم هجومًا مسلحًا. لذلك يوجد عدة ضوابط يجب توافرها حتى يكون استعمال الدفاع الشرعي ضد الهجوم السيبراني مشروعًا. وهي كالآتي:

أولًا: ضرورة أن يكون العدوان أو الهجوم السيبرانى حالًا ومباشراً:

ينبغي أن يكون العدوان أو الهجوم السيبرانى حالاً وقائمًا بالفعل، بمعنى أن يكون هذا الهجوم قد وقع فعلًا، ولكنه لم ينته بعد، وإنه مستمر وقائم بالفعل، وهذا هو مبرر إعطاء الدولة حق الدفاع الشرعي بعيدًا عن الموافقة المسبقة لمجلس الأمن. أما إذا كان العدوان لم يقع بعد، أو انه قد وقع وانتهي وتمت أثاره فلا مجال لإثارة حق الدفاع الشرعي، إذ يتعين هنا إبلاغ مجلس الأمن بما حدث، وعلى

(1) **Terry D. Gill and Paul A. L. Ducheine**: Anticipatory Self-Defense in the Cyber Context,op.cit. p. 445.

المجلس فى هذه الحالة اتخاذ الإجراءات والتدابير اللازمة.

ويقصد بأن يكون الهجوم السيبراني مباشرًا أن تقوم الدولة المعتدية بعدوانها بصفة مباشرة مستخدمة في ذلك قواتها المسلحة، ويقصد بالعدوان المباشر في هذا الصدد، استعمال الدولة لقواتها المسلحة بطريقة غير مشروعة ضد دولة أخري.

ومن ثم فبمجرد حيازة دولة لنوع من الأسلحة الذرية أو النووية، أو قيامها ببعض المناورات، هذا لا يعني حلول عدوان، ولا يكفي أن يكون الخطر وشيك فقط، بل وحتى الخطر المستقبلي لا يعد عدوانًا، بل حتى الاستعداد للهجوم كإعداد القوات المسلحة، لأن الدولة المهددة بوقوع اعتداء عليها لها أن تلجأ بشكوى إلى مجلس الأمن ليقوم باتخاذ التدابير اللازمة وفقا للمادة ٣٩ من الميثاق، وإذا حصل العدوان وتم، فلا يجوز اللجوء إلى الدفاع الشرعي لأنَّه يعد بمثابة انتقام وهو أمر غير مشروع في القانون الدولي العام([1]).

وقد وقع خلاف حول التهديد بالعدوان هل يعد مبررا لحق الدفاع الشرعي، حيث ذهب الفقه الدولي بشأن ذلك إلى اتجاهين:

الاتجاه الأول: يستدل أنصار هذا الاتجاه بالمادة (٥١) من الميثاق التي لم تحدد العدوان أوالتهديد به، وكذا تطور التكنولوجيا العسكرية، فيمكن أن يوجه صاروخ عابر للقارات فيضرب الدولة في خلال ساعات، فيقتضي الأمر التوسيع من مفهوم العدوان المسلح، ليشمل حالات الاعتداء غير المباشر والتهديد بالعدوان([2]).

الاتجاه الثاني: يرى أن الدفاع الشرعي لا يكون إلا ضد عدوان مباشر، ومما

(1) **V. Upeniece:** Conditions for the lawful exercise of the right of self-defence in international law, SHS Web of Conferences, 2018, pp.1-8.

(٢) د. محمد يونس الصائغ، حق الدفاع الشرعي وإباحة استخدام القوة في العلاقات الدولية، مرجع سابق، ص١٩٢.

يدعم هذا الرأي ما حدث في قضية خليج الخنازير في كوريا سنة ١٩٦١ ، حيث تأمر عدد من المتمردين الكوبيين للإطاحة بحكم الرئيس " فيدل كاسترو "، مستفيدين من دعم حكومة الولايات المتحدة الأمريكية التي تولت أمر إمدادهم بالسلاح وتدريبهم في قواعد في فلوردا وجواتيمالا، وعندما تمكنت الحكومة الكوبية من القضاء على هؤلاء المتمردين وقتلت معظمهم، قامت بتقديم شكوى الى الجمعية العامة للأمم المتحدة متهمة الولايات المتحدة الأمريكية بارتكاب عدوان غير مباشر ضدها، فاكتفت الجمعية العامة باتخاذ قرار دعت فيه أعضاء الأمم المتحدة إلى اتخاذ التدابير الكفيلة بإزالة التوتر بين الدولتين المتنازعتين(١).

وفى عقدنا أن الهجوم السيبراني ينبغى أن يكون قد وقع فعلاً لكنه لم ينته بعد، وأنه عدوان مستمر وقائم بالفعل وهذا هو مبرر إعطاء الدولة رخصة الدفاع الشرعي بعيدًا عن الموافقة المسبقة لمجلس الأمن. وأما إذا كان الهجوم السيبرانى لم يقع بعد، أو أنه قد وقع وانتهى وتمت آثاره فلا مجال لإثارة حق الدفاع الشرعي، إذ يتعين هنا إبلاغ مجلس الأمن بما حدث، ويتعين على مجلس الأمن في مثل هذه الحالة اتخاذ الإجراءات والتدابير المناسبة باعتباره صاحب الاختصاص الأصيل بحفظ

---

(١) ويؤكد البعض على ذلك بقوله أن:

«The reference to the imminence of an attack is more the attempt to predict the future than constitution of the certain fact, because in different situations there may be a certain degree of uncertainty about the perfection of received information about the adversary's plans, intentions, and motivations». **Muller K.P., Catillo J.J., Morgan F.E., Pegahi N., Rosen B.:** Striking first. Preemptive and Preventive Attack in the U.S. National Security Policy. RAND Corporation, 2006.

كما يؤكد البعض الآخر على أن:

«The armed attack of the adversary must be evident to the victim state, namely, the victim state can lawfully intercept the armed attack when it is in process of being started». **Dinstein Y. War:** Aggression and Self-Defence, Cambridge University Press, 2005, p. 187.

السلم والأمن الدوليين.

وعلى هذا الأساس فإنه لا يجوز الدفاع الشرعي في مواجهة الهجوم السيبرانى المحتمل حتى لو كان وشيك الوقوع، كما أنه لا ينشأ كذلك في مواجهة الخطر المستقبل حتى لو كان هذا الخطر المستقبل منطويًا على تهديد صريح أو ضمني باستخدام القوة المسلحة كأن توجه دولة إنذاراً إلى دولة أخرى لتنفيذ شروط معينة تحت طائلة استخدام القوة المسلحة في حالة الامتناع عن تنفيذ تلك الشروط، ففي مثل هذه الحالة يكون بإمكان الدولة التي وجه إليها التهديد التقدم بشكوى إلى مجلس الأمن لاتخاذ ما يراه كفيلاً في هذا الصدد وفقًا لنص المادة(٣٩) من ميثاق الأمم المتحدة.

ثانياً: الضرورة والفورية ضد الهجمات السيبرانية:

من الجدير بالذكر أن حالة الضرورة ظاهرة تؤثر علي جميع الأنظمة القانونية، من حيث الاهتمام بالمجهول المتوقع أو غير المتوقع، فحالة الضرورة لها القدرة علي تحديد الثغرات القانونية وتحديد الحاجة إلي التغيير في القانون الحالي، حيث انبثقت العديد من القواعد الموضوعية للقانون الدولي من هذه الظاهرة مثل حق الدفاع عن النفس([1]).

وتُعني حالة الضرورة اللازمة لمباشرة حق الدفاع الشرعي" هي أن تكون أعمال الدفاع هي الوسيلة الوحيدة لصد العدوان، وألا تكون هناك وسيلة أخري لصد العدوان أو الهجوم المسلح الواقع علي الدولة([2]).

---

(1) **Jens D. O., Larry M.:** Necessity in International Law, Oxford University Press, 2016, p. 39.

(٢) **د. أبو الخير احمد عطية:** نظرية الضربات العسكرية الاستباقية (الدفاع الوقائي) في ضوء قواعد القانون الدولي، دار النهضة القاهرة، ٢٠٠٧ ص ٥٨.

ويذهب الدكتور مصطفي فؤاد إلي الربط بين مفهوم القانون بصفة عامة، ومفهوم الضرورة. فالقانون في نظر سيادته هو وسيلة تستهدف المحافظة علي كيان الدولة، فإذا ما تعارضت هذه الوسيلة مع كيان الدولة فإنه يجب التضحية بالقانون في سبيل سلامة الدولة(١).

وبعبارة أخرى إنه يلزم وجود خطر جسيم يهدد الدولة المعتدي عليها لا يمكن تداركه، إلا من خلال انتهاك التزام دولي تجاه الدولة الأخرى، شريطة ألا يترتب عليه ضرر أكبر من الضرر الواقع علي الدولة المعتدي عليها، وألا تكون قد ساهمت بنفسها في إحداث حالة الضرورة، أو اتفقت علي عدم الاحتجاج بها، فالهجوم المسلح المستمر أو الوشيك شرط لا غني عنه، ولا يشترط شكل معين في الهجوم، فيمكن أن يكون هجومًا واحدًا واسع النطاق، أو سلسلة من الهجمات الصغيرة ذات الصلة من نفس المصدر والتي تشكل معًا هجومًا واحدًا، ويمكن أن يكون هجومًا وشيكًا بشكل واضح في المستقبل القريب(٢).

كذلك يشترط أن يكون الدفاع عن النفس فوريًا بمجرد وقوع هجوم مسلح وتحديد مصدر الهجوم(٣)، حيث يجب علي الدولة المدافعة أن تشرع في إجراءاتها الدفاعية بمجرد أن تكون قادرة علي الدفاع الشرعي، ولكن سرعة الرد والدفاع ليست قاعدة ثابتة، فقد تحتاج الدولة إلي استكشاف ما إذا كان هناك بدائل ممكنة ومجدية لاستخدام القوة، وقد تحتاج إلي نشر قوات إلي مصدر الهجوم تعبئة القوات، تلقي

---

(١) **د. مصطفي فؤاد:** فكرة الضرورة في القانون الدولي، منشأة المعارف، الإسكندرية، ١٩٨٧، ص٢٣.

(2) **Terry D. Gill and Paul A. L. Ducheine:** Anticipatory Self-Defense in the Cyber Context,op.cit, p 449.

(3) **Mateusz Piątkowski:** The Definition of the Armed Conflict in the Conditions of Cyber Warfare, PPSY, vol. 46, no. 1, 2017, p. 276.

المساعدات من أجل أن تكون قادرة علي الرد، وما يهمنا الفرض الأخير وهو عدم قدرة الدولة على تحديد مصدر العدوان أو المتدخل، لأنه وثيق الصلة بالهجوم السيبراني([1]).

ثالثاً: ضرورة تناسب الدفاع الشرعي ضد الهجمات السيبرانية:

يقصد بالتناسب في سياق الدفاع الشرعي عن النفس " ألا تتجاوز تدابير الدفاع الشرعي تلك المطلوبة لصد الهجوم السيبرانى([2])، وأن تكون متناسبة مع حجم وأهداف الهجوم الشامل"([3])، بمعنى أن يكون استخدام الدفاع الشرعي عن النفس بهدف السعي إلي إيقاف الهجوم والحد من استخدام القوة المسلحة المعادية لاستعادة الوضع إلي ما كان قبل الهجوم. فعلي سبيل المثال: أن تقوم دولة باستخدام القوة للدفاع عن نفسها ضد دولة أخري استخدمت الهجوم السيبراني ضدها، ثم تتحايل وتقوم باحتلال أراضي هذه الدولة مستندة إلي الدفاع الشرعي، فهنا قد تجاوز الدفاع الهدف المرجو منه([4]).

ونشير إلي أن التناسب في الدفاع الشرعي لا يتطلب معادلة رياضية معقدة بالنسبة للهجوم السيبراني، فإذا ارتقي الهجوم السيبراني إلى مرتبة الهجوم المسلح،

---

(1) **Terry D. Gill and Paul A. L. Ducheine**: Anticipatory Self-Defense in the Cyber Context,op.cit, p 449.

(2) **Stephen Moore:** Cyber Attacks and the Beginnings of an International Cyber Treaty, Op, Cit, p. 240.

(3) **Terry D. Gill and Paul A. L. Ducheine**: Anticipatory Self-Defense in the Cyber Context,op.cit, p 450.

حيث أكد على أن:

«Proportionality in the context of self-defense refers to the requirement that measures of self-defense must not exceed those required under the circum-stances to repel the attack and prevent further attacks from the same source in the proximate future».

(4) **David E. Graham:** Cyber Threats and the Law of War, Op, Cit, p. 93.

فقد يكون الرد هو استخدام أسلحة إلكترونية أو قوة مسلحة أو مزيج من الأثنين لوقف هذا الهجوم، شريطة ألا يتجاوز الرد المطلوب لصد الهجوم. كذلك فإن التناسب لا يسمح باتخاذ تدابير من شأنها إطالة أمد الصراع أو تفاقمه دون داع(١).

ونحن نرى أنه إذا كان فعل الدفاع الشرعى لا يتناسب مع جسامة وحجم الهجوم السيبراني المسلح، أى يتجاوز فعل الهجوم السيبرانى المسلح اعتبر ذلك تجاوزًا فى استعماله، واعتبر عدوانًا وليس دفاعًا. كما نؤكد على أن معيار التناسب في القوانين الجنائية الداخلية هو معيار موضوعي، قوامه مسلك الشخص العادي إذا وضع في نفس الظروف المحيطة بالمدافع، ويطبق هذا المعيار في المجال الدولي، حيث يقاس مسلك الدولة عند الدفاع بمسلك دولة معتادة، وضعت في نفس ظروف الدولة المعتدى عليها.

ولقد اثير التساؤل هل يجوز الدفاع الشرعى الاستباقى ضد الهجمات السيبرانية؟
الحقيقة أن جانب فقهى يجيز ذلك بقوله: " تكون الإجراءات التي يتم اتخاذها للدفاع عن النفس استباقيًا، قانونية، عندما تكون "ضرورة هذا الدفاع عن النفس فورية، وحالة، ولا تترك أى خيار من الوسائل، ولا لحظة للتداول"(٢).

ومن جانبنا نؤكد على أن الضرورة والتناسب يجب أن يتوافرا جنبًا إلى جنب فى حالة الدفاع الشرعى الاستباقي عن النفس ضد الهجمات السيبرانية. والتناسب في الدفاع لا يعني التماثل التام بين فعل الهجوم السيبرانى المسلح وفعل الدفاع، فإختلاف وسيلة الدفاع عن وسيلة الإعتداء لا يعني توافر هذا الشرط.

---

(1) **Stephen Moore:** Cyber Attacks and the Beginnings of an International Cyber Treaty, Op, Cit, p. 240.

(2) **Eric Jensen:** Computer Attacks on Critical National Infrastructure: AUse of Force Invoking the Right of Self-Defense, SJIL, vol. 38, 2002, p. 207.

رابعاً: ينبغي أن يكون الدفاع الشرعى الوسيلة الوحيدة لصد الهجمات السيبرانية:

بمعنى أنه إذا وجدت وسيلة أخرى لصد الهجمات السيبرانية غير استخدام القوة المسلحة كان على الدولة المستهدفة بالهجوم عندئذ أن تتبع تلك الوسيلة بحيث لا ينشأ لها حق استخدام القوة المسلحة بحجة الدفاع الشرعي. ولكن لا بد من الإشارة في هذا الصدد إلى أن الحديث عن وجوب أن يكون الدفاع هو الوسيلة الوحيدة لرد الهجوم السيبراني، يُعني أنه الوسيلة الوحيدة الممكنة بالفعل، والمشروعة والتي تكفل الحفاظ على حقوق الدولة وسلامتها واستقلالها(١).

فإذا وجدت وسائل أخرى لا تتمتع بتلك الصفات فإن هذا لا يحرم الدولة المستهدفة بالعدوان من استخدام حقها في الدفاع الشرعي، ومثال ذلك: أن تبادر دولة إلى شن العدوان على دولة أخرى بهدف إجبارها على الرضوخ لمطالب الدولة المعتدية، كأن تطالبها بالتنازل عن منطقة حدودية متنازع على ملكيتها فيما بينهما، أو تطلب منها تسليم أحد رعاياها دون اتباع الأصول القانونية، ففي مثل هذه الحالة لا يمكن أن يُسلب من الدولة المستهدفة بالعدوان حقها في الدفاع الشرعي بحجة أن هناك وسيلة أخرى لرد العدوان الواقع عليها، وذلك إذا ما بادرت إلى القبول بمطالب الدولة المعتدية. فمثل هذا الرضوخ قد يمنع بالفعل العدوان ويوقفه إلا أنه لا يمكن اعتباره أحدى الوسائل التي من شأن توافرها أن يسلب الدولة حقها في الدفاع

---

(1) **CF. Martin:** Introduction aux relations internationals, private, Toulouse, 1982, p. 167.

حيث أكد على أن:

«Coutumierement on considére que pour être légitime la defense doit repondre à trios conditions: elle doit être presenter et urgente, ne laissant ni le choix des moyen, ni le choix des moyen, ni le temp de deliberer, en second lieu elle ne doit la proportionner à l'attaque, enfin elle doit intervener en dernier resort alors qu'attaque, qu'aucun autre moyen d'obtenir satifaction n'aura être efficace».

الشرعي، لأن الوسيلة التي ينبغي الاعتداد بها كسبب سالب لحق الدولة في الدفاع الشرعي يجب أن تكون وسيلة ممكنة بالفعل ومشروعة وتحافظ أيضًا على حقوق الدولة وسلامتها واستقلالها وكرامتها، وإلا فإن الحق في الدفاع الشرعي يظل قائمًا ومتاحًا([1]).

خامساً: خضوع أعمال الدفاع الشرعي لرقابة مجلس الأمن:

ينبغي أن يتسم فعل الدفاع الشرعى بالصفة المؤقتة لحين تدخل مجلس الأمن، إذ ينبغي أن يكون فعل الدفاع مؤقتًا، وذلك عند غياب مجلس الأمن وإلى أن يتخذ هذا المجلس التدابير المناسبة لمواجهة العدوان، وهذا واضح في نص المادة (٥١) من الميثاق التي أشارت إلى أن الدولة تمارس حقها في الدفاع الشرعي (... إلى أن يتخذ مجلس الأمن التدابير اللازمة لحفظ السلم والأمن الدولي).

وتهدف هذه الرقابة إلى وضع المجلس أمام مسؤولياته بالعمل أولاً على عدم تجريد مبدأ حظر استخدام القوة من مضمونه، وعن طريق مراجعة الوقائع وبحثها يمكن للمجلس أن يحدد مدى التناسب بين أعمال الدفاع وأعمال الاعتداء، وأن يقرر بناء على ذلك وقف ممارسة أعمال الدفاع واتخاذ التدابير الضرورية والملائمة لإعادة السلم والأمن الدوليين إلى نصابهما([2]).

(1) **Roberto Ago:** Le Fait international illicite de l'Etat, sources de respensabilité internationale, ACDI, 1961/II, P. 98.

(2) **Moore J. N:** The secret wor in contral America and Futur or the world order, AJIL, 1986, n. 1, vol. 80, P.89.

المبحث الثالث
الجهود الدولية إزاء حق الدفاع الشرعى ضد الهجمات السيبرانية

تجدر الإشارة بداية الى أن الهجوم السيبراني يُعد أحد أهم القضايا التي تحتل حيزًا مهما في الدراسات والنقاشات المثارة على الساحة الدولية خلال الفترة الأخيرة، كما أنه من أخطر أنواع الجرائم التي ترتكب عبر شبكة الإنترنت، وتتّضح خطورة هذا الهجوم من خلال النظر إلى حجم التهديدات التي يفرضها على الأمن القومي للدول([1]).

وقد أدى ظهور الجرائم السيبرانية – كنمط جديد من أنماط الجريمة وما تتميز به هذه الجرائم من خاصية عابرة للحدود الإقليمية للدول– إلى توجه الدول والمنظمات الدولية ببذل وتكثيف الجهود الرامية لمواجهة ومجابهة الخطورة التي يشكلها هذا الإجرام المستحدث([2])، لا سيما وأنه من الجرائم العابرة للحدود، وفيما يلي سوف نستعرض أهم الجهود الدولية، سواء تمثل ذلك فى جهود منظمة الأمم المتحدة كمنظمة عالمية أو الجهود الفقهية.

وبناءً عليه سوف نقسم هذا المبحث الى مطلبين على النحو الآتي:

المطلب الأول: الفقه الدولى وحق الدفاع الشرعى ضد الهجمات السيبرانية.

المطلب الثانى: منظمة الأمم المتحدة وحق الدفاع الشرعى ضد الهجمات السيبرانية.

---

(1) **Blinding weapons:** Reports of the meetings of experts convened by the international committee of the red cross on battlefield laser weapons, 1989– 1991, ICRC, 1993, P 78.

(2) **Heather Harrison Dinniss:** The status and use of computer network attacks in international law, Phd thesis, London school of a economics and Political science, 2008, P. 33.

المطلب الأول
الفقه الدولى وحق الدفاع الشرعى
ضد الهجمات السيبرانية

من الجلي بالبيان أنه ترتب على غياب توجيه رسمي من الأمم المتحدة، ظهور اجتهادات فقهية عديدة لمعالجة مسألة الهجمات السيبرانية(١)، والاستجابة الدولية الأهم والأبرز لمعالجة هذه المسألة جاءت فيما يسمى دليل «تالين» للقانون الدولي المنطبق على الحرب الإلكترونية، والذي قام بإعداده مجموعة من أبرز فقهاء القانون الدولي؛ هذا إلى جانب المبادئ الواردة فى إعلان « ريتشي » بشأن مبادئ الاستقرار السيبراني والسلام السيبراني والذي أعده فريق الرصد الدائم المعني بأمن المعلومات التابع للاتحاد العالمي للعلماء، وعليه نتناول اولاً دليل تالين، ثم نوضح ثانيًا إعلان ريتشي بشأن مبادئ الاستقرار السيبراني والسلام السيبراني، وذلك تباعًا على النحو التالي:

أولاً: دليل تالين (Tallinn) والهجوم السيبراني:

يمثل دليل تالين محاولة من قبل مجموعة مشكلة من تسعة عشر خبيرًا دوليًا لعمل وثيقة غير ملزمة لتطبيق القانون الدولى على الهجمات السيبرانية. حيث اعتمد الخبراء المعنيون قواعد دليل تالين من خلال استخدام مبدأ الإجماع. وأكدوا على إنه يحمل قوة مقنعة كافية لتبرير استخدامه.

ويقرر دليل " تالين" – من حيث المبدأ – أن أحكام ميثاق الأمم المتحدة قابلة للتطبيق على الهجمات والحروب السيبرانية، كما يناشد الدول ألا تعامل الفضاء السيبراني على أنه فراغ قانوني لا تنطبق عليه المبادئ القانونية المطبقة في

(1) **Scott J. Shackelford:** From nuclear war to net war: Analogizing cyber attacks in international law, BJIL, vol. 27, no. 1, 2009, p.217.

الفضاءات المادية، وينبغي على المجتمع الدولي الاستجابة والاستعداد للهجمات السيبرانية، والالتزام بمتطلبات القانون الدولي([1]).

وقد قام خبراء تالين بتعريف العمليات السيبرانية على أنها: « تلك التي تتضمن استخدام القوة أو التهديد بها عندما يكون نطاقها وأثرها قابل للمقارنة مع العمليات غير السيبرانية التي تصل لمستوى استخدام القوة([2]).

وعلى الرغم من القصور الذى شاب هذا التعريف، إلا أنه لا يخلو من بعض المزايا والتى منها: أن قواعد استخدام القوة في المجال السيبراني لا تختلف عن تلك الموجودة في أي مجال آخر.

ومن زاوية أخرى يحدد الدليل الإجراءات التي قد تتخذها الدول للرد على الهجمات السيبرانية، حيث تنص 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 فى الدفاع عن

---

(١) تجدر الإشارة الى أنه قد تبنى NATO إعداد دليل «تالين»، بشأن القانون الدولي المطبق على الحرب السيبرانية، بإصداريه لعامي ٢٠١٣، ٢٠١٧، وهو توجيه غير ملزم بشأن القواعد الدولية التي تحكم العمليات السيبرانية، حيث استضاف المركز التعاوني للدفاع السيبراني، التابع للحلف بمقره فى مدينة «تالين» عاصمة «إستونيا»، وصياغة هذا الدليل فى الفترة من عام ٢٠٠٩ وحتى ٢٠١٧، بجهود فريق خبراء قانونيين دوليين برئاسة البروفيسور Michael N. Schmit.

راجع حول ذلك بالتفصيل:

Michael N. S: Tallinn Manual on the international law applicable to cyber warfare, Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence General, Cambridge University Press,2013.

(2) **Michael N. S:** Tallinn Manual on the international law applicable to cyber warfare,op. Cit.p.107.

النفس"(١).

ووفقًا لدليل "تالين" فإن العمليات السيبرانية تعتبر استخدامًا للقوّة، عندما يكون مستواها وتأثيرها متقاربين مع العمليات غير السيبرانية، وذلك اعتمادًا على معيار النطاق والأثر فى تحديد الدرجة التي يجب أن يصل إليها الهجوم السيبراني، كاستخدام للقوة أو هجوم مسلح، ومن ثم يمكن اعتبار الهجوم السيبراني هجومًا مسلحًا إذا أحدث ضررًا، أو يصل إلى درجة الشدة، والمقصود بذلك أن يحدث أضرارًا مادية جسيمة.

واستند خبراء تالين فى اعتماد هذا الاختبار على رأي محكمة العدل الدولية فى قضية « نيكاراجوا »، على أساس أنه من الأنسب لتحديد الدرجة المناسبة للأعمال التي تصل إلى حد استخدام القوة والهجمات المسلحة، وبالقياس على الهجمات السيبرانية، اتفق خبراء دليل تالين على أن قيام دولة بتزويد قوات أو أفراد بأجهزة وتدريبهم لشن هجمات سيبرانية ضد دولة أخرى، يعد ذلك استخدامًا غير مشروع للقوة(٢).

وقد طُبق هذا المعنى بصورة واضحة فى عملية استخدام الهجمات السيبرانية فى الحرب بين جورجيا وروسيا فى أغسطس ٢٠٠٨ ، وفي الهجمة السيبرانية

---

(١) حيث اكدت القاعة ١٣ من الدليل على ذلك بقولها أن:

«Self-defence against armed attack A State that is the target of a cyber operation that rises to the level of an armed attack may exercise its inherent right of self-defence. Whether a cyber operation constitutes an armed attack depends on its scale and effects».

(2) **Michael N. S**: Peacetime Cyber Responses and wartime Cyber Operations inder International Law: An Analytical Vade Mecum", HNSJ, vol. 8, 2017, p.245.

العالمية – فيروس الفدية(١)– التي طالت أكثر من ٦٠ دولة على مستوى العالم فى ٢٧ يونيو ٢٠١٧ – منهم بريطانيا ومصر وروسيا وأوكرانيا وألمانيا والمكسيك وإسبانيا، إلى ظهور الفضاء السيبراني على الساحة الدولية على نحو مباشر وعلني فى الصراع الدولي، وكأداة ووسيلة فى الصراع المسلح، لذلك ثار الجدل حول مدى اعتبار تلك الهجمات عملً من أعمال الحرب، وتقارب الهجمات السيبرانية الهجمات التقليدية فى النتائج مع اختلاف الوسائل وإستراتيجيات التنفيذ، مما أدى إلى خلق حرب مفتوحة يمكن أن تكون هناك صعوبة فى تحديد أطرافها، لذا تسعى الدول إلى تطوير أساليب جديدة فى الحروب المستقبلية(٢).

ولذا وضعت اللجنة مجموعة من الشروط التي يجب أن تتسم بها الهجمات السيبرانية؛ حتى ترقى إلى درجة الهجوم المسلح، وبالتالي تعطي الدولة المعتدى عليها حق الدفاع الشرعي وتفعيل المادة (٥١) من الميثاق ومنها، الحدة أو الجسامة، حيث اعتبرت اللجنة أن أهم المعايير التي يجب الاستناد إليها في تحديد المستوى المطلوب لوصول العمليات الإلكترونية إلى مرتبة الهجوم المسلح يتمثل في جسامة هذا التصرف أو حدته، ومدى تأثيره على الدولة المعتدى عليها، ولكن الصعوبة الأبرز في هذا الشرط كانت – مرة أخرى– تتمثل في مستوى هذه الحدة، أو الحد المطلوب لتصنف العملية الإلكترونية على أنها جسيمة، وهو ما خلق فجوة فى قرار محكمة العدل الدولية في حكمها بقضية نيكاراجوا، لذلك رأت اللجنة ضرورة وضع معيار دقيق يستند إليه لسد هذه

---

(١) **وفيروس الفدية** هو نوع خبيث من البرامج يقفل أجهزة الحاسوب الشخصى أو اللوحى أو الهواتف الذكية، أو يضع تشفيرًا على ملفاتك ثم يطلب منك فدية مقابل اعادتها إليك في حالة سليمة.

(٢) **د. هاني محمد خليل العزازي**: النظام القانوني الدولي لمُكافحة المَخاطر السيبرانية، مرجع سابق، ص٥٢٠.

الفجوة(١).

ولذا فقد أقرت اللجنة في هذا السياق أن جوهر المعيار يتمثل فى الضرر المادي على الأفراد والممتلكات في الدولة المعتدى عليها بهجوم إلكتروني، حيث إن العمليات الإلكترونية ترقى إلى مستوى الهجوم المسلح الوارد في المادة (٥١) في الحالة التي تعكس فيها هذه العمليات ضررا ماديًا حال على الأفراد أو على الممتلكات في الدولة المعتدى عليها، وفي سبيل ذلك قامت اللجنة بالمقاربة بين أثر الهجمات العسكرية التقليدية والهجمات الإلكترونية استنادًا إلى قياس نتائج الأخيرة، وفيما إذا كانت منتجة لأضرار مماثلة للهجمات العسكرية التقليدية أم لا(٢).

كما أقرت اللجنة – أيضًا – معيار الضرر الحال، ومعيار الهجوم المباشر، حيث يتحقق الأول في حالتين: الأولى: عندما يقع الضرر فعلًا على الدولة المعتدى عليها، والحالة الثانية: وهي الأكثر تعقيدًا- عندما لا يكون الضرر قد وقع فعلا وإنما هو ضرر وشيك الوقوع، وهو أيضًا – بحسب اللجنة- ينشيئ الحق فى الدفاع عن النفس، وفي هذه الحالة الأخيرة يبرز السؤال حول المعنى الدقيق لمصطلح الحلول، والفرق- إن وجد- بين الضرر الحال والضرر المحتمل فى سياق العمليات الإلكترونية(٣).

وفي هذا المضمار استندت اللجنة إلى معيارين: معيار الفترة الزمنية **الكافية التي يمكن أن تستغلها الدولة المعتدى عليها لتجنب وقوع الضرر من خلال تواصلها بالدولة منشأت الاعتداء للتراجع عن هذا التصرف، وبعبارة أخرى فإن**

(1) **Charles C. P:** This Means War! (Maybe?) — Clarifying Casus Belli in Cyberspace, ORIL , vol. 15, 2013, P. 423.

(٢) **د. رزق أحمد سمودي:** حق الدفاع عن النفس نتيجة الهجمات الإلكترونية في ضوء قواعد القانون الدولي العام، ٢٠١٨، ص٣٥١.

(3) **Charles C. P:** This Means War! (Maybe?)—Clarifying Casus Belli in Cyberspace, Op, Cit, P. 424.

الخطر الحال هو الذي سوف يقع لا محالة دون أي قدرة للدولة المعتدى درءه(١).

أما المعيار الثاني: **والمتمثل في شرط الهجوم المباشر الوارد في دليل "تالين"، فإن هذا الإطار الأخير لا يمكن أن يرتقي بالتصرف إلى مرتبة الهجوم المسلح استنادا إلى عدم القدرة على تحديد علاقة السببية بين الفعل والضرر، ولذلك يجب عدم الخلط بين الحال والمباشرة كشرطين متميزين جاء بهما دليل "تالين"، حيث إن الأول يتمثل في خروج الضرر إلى حيز الوجود، والثاني يرتبط بالعلاقة بين التصرف والضرر(٢).**

ونحن نرى – وكما ذهب البعض(٣) وبحق – أن هذا الدليل ليس صكا دوليًا رسميًا أو مُلزِمًا، أو يمثل وجهة نظر الدول التي شارك خبراء من جنسيتها فى وضع الدليل، وإنما هو رؤية الخبراء المستقلين الذين صاغوه بصفاتهم الشخصية. ومع ذلك فإن أهميته كبيرة، كوثيقة رائدة فى مجال العمليات السيبرانية، وخطوة مهمَّة لتنظيم الفضاء السيبراني.

ثانيًا: إعلان "Ritchie's" بشأن مبادئ الاستقرار السيبراني والسلام السيبراني:

أُعد إعلان "ريتشي" بشأن مبادئ الاستقرار السيبراني والسلام السيبراني

---

(1) **See, Daniel Bethlehem:** Principles Relevent to the Scope of Self-Defence Against Imminent or Actual Armed Attack by Nonstate Actors, AJIL, vol. 106, 2012, p. 769.

(٢) **د. رزق أحمد سمودي:** حق الدفاع عن النفس نتيجة الهجمات الإلكترونية في ضوء قواعد القانون الدولي العام ، مرجع سابق، ص٣٥٤.

(٣) **د. محمد عادل محمد عسكر:** وضع العمليات السيبرانية في القانون الدولي مع التطبيق على ممارسة التجسس وقت السلم، دراسة على ضوء دليل "تالين" بشأن القانون الدولي المطبّق على العمليات السيبرانية، ٢٠١٣ ، ص٧٠.

بواسطة فريق الرصد الدائم، المعني بأمن المعلومات التابع للاتحاد العالمي للعلماء WFS، حيث اعتمدته الجلسة العامة للاتحاد العالمي للعلماء في الدورة الثانية والأربعين للحلقات الدراسية الدولية بشأن الطوارئ العالمية، في اريتشي (صقلية)، في ٢٠ أغسطس ٢٠٠٩. وكان من أبرز التقارير لهذا الاتحاد التقرير المعنون بـ " نحو نظام عالمي للفضاء السيبراني "إدارة التهديدات من الجريمة السيبرانية الى الحرب السيبرانية" والذي يعد إحدى الوثائق الرئيسية التي قدمها المجتمع المدني ، الى القمة العالمية لمجتمع المعلومات التي عقدتها الأمم المتحدة في جنيف في ٢٠٠٣(١).

وقد نشر فريق الرصد ورقات عديدة بشأن الأمن السيبراني والحرب السيبرانية، ويتناول بانتظام قضايا أمن المعلومات باعتبارها موضوعًا من موضوعات الطوارئ الحرجة أثناء الدورات العامة للاتحاد العالمي للعلماء التي تنعقد فى شهر أغسطس من كل عام فى إيريتشي. ويُبين هذا الإعلان أن تحقيق الاستقرار السيبراني وتحقيق السلام السيبراني أمران متداخلان تداخلًا وثيقًا، ويتسم الإعلان بالإيجاز ويركز على العناصر الأساسية للسلام السيبراني، وهي كالتالي(٢):

١. يجب على جميع الحكومات الاعتراف بأن القانون الدولي يضمن للأفراد التدفق الحر للمعلومات والأفكار؛ وتنطبق هذه الضمانات أيضًا على الفضاء السيبراني، وينبغي عدم فرض القيود إلا عند الاقتضاء، على أن تخضع لعملية مراجعة قانونية.

---

(١) **د. أميرة عبد الجواد:** المخاطر السيبرانية وسبل مواجهتها في القانون الولي العام،ملة الشريعة والقانون، ع ٣٥، ٢٠٢٠، ص ٥١٢.

(٢) **د. هاني محمد خليل العزازي:** النظام القانوني الدولي لمُكافحة المَخاطر السيبرانية، مرجع سابق، ص٥٢١.٥٢٢.

٢. ينبغي لجميع البلدان العمل معًا لوضع مدونة مشتركة للسلوك السيبراني وإطار قانوني عالمي منسق، بما فى ذلك أحكام إجرائية تتعلق بالمساعدة فى التحقيق والتعاون بما يكفل احترام الخصوصية وحقوق الإنسان، وينبغي لجميع الحكومات ومزودي الخدمات والمستعملين دعم الجهود المبذولة فى سبيل إنفاذ القانون الدولي ضد مرتكبي الجرائم السيبرانية.

٣. ينبغي لجميع المستعمِلين ومزِودي الخدمة والحكومات العمل معًا لضمان ألا يستخدم الفضاء السيبراني بأي شكل من شأنه أن يفضي إلى استغلال المستعمِلين، لا سيما الشباب والمستضعفين منهم، من خلال العنف أو الإذلال.

٤. ينبغي للحكومات والمنظَّمات والقطاع الخاص بما فى ذلك الأفراد، تنفيذ برامج شاملة للأمن وتحديثها بناءً على أفضل الممارسات والمعايير المقبولة دوليًا، واستعمال تكنولوجيات حماية الخصوصية والأمن.

٥. ينبغي لمطِّوري البرمجيات والمعدَّات السعي إلى تطوير تكنولوجيات آمنة تُعزز القُدرة على التصِدي وتقاوم نقاط الضعف.

٦. ينبغي للحكومات أن تُشارك بفعالية فى جهود الأمم المتحدة الرامية إلى النهوض بالأمن السيبراني والسلام السيبراني فى العالم، وأن تتفادى استعمال الفضاء السيبراني من أجل النزاعات المسلحة وبالتالى استعمال حق الدفاع الشرعى.

المطلب الثانى
منظمة الأمم المتحدة وحق الدفاع الشرعى
ضد الهجمات السيبرانية

فى سبيل تعزيز العمل المشترك بين الدول؛ وذلك للحد من انتشار الجرائم المعلوماتية، ومواجهة المخاطر السيبرانية، قد عقدت فى سبيل ذلك العديد من المؤتمرات بداية من المؤتمر السابع الذي عقد فى ميلانو ١٩٨٥ حتى المؤتمر الثاني عشر فى ٢٠١٠، بالإضافة إلى المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات والذى عقد تحت إشراف الأمم المتحدة فى عام ١٩٩٤ ، ونتج عنه عدة توصيات ذات صلة بجرائم المعلومات، بعضها تناول الأفعال التي تقع تحت طائلة الإجرام المعلوماتي، والبعض الآخر يتمثل فى الإجراءات الواجب اتباعها لتطبيق القواعد الموضوعية.

وهكذا أصدرت منظمة الأمم المتحدة عدة قرارات وتوصيات بشأن العمليات السيبرانية، ونبين ذلك على النحو التالى:

أولا: قرارات الجمعية العامة للأمم المتحدة بشأن الهجوم السيبراني:

أصدرت الجمعية العامة للأمم المتحدة مجموعة من القرارات بشأن جرائم الهجوم السيبراني منها على سبيل المثال:

١. القرار رقم ٦٣/٥٥ الصادر في ٤ ديسمبر ٢٠٠٠ م، بشأن مكافحة سوء استخدام تكنولوجيا المعلومات لأغراض إجرامية، وقد أوصى بأن" تضمن الدول فى قوانينها وممارساتها عدم توفير ملاذات آمنة لكل من يسيء استخدام تكنولوجيا المعلومات لأغراض إجرامية، وضمان حماية سرية المعلومات وسلامة

أنظمة الحاسوب، ضد أي اعتداء غير مشروع، مع تقرير عقوبة على ذلك الفعل"([1]).

٢. القرار رقم ٥٦ / ١٢١ في ١٩ ديسمبر ٢٠٠١، بشأن مكافحة سوء استخدام تكنولوجيا المعلومات لأغراض إجرامية، وقد دعا القرار الدول الأعضاء عند وضع التشريعات الوطنية لمكافحة إساءة استعمال تكنولوجيا المعلومات، أن تأخذ بعين الاعتبار عمل لجنة منع الجريمة والعدالة الجنائية([2]).

٣. القرار رقم ٥٧ / ٢٣٩ عام ٢٠٠٢، بشأن إرساء ثقافة عالمية للأمن السيبراني، حيث اعتمدت فيه قرارًا بشأن الأمن السيبراني والذي سلمت فيه بضرورة دعم الجهود الوطنية بتبادل المعلومات والتعاون فى هذا المجال على الصعد الوطنية والإقليمية والدولية؛ كي يتسنى التصدي الفعال لما تتسِم به هذه التهديدات السيبرانية بصفة متزايدة، من طابع عابر للحدود الوطنية. ويشهد هذا القرار على التزام العالم بإنشاء ثقافة عالمية للأمن السيبراني، وأهم ما فى القرار أنَه يؤكِد أن الأمن السيبراني للهياكل الأساسية الحيوية للمعلومات مسئولية مُلقاة على

---

(1) Resolution adopted by the General Assembly [on the report of the Third Committee (A/55/593)], General Assembly, United Nations, Fifty-fifth session Agenda item 105, 22 January 2001, p. 2.

حيث ذهبت الجمعية العامة في هذا الصدد الى القول بأن:

«States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies».

(2) Resolution adopted by the General Assembly [on the report of the Third Committee (A/56/574)], General Assembly, United Nations, Fifty-sixth session Agenda item 110, 23 January 2002, p.2.

حيث ذهبت الجمعية العامة في هذا الصدد الى القول بأن:

«Invites Member States, when developing national law, policy and practice to combat the criminal misuse of information technologies, to take into account, as appropriate, the work and achievements of the Commission on Crime Prevention and Criminal Justice and of other international and regional organizations».

عاتق الحكومات، ومجال يجب عليها أن تحمل فيه لواء الصدارة وطنيًا، بالتنسيق مع أصحاب المصلحة ذوي الشأن([1]).

٤. القرار رقم ١٧٧ / ٦٠ عام ٢٠٠٥، بشأن تشجيع التعاون الدولي لمكافحة الجرائم الإلكترونية، وتقديم المساعدة للدول الأعضاء فى هذا المجال([2]).

٥. القرار رقم ٢١١ / ٦٤ عام ٢٠١٠، الذي يدعو الدول إلى تحديث قوانينها فى مجال الجرائم الإلكترونية، والخصوصية، والبيانات الشخصية، والتجارة والتوقيع الإلكترونيين، وكذلك اعتماد اتفاقيات إقليمية بهذا الشأن([3]).

٦. القرار رقم ٦٥ / ٤١ والذي صادقت الجمعية العامة للأمم المتحدة عليه فى يناير ٢٠١١ والذي دعا الى تقرير فريق الخبراء الحكوميين فى مجال المعلومات والاتصالات السلكية واللاسلكية فى سياق الأمن الدولي. وتضمنت استنتاجات فريق الخبراء من بينها ما ذكرته من أنَ هناك دول تستحدث تكنولوجيا المعلومات والاتصال كوسائل للحرب والاستخبارات، ولفتت اللجنة الدولية فى هذا الصدد انتباه الدول إلى عواقب الحرب السيبرانية، وهي مجموعة من الهجمات على شبكة الحواسيب خلال حالات النزاع المسلَّح، وقد تشمل هذه العواقب سيناريوهات كارثية مثل: التشويش على نُظم مُراقبة الملاحة الجوية، والتسبب

---

(1) Resolution adopted by the General Assembly [on the report of the e Second Committee (A/57/529/Add.3)], General Assembly, United Nations, Fifty-seventh session Agenda item 84 (c) , 31 January 2003, p.2-3.

(2) Resolution adopted by the General Assembly [on the report of the Third Committee (A/60/510 and Corr.1)], General Assembly, United Nations, Sixtieth session Agenda item 106 , 20 March 2006, p.1

(3) **Ntoko Ntonga Rene:** The legal and institutional framework for the enforcement of cybersecurity regulations in cameroon, University of Yaoundé II, Cameroon. P.1 eT.s

بتصادم الطائرات أو تحطمها، أو قطع إمدادات الكهرباء أو الماء على السكان المدنيين، أو إلحاق أضرار بالمرافق الكيميائية أو النووية. وتذكر اللجنة الدولية بضرورة التزام كل الأطراف فى النزاعات المسلَّحة باحترام قواعد القانون الدولي الإنساني إذا لجأت إلى وسائل وأساليب الحرب الإلكترونية، ومن هذه القواعد مبادئ التمييز والتناسبية والحيطة(١).

ثانياً: قرارات المجلس الاجتماعي والاقتصادي للأمم المتحدة بشأن الهجوم السيبراني:

اتخذ المجلس الاقتصادي والاجتماعي التابع للأمم المتحدة توصية بأن تأخذ المنظمة الدولية على عاتقها دورًا رئيسيًا في رسم سياسة منع الجريمة وتحقيق العدالة الجنائية الدولية، وقد تحقق ذلك بموافقة الجمعية العامة للأمم المتحدة في عام ١٩٥٠م على هذه التوصية، التي بموجبها تم إنشاء اللجنة الاستشارية لخبراء منع الجريمة ومعاملة المجرمين التي يقع على عاتقها مهمة مكافحة الجريمة، وتقديم المشورة للأمين العام، وإيجاد البرامج ووضع الخطط، ورسم سياسات لتدابير دولية في مجال منع الجريمة ومعاملة المجرمين(٢).

وفي سبتمبر عام ٢٠١١ عقد المجلس الاقتصادي والاجتماعي للأمم المتحدة، اجتماعًا لمناقشة أمن الفضاء الإلكتروني والتنمية، والقضايا والتحديات ذات الصلة، واشترك فى المناقشات إدارة الشئون الاقتصادية والاجتماعية، والاتحاد الدولي للاتصالات، ورئيس لجنة الأمم المتحدة المعنية بتسخير العلم والتكنولوجيا لأغراض التنمية، ومنظومة الأمم المتحدة، والقطاعين العام والخاص، بالإضافة إلى منظمات

(١) د. **هاني محمد خليل العزازي**: النظام القانوني الدولي لمُكافحة المَخاطر السيبرانية، مرع سابق، ص٥٠٢.

(٢) د. **قطاف سليمان**: مواجهة الجرائم السيبرانية في ضوء الاتفاقيات الدولية، مجلة البحوث القانونية والاقتصادية، المجلد:٥، العدد٢، ٢٠٢٢، ص٧٣.

المجتمع المدني المهتمَّة بمجالات الفضاء السيبراني والجرائم الإلكترونية، وحددت أهداف الاجتماع بأنها " تتمثل فى بناء وعيٍ على مستوى السياسات الدولية، عبر تزويد أعضاء المجلس الاقتصادي والاجتماعي، بصورة عن الوضع الحالي والتحديات المتعلقة بأمن الفضاء الإلكتروني وارتباطه بالتنمية؛ وتحديد أفضل السياسات المتعِّلقة بهذا المجال، والمبادرات المطبَّقة فى مختلف أنحاء العالم؛ لبناء ثقافة أمن الفضاء السيبراني، وكذا استكشاف خيارات للاستجابة العالمية بشأن تزايد معدلات الجريمة السيبرانية"(١).

علاوة على ذلك فقد ناقش الاجتماع الفوارق الاقتصادية بين الدول، وعدم قدرة الدول النامية منها على مكافحة الجرائم السيبرانية، وكذلك افتقاد الشراكة بينها وبين الدول الصناعية، مما يؤدي إلى خلق ملاذ آمن لمهاجمي الفضاء السيبراني لارتكاب جرائمهم. كما تم مناقشة الحاجة إلى إبرام اتفاقية دولية بشأن الفضاء الإلكتروني، بما يشمل احتمال البناء على اتفاقية «بودابست» باعتبارها تنسيقًا بين الدول بشأن بعض الجرائم السيبرانية، كالتعدي على حق المؤلف، والغش، واستغلال الأطفال في المواد الإباحية، وجرائم الكراهية، وانتهاكات أمن الشبكات.

وقرر «لازاروس كابامبي » رئيس المجلس الاقتصادي والاجتماعي، أن أعضاء الاجتماع قد اتفقوا على أن الأمن السيبراني قضية عالمية، لا يمكن حلها إلا عبر شراكة عالمية، لا سيما من خلال الأمم المتحدة التي يمكنها استخدام قدراتها الإستراتيجية والتحليلية لمعالجة مثل هذه القضايا(٢).

---

(١) **د. هاني محمد خليل العزازي**: النظام القانوني الدولي لمُكافحة المَخاطر السيبرانية، مرع سابق، ص٥٠٣.

(٢) ومن الجدير بالذكر أنه قد اتخذت مبادرات من قبل العديد من المنظمات بشأن الهجوم السيبراني كالاتحاد الدولي للاتصالاتITU ، الإنتربول (منظمة التعاون الاقتصادي، OECD مؤسسة =

وإن كان لنا أن ندلى برأينا فإننا نؤكد على أن قرارات منظمة الأمم المتحدة ممثلة أجهزتها كالجمعية العامة والمجلس الاقتصادى والاجتماعى لم تتناول معالجة مسألة حق الدفاع الشرعى ضد الهجمات السيبرانية، وأن قراراتها اقتصرت على المناشدة أو الدعوة أو الطلب أو السعى، وإن شئت فقل الرجاء من الدول بإتخاذ الحيطة ووضع التشريعات لمواجهة الهجمات السيبرانية، ونسيت وتناست أنها منظمة عالمية تتمتع بالشخصية القانونية الدولية الوظيفية الموضوعية فى مواجهة الدول أعضاء المجتمع الدولى؛ أي أن قراراتها تسرى على الدول الأعضاء وغير الأعضاء.

كما أغفلت النص فى قراراتها على الشروط الواجب توافرها لاستخدام حق الدفاع الشرعى ضد الهجمات السيبرانية وضوابطه، واكتفت بتركها للقواعد العامة وخصوصًا المادة (٥١) من الميثاق.

=

الإنترنت للأسماء والأرقام المخصصة، (ICANN) والمنظمة الدولية لتوحيد المقاييسISO، واللجنة الكهرو تقنية الدوليةIEC, وفرق عمل هندسة الإنترنت ومنظمة التعاون الاقتصادي للمحيط الهادئ وآسيا APEC ,ومنظمة الدول الأميركيةOAS ، ورابطة دول جنوب شرق آسيا ASEANوجامعة الدول العربية، والاتحاد الأفريقي.

راجع:

Tun Hirt: Droit international et légitme défense dans le cyberespace, University of Strasbourg, 2019, p. 2.

الخاتمـــة

لقد أسردنا بالتفصيل المناسب الإطار القانوني الحالي الذي يحكم ممارسة حق الدفاع الشرعي عن النفس وثيق الصلة وقابل للتطبيق علي الهجمات المسلحة السيبرانية، حيث يوفر هذا الإطار الحق في الدفاع عن النفس ردًا علي هجوم مسلح مستمر وفقًا للشروط المنصوص عليها في ميثاق الأمم المتحدة، فحق الدفاع الشرعي ثابت منذ نشأت القانون الدولي العرفي ولا خلاف في حق الدول في استخدامه للدفاع عن نفسها وعن بقائها ضمن الجماعة الدولية، ولكن مع التطور الملحوظ والسريع للتكنولوجيا ظهرت حروب الجيل الرابع والخامس متمثلة في الحرب عن بعد عن طريق الإنترنت والكمبيوتر، وهو ما دفع القانون الدولي إلي محاولة مواجهة هذا التطور وهذه الحروب عن طريق وضع الإطار القانوني لحق الدفاع الشرعي ضد الحروب الإلكترونية، وكذا محاولة تطبيق نص المادة ٥١ من ميثاق الأمم المتحدة علي الهجمات السيبرانية.

أولاً: النتائج:

١- إن الهجوم السيبراني يُعد استخدامًا للقوة نتيجة الآثار التي يخلفها مقارنة بالهجوم المسلح، وكلاهما يحقق ذات النتيجة، ويمكن أن تكون نتائج الهجوم السيبراني أكثر تدميرًا وخطورة، لذا فهو يرتقي إلي مستوي الهجوم التقليدي. كما أن الفقرة الرابعة من المادة الثانية من ميثاق الأمم المتحدة جاءت مرنه بالشكل الكافي لاستيعاب الهجوم السيبراني كصورة من صور القوة نتيجة الأثار المتشابهة بالنسبة للقوة العسكرية التقليدية.

٢- إن الدولة المعتدي عليها يكون لها الحق في استخدام القوة للدفاع عن النفس وفقًا للمادة (٥١) من الميثاق، وأن يكون الرد علي الهجوم السيبراني ضروريًا لكي يكون قانونيًا، ينطبق عليه وصف الدفاع الشرعي، كما يجب أن يستوفي رد

الفعل في الدفاع عن النفس ضد الهجمات السيبرانية التي ترتقي إلي مستوي الهجوم المسلح بمتطلبات الضرورة والفورية والتناسب التي نصت عليها اتفاقية جنيف في اللحق الإضافي.

٣- من المبادئ المستقرة في القانون الدولي المعاصر، أن استخدام القوة أو التهديد بها في العلاقات الدولية يعد عملًا غير مشروع، إلا أن هناك مجموعة من الأطر التفسيرية المرتبطة بالهجمات السيبرانية يدور حول تفسير مصطلح القوة بين معيار يعتمد على العنصر الحركي للقوات المسلحة، وأخر يشمل كافة صور استخدام القوة متى ترتب عليها انتهاك وتأثير واضح على الأمن القومي لدولة أخرى.

٤- إن تأثير الهجمات السيبرانية ترقي في العادة إلي الهجوم المسلح لأنهما يحملان ذات الهدف والغاية.

٥- يتجلى الفرق بين الهجوم السيبراني والجريمة السيبرانية في اختلاف الهدف، فهدف الهجوم السيبراني سياسي تظهر عليه علامات سياسة الدولة، بينما يكون هدف الجريمة السيبرانية مادي.

٦- بدى لنا أن تأكيد احترام مبدأ التناسب على الهجمات السيبرانية لا زال غامضًا، ذلك المبدأ الذي يستلزم الغاء أو تعليق آية هجوم إذا تبين أن الهدف المقصود ليس هدفًا عسكريًا أو أنه مشمول بحماية خاصة، أو قد يحدث خلطًا من الخسائر أو الأضرار في المدنيين والأعيان المدنية تتجاوز ما ينتظر أو يسفر عنه ذلك الهجوم من ميزة عسكرية مباشرة.

ثانياً: التوصيات:

١- ينبغي تعديل ميثاق الأمم المتحدة ليتضمن حظر الهجمات السيبرانية بشكل واضح، وذلك لأنها أصبحت تهدد الأمن والسلم الدوليين.

٢- ضرورة الحاجة إلى وجود قوانين وطنية حديثة وفعالة لمحاكمة الجرائم السيبرانية على النحو الملائم.

٣- ضرورة الحاجة إلى خلق ثقافة عالمية للأمن السيبراني، والاقرار بمسؤولية الحكومات عن قيادة جميع عناصر المجتمع لفهم أدوارهم ومسؤولياتهم فيما يتعلق بالأمن السيبراني.

٤- إجراء تقييم دولي مفصل للجهود الوطنية للدول الأعضاء في مجال الأمن السيبراني، وتبادل التدابير الناجحة وأفضل الممارسات التي يمكن أن تساعد الدول الأعضاء الأخرى في جهودها.

٥- تبادل الاستراتيجيات وأفضل الممارسات الوطنية للأمن السيبراني وتعزيز التعاون الدولي للتصدي للجهات الفاعلة.

٦- ضرورة انشاء استراتيجية دولية لإنشاء نظام رقمي للحد من مخاطر الهجوم السيبراني.

٧- ضرورة إبرام إتفاقيات دولية تعمل على تقييد استخدام تكنلوجيا المعلومات فى صورة هجمات سيبرانية، إذا كان من العسير برمجتها وفقًا للتطبيق الأمثل لقواعد القانون الدولي الإنساني، وفي ضوء الموازنة بين المصالح القومية والدفاع عن النفس، وبين الأثار غير الإنسانية التي قد تتسبب فيها تلك الهجمات.

قائمة المراجع

أولاً: المراجع العربية:

١- المعاجم

- **منير البعلبكي:**" المورد : قاموس إنجليزي –عربي"، دار العلم للملايين، بيروت.

٢- المراجع القانونية:

١- **د: أبو الخير احمد عطية:** نظرية الضربات العسكرية الاستباقية (الدفاع الوقائي) في ضوء قواعد القانون الدولي، دار النهضة، القاهرة ٢٠٠٧.

٢- **د: جعفر جاسم:** حرب المعلومات بين إرث الماضي وديناميكية المستقبل، دار البداية للنشر، ٢٠١٠.

٣- **د: حازم عتلم:** قانون النزاعات المسلحة الدولية- النطاق الزمني، الطبعة الأولي، دار النهضة، القاهرة، ٢٠٠٨.

٤- **د: رأفت علوه:** قرصنة الإنترنت، مكتبة التجمع العربي للنشر عمان، الطبعة الأولي، ٢٠٠٦.

٥- **د: ربيع محمد يحيي:** إسرائيل وخطوات الهيمنة علي ساحة الفضاء السيبراني في الشرط الأوسط، دراسة حول استعدادات ومحاور عمل الدولة العبرية في عصر الإنترنت، مركز الإمارات للدراسات والبحوث الاستراتيجية، ٢٠١٣.

٦- **د: عادل عبد الصادق:** أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، وحدة الدراسات المستقبلية مكتبة الإسكندرية، ٢٠١٦.

٧- **د: فاروق حسين:** فيروسات الحاسب الألي: دار هلا للنشر، القاهرة، الطبعة الأولي، ١٩٩٩.

٨- **كلارك ريتشارد:** حماية الفضاء الإلكتروني في دول مجلس التعاون الخليجي، الطبعة الأولي، مركز الإمارات للدراسات والبحوث الاستراتيجية، ٢٠١١.

٩- **د. مصطفي فؤاد:** فكرة الضرورة في القانون الدولي، منشأة المعارف، الإسكندرية، ١٩٨٧.

١٠– **وليد غشان جلعود:** دور الحرب الإلكترونية في الصراع العربي الإسرائيلي، رسالة ماجستير، جامعة النجاح الوطنية ، ٢٠١٣.

١١– **د.يحيى مفرح الزهراني:** الأبعاد الاستراتيجية والقانونية للحرب السيبرانية، مجلة البحوث والدراسات، كلية العلوم الاستيراتيجية، جامعة نايف للعلوم الأمنية، المملكة العربية السعودية، العدد (٢٣)، السنة (١٤)، ٢٠١٧.

ثانياً: المراجع الأجنبية:

A- Books:

1- **Allen D. Walker:** Applying International Law to the CyberAttacks in Estonia, Air Command and Staff College, 2008.

2- **Annette Froehlich:** Outer space and cyber, European space policy institute, Vienna, Austria, 2021.

3- **Arif Sari:** Applying methods of scientific inquiry into intelligence, security and counterterrorism, United States of America, 2019.

4- Ben Buchanan: The cybersecurity dilemma hacking trust, and fear between nations, Oxford University press, 2017.

5- **Denis Goulet:** Technology, the Two Edged Sword, East-West Technology and Development Institute, East-West Center, 1976.

6- **David H. Brandin, Michael A. Harrison:** The Technology War, Wiley, University California, 1987.

7- **Gary Brown, Colonel, Keira Poellet, Major:** The Customary International Law of Cyberspace, Strategic Studies Quarterly, 2012.

8- **Hitoshi N ،.Robert M.:** New Technologies and the Law of Armed Conflict, Australian National Of Law, Australia, 2013.

9- **James A. G:** Cyber warfare, London and New York, 2015.

10- **Jens D. O ،.Larry M.:** Necessity in International Law, Oxford University Press, 2016.

11- **Johann-Christoph Woltag:** Cyber Warfare: Military Cross-border Computer Network Operations Under International Law, Intersentia, 2014.

12- **Julia Cresswell:** "Oxford Dictionary of word Origins: Cybernetics", Oxford Reference Online, Oxford University Press, 2010.

13- **K. Saalbach:** " Cyber War, Methods and Practice", University of Osnabruck-17 Jun 2014.

14- Kubo Mačák: Is the international law of cyber security in crisis?, University of Exeter, United Kingdom, 2016.

15- **Martin C. Libicki:** Conquest in Cyberspace: National Security and Information Warfare, New York: Cambridge University Press, 2007.

16- **Mark Galeotti:** Russia's Five-Day War: The invasion of Georgia, August 2008.

17- **Michael N. S:** Tallinn Manual on the international law applicable to cyber warfare, Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence General, Cambridge University Press,2013.

18- Miranda Grange: Cyber warfare and the law of armed conflict, University of Wellington, 2014.

19- **Neil Robinson :** Stocktaking Study of Military Cyber Defense Capabilities in the European Union (milCyberCAP): Unclassified Summary. RAND Research Report 286 (Santa Monica, CA: RAND, 2013.

20- **Norbert Wiener:** "Cybernetic or control communication in the animal and the machine, M.I.T, Press, Second Edition, Cambridge, Massachusetts, 1948.

21- **Paul A. Walker:** Rethinking Computer Network "Attack": Implications for Law and U.S. Doctrine, National security law brief, 2011.

22- **Thomas Wingfield:** When is a Cyberattack an "Armed Attack?": Legal Thresholds for Distinguishing military activities in cyberspace, Cyber Conflict Studies Association, 2006.

23- **Tim Jordan:** Cyberpower the culture and politics of cyberspace and the internet, London, 1999.

24- **Tim Jordan:** Hacking: Digital Media and Technological Determinism polity press, Cambridge, 2008.

25- **Sabu M. Th, Bharat B, Pradeep K. A:** Managing trust in cyberspace, A Chapman & Hall Book, New York, 2014.

26- **Sahovic Milan:** Principles of international law concerning friendly relation and cooperation, Institute of international politics and economics, Dobbs Ferry, Oceana,Belgrade, 1972.

27- **Scoot j Shckelford:** " State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem", University of Cambridge, Dept of politicos and International Studies, Cambridge, UK, 2009.

28- **Sonia Boulos:** Cyberspace Risks and Benefits for Society, Security and Development The tallinn manual and Jus ad Bellum: Some critical notes, Springer International Publishing AG, 2017.

29- **Sirohi M. N:** Cyber Terrorism and Information Warfare, 2015.

30- **Tom Gjelten:** Extending the Law of War to Cyberspace, Sept. 22, 2010.

31- **Tun Hirt:** Droit international et légitme défense dans le cyberespace, University of Strasbourg, 2019.

32- **Steven F., Nalhan C:** Human aspects of information security and assurance, University of Nottingham, Nottingham U K, 2021.

B- <u>Article:</u>

1- **Ashley Deeks:** An International Legal Framework for Surveillance, Virginia journal of international law, vol. 55,2015.

2- **Ashley S. Deeks**: "Unwilling or Unable": Toward a Normative Framework for Extraterritorial Self-Defense, Virginia Journal Of International Law, vol. 52, 2012.

3- **Bradley Raboin:** Corresponding Evolution: International Law and the Emergence of Cyber Warfare, Journal of the National Association of Administrative Law Judiciary, vol. 31, 2011.

4- **Charles C. P:** This Means War! (Maybe?)—Clarifying Casus Belli in Cyberspace, ORIL , vol. 15, 2013.

5- **Clémentines Bories:** Appréhender la cyberguerre en droit international. Quelques réflexions et mises au point, Revue du Centre de recherches et d'études sur les droits fondamentaux, vol. 6, 2014.

6- **Daniel B. Silver:** Computer Network Attack as a Use of Force Under Article 2(4) of the United Nations charter, International Law Studies, vol. 76 , 2002.

7- **Diego Rafael Canabarro and Thiago Borne**:" Reflection on the fog of Cyber War", National Center for Digital Government, Policy working Paper, March 1, no. 13, 2013.

8- **Dieter Fleck:** Searching for International Rules Applicable to Cyber Warfare: A Critical First Assessment of the New Tallinn Manual' Journal of Conflict and Security Law, vol. 18, no. 2, 2013.

9- **David E. Graham:** Cyber Threats and the Law of War, Journal of National Security Law & Policy, vol. 4, 2010.

10- **Davis Brown:** A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict, Harvard International Law Journal, vol. 47, 2006.

11- **Eric Jensen:** Computer Attacks on Critical National Infrastructure: AUse of Force Invoking the Right of Self-Defense, Stanford Journal of International Law, vol. 38, 2002.

12- **Gary D. Brown:** International law applies to cyber warfare! now what?, Southwestern Law Review, vol. 46, 2017.

13- **Jordan J. Paust:** Self-Defense Targetings of Non-State Actors and Permissibility of U.S. Use of Drones in Pakistan, 19 Journal Of transnational Law & Policy, vol. 19, 2010.

14- **Inaki N., Russell B**.: Peacetime Espionage, International Law and the Existence of Customary Exceptions, Cornell International Law Journal, vol. 51, 2019.

15- **Laurie R. Blank:** International Law and Cyber Threats from Non-State Actors, International Law Studies, vol. 89, 2013.

16- **M. Condron:** Getting it Right: Protecting American Critical Infrastructure in Cyberspace, 20 Harvard Journal of International Law, vol. 16, 2007.

17- **Marco Roscini:** " World Wide Warfare – Jus ad bellum and the use of Cyber Force",Max Planck Yearbook of United Nations Law ,vol. 14, 2010.

18- **Matthew C. Waxman:** Self-defensive Force against Cyber Attacks: Legal, Strategic and Political Dimensions, International Law Studies,vol. 89, 2013.

19- **Matthew C. Waxman:** Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4), Yale Journal Of International Law, vol. 36, 2011.

20- **Mateusz Piątkowski:** The Definition of the Armed Conflict in the Conditions of Cyber Warfare, Polish Political Science Yearbook vol. 46, no. 1, 2017.

21- **Michael N. S:** Cyber Operations and the Jus in Bello: Key Issues. Naval War College International Law Studies, vol, 87, 2011.

22- **Michael N. S:** The law of cyber warfare: quo vadis? Stanford law and policy review, vol. 25, 2014.

23- **Michael N. S Wired Warfare:** Computer Network Attack and Jus in Bello, IRRC, vol. 84, no. 84, 2002.

24- **Michael N. S :** Computer Network Attack and the Use of Force in International Law through on a Normative", The Colombia Journal of Transitional Law, vol. 27, 1999.

25- **Myriam Dunn:** "The Cyberspace Dimension in Armed Conflict: Approaching a Complex Issue with Assistance of the Morphological Method", Information and Security: An International Journal vol. 7, 2001.

26- **Noam Lubell:** Lawful targets in cyber operations: Does the principle of distinction apply? International law studies, 2013.

27- **Oona A. Hathaway:** The Law of Cyber-Attack, Yale Law School, vol. 100, 2012.

28- **Peter Z. Stockburger:** Known Unknowns: State Cyber Operations, Cyber Warfare, and the Jus Ad Bellum, American University International Law Review, vol. 16, 2016.

29- **Petr Hruza:** cyberwarfar, International Conference Knowldege -based organization,vol. XXIII, no. 1, 2017.

30- **Terry D. G. and Paul A. L. D.:** Anticipatory Self-Defense in the Cyber Context, International Law Studies, Vol. 89, 2013.

31- **Scott J. Shackelford:** From nuclear war to net war: Analogizing cyber attacks in international law, Berkeley Journal of International Law, vol. 27, no. 1, 2009.

32- **Shin Beomchul:** " The Cyber Warfare and the Right of Self –Defense: Legal Perspectives and the Case of the United States, IFANS, v.19, n1, June, 2011.

33- **Stephen Moore:** Cyber Attacks and the Beginnings of an International Cyber Treaty, International Law; Commercial Law, vol. 39, 2013.

34- **Terry D. Gill and Paul A. L. Ducheine:** Anticipatory Self-Defense in the Cyber Context, Naval War College International Law Studies, vol. 89,2013.

35- **U. M. Mbanaso: The Cyberspace:** Redefining A New World, IOSR Journal of Computer Engineering, 2015.