انطباق مفهوم الهجوم المسلح على الهجمات السيبرانيه

الباحثة نهى جاسم محمد العلوش أ.م.د. قحطان عدنان عزيز
كليه القانون /جامعة بابل

المستخلص:
يعـد التقـدم الحاصـل فـي مجـال المعلومـات والاتصـالات لـم يقتصـر فقـط علـى الجانـب الايجـابي المتعلـق بالتكنولوجيـا وتطـوير البنـى التحتيـة، وإنمـا ظهـر جانـب آخـر وهـو الجانـب السـلبي الـذي لـه تـداعيات خطيـرة علـى مسـتقبل الدولـة وسـيادتها. حيـث أدى الـى إضـعاف دور الخصوصـية، وشـجع بشـكل كبيـر علـى انتشـار الجـرائم، ممـا أصـبح يشـكل تهديـد للامـن والسـلم الـدوليين. إذ يتمثـل الجانـب السـلبي بظـاهرة الهجمـات السـيبرانية التـي أصبحت تهدد أمن الدولة وسلامة مواطنيها والبنى التحتية الحيوية مما يستدعي وضع حد لها.
وبـذلك توصـلت هـذه الـدول فـي العقـد الاخيـر إلـى أحـدث هـذه الوسـائل والتـي تتسـم بالتعقيـد واجتيـاز الحـدود التقليديـة، وهـي الهجمـات السـيبرانية التـي مـن شـأنها التـدمير الكلـي للبنيـة التحتيـة للخصـم، والتـي تتسـبب بآثـار فادحـة علـى الاعيـان العسـكرية والمدنيـة للخصـم وذلـك كلـه مـن دون الحاجـة إلـى الـدخول فـي أي اشـتباك حقيقـي ومـادي مـع الخصـم، ومـن دون الحاجـة لتحمـل أعبـاء ماليـه ومخـاطر المواجهـة المسـلحة التـي يتحملهـا المهـاجم فـي إطار الاسلحة التقليدية.

Abstract:
The progress made in the field of information and communications is not only limited to the positive aspect related to technology and infrastructure development, but another aspect has appeared, which is the negative aspect that has serious repercussions on the future of the state and its sovereignty. Where it weakened the role of privacy, and greatly encouraged the spread of crimes, which became a threat to international peace and security. The negative side is represented by the phenomenon of cyber-attacks, which threatens the security of the state, the safety of its citizens and vital infrastructure, which calls for an end to it.
Thus, in the last decade, these countries have come up with the latest of these methods, which are characterized by complexity and crossing traditional borders, which are cyber-attacks that will completely destroy the infrastructure of the opponent, and cause severe effects on the military and civilian objects of the opponent, all without the need to engage in

any real clash materially with the opponent, and without the need to bear the financial burdens and risks of armed confrontation that the attacker bears within the framework of conventional weapons.

المقدمه:

أولا: موضوع الدراسه:

يعد التقدم الحاصل في مجال المعلومات والاتصالات لم يقتصر فقط على الجانب الايجابي المتعلق بالتكنولوجيا وتطوير البنى التحتية، وإنما ظهر جانب آخر وهو الجانب السلبي الذي له تداعيات خطيرة على مستقبل الدولة وسيادتها. حيث أدى الى إضعاف دور الخصوصية، وشجع بشكل كبير على انتشار الجرائم، مما أصبح يشكل تهديد للامن والسلم الدوليين. إذ يتمثل الجانب السلبي بظاهرة الهجمات السيبرانية التي أصبحت تهدد أمن الدولة وسلامة مواطنيها والبنى التحتية الحيوية مما يستدعي وضع حد لها.

وبذلك توصلت هذه الدول في العقد الاخير إلى أحدث هذه الوسائل والتي تتسم بالتعقيد واجتياز الحدود التقليدية، وهي الهجمات السيبرانية التي من شأنها التدمير الكلي للبنية التحتية للخصم، والتي تتسبب بآثار فادحة على الاعيان العسكرية والمدنية للخصم وذلك كله من دون الحاجة إلى الدخول في أي اشتباك حقيقي ومادي مع الخصم، ومن دون الحاجة لتحمل أعباء ماليه ومخاطر المواجهة المسلحة التي يتحملها المهاجم في إطار الاسلحة التقليدية.

وان اللجوء المتزايد للدول إلى استخدام الهجمات السيبرانية في نزاعاتها، جعل قواعد القانون الدولي أمام اختبار حقيقي ومعقد يدور حول مدى إمكانية تطبيق تلك القواعد الدولية التي قننت قبل عقود من الزمن على الهجمات السيبرانية.

لذلك فقد أثبتت الدراسات بأن آثار الهجمات السيبرانية على البنى التحتية الحيوية مثل محطات الكهرباء والماء هي ذات الاثار الناجمة عن أسلحة الدمار الشامل فكلما كانت الدولة أكثر تقدما من الناحيه التكنولوجية تكون أكثر عرضة للتهديدات السيبرانية.

ومن خلال دراستنا لموضوع (الهجمات السيبرانيه) يجب علينا بيان ما مدى انطباق مفهوم القوه المسلحه والهجوم المسلح على تلك الهجمات وأيضا تمييز الهجمات السيبرانيه عن الحرب السيبرانيه والجريمه السيبرانيه

ثانيا: اهميه الدراسه:

بالرغم من ان الهجوم السيبراني الذي أصبح بلا شك يسبب دماراً هائلا لا يقل عن الهجوم المسلح، الا انه مازال خارج دائرة الهجمات المسلحة مما زاد الامر تعقيدا كون موقف ميثاق الامم المتحدة والقانون الدولي ليس واضحا بشأن الهجمات السيبرانية بوصفها وليدة التطورات الحديثه للتكنولوجيا. لذا أصبحت بعض الدول تستغل هذه الاشكالية لتحقيق أهدافها عبر الفضاء السيبراني دون رادع. في بعض الاحيان هناك صعوبة في تحديد هوية المهاجم وكذلك غياب التشريعات التي تخص الهجمات السيبرانية مما يخلق ثغرة تساعد بشكل كبير على شن الهجمات الالكترونية. ومن ثم هذا سيؤدي الى عدم القدرة على ملاحقة المهاجم قانونيا بخلاف الحرب التقليدية.

ثالثا: اشكاليه الدراسة:

يتنـاول موضـوع هـذا البحـث الـدفاع الشـرعي ضـد الهجمـات السـيبرانية وبالنسـبه لاشـكاليه هـذا البحـث فانهـا تتمحـور حـول مـدى امكانيـه اسـتخدام القـوه العسـكريه للـرد علـى الهجمـات السـيبرانيه التـي تقـوم بهـا الـدول او جهات أخرى.

رابعا: اهداف الدراسة:

ان الأهـداف المحـددة فـي محـور الدراسـة هـي مناقشـه وتحليـل المـواد القانونيـة بخصـوص الموضـوع ومـدى كفايتهـا وتقـديم المقترحـات وكـذلك اسـتعراض مواقـف الـدول ودراسـة المشـاكل التـي بنيـت مـن ذلـك والوقـوف حولها.

خامسا: منهجية الدراسة:

امـا بخصـوص منهجيـه دراسـتنا سـوف يكـون المـنهج العلمـي المتبـع فـي دراسـة هـذا الموضـوع هـو المـنهج التحليلي الذي يستهدف الوصف الدقيق والموضوعي والى استعراض النصوص وتحليلها.

خامسا: خطه البحث:

المبحث الأول: الهجمات السيبرانيه كقوه وهجوم مسلح
المطلب الأول: الهجمات السيبرانيه بأعتبارها (قوه مسلحه)
المطلب الثاني: الهجمات السيبرانيه بأعتبارها (هجوم مسلح)
المبحث الثاني: التمييز بين الهجمات السيبرانيه والجريمة السيبرانيه والحرب السيبرانيه
المطلب الأول: التمييز بين الهجمات السيبرانيه والجرائم السيبرانيه
المطلب الثاني: التمييز بين الهجمات السيبرانية والحرب السيبرانية

المبحث الأول: انطباق مفهوم (الهجوم المسلح) على الهجمات السيبرانيه

عرفنـا (الهجـوم السـيبراني) أو "الهجـوم الإلكترونـي" هـو أي نـوع مـن المنـاورة الهجوميـة التـي تسـتهدف أنظمـة معلومـات الكمبيـوتر أو البنيـة التحتيـة أو شـبكات الكمبيـوتر أو أجهـزة الكمبيـوتر الشخصـية ويعـرف المهـاجم بأنـه هـو شـخص أو عمليـة تحـاول الوصـول إلـى البيانـات أو الوظـائف أو المنـاطق المحظـورة الأخـرى فـي النظـام دون الحصـول علـى إذن ويحتمـل أن يكـون ذلـك بقصـد ضـار, فيجـب علينـا أيضـا الاطـلاع علـى مفهـوم الهجـوم المسـلح وتعريفـه حيـث يعـرف الهجـوم المسـلح بأنـه هـو كـل عمليـه عسـكريه تهـدف إلـى احـتلال منطقـة أو تحقيـق غـرض أو تحقيـق هـدف أكبـر سـواء كـان اسـتراتيجيًا أو عملياتيًـا أو تكتيكيًـا مـن خـلال إسـقاط عـدواني. وتسـتخدم وسـائل الإعـلام أيضًـا مصـطلحًا آخـرًا للهجـوم وهـو «الغـزو». اعتبـر الهجـوم وسـيله بـارزه لتحقيـق النصـر رغـم اشـتماله علـى شـق دفـاعي فـي مرحلـه مـا مـن التنفيـذ والـدليل السـريع لحجـم الهجـوم او مـداه هـو الاخـذ بعـين الاعتبـار عـدد القـوات المشـاركه مـن الجانـب المبـادر فـي الهجـوم وينفـذ الهجـوم بشـكل أساسـي كوسـيله لتـأمين التحـرك فـي المواجهـات بـين المتنـازعين ويمكـن شـن الهجمـات فـي البـر او البحـر او الجـو وبعـد معرفتنـا بالهجمـات او الهجـوم السـيبراني نريـد ان نعـرف مـدى انطبـاق مفهـوم الهجـوم المسـلح علـى تلـك الهجمـات وسـوف نتطـرق فـي هـذا البحـث الـى الهجمـات السـيبرانيه كقـوه وهجـوم مسـلح حيـث قسـم هـذا المبحـث الـى مطلبـين اثنـين جـاء فـي المطلـب الأول الهجمـات السـيبرانيه بأعتبارهـا (قـوه مسـلحه) والمطلـب الثـاني الهجمـات السـيبرانيه بأعتبارهـا (هجـوم مسـلح) امـا

بخصوص المبحث الثاني سوف نتطرق فيه الى التمييز بين الهجمات السيبرانيه والجريمة السيبرانيه والحرب السيبرانيه بحثنا في المطلب الأول التمييز بين الهجمات السيبرانيه والجرائم السيبرانيه والمطلب الثاني التمييز بين الهجمات السيبرانية والحرب السيبرانية

المطلب الأول: الهجمات السيبرانيه بأعتبارها (قوه مسلحه)

عرفت القوات المسلحة بموجب القاعده الرابعه من القانون الدولي الإنساني العرفي (تتكون القوات المسلحة لأي طرف في النزاع من جميع أفراد قواته المسلحة والمجموعات والوحدات النظامية التي تكون تحت قيادة مسؤولة أمام ذلك الطرف عن سلوك مرؤوسيها) [1]

حيث تكرس ممارسة الدول هذه القاعدة كإحدى قواعد القانون الدولي العرفي المنطبقة في النزاعات المسلحة الدولية ومن أجل الغاية المتوخاة من مبدأ التمييز، يجوز أن تطبق هذه القاعدة أيضاً على القوات المسلحة التابعة للدول في النزاعات المسلحة غير الدولية [2]

حيث ترد هذه القاعدة في المادة 43 (1) من البروتوكول الإضافي الأول[3] وتنص الكثير من كتيبات الدليل العسكري على أن القوات المسلحة كطرف في النزاع تتكون من جميع المجموعات المسلحة النظامية التي تكون تحت قيادة مسؤولة أمام ذلك الطرف عن سلوك مرؤوسيها وتشمل الممارسة، تلك الخاصة بدول ليست أو لم تكن في حينها أطرافاً في البروتوكول الإضافي الأول ويغطي تعريف القوات المسلحة هذا، في جوهره، جميع الأشخاص الذين يقاتلون بالأصالة عن طرف في نزاع ويتبعون قيادته. ونتيجة لذلك، فالمقاتل هو أي شخص يشارك تحت قيادة مسؤولة في أعمال عدائية في نزاع مسلح بالأصالة عن طرف في نزاع. كما تطبق الشروط المفروضة على القوات المسلحة على المجموعات المسلحة بصفتها هذه فبالتالي فإن أفراد مثل هذه القوات المسلحة هم عرضة للهجمات

واعتمد تعريف القوات المسلحة هذا على التعاريف السابقة الموجودة في لائحة لاهاي المتعلقة بقوانين وأعراف الحرب البرية واتفاقية جنيف الثالثة التي سعت لتحديد من هم المقاتلون المؤهلون لوضع أسير الحرب. فالمادة 1 من لائحة لاهاي تشترط عدم انطباق قوانين الحرب وحقوقها وواجباتها على الجيوش فقط، وإنما أيضاً على الميليشيات والوحدات المتطوعة التي تتوفر فيها أربعة شروط:

1- يجب أن يكون على رأسها شخص مسؤول عن مرؤوسيه؛
2- يجب أن تكون لها شارة مميزة ثابتة يمكن التعرف عليها عن بعد؛
3- يجب أن تحمل الأسلحة علناً؛
4- يجب أن تلتزم في عملياتها بقوانين الحرب وأعرافها[4].

[1] القانون الدولي الإنساني العرفي القاعده 4
[2] أنظر المؤتمر الدبلوماسي لتأكيد وتطوير القانون الدولي الإنساني المطبق في النزاعات المسلحة، CDDH, Official Records, Yves Sandoz, Christophe Swinarski, Bruno Zimmermann (eds.), Commentary on the Additional Protocols, ICRC, Geneva, 1987, §4462.
[3] البروتوكول الإضافي الأول، المادة 43 (1) (تم اعتمادها بالإجماع) (ترد في المجلد الثاني، الفصل الأول
[4] لائحة لاهاي المتعلقة بقوانين وأعراف الحرب البرية، المادة 1

وبالإضـافة إلـى ذلـك، تـنص هـذه المـادة علـى أنّ الميليشـيات أو الوحـدات المتطوعـة (المعروفـة بقـوات مسـلحة "غيـر نظاميـة") التـي تقـوم فـي بلـد مـا مقـام الجـيش، أو تشـكل جـزءاً منـه، تنـدرج فـي فئـة "الجـيش[5]" ويسـتخدم هـذا التعريف أيضاً في المادة 4 من اتفاقية جنيف الثالثة، مع إضافة حركات المقاومة المنظمة[6]

وهكـذا فـإنّ لائحـة لاهـاي واتفاقيـة جنيـف الثالثـة تعتبـران أنّ جميـع أفـراد القـوات المسـلحة هـم مقـاتلون وتطلبـان مـن الميليشـيات والوحـدات المتطوعـة، بمـا فيهـا حركـات المقاومـة المنظمـة، أن تلتـزم بأربعـة شـروط حتـى يعتبـر أفرادهـا مقـاتلين مـؤهلين لوضـع أسـير الحـرب. والفكـرة التـي تتضـمنها هـذه القواعـد هـي أنّ القـوات المسـلحة النظاميـة تسـتوفي هـذه الشـروط الأربعـة بجوهرهـا. ولـذلك وفـي مـا يتعلـق بـالقوات المسـلحة النظاميـة، لا يجـري تعـداد هـذه الشـروط بشـكل صـريح. فـالتعريف الـوارد فـي البروتوكـول الإضـافي الأول لا يميّـز بـين القـوات المسـلحة النظاميـة والمجموعـات أو الوحـدات المسـلحة الأخـرى، ولكنـه يعـرّف كافـة القـوات والمجموعـات والوحـدات المسـلحة التـي تكـون تحـت قيـادة مسـؤولة عـن سـلوك مرؤوسـيها أمـام طـرف فـي النـزاع، كقـوات مسـلحة لـذلك الطـرف. ويعبّـر التعريفـان عـن نفـس الفكـرة، أي أنّ جميـع الأشـخاص الـذين يقـاتلون باسـم طـرف فـي النـزاع- الـذين "ينتمـون إلـى" طـرف، بحسـب كلمـات المـادة 4 مـن اتفاقيـة جنيـف الثالثـة هـم مقـاتلون. غيـر أنّ الشـروط الأربعـة الـواردة فـي لائحـة لاهـاي واتفاقيـة جنيـف الثالثـة قـد خُفّضـت إلـى شـرطين فـي البروتوكـول الإضـافي الأول، بحيـث أصـبح الفـارق الرئيسـي هـو اسـتثناء متطلبـات الرؤيـة فـي تعريـف القـوات المسـلحة بصـفتها هـذه. فشـرط الرؤيـة وثيـق الصـلة بحـق اسـتفادة المقاتـل مـن وضـع أسـير الحـرب (انظـر القاعـدة 106). لـذلك، رفـع البروتوكـول الإضـافي الأول هـذا المطلـب مـن تعريـف القـوات المسـلحة (المـادة 43) وأثبتـه فـي الـنص الـذي يعنـى بالمقاتلين ووضع أسير الحرب (المادة 44)

واضـافه الـى ذلـك، فالمـادة 43 مـن البروتوكـول الإضـافي الأول لا تشـير إلـى مطلـب احتـرام قـوانين وأعـراف الحـرب، وإنّمـا تتضـمّن وجـوب أن تخضـع هـذه القـوات المسـلحة لنظـام انضـباط داخلـي يعـزّز الالتـزام بالقـانون الـدولي الإنسـاني. غيـر أنّ هـذا التغييـر لا يبـدّل جـوهر تعريـف القـوات المسـلحة بالنسـبة إلـى المقـاتلين المـؤهلين لوضـع أسـير الحـرب. إنّ شـرط وجـود نظـام انضـباط داخلـي يكمّـل الأحكـام المتعلقـة بمسـؤولية القيـادة (انظـر القاعـدتين 152-153)[7]، وهـو مـلازم لواجـب إصـدار التعليمـات التـي تلتـزم بالقـانون الـدولي الإنسـاني (انظـر التعليق على القاعدة 139) [8]

وقـد اكـدت المادتـان 43 و44 مـن البروتوكـول الإضـافي الأول مـا جـرى الـنص عليـه فـي المـادة 85 مـن اتفاقيـة جنيـف الثالثـة، أي "يحـتفظ أسـرى الحـرب الـذين يحـاكمون بمقتضـى قـوانين الدولـة الحـاجزة عـن أفعـال اقترفوهـا قبـل وقـوعهم فـي الأسـر بحـق الإفـادة مـن أحكـام هـذه الاتفاقيـة، حتـى ولـو حكـم علـيهم"، وهـذا يعنـي أنهـم يحتفظـون بوضـعهم. وهكـذا فـإنّ هـذه النصـوص "تحـول دون أيـة محاولـة لحرمـان أفـراد قـوات مسـلحة مسـتقلة أو نظاميـة مـن

[5] المرجع السابق نفسه
[6] اتفاقية جنيف الثالثة، المادة 4
[7] المرجع السابق
[8] Yves Sandoz, Christophe Swinarski, Bruno Zimmermann (eds.), Commentary on the Additional Protocols, ICRC, Geneva, 1987, §1675.

وضـع أسـير الحـرب بالتـذرّع أنّ قـواتهم لا تنفـذ بعـض أحكـام القـانون العرفـي أو التقليـدي للنزاعـات المسـلحة (كمـا قد تتذرّع به الدولة الحاجزة) [9]

إنّما مـا يبـرّر فقد الشـخص لوضـع أسـير الحـرب يتمثـل فقـط فـي إخفاقـه فـي تمييـز نفسـه عـن المـدنيين (انظـر القاعـدة 106) أو إلقاء القبض عليه كجاسوس (انظر القاعدة 107) أو مرتزق (انظر القاعدة 108)

ويطبـق التعريـف فـي المـادة (43) مـن البروتوكـول الإضـافي الأول الآن، وبشـكل عـام علـى كافـة أشـكال المجموعـات المسـلحة التـي تنتمـي لطـرف فـي نـزاع مسـلح لتحديـد مـا إذا كانـت تشـكّل قـوات مسـلحة ولـذا لـم يعـد مـن الضـروري التمييـز بـين القـوات المسـلحة النظاميـة وغيـر النظاميـة فكـل مـن يسـتوفي منهـا شـروط المـادة (43) مـن البروتوكول الإضافي الأول هي قوات مسلحة.

أن الهجـوم الالكترونـي بـرز كواحـد مـن خيـارات الامـن الـوطني الواعـدة وألاكثـر إتاحـة لانجـاز المهمـة والـدفاع عـن الـنفس وهـو يشـمل أنشـطة تهـدف إلـى تعطيـل، منـع، إضـعاف أو تـدمير المعلومـات الموجـودة فـي أجهـزة الكمبيوتر وشبكات الكمبيوتر أو أجهزة الكمبيوتر والشبكات نفسها [10]

فقـد نصـت المـادة (2) الفقـرة الرابعـة مـن ميثـاق الأمـم المتحـدة علـى ان لايمتنـع أعضـاء الهيئـه جميعـا فـي علاقـاتهم الدوليـة عـن التهديـد باسـتعمال القـوة او باسـتخدامها ضـد سـلامه الاراضـي أو الاسـتقلال السياسـي لايـة دولـة او علـى وجـه لا يتفـق مـع مقاصـد الامـم المتحـدة حيـث بينـت المـادة المـذكوره ان اسـتعمال القـوة أو التهديـد بهـا ضـد سيادة الدول يتنافى مع أهداف الميثاق التي تهدف الى حفظ الامن والسلم الدوليين.

كمـا ورد فـي نـص المـادة أعـلاه مصـطلح القـوة مـن دون تحديـد نـوع القـوة المسـتخدمة حيـث جـاءت مطلقـة لتشـمل جميـع انـواع القـوه[11] احيانـا يصـطحب لفـظ القـوة فـي ميثـاق ألامـم المتحـدة مصـطلح "المسـلحة" التـي ذكـرت فـي الديباجـة والمـادة (41) مـن الميثـاق الا ان مصـطلح "القـوة" جـاء فـي الفقـرة(4)مـن المـادة (2) وحـده مـن دون مصـطلح (المسـلحة) ممـا زاد الامـر تعقيـدا حيـث أدى الـى اخـتلاف آراء الفقهـاء بشـان المعنـى المقصـود بـالقوه فبخصـوص ذلـك ظهـر اتجـاهين مختلفـين فيمـا يتعلـق بتفسـير مصـطلح القـوه حيـث رأى الاتجـاه الأول ان المقصـود بـالقوه هـي قـوه عسـكريه فقـط بينمـا رأى الاتجـاه الاخـر ان المقصـود بـالقوه لـيس القـوه العسـكريه فقـط انمـا المقصـود أوسـع مـن ذلـك حيـث يشـمل كـل مـن الضـغط الاقتصـادي والسياسـي الـذي يعـد تهديـدا للاسـتقلال السياسـي للدولـه والذي يعادل التهديد العسكري من حيث الخطوره [12]

الاتجـاه الاول: يأخـذ أنصـار هـذا الاتجـاه بالتفسـير الضـيق للمـادة الثانيـة/ الفقـرة الرابعـة الـذي يقضـي بـان المقصـود بـالقوة هـي القـوة العسـكرية فقـط ويسـتندون فـي رأيهـم الـى أن المقصـود مـن نـص المـادة اعـلاه يجـب ان يكـون فـي حـدود ديباجـة الميثـاق ونصوصـه الاخـرى ذات الصـلة, و ان المـادة (2) الفقـرة (4) يجـب ان تفسـر علـى أنهـا تجسـد المعنـى الضـيق للقـوة المحصـورة فـي القـوة العسـكرية أو المسـلحة كمـا ان المـادة(44)مـن الميثـاق تـنص

[9] Michael Bothe, Karl Josef Partseh, Waldemar A. Solf, *New Rules for Victims of Armed conflicts*, Martinus Nijhoff, The Hague, 1982, p. 239.

[10] Brian T. O'Donnell and James C. Kraska, HUMANITARIAN LAW: DEVELOPING INTERNATIONAL RULES FOR THE DIGITAL BATTLEFIELD, Journal of Conflict and Security Law, Vol. 8 No. 1. 2003 . p.138.

[11] Bryan A Garner, Blacks law Dictionary (8 th ed, st Paul Minm, Thomson West, 2009) 115.

[12] كمال الدين، النزاع المسلح والقانون الدولي العام، المؤسسة الجامعية للدراسات والنشر والتوزيع، بيروت،ط1 ,1997 ، ص31

على اعتبار ان مضمونها يقصد به القوة المسلحة وأيضا يستندون انصار هذا الاتجاه على ان الاقتراح الذي قدم في مؤتمر سان فرانسيسكو من البرازيل لاعتبار إجراءات الضغط السياسي من قبيل الاستخدام غير المشروع للقوة الا ان هذا المقترح تلقى الرفض[13] فوفقا لهذا الاتجاه لا يمكن اعتبار الهجوم السيبراني قوة لانه لا يرقى الى مستوى الهجوم المسلح.

الاتجاه الثاني: ذهب أنصار هذا الاتجاه الى ان مفهوم القوة لا ينحصر فقط بالقوة العسكرية ولكن يشمل كل أنواع التهديد بغض النظر عن الوسيلة المستخدمة في التهديد طالما ان النية عدائية. حيث ان الفقرة 4 من المادة 2 جاءت مرنة بالشكل الكافي لاستيعاب الهجوم السيبراني نتيجة لآثارها المتشابهة بالنسبة للقوة العسكرية التقليدية لذلك فأن الكود الضار او الفايروسات لها نفس خصائص الاسلحه التي يمكن ان تكون أداة للتخريب والتدمير كالسلاح الحركي. اضافه الى ذلك أوضحت محكمة العدل الدولية في الفتوى التي اصدرتها بخصوص مشروعية استخدام ألاسلحة النووية حيث ان الفقرة (4) من المادة (2) من ميثاق الامم المتحدة لا تشير الى أسلحة محددة، ومن ثم فان هذه المادة تنطبق على اي استخدام للقوة بصرف النظر عن الوسائل المستخدمة [14]

وفق لما ذكر سابقا فان الهجوم السيبراني عندما يصل الى مستوى استخدام القوة فليس من الضروري التطرق الى الوسيلة التي تم التنفيذ من خلالها الوسائل الالكترونية حيث يتم التعامل على أنها قوة لها نتائج على الارض بغض النظر عن الوسيلة المستخدمة لذا ليس من الضروري ان يوجد سبب يجعل الاسلحة لها آثار متفجرة، كما ان الاسلحة البيولوجية والكيميائية ليست من ألاسلحة الحركية ولكن يبدو ان محكمة العدل الدولية(ICJ) اكدت في قضية الانشطة العسكرية وشبه العسكرية (نيكارغوا ضد الولايات المتحدة) بأنه متى ما إتخذ التدخل شكل إستخدام أو التهديد بإستخدام القوة فإن قاعدة عدم التدخل الواردة في القانون الدولي العرفي تتطابق مع المادة (2) فقره (4) من ميثاق الأمم المتحدة[15]

وقد تعاملت ضمنا على أنها استخدام للقوة حيث كلما زاد فاعلية سلاح جديد مقارنه بالسلاح التقليدي زاد احتمال ان يكون استخداما للقوه او هجوما مسلحا ليست تسميه الجهاز (الكومبيوتر) أو الوسيلة المستخدمة كافية لاعتبار قوه او سلاحا بل ان القصد من الاستخدام هو التأثير الذي يعد نقطة الالتقاء ما بين الهجوم السيبراني والقوة العسكرية حيث ان استخدام أي جهاز أو عدد من الاجهزة مما يؤدي الى خسائر كبيرة في الارواح أو تدمير كبير للممتلكات ينبغي عده مستوفيا لشروط الهجوم المسلح**[16]** وعده مستوفيا للشروط لانه قام بخسائر كبيره وتدمير للممتلكات واصبح ذو اثر على المجتمع كما ذكر دينشتاين[17] في كتابه (الحرب والعدوان

[13] مصطفى احمد ابو الوفاء، المبادئ العامة في القانون الدولي المعاصر، إشراك للطباعة والنشر، مصر، 2006 ، ص260.

[14] Miranda Grange, (Cyber Warfare and the Law of Armed Conflict), Research Paper, Faculty of Law, Victoria University of Wellington, 2014, P1.

[15] ICJ, Military and paramilitary activities in and against Nicaragua (Nicar .v. U.S.), 1986, ICJ. 14, (June 27), para. 209

[16] Priyanka R. Dev, (Use of Force and Armed Attack) Thresholds in Cyber Conflict; The Looming Definitional Gaps and the Growing Need for Formal U.N. Response, Texas International Law Journal, Vol. 50, Issue 2, 2015, P380.

[17] دينشتاين: هو باحث إسرائيلي واستاذ فخري في جامعه تل ابيب مختص في القانون الدولي ومرجع بارز في قوانين الحرب خريج جامعه نيويورك ولد في 2 يناير 1936

والـدفاع عـن الـنفس) ان الاضـرار الناجمـة عـن الهجمـات السـيبرانية كفيلـة بـأن تجعـل الهجـوم الالكترونـي يرتقـي بمسـتوى الهجـوم المسـلح حيـث ان الوفيـات الناجمـة عـن تعطيـل أنظمـة دعـم الحيـاه التـي يـتحكم فيهـا جهـاز الحاسـوب و انقطـاع التيـار الكهربـائي بشـكل تـام وكـذلك تعطيـل أجهـزة الحاسـوب التـي تـتحكم فـي محطـات الميـاه والسـدود ممـا ينـتج عنـه فيضـانات فـي المنـاطق المأهولـة بالسـكان دليـل كـافي لاعتبـار الهجـوم السـيبراني قـوة وعـدوان حيـث ان بعـض البـاحثين يؤكـدون أن اسـتخدام شـبكة الكمبيـوتر فـي الهجـوم يشـكل اسـتخدام للقـوة (قـوه مسـلحه) فـي حـين أن الـبعض الاخـر يـذهب إلـى أن الهجـوم لـه تـأثير غيـر قسـري ويقصـد بـه لا يوجـد اكـراه فـي الهجوم حيث نصت المادة 2(4) من ميثاق ألامم المتحدة على أنه:

(يمتنـع أعضـاء الهيئـة جميعـا فـي علاقـاتهم الدوليـة عـن التهديـد باسـتعمال القـوة أو اسـتخدامها ضـد سـالمة الاراضـي أو الاستقلال السياسي لاية دولة أو على أي وجه آخر لا يتفق ومقاصد الامم المتحدة)

المعنـى العـادي لمصـطلح (القـوه) واسـع و يشـمل المفـاهيم التقليديـة للهجمـات الحركيـة، فضـلا عـن غيرهـا مـن التـدابير القسـرية التـي تحتـوي علـى الاكـراه علـى سـبيل المثـال: الادوات الماليـة أي مـنح أو حجـب التسـامح أو المهـل للمطالبـة بالـديون للمنتفعـين؛ ألادوات الدبلوماسـية أي التفـاوض والـدعوة بـين ممثلـي الدولـة ألادوات ألايديولوجيـة أو الدعائيـه إي نشـر علامـات ورمـوز مختـارة بعنايـة لقطاعـات المجتمـع ذات الصـلة مـع تخصيصـها للتـأثير علـى النخبـة الحاكمـة [18] بموجـب قـراءة مفهـوم (القـوة) فـأن كـل هـذه ألادوات العسـكرية، الاقتصـادية، الدبلوماسية وألايديولوجية قد تكون خاضعة للتنظيم بموجب الميثاق.

مـع ذلـك، فـي ضـوء (الهـدف والغـرض) مـن الميثـاق، فـأن (القـوة) يجـب أن تقـرأ بصـورة أكثـر ضـيقا إذ أن الهـدف الصـريح مـن ميثـاق ألامـم المتحـدة هـو الحفـاظ علـى السـلم وألامـن الـدوليين، فضـلا عـن (أن ننقـذ ألاجيـال القادمـه مـن الحـرب) ويـوحي مفهـوم القـوة فـي عـام 1945 اقتصـاره علـى المفهـوم العسـكري فقـط. حيـث أن تـاريخ صـياغة الميثـاق يعـزز هـذا الاسـتنتاج، فخـلال ألاعمـال التحضـيرية قـدم اقتراحـا لتوسـيع نطـاق المـادة 2(4) إلـى المفـاهيم الاسـتراتيجية ألاخـرى تحديـدا إلاكـراه الاقتصـادي الا أن ألامـم المتحـدة رفضـت مثـل هـذا الاقتـراح [19] فمـن خـلال اسـتبعاد صـراحة إلاكـراه الاقتصـادي مـن تعريـف القـوة فـي صـياغة المـادة 2(4) هنـاك إقـرار ضـمني بـرفض الادوات إلايديولوجية والدبلوماسية كذلك.

أن الاسـلحة إلالكترونيـة هـي متعـددة ويمكـن أن تكـون إمـا ممثـل مسـاعد فـي مسـرح الصـراع أو الحـدث الرئيسـي فهـي ليسـت أسـلحة متجانسـة إضـافة إلـى ذلـك أن آلاثـار الضـارة الناجمـة عـن الهجمـات إلالكترونيـة لا تعـد ولا تحصـى ألامـر الـذي يجعـل تصـنيفها علـى حـد سـواء أكثـر تعقيـدا وأكثـر ضـرورة فـي الحقيقـة وذلـك لان آثـار الهجمـات إلالكترونيـة يمكـن أن تتـراوح (مـن إزعـاج بسـيط) مثـل هجـوم دوس (DDoS)[20] الـذي يعطـل حركـة المـرور علـى الشـبكة مؤقتـا إلـى (التـدمير المـادي) مثـل تغييـر ألاوامـر لمولـد الطاقـة الكهربائيـة ألامـر الـذي يـؤدى إلى انفجارها

[18] Michael Gervais, Cyber Attacks and the Laws of War,p.511.

[19] Michael Gervais, Cyber Attacks and the Laws of War,p.512.

[20] DDOS: يقصد به هجمات حجب الخدمه الموزعه

وحتـى المـوت مثـل تعطيـل خطـوط الطـوارئ الاول للمسـتجيبين بحيـث لا يمكـن إجـراء مكالمـات للشـرطة أو خـدمات الإسـعاف وأن التعامـل مـع مختلـف أشـكال الهجمـات الالكترونيـة بمثابـة اسـتخدام القـوة يتطلـب قـراءة واسعة للمادة 2(4) يتضمن الضرر غير المادي.

فـي الحقيقـة، توجـد العديـد مـن النمـاذج الممكنـة لتحديـد مـا إذا كـان الهجـوم الالكترونـي يرتفـع إلـى مسـتوى القـوة الـنهج ألاول فـي تحليـل القـوة هـو فحـص طريقـة التسـليم أو ألالقـاء فبموجـب هـذا النمـوذج يـتم تصـنيف ألاسـلحة إلالكترونيـة مـن خـلال طريقـة محـددة لتقـديم هجـوم علـى العـدو سـواء كـان هـو فيـروس، دودة، اقتحـام الشـبكة، أو بعـض الهجمـات إلالكترونيـة ألاخـرى فحظـر هـذا النمـوذج للهجمـات الالكترونيـة يكـون علـى أسـاس كيفيـة تنفيـذها. فالاضـرار الجسـيمة التـي يمكـن ان تسـببها أنـواع معينـة مـن الهجمـات الاكترونيـة فـي جميـع أنحـاء العـالم بالمقارنـة مـع آثـار محـدودة لهجمـات اخـرى يـوفر ألاسـاس لهـذا الـنهج اذ هنـاك اسـلحة الكترونيـة معينـة هـي بطبيعتهـا أكثـر تدمير وخطورة [21]

الـنهج الثـاني لتحليـل القـوة ينظـر الـى الاسـلحة إلالكترونيـة بموجـب نمـوذج صـارم للمسـؤولية بموجـب هـذا الـنهج فـأن أي اسـتخدام للهجمـات إلالكترونيـة ضـد البنـى التحتيـة الحرجـة يكـون أو يمثـل القـوة، حيـث يـؤذن بالـدفاع عـن الـنفس ضـد الهجمـات إلالكترونيـة التـي تسـتهدف البنيـة التحتيـة الحيويـة ويجـادل أنصـار المسـؤولية الصـارمة بأنـه النمـوذج المناسـب بسـبب الطبيعـة المـدمرة آلانيـة للهجمـات إلالكترونيـة والتـي تخلـق مسـتوى كـاف مـن ضـرر تبـرر الدفاع عن النفس الاستباقي.

أمـا الانتقـادات التـي وجهـت الـى هـذا النمـوذج أن آثـار الهجمـات الالكترونيـة قـد تكـون عشـوائية وغيـر منضـبطة، كما أنها لا تستهدف دائما وعمدا البنية التحتية الحيوية التي قد تتعطل في النهايه بأعتبارها نتيجة ثانويه [22]

المـنهج الثالـث لتحليـل القـوة يتنـاول الهجمـات إلالكترونيـة كـأدوات تعـادل الأسـلحة الحركيـة التقليديـة وذلـك مـن خـلال النظـر إلـى النتـائج المباشـرة للهجـوم فـأذا كانـت النتيجـة تـؤدي الـى حظـر اسـتخدام القـوة التـي تسـببها اسـلحة حركيـة معينـة، فيجـب أن ينظـر الـى الاسـلحة إلالكترونيـة بطريقـة مماثلـة. لـذلك، فـأن فـالهجوم إلالكترونـي هـو استخدام للقوة إذا كان المهاجم يسعى إلى إحداث دمار مادي مباشر أو إلاصابة أو الوفاة [23]

الخلـل فـي هـذا المـنهج هـو أن معظـم الهجمـات إلالكترونيـة لا تسـبب أضـرارا ماديـة مباشـرة أو المـوت، علـى سـبيل المثـال، الهجـوم الـذي يـؤدي الـى اغـلاق مؤقـت لخطـوط الاتصـال بشـرطة الطـوارئ وخـدمات الاسـعاف قـد لا يسـبب ضـرر مـادي أو حالـة وفـاة مباشـرة ولكـن يمكـن بسـهولة أن تسـبب ذلـك بشـكل غيـر مباشـر علـى حـد سـواء' لـذلك أن رسـم خـط بـين الاثـار المباشـرة وغيـر المباشـرة لهجـوم إلالكترونـي هـو صـعب جـداً يفتـرض النمـوذج الـذي حقق عنصر

جـذب مـن قبـل فقهـاء القـانون "شـميت" ينـادي بـالنهج القـائم علـى النتيجـة هـذا الاطـار يتطلـب فحـص مـا إذا كانـت النتـائج المتوقعـة إلـى حـد معقـول مـن الهجـوم الالكترونـي تشـبه عواقـب شـن الهجـوم التقليـدي ام لا. يـوفر "شـميت" سـتة معـايير لتقيـيم عواقـب الهجمـات الالكترونيـة علـى الدولـة المسـتهدفة: الشـدة، الفوريـة، القابليـة للقيـاس،

[21] Michael Gervais, Cyber Attacks and the Laws of War,p.512.
[22] Michael Gervais, Cyber Attacks and the Laws of War,p.512.
[23] Michael Gervais, Cyber Attacks and the Laws of War,p.510

المباشرة، الغزو، والشرعية المفترضة اذ أسهم الهجوم الالكتروني بقواسم مشتركة كافية بين العوامل الستة حيث له ما يبرره من تمديد الحظر المفروض على القوة فبموجب معايير (شميت) أن شدة هذا الهجوم الالكتروني لا يرقى الى القوة بينما كانت الهجمات الاكترونية الفورية وكانت النتائج ضئيلة لا سيما اذا لم يكن هناك أي ضرر مادي أو معاناة للقياس وانما تسبب هذه الاضطرابات في الغالب إزعاج مؤقت على سبيل المثال، تعرضت دولة إستونيا وهي إحدى جمهوريات الإتحاد السوفيتي السابق عام 2007 الى هجوم سيبراني واسع، أدى الى شل نشاط الدولة بالكامل وقد إستمر هذا الهجوم لمدة ثلاثة أسابيع تم خلالها إستهداف المواقع الإلكترونية الحكومية والبنوك والبنى التحتية مما أدى الى شلل تام في الخدمات الإلكترونية والأنظمة البنكية[24] ومن الجدير بالذكر إن إستونيا تعد من أوائل الدول المتقدمة في تكنولوجيا المعلومات ومع ذلك وقفت عاجزة أمام هذا الهجوم العنيف، الذي يجمع الخبراء بأنه يكاد يكون الهجوم السيبراني الأول الذي يتم على هذا المستوى مسبباً خسائر بعشرات الملايين من الدولارات إضافة الى شل البلاد[25] تعطل حركة المرور التي سببها هجوم ذي صلة غير مباشرة لتأثير قسري نتيجة قرار الحكومة الاستونية لازالة التمثال فعلى الرغم من أن هذا الهجوم يعتبر تدخلا غير شرعي، إلا أن النتائج الصافية لا تشبه بما فيه الكفاية لكونها قوة.

المطلب الثاني: الهجمات السيبرانيه بأعتبارها (هجوم مسلح)

عندما يكون هنالك صراع بين الدول يطالب ميثاق الامم المتحدة من اعضائه تسوية منازعاتهم الدولية بالوسائل السلميه على وجه لا يجعل السلم وألامن الدوليتين عرضة للخطر [26]. وبالتالي فإن سلطة الدولة بأستخدام القوة تنبع سواء من مجلس ألامن أو من خلال حق الدولة في التصرف دفاعا عن النفس الفردي أو الجماعي.

سؤالنا هنا هو ما إذا كانت الهجمات الالكترونية يمكن أن تصل إلى عتبة (الهجوم المسلح) الذي يقوم بتشغيل الحق في الدفاع عن النفس بموجب المادة 51 من الميثاق وهو الاستثناء على تحريم اللجوء إلى التهديد أو استخدام القوة والتي تنص على ما يلي:

"ليس في هذا الميثاق ما يضعف أو ينتقص الحق الطبيعي للدول فرادى أو جماعات، في الدفاع عن أنفسهم إذا اعتدت قوة مسلحة على أحد أعضاء "ألامم المتحدة" وذلك إلى أن يتخذ مجلس ألامن التدابير اللازمه لحفظ السلم والامن الدولي"[27]

حيث يرى بعض الفقهاء أن أي استخدام للقوة من جانب القوات المسلحة النظامية يشكل هجوم مسلح في حد ذاته. فبموجب هذا الرأي، يعتبر أي عمل هجومي من قبل وحدة الانترنت العسكرية هو هجوم مسلح لانها تتبع من القوات المسلحة للدولة. مما تجدر الاشارة اليه في هذا الخصوص أنه في الولايات المتحدة، الصين، إيران، إسرائيل والدول ألاخرى في جميع أنحاء العالم قد تم أنشاء بالفعل وحدة الانترنت العسكريه لذلك ينظر

[24] محمد علي رعايت كنده فلاح، مصدر سابق، ص74

[25] المصدر نفسه ، ص76

[26] المادة 2 (3) من ميثاق الامم المتحدة.

[27] انظر في ذلك أيضا نص الماده (42-7) من معاهدة لشبونة في 13كانون الاول عام 2007 هو نص الاتحاد الاوروبي في المادة42_7 ،كذلك الحال بالنسبة الى حلف شمال الاطلسي في 4 نيسان 1949 ايضا في دليل تالين القاعدة 16

الـى ألاعمـال الهجوميـة مـن قبـل تلـك الوحـدات علـى الانترنـت فـي حـد ذاتـه بمثابـة هجـوم مسـلح الـذي يطلـق الحـق في ممارسة الدفاع عن النفس الفردي أو الجماعي [28]

بينمـا يـرفض آخـرون هـذا الـنهج فـي حـد ذاتـه مسـتندين الـى اختبـار محكمـة العـدل الدوليـة الـذي يقـوم علـى النطـاق والاثـار وأعتبـاره المعيـار ألانسـب لتحديـد متـى يـتم تشـغيل المـادة 52حيـث تـرى بـأن هنـاك تمييـز جـوهري بـين اسـتخدام القـوة والهجـوم المسـلح ففـي القضـية المعنونـة الانشـطة العسـكرية وشـبه العسـكرية فـي نيكـاراغوا وضدهـا بـين نيكـاراغوا والولايـات المتحـدة فـي 27 حزيـران عـام 1986 حيـث حـددت محكمـة العـدل الدوليـة الفـرق فـي المقـام الاول علـى أسـاس النطـاق والاثـار هكـذا قـررت أنـه لـيس كـل اسـتخدام للقـوة يبـرر ممارسـة حـق الـدفاع عـن الـنفس مـن جانـب واحـد [29]بغـض النظـر عـن حجـم أو تـأثير الهجـوم سـواء كـان حركـي أو الكترونـي، فـأن نـوع السـلاح المسـتخدم هنـا فـي الهجـوم المسـلح هـو سـلاح غيـر مـادي فعنـدما تسـتخدم الهجمـات الالكترونيـة لـدعم القـوات التقليديـة تعتبـر اسـلحة وبالتـالي يجـب أن يـنظم اسـتخدامها ويـدعم هـذه التصـريحات رأي محكمـة العـدل الدوليـة فـي 8 تمـوز 1996بعنـوان مشـروعية التهديـد أو اسـتخدام الاسـلحة النوويـة حيـث توضـح الفقـرة 10 أن الحظـر العـام لاسـتخدام القـوة التـي يسـنها ميثـاق ألامـم المتحـدة لا يخـل بأسـتخدام ألاسـلحة الخاصـة وينطبـق علـى أي استخدام للقوة بغض النظرعن ألاسلحة المستخدمة [30]

وهكـذا يمكننـا أن نقـدر أن الهجمـات الالكترونيـة قـد تـأتي ضـمن اسـتخدام القـوة بـالمعنى المقصـود فـي المـادة2 (4) مـن ميثـاق الامـم المتحـدة شـرط أن آثـار هـذه الهجمـات قابلـة للمقارنـة مـن حيـث الفتـك والـدمار مـع تلـك الناجمـة مـن هجوم تقليدي أو نووي أو بيولوجي أو كيميائي [31]

يعـرف القـانون الـدولي الإنسـاني الهجمـات علـى أنهـا أعمـال العنـف ضـد الخصـم سـواء تـم القيـام بهـا علـى سـبيل الهجـوم أو الـدفاع وبغـض النظـر عـن المنطقـة التـي تنفـذ فيهـا مثـل تلـك الأعمـال[32] تكمـن القاعـدة الأساسـية التـي تحكـم الهجمـات فـي أنـه يجـب علـى أطـراف النـزاع أن تميـز دومـا بـين السـكان المـدنيين والمقـاتلين وبـين الأعيـان المدنيـة والأهـداف العسـكرية ويجـوز لأطـراف النـزاع توجيـه عملياتهـا ضـد الأهـداف العسـكرية دون غيرهـا، وبالتـالي يحظـر شـن الهجمـات العشـوائية [33] ويـنص القـانون الإنسـاني علـى أن القـادة العسـكريين تترتـب علـيهم مسـؤولية اتخـاذ تـدابير وقائيـة عنـد الإعـداد للهجمـات وتنفيـذها بغـرض الحـد مـن آثارهـا الضـارة المحتملـة والتأكـد مـن عـدم شـنها بطريقـة عشـوائية (وأن تكـون الأضـرار علـى المـدنيين متناسـبة مـع مـا ينتظـر أن يسـفر عنـه الهجـوم من ميزة عسكرية ملموسة ومباشرة [34]

امـا دليـل تـالين فيـنص علـى أن العمليـات الالكترونيـة تشـكل اسـتخدام القـوة حينمـا يكـون مسـتواها الدرجـة /عتبـة الشـدة وآثارهـا مقارنـة مـع العمليـة التقليديـة ليسـت الالكترونيـة قـد وصـلت إلـى مسـتوى مـن توظيـف القـوة ويركـز

[28] Michael Gervais, Cyber Attacks and the Laws of War, p.542.
[29] Ibid, p.542
[30] أكد مجلس الامن هذا الرأي عندما أذن الولايات المتحدة للرد بقوة في الدفاع عن النفس لهجمات 9/11،حيث كانت "أسلحة" الطائرات المختطفة
[31] Laurn Baudin , Les cyber - attaques dans les conflits armé: qualification juridique, imputabilité et moyens de réponse envisagés, L'Harmattan,Paris, 2014,p.021.
[32] المادة 49-1, البروتوكول 1
[33] المادة 48 من البروتوكول 1، والقواعد 7 و11 - 13 من القانون الدولي الإنساني العرفي في دراسة اللجنة الدولية للصليب الأحمر
[34] المادتان 57 و58 من البروتوكول 1، والقواعد 14-24 من دراسة القانون الدولي الإنساني العرفي للجنة الدولية للصليب الأحمر

التحليـل علـى العوامـل الكميـة والنوعيـة.[35] امـا المؤشـرات التـي تسـمح بوصـف العمليـة إلالكترونيـة باعتبارهـا استخدام للقوة فهي شدة الضرر, الفورية , السبب والنتيجة, درجة الغزو التغلغل في النظام, تقييم آلاثار, الطابع العسكري , مشاركة الدولة بالاضافة الى قرينة الشرعية [36]كما تنص القاعدة رقم 13 من دليل تالين:

"الدولـة التـي تكـون هـدف فـي عمليـة الكترونيـة بمسـتوى مماثـل لتلـك التـي تنـدرج تحـت هجـوم مسـلح لـديها القـدرة علـى ممارسـة حقهـا الاصـيل فـي الـدفاع عـن الـنفس والحقيقـة أن العمليـة الالكترونيـة يمكـن أن تصـنف علـى أنهـا هجوم مسلح لا يتوقف فقط على حجمها ولكن أيضا الاثار التي تنتجها".[37]

ولقـد اكـدت الولايـات المتحـدة الامريكيـة هـذا المنظـور عـام 2003 حيـث اعترفـت بضـرورة وقايـة وحمايـة أنظمـة الكمبيـوتر مـن تهديـدات وشـيكة واصـفة أجـزاء رئيسـية مـن الفضـاء الالكترونـي بأعتبارهـا تمثـل البنـى التحتيـه الوطنيـه الحساسـه [38] فـأذا كـان هـدف الهجـوم الالكترونـي هـو أحـداث ضـرر للبنيـة التحتيـة الحرجـة هـدف حيـوي فهذا يبرر اتخاذ تدابير للدفاع عن النفس.

يتبـين لنـا إن أعمـال العنـف المسـلح يحكمهـا أمـرن[39]: فهـي إمـا أن تكـون: مباشـرة وتـؤدي بطبيعتهـا الـى إلحـاق أذى مـادي بالأعيـان العسـكرية والمدنيـة أو غيـر مباشـرة أي تلحـق الأذى بعـد وقـوع الهجـوم أيـاً كانـت الوسـيلة أو الطريقـة. وعلـى وفـــق ذلـك فـإن التركيـز علـى آثـار النشـاط السـيبراني وجسـامته سـيبين إن وصـف الهجـوم متحقق فيـه علـى سـبيل المثـال عنـدما تتعـرض الحواسـيب أو الشـبكات فـي دولـة مـا للهجـوم السـيبراني فقـد يـؤدي ذلـك الـى حرمـان المـدنيين مـن الإحتياجـات الأساسـية كميـاه الشـرب والرعايـة الطبيـة والكهربـاء. ويمكـن أن تتـدخل النشـاطات السـيبرانية فـي تعطيـل خـدمات إنقـاذ الأرواح كالمستشـفيات أو أن تعطـل البنـى التحتيـة الحيويـة مثـل السـدود والمفـاعلات النوويـة وأنظمـة الـتحكم فـي الطـائرات وجـراء كـل هـذا قـد يتضـرر مئـات الآلاف مـن السـكان [40] فهـذه النشـاطات وعلـى وفـق جسـامتها وآثارهـا سـواء المباشـرة منهـا او غيـر المباشـرة تعـد هجومـاً سـيبرانياً أي ينطبق عليها وصف (الهجوم).

المبحث الثاني: التمييز بين الهجمات السيبرانيه والجريمة السيبرانيه والحرب السيبرانيه

لا شـك بـأن هنـاك فـرق بـين مصـطلح الهجمـات السـيبرانيه والجريمـة السـيبرانية والحـرب السـيبرانيه الـذي كثيـرا مـا يـتم الخلـط بينـهم مـن قبـل المهتمـين فـي هـذا المجـال. الخلـط بـين هـذه المصـطلحات يـؤدي الـى خلـق مشـكلة جديـدة قـد

[35] دليل تالين القاعده 95

[36] هذه النقاط التي اقترحها SCHMITT. N Michaël سابقا في تحليله للعمليات االالكترونية ،
.أنظر كتاب:
,Laurn Baudin , Les cyber op.cit,p332
.imputabilité et moyens, 2014,p. 021

[37] Laurn Baudin , Les cyber .op.cit.p.121-122

[38] هي مجموعة من المؤسسات العامة والخاصة في مجموعة متنوعة من القطاعات التي لا غنى عنها لبقاء البلد. فعلى سبيل المثال في الولايات المتحدة البنى التحتية الحساسة لا تقابل فقط البنية التحتية المادية ولكن أيضا الالكترونية امدادات المياه والصحة العامة، وتشمل الاتصالات،الطاقة ،المالية ،المصرفية ،النقل كل هذا هو عام أو خاص.

[39] احمد عبيس الفتلاوي، مصدر سابق، ص7.

[40] لوارن جيزيل،ماهي القيودالتي يفرضها قانون الحرب على الهجمات السيبرانية،اللجنة الدولية للصليب الاحمر، 28/6/2013. متاح على الموقع الرسمي:(أخر زيارة بتاريخ 5/8/2021)
.warefare-https://www.ICrc.org.Cyber

تـؤدي الـى خـرق القـانون الـدولي فيمـا لـو ان الدولـة المعتـدى عليهـا قـد تصـرفت بغـض النظـر عـن تحديـد نـوع الاعتـداء هـل هـو هجـوم سـيبراني أم جريمـة سـيبرانية ام حـرب سـيبرانيه ؟ حيـث أن حـق الدولـة المعتـدى عليهـا فـي الهجـوم السـيبراني يكـون مختلـف عـن حقهـا فـي الـرد علـى الجريمـة السـيبرانية والحـرب السـيبرانيه فيمـا يـأتي مـن هـذا المطلـب سـنحاول توضـيح أوجـه التمييـز بـين الهجمـات السـيبرانيه والجريمـة السـيبرانيه والحـرب السـيبرانيه من خلال هذا المطلب على شكل فرعين كما موضح ادناه

المطلب الأول: التمييز بين الهجمات السيبرانيه والجرائم السيبرانيه

ان الهجـوم السـيبراني كمـا ذكرنـا سـابقاً هـو عبـاره عـن التصـرفات الإلكترونيـة التـي تتسـبب فـي قتـل أو دمـار أو أضـرار ماديـة تقـوم بهـا دولـة أو مجموعـة مسـلحة ضـد دولـة أخـرى , بينمـا الجريمـة السـيبرانية تشـمل مجـالاً أوسـع بكثيـر مـن ذلـك أي تتضـمن كـل النشـاطات الإلكترونيـه غيـر القانونيـة بمـا فـي ذلـك "إسـتخدام الوسـائل المعتمـدة علـى الكمبيـوتر لإرتكـاب أعمـال غيـر قانونيـة فـي التشـريعات الوطنيـة" [41] ان الحداثـة التـي تتميـز بهـا الجريمـة السـيبرانيه وإخـتلاف الانظمةالقانونيـة والثقافيـة بـين الـدول أدت الـى عـدم الإتفـاق علـى تعريـف موحـد لهـذا الـنمط مـن الجـرائم خشـية حصـرها فـي مجـال ضـيق[42] لـذلك ظهـرت عـدة إتجاهـات فـي تعريـف الجريمـة السـيبرانية فمـن الفقهـاء مـن إعتمـد علـى وسـيلة إرتكـاب الجريمـة كأسـاس لتعريفـه وهـذا مـا ذهـب اليـه مكتـب تقيـيم التقنيـة فـي الولابـات المتحـدة (OTA) إذ عرفهـا بأنهـا "الجـرائم التـي تـؤدي فيهـا البيانـات الكمبيوتريـة والبـرامج المعلوماتيـة دورا رئيسـيا" [43] كماعرفـت بأنهـا: الجـرائم التـي يسـتخدم فيهـا الحاسـوب وشـبكاته العالميـة كوسـيلة مسـاعدة لإرتكـاب الجريمـة كإسـتخدامه فـي النصـب والإحتيـال وغسـل الأمـوال وتشـويه السـمعة والسـب[44] وتعـرف كـذلك بأنهـا:"أي جريمـة سـاعدت أو ارتكبـت عـن طريـق إسـتخدام الكمبيـوتر والشـبكة والأجهـزة الصـلبة"[45] هـذا الإتجـاه انتقـد لأنـه لا يمكـن إعتبـار الجريمـة سـيبرانية لمجـرد إسـتخدام الحاسـب الآلـي فـي إرتكابهـا بـل لابـد مـن الرجـوع الى العمل الأساسي المكون لها والنية الاجرامية الداخلة فيها [46]

وقـد ذهـب عـدد مـن الفقهـاء الـى الأخـذ بمبـدأ شخصـية المجـرم، أي: إعتمـدوا علـى أسـاس تـوافر المعرفـة بتقنيـة المعلومـات فـي تعـريفهم للجريمـة السـيبرانية كـالتعريف الصـادر عـن وازرة العـدل الأمريكيـة حيـث عرفتهـا بأنها:"أيـة جريمـة لفاعلهـا معرفـة فنيـة بتقنيـة الحاسـبات تمكنـه مـن إرتكابهـا ". ولكـن يتضـح قصـور هـذا الإتجـاه في عدم إهتمامه بتوافر العناصر الأخرى في تصنيف الجريمة[47]

---

[41] Oona Hathaway, op .cit , p.834.

[42] محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية ،2004، ص43.

[43] محمد عبيد الكعبي، الجرائم الناشئة عن إستخدام غير المشروع لشبكة الإنترنت، دار النهضة العربية القاهرة، دون سنة طبع، ص 33.

[44] مصطفى محمد موسى،التحقيق الجنائي في الجرائم الإلكترونية ،ط أولى، مطابع الشرطة، القاهرة 2009، ص 112

[45] Sarah Gorden & Richard Ford, on the Definition and Classification of Cybercrime , 27. Computer Virology 13, 13 (2006), Note 64, p. 14.

[46] غازي عبد الرحمن هيان الرشيد، الحماية القانونية من جرائم المعلوماتية (الحاسب والإنترنت) إطروحة مقدمه الى مجلس كليه الحقوق، الجامعة الإسلامية في لبنان ،كلية الحقوق،2004،ص 107

[47] محمد عبيد الكعبي، مصدر سابق، ص 34

وقـد إعتمـد بعضـهم علـى موضـوع الجريمـة كأسـاس لبيـان مفهـوم الجـرائم السـيبرانية ومـن أشـهر مؤيـدي هـذا الإتجـاه الفقيـه روزنـبلات(Rosenblatt) الـذي عرفهـا بـالقول: "نشـاط غيـر مشـروع موجـه لنسـخ أو تغييـر أو حذف أو للوصول الى المعلومات المخزنة داخل الحاسب أو التي تحول عن طريقه"[48]

ويـرى أصـحاب هـذا الإتجـاه بـأن الجريمـة السـيبرانية لا يشـترط أن يكـون النظـام المعلومـاتي أداة إرتكابهـا، بـل هي التي تقع عليه أو في نطاقه"[49]

وهنـاك إتجـاه أخيـر عمـد أصـحابه الـى تعريـف الجريمـة السـيبرانية عـن طريـق دمـج أكثـر مـن أسـاس لوضـع تعريـف شـامل لهـا ليتضـمن كافـة أركانهـا، فتوسـع مؤيـدي هـذا الإتجـاه فـي تعـريفهم للجريمـة السـيبرانية فـذهبوا بـالقول بأنهـا: "هـي الجريمـة التـي يسـتخدم فيهـا الحاسـب الآلـي كوسـيلة أو أداة لإرتكابهـا أو يمثـل إغـراءاً بـذلك، أو جريمة يكون الحاسب الآلي نفسه ضحيتها" [50]

فممـا سـبق يتضـح إن الجريمـة السـيبرانية لا تشـمل فقـط الجـرائم التـي ترتكـب عـن طريـق الكمبيـوتر بـل تشـمل أيضـاً أيـة جريمـة تتضـمن إسـتخدام أو إسـتهداف الكمبيـوتر[51] ومـمـا يؤيـد هـذا الإتجـاه مـا جـاء فـي إرشـادات الإسـكوا[52](ESCWA) للتشـريعات السـيبرانية فـي بيـان مفهـوم الجريمـة السـيبرانية إذ ذهـب إلـى "إن الجريمـة السيبرانية تنقسم على نوعين أساسيين:

النـوع الأول هـو الـذي يكـون فيـه الحاسـوب أداة تنفـذ بواسـطتها الجريمـة والنـوع الثـاني هـو الـذي يكـون فيـه جهـاز الحاسـوب وشـبكات الحواسـيب وبرامجهـا موضـوعا للجريمـة، أي: إن الفعـل الجرمـي إرتكـب علـى هـذا الجهـاز" [53]

وقـد ترتكـب الجريمـة السـيبرانية لعـدة أغـراض كتحقيـق مكاسـب ماديـة معينـة أو لإثبـات الفاعـل لمهارتـه الفنيـة وقدرتـه علـى إختـراق أجهـزة الحاسـب أو بهـدف التسـلية والترفيـه أو لمجـرد الرغبـة فـي الإضـرار بـالغير[54]ومـن أمثلـة الجـرائم السـيبرانية الممارسـات الإحتياليـة علـى الإنترنـت مشـاركة الصـور الإباحيـة لأطفـال وتخزينهـا علـى الكمبيوتر, القـذف والسـب عبر الوسائل الإلكترونية وغيرها من النشاطات المخالفة بموجب القوانين الوطنية.

---

[48] غازي عبد الحمن هيان الرشيد، مصدر سابق، ص 106

[49] أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي الإسكندرية، ط ثانية ،2006، ص 85-86.

[50] غازي عبد الرحمن هيان الرشيد، مصدر سابق ص 108

[51] Debra Little John Shinder, sence of the Cybercrime: computer forensics Handbook, 16

[52] و هي اللجنة الإقتصادية و الإجتماعية لغرب آسيا و هي جزءاً من الأمانة العامة لأمم المتحدة تعمل بإشراف المجلس الاقتصادي والإجتماعي،تأسست إبتداء بعنوان اللجنة الاقتصادية لغرب آسيا في9آب 1973بموجب قرارالمجلس الاقتصادي والإجتماعي1818(د-55)وأعيد تتسميتها من قبل المجلس نفسه بموجب القرار1985/69الصادر في تموز1985فأصبحت اللجنة الاقتصادية والإجتماعية لغربي اسيا و تتخذ بيروت مقرا دائما لها،من أهدافها تحفيز التنمية الاقتصادية والإجتماعية في الدول الأعضاء وتعزيز التعاون بينهم، و تحقيق التكامل الإقليمي بين المنطقة العربية و المناطق الأخرى . تتألف من 18 بلدا عربيا في منطقة غرب آسيا.

[53] إرشادات الإسكوا للتشريعات السيبرانية ،مشروع تنسيق التشريعات السيبرانية لتحفيز مجتمع المعرفة في المنطقة العربية ،بيروت ،2012،ص 117

[54] محمد علي قطب، الجرائم المعلوماتية وطرق مواجهتها، الأكاديمية الملكية للشرطة، البحرين 2010، متوفر على الموقع:(أخر زيارة بتاريخ 2021/5/3http://www.policemc.gov.bh/mcms-store/pdf

إن الجـرائم السـيبرانية وإن كانـت تشـترك مـع الهجمـات السـيبرانية فـي البيئـة التـي تحـدث فيـه أي الفضـاء إلا إنهـا تختلـف عنهـا مـن حيـث الأشـخاص والأهـداف فغالبـاً مـا يكـون مرتكبـي الجـرائم السـيبرانية هـــم الأفـراد وتوجـة ضـد مؤوسسـات ماليـة أو شـركات وحتـى أفـراد داخـل أو خـارج إقلـيم الدولـة بخـلاف الهجمـات التـي تـتم مـن قبـل دول أومجموعات حكومية أو غير حكومية ضد دولة أخرى[55]

إن الإخـــتلاف الآخـر يكمـن فـي إن الجـرائم السـيبرانية غالبـاً مـا يكـون الهـدف منهـا تحقيـق مكاسـب شخصـية كسـرقة الملكيـة الفكريـة عـن طريـق شـبكات الحاسـب الآلـي أو التسـلل الـى أنظمـة المصـارف والتلاعـب بأرقـام الحسـابات وتحويـل الأمـوال , بخـلاف الهجمـات السـيبرانية التـي يسـتهدف مرتكبوهـا الأمـن القـومي والسياسـي للدولـة أو يقـوم هـؤلاء بتخريـب الشـبكات التـي تـتحكم بـالبنى التحتيـة الأساسـية فـي الدولـة وتـدميرها بقصـد إرباكهـا وزعزعة النظام فيها لتحقيق أهداف أمنية أو عسكرية أو سياسية[56]

كمـا ان الهجـوم السـيبراني هـو فعـل يقـوض مـن قـدرات ووظـائف شـبكات الحاسـوب مـن أجـل هـدف قـومي أو سياســي مــن خــلال اســتغلال نقــاط الضــعف لــتمكن المهــاجم مــن خــرق الانظمــة والعبــث بهــا. [57] ان الهجــوم الالكترونـي لـه القـدرة علـى اغـلاق أجهـزة الطـرد المركـزي النوويـة والشـبكات الكهربائيـة وأنظمـة الـدفاع الجويـة الـذي يعـد تهديـدا خطيـرا للأمـن القـومي لـذا ينبغـي التعامـل مـع الهجمـات السـيبرانيه بوصـفها أعمـال حـرب لانهـا تشـبه الهجمـات المسـلحة التـي ينظمهـا قـانون الحـرب حيـث يتضـح بـأن الهـدف مـن الهجـوم السـيبراني يعطـي صـورة واضـحة و انــه جــاء مــن نتــاج سياســة الدولــة ولــيس شــخص او جماعــة قرصــنة فــي حــين ان تعريــف الجريمــة السـيبرانية هـي عبـارة عـن مخالفـة ترتكـب ضـد الجماعـات او الاشـخاص بـدافع إجرامـي كالـدخول غيـر المصـرح بـه وإتـلاف البيانـات المخزونـة فـي الأنظمـة او الاعتـراض غيـر القـانوني لهـا عـن طريـق نقلهـا مـن جهـاز حاسـوب الـى جهـاز اخـر كإدخـال بيانـات خاطئـة او العبـث بهـا. كمـا عرفـت بأنهـا" "سـلوك غيـر مشـروع يعاقـب عليـه القـانون ويكون صادر عن أرادة جرمية محله معطيات الحاسوب"[58]

وقـد عـرف الفقيـه الالمـاني(Ulrich Sieber) الجـرائم السـيبرانيه بأنهـا "الاعتـداءات القانونيـة التـي يمكـن ان ترتكـب بواسـطة المعلوماتيـة بغـرض تحقيـق الـربح أضـافه الـى ذلـك يبـدو ان الهـدف مـن الجريمـة السـيبرانية يكـون مختلـف تمامـا عـن الهـدف مـن الهجـوم السـيبراني لان نتيجـة الهجـوم هـي مـن تحـدد مـن يقـف وراءه، حيـث ان" الهجـوم السـيبراني تقـوم بـه دولـة أو منظمـات ارهابيـة مـن أجـل مقتضـيات الامـن القـومي بينمـا الجريمـة السـيبرانية تكـون بعيـدة عـن سياسـة الدولـه ويسـتبعد ان تكـون الدولـة هـي المهـاجم بـل يكـون أشـخاص أو مجـاميع قرصـنة مـن يقوم بتنفيذ الجريمة السيبرانية[59]

لـذلك فـان الهجـوم السـيبراني يكـون مـن ضـمن اختصـاص القـانون الـدولي العـام لانـه يمثـل خـرق لسـيادة الدولـه وفقـا لمبـدأ اقليميـة القـانون. وبالتـالي ان مـا يميـز الهجـوم السـيبراني عـن الجريمـة السـيبرانية هـو ان الهجـوم السـيبراني

---

[55] Oona Hathaway,op.cit , p. mcms 834

[56] Oona Hathaway , op . cit, p.835

[57] Ian Traynor, Russia Accused of Unleashing Cyber War to Disable Estonia, Guardian London, May 17, 2007

[58] د. نائل عبد الرحمن صالح، واقع جرائم الحاسب في التشريع االاردني، مؤتمر القانون والكمبيوتر والانترنيت، كلية الشريعة والقانون، جامعة الامارات العربية المتحدة، الطبعة الثالثة، المجلد الاول, 2004 ,ص 192

[59] د. كامل سعيد ,جرائم الكمبيوتر والجرائم الاخرى في مجال التكنولوجيا, بحث مقدم الى المؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرية, 1993 ،ص516

يهدف الى إضعاف أو تدمير قدرات الدولة من خلال شبكات الانترنت لغرض سياسي أو لمقتضيات الامن القومي وهذا لا نجده في الجريمة السيبرانيه حيث يكون هدفها مقتصر على السرقة من أجل الحصول على منافع مالية او نقدية[60] ففي كلا الحالتين تكون الدولة مسؤولة مسؤولية دولية عن اعمال مواطنيها والتي تسبب ضررا بمصالح الدول الأخرى وهذا ما يؤدي الى الحد من الهجمات السيبرانية.

المطلب الثاني: التمييز بين الهجمات السيبرانية والحرب السيبرانية

يعد مفهوم الحرب السيبرانية (cyber warfare) مفهوم جديد على صعيد النزاعات المسلحة في القرن الحادي والعشرين حيث هذه الحرب تشتمل على أساليب ووسائل قتالية تتألف من عمليات إلكترونية ترقى الى مستوى النزاع المسلح أو تستخدم في سياقه. الحرب السيبرانية هي التدمير الكلي او الاخلال لأنظمة المعلومات والإتصالات التابعة للعدو التي يعتمد عليها لمعرفة نفسه؟ أي من هو أين هو ماذا يفعل ومتى، وماهي التهديدات التي تحتل مركز الصدارة في قائمة أولوياته.؟

وفي الواقع إن الحرب السيبرانية تهدف الى الإخلال بتوازن المعلومات والمعرفة لصالح قوات الدوله لاسيما في غياب التوازن العسكري. وعليه إن إستخدام التفوق العلمي في الحرب السيبرانية سوف يغطي النقص الحاصل في التجهيزات والقوات العسكرية وبالتالي يمكن تحقيق النصر فيه[61]

وتعرف الحرب السيبرانية بأنها استعمال الحواسيب كسلاح أو أداة للقيام بأعمال عنف بقصد ترعيب أو تغيير رأي مجموعة أو دولة ما، ويتم إستخدامه لأغراض أيديولوجية وسياسية عن طريق إستهداف البنى التحتية الحيوية كالطاقة، النقل، الإتصال والخدمات الضرورية كالطوارئ والشرطة[62]

وجاء تعريف الحرب السيبرانية في قاموس جامعة كامبريدج بأنها " أي نشاط يستخدم الإنترنيت لمهاجمة الأجهزة الإلكترونية التابعة لدولة ما وذلك بقصد الإضرار بأشياء كأنظمة الإتصالات والنقل وموارد المياه والطاقة، إن إستخدام الحرب السيبرانية قد يؤدي الى زعزعة إستقرار الأنظمة المالية، نظام الهاتف أو شبكة الكهرباء، وقد يغير الأمن القومي بشكل جذري بسبب هجوم قد يأتي من أي مكان"[63]

وفي مناسبة أخرى عرفت بأنها: "الإستعمال الدفاعي أو الهجومي للمعلومات وأنظمتها بقصد تعريض عناصر المعلومات (المعلومات، العمليات القائمة على المعلومات، الأنظمة المعلوماتيه، شبكات الإنترنت) التابعة للعدو في الفضاء السيبراني للخطر[64] وعرفتها مؤسسة ارند[65](RAND) بأنها: "الحرب السيبرانية

---

[60] د. عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن الانترنيت، دار النهضة العربية، القاهرة، 2004، ص 158.

[61] جنك ودفاع سايبر، مصدر سابق، ص 44

[62] برويز حسيني و حسين ظريف منش، مصدر سابق ،ص 45

[63] تمت زياره الموقع الالكتروني في 3\4\2021 http://dictionary.cambridge.arfare org/us/dictionary/english/cyberwh

[64] كاوه سيد مفيدي ، جنك سايبري ، سكيور تاركيت، مارس/2004 ، ص 7.

[65] مؤسسة ارند أو مؤسسة الأبحاث والتطوير هي منظمة غير ربحية تأسست عام 1948 من قبل شركة طائرات دوغلاس لتقديم تحليلات وأبحاث للقوات المسلحة الأمريكية.

هـي حـرب الـدول والمنظمـات الدوليـة ضـد دول أخـرى مـن أجـل تـدمير شـبكات الكمبيـوتر والمعلومـات وهـذه الحرب تتم عن طريق الفايروسات أحصنة طروادة والبرمجيات الخبيثة الأخرى"[66]

إن الحـرب السـيبرانية لهـا مـن الخصـائص مـا يميزهـا عـن النزاعـات المسـلحة التقليديـة سـواء مـن حيـث ماهيتهـا أم محتواهـا، فـبخلاف النزاعـات المسـلحة التقليديـة لا يمكـن تحديـد وقـت بـدء الحـرب السـيبرانية أو إنتهائهـا، بـل إن فاعليـة الحـرب السـيبرانية تكمـن فـي عـدم إمكانيـة تحديـد وقـت بـدءها إن صـعوبة التوصـل ومعرفـة مصـدر الحـرب السـيبرانية تشـكل عامـل اخـتلاف آخـر وذلـك لعـدة أسـباب منهـا، تعـدد الجهـات الفاعلـة فـي الفضـاء السـيبراني كالدول والمنظمات والجماعات الحكوميه وغير الحكومية والأرهابيين والقراصنة وحتى الأفراد

ممـا سـبق يتضـح لنـا إن الحـرب السـيبرانية وإن كانـت تتفـق كثيـرا مـع الهجمـات السـيبرانية، إلا إن ذلـك لا يعنـي عـدم وجـود مـا يميزهمـا عـن بعـض، فـالحرب السـيبرانية هـي نـوع أو جـزء مـن الهجمـات السـيبرانية التـي تحـدث فـي أثنـاء نـزاع مسـلح دائـر أو التـي تنـتج أثـار ماديـة (أو مايـسمى بالآثـار الحركيـة) تشـبه وتعـادل آثـار الهجمـات المسـلحة التقليديـة. بينمـا الهجمـات السـيبرانية هـي كـل نشـاط إلكترونـي ضـار بالـدول الأخـرى سـواء كـان فـي وقـت السـلم أم فـي أثنـاء نـزاع مسـلح دائـر وسـواء نتجـت عنـه أثـار ماديـة جسـيمة فـي الأرواح أو الممتلكـات أو لـم يـؤدي إلا الـى تشـويش أنظمـة الكمبيـوتر فيهـا مـادام كـان ذلـك لأغـراض أمنيـة وعسـكرية وأحـدث إربـاك فـي عمـل الحكومة التابعة لتلك الدولة.

الخاتمه:

تشكل الهجمات السيبرانيه تهديداً خطيراً للخدمات والبنى التحتيه وتعطيل استخدام الدوله للاليات الإلكترونية في ادارة شؤونها الداخلية، أو تدمير الأجهزة الإلكترونية الخاصة بالأمن القومي للدولة بشكل متسارع مقارنة بالإجراءات الدفاعية لمواجهتها.

وتعتبر الهجمات السيبرانية هي واحدة من أهم التحديات المعاصرة التي تواجه المجتمع الدولي، لما لها من تداعيات على الأمن القومي للدول وتهديدا للسلم والأمن الدوليين.

ومن خلال بحث ودراسه في هذا الموضوع توصلنا الى عدد من الاستنتاجات والمقترحات وعلى النحو التالي:

الاستنتاجات:

1. تكمن الميزة النسبية للهجمات السيبرانية في إنخفاض تكاليفها وسهولة اللجوء اليها إذ لا تتطلب حشوداً من المقاتلين العسكريين والآلاف من الأسلحة والوسائل كالنزاعات المسلحة التقليدية ، بل يكفي لتنفيذها شخص أو مجموعة صغيرة ممن لديهم الخبرة والمهارة في التكنولوجيا السيبرانية وثغرات البرامج والأنظمة الكمبيوترية لإستخدامها ضد دولة أو دول أخرى، إلا إن هذه الميزة تتحول الى مصدر قلق كبير إذا ما نظرنا إلى آثار هذه الهجمات و تبعاتها على السكان المدنيين والبيئة فيما لو تم تنفيذها على منشأة نووية أو مصادر الطاقة كشبكة الكهرباء والمياه.
2. فيما يخص الهجمات السيبرانية التي تحدث في أثناء النزاع المسلح التقليدي فقد أجمع الفقهاء الدوليين على خضوعها للقانون الدولي الإنساني؟ إلا إن التحدي الأكبر هو تلك الهجمات التي تحدث في وقت السلم ومدى إمكانية عدها

---

[66](Cyber Warfare(2015) available at:

http://www.rand.org/topics/cyberwarfare.html تمت زياره الموقع الالكتروني في 3\4\2021

هجوما مسلحا يثير حق الدفاع الشرعي، ومتى تعد خرقا لمبدأ "عدم التدخل" الذي يسمح فقط بإستخدام التدابير المضادة والطرق السلمية الأخرى في مواجهتها.

3. أن تأثير الهجمات السيبرانية تكون بمثابة الهجوم التقليدي (المسلح) لأنهما يحملان ذات الهدف والغاية.

المقترحات:

1. يجب على الدول إتخاذ خطوات جدية لمكافحة الهجمات السيبرانية بإعتماد تدريس وتعليم الفضاء السيبراني والمخاطر الناشئة عنه لاسيما على المستوى الدولي في المؤسسات الأكاديمية
2. وضع بنية تحتية في مجال البرمجيات وتوفير وسائل وأدوات تقنية وتعظيم التعاون بين مؤسسات الدولة العسكرية والتكنولوجية على كافة الأصعدة، لتطوير القدارت العسكرية سواء الدفاعية أم الهجومية للحفاظ على سرية المعلومات والبيانات العسكرية والتصدي للهجمات السيبرانية.
3. فصل بين البنية التحتية والشبكات السيبرانية العسكرية عن المدنية وذلك لحماية السكان المدنيين من مخاطر الهجمات السيبرانية.

المصادر العربيه:

اولاً:الكتب

احمد خليفه الملط , الجرائم المعلوماتيه , دار الفكر الجامعي الاسكندريه, ط الثانيه ,2006

كمال الدين، النزاع المسلح والقانون الدولي العام، المؤسسة الجامعية للدراسات والنشر والتوزيع، بيروت،ط1 ,1997

محمد عبيد الكعبي، الجرائم الناشئة عن إستخدام غير المشروع لشبكة الإنترنت، دار النهضة العربية، القاهرة، دون سنة طبع

محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية ،2004

مصطفى احمد ابو الوفا، المبادئ العامة في القانون الدولي المعاصر، إشراك للطباعة والنشر، مصر، 2006.

مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، ط أولى، مطابع الشرطة، القاهرة 2009

ثانياً: البحوث والدراسات

احمد عبيس نعمة الفتلاوي، "الهجمات السيبرانية مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر"، بحث مقبول للنشر في مجلة المحقق الحلي، كلية القانون، جامعة بابل، 2015

إرشادات الإسكوا للتشريعات السيبرانية، مشروع تنسيق التشريعات السيبرانية لتحفيز مجتمع المعرفة في المنطقة العربية، بيروت ،2012

ثالثا: الاطروحات والرسائل

أ. الاطروحات

1-غازي عبد الرحمن هيان الرشيد، الحماية القانونية من جرائم المعلوماتية

(الحاسب والإنترنت)، إطروحة لنيل درجة الدكتواره في القانون، الجامعة

الإسلامية في لبنان، كلية الحقوق،2004

رابعاً: الصكوك والوثائق الدوليه

أ-الصكوك الدوليه

اتفاقيه جنيف الثالثه عام 1949

البروتكول الثاني لاتفاقيه جنيف عام 1977

ب-الوثائق الدوليه

1. القرار رقم 239/57 بتاريخ 31/كانون الثاني/يناير 2003
2. اللجنـــة الدوليـــة للصـــليب الاحمـــر، "الملحقـــان" البروتوكـــولان الإضـــافيان الـــى إتفاقيـــة جنيف المعقودة في 12 آب/اغسطس 1949" جنيف، سويسرا، ط4، 1997

المصادر الفارسيه

اولاً:الكتب

محمـــد علـــي رعايـــت كننـــده فـــلاح، جنـــك ســـايبري وتهديـــد أمنيـــت ملـــي جمهـــوري إســـلامي ايارن،بايـــان نامـــه كارشناســـي أرشد،دانشـــكاه آازد اســـلامي ،دانشكده ادبيات و علوم إنساني ،قم 1391 (2012)

المواقع الالكترونيه:

لـــو ارن جيزيـــل، مـــا هـــي القيـــود التـــي يفرضـــها قـــانون الحـــرب علـــى الهجمـــات السيبارنية، اللجنة الدولية للصليب الاحمر، 28/6/2013. متاح على الموقع الرسمي: https://www.icrc.org.Cyber-warefare

محمد علي قطب، الجرائم المعلوماتية وطرق مواجهتها، الأكاديمية الملكية للشرطة، البحرين 2010، متوفر على الموقع:(أخر زيارة بتاريخ 2021/5/3 mcms-store/pdf/http://www.policemc.gov.bh

المصادر الاجنبيه :

First: Books

Gerard Mc Hugh and Manuel Bessler, Humanitarian Negotiations with Armed Groups , A manual for Parctitioners, United Nitions,New York, January , 2006

Gray, C," International Law and the Use of Force", Oxford University Press, Oxford, 2000

Jullia Cresswell, "Oxford Dictionary of word origins. Cybernetics", Oxford Reference online, Oxford University Press, 2010

Marcel de Haas, Russia's Military Doctrine Development, at Stephen J. Blank. "Russian Military Politics and Russia's 2010 Defense

Michael S. Fuertes, "Cyber warfare, Unjust Actins in a just war" Florida International University, Full 2013.

Oona` A.Hathway , Rebecca Crootof , Philip Levtiz , aley Nix, Aileen Nowlan ,William Perdue and Julia Spiegel, "The Law of Cyber –Attack", California Law Review, 2012

Zegveld, Liesbeth. Accountability of Armed Opposition Groups in International Law. Cambridge University Press, Cambridge, Geneva, 2002

SECOND: Researches and Studies.

Beter Margulies, Networks in International armed Conflicts: Crossing Borders and Defining “Organized Armed Group”, 2013

Miranda Grange ،(Cyber Warfare and the Law of Armed Conflict) ،Research Paper ، Faculty of Law ،Victoria University of Wellington2014 ،

Brian Kerbs "Report: Russian Hacker form Fuelled Georgia Cyber Attacks", the Washington Post, 16 Oct. 2008

Oona A. Hathaway, Rebecca Crootof , Philip Levitz, Haley Nix, Aileen Nowlan , William Perdue & Julia Spiegel, "The law of Cyber-Attack", California law review, 2012.

Sarah Gorden & Richard Ford, on the Definition and Classification of Cybercrime, 2 J. Computer Virology 13, 13 (2006).