مركز البيدر للدراسات والتخطيط
Al-Baidar Center For Studies And Planning

الهجمات السيبرانية ومسؤولية الدول عنها

زهراء عماد محمد كلانتر

إصدارات مركز البيدر للدراسات والتخطيط

عن المركز

مركز البيدر للدراسات والتخطيط منظمة عراقية غير حكوميّة ،وغير ربحّية، تأسس سنة ٢٠١٥م، ومُسجل لدى دائرة المنظمات غير الحكومية في الامانة العامة لمجلس الوزراء.

ويسعى المركز للمساهمة في بناء الدولة، عن طريق طرح الرؤى والحلول العملية للمشاكل والتحديات الرئيسة التي تواجهها الدولة، وتطوير آليات إدارة القطاع العام، ورسم السياسات العامة ووضع الخطط الاستراتيجية، وذلك عن طريق الدراسات الرصينة المستندة على البيانات والمعلومات الموثقة، وعن طريق اللقاءات الدورية مع الجهات المعنية في الدولة والمنظمات الدولية ذات العلاقة. ويسعى المركز لدعم الاصلاحات الإقتصادية والتنمية المستدامة وتقديم المساعدة الفنية للقطاعين العام والخاص، كما يسعى المركز لدعم وتطوير القطاع الخاص، والنهوض به لتوفير فرص عمل للمواطنين عن طريق التدريب والتأهيل لعدد من الشباب، بما يقلل من اعتمادهم على المؤسسة الحكومية، ويساهم في دعم اقتصاد البلد والارتقاء به.

ويسعى ايضاً للمساهمة في بناء الانسان، باعتباره ثروة هذا الوطن، عن طريق تنظيم برامج لاعداد وتطوير الشباب الواعد، وعقد دورات لصناعة قيادات قادرة على طرح وتبني وتطبيق رؤى وخطط مستقبلية، تنهض بالفرد والمجتمع وتحافظ على هوية المجتمع العراقي المتميزة ومنظومته القيمية، القائمة على الالتزام بمكارم الاخلاق، والتحلي بالصفات الحميدة، ونبذ الفساد بانواعه كافة، ادارية ومالية وفكرية واخلاقية وغيرها.

ملاحظة:

الآراء الواردة في هذا المقال لا تعبر بالضرورة عن وجهة نظر المركز، إنما تعبر فقط عن وجهة نظر كاتبها.

www.baidarcenter.org

info@baidarcenter.org

الهجمات السيبرانية ومسؤولية الدول عنها

زهراء عماد محمد كلانتر

المقدمة

إن سنة الحياة هي التغيير المستمر، ويتسم عصرنا حاليا بتزايد سرعته باستمرار،من خلال تطور المجتمعات البشرية التي غالباً ما تمر بمنعطفات تاريخية تحددها الثورات في العلوم و التكنولوجيا وتطور وسائل الإنتاج المتاحة و انعكاساتها على المجتمع، و كامتداد لهذه المنعطفات الحادة في التاريخ البشري، فإننا الآن نعيش ثورة جديدة يشهدها قطاع وسائل الاتصال، ولا سيما في نطاق تكنولوجيا المعلومات.

إن الاعتماد المتزايد على شبكة الإنترنت في معظم أمور الحياة من اقتصاد وثقافة واجتماع زاد من المخاطر أيضاً، فهذا التطور أتاح سبلاً جديدةً في التعامل الدولي لم تكن ملحوظة أو متوقعة عند وضع النظم القانونية السائدة،فبعد أن كان التعامل الدولي خلال النزاعات المسلحة يتم على الأرض أو الجو أو البحر، أصبح بفضل هذه التقنيات يتم بطريقة إلكترونية ضمن نظام معلوماتي يختلف كلياً عن النزاعات المسلحة التقليدية، وغدا الفضاء السيبراني منافساً حقيقياً للنطاق الدولي التقليدي، وبدأ يلوح شبح التهديد بالهجمات السيبرانية أكثر من أي وقت مضى ومع تزايد الاعتماد العالمي على التكنولوجيا الرقمية، تزايد معه أيضاً التعرض للهجمات على البنى التحتية الحرجة من خلال الفضاء السيبراني.

وقد أصبحت الهجمات السيبرانية إحدى السبل والأساليب المؤثرة من دون تكاليف كبيرة، فبعد أن كان النظام التقليدي يعتمد على القوة العسكرية البشرية لمواجهة باقي الدول أو السيطرة عليها براً أو جواً أو بحراً و الذي كان يكلف الدول الكثير من الخسائر البشرية والمادية ويتطلب الوقت والجهد، فإن النظام الدولي المعلوماتي (السيبراني) يعتمد أساساً على الوسائل الإلكترونية لكل شؤون الأفراد والمجتمعات، وأصبح بإمكان الدول التأثير على الأخرى وشل نظامها المصرفي أو الأمني أو العسكري بكبسة زر واحدة عن بعد دون تكبد العناء ومن دون وقوع خسائر بشرية في

صفوفها، إلا إن ما تحققه من دمار في الدولة المعتدى عليها قد يفوق آثار النزاع المسلح التقليدي سواء في خسارة الأرواح البشرية أو دمار البنى التحتية.

ورغم أنّ المعالم الدقيقة للهجمات السيبرانية لا تزال غير محددة، فإنّ الهجمات الكبيرة ضد البنى التحتية للمعلومات و خدمات الإنترنت في العقد الأخير، تعطي صورة ما عن الشكل والنطاق المحتملين للنزاع في الفضاء السيبراني، وأصبحت الهجمات السيبرانية إحدى أهم التحديات القائمة، ومفهوم جديد للحرب الخفية الحالية، و الظاهرة للعيان في المستقبل القريب كبديل للحرب التقليدية.

ماهية الهجمات السيبرانية

إنّ التطور المتسارع في تكنولوجيا المعلومات و الاتصالات أدّى إلى اعتماد المجتمعات في مختلف الأبعاد السياسية و الأمنية و الاجتماعية و الاقتصادية،على شبكات الكمبيوتر و الإنترنت. إنّ هذا التطور لم يكن خالياً من المخاطر، إذ قلة التكلفة و ثغرات برامج شبكات الاتصال وصعوبة كشف الهوية، تسمح للدول وحتى الجهات غير الحكومية أو الأفراد، بمهاجمة شبكات دول أخرى و الإضرار بالبنى التحتية المعلوماتية و الحيوية التابعة لها، كتعطيل شبكات الكهرباء و قطع نظام الاتصالات و تحطيم الطائرات، وغيرها من البنى التحتية التي تعتمد في تشغيلها وعملها على شبكات الكمبيوتر و الإنترنت. و مع تزايد الاعتماد على الإنترنت، لاسيما في المجالات التي تتعلق بالأمن القومي كالشبكات العسكرية والأمنية، تزايد الحديث عن أهمية مواجهة هذه التهديدات. وفي هذا الإطار ظهر مفهوم الهجمات السيبرانية (Cyber Attacks) وهي تصرفات إلكترونية تقوم بها الدول أو الجهات التابعة لها ضد أنظمة و شبكات كمبيوترية تابعة لدول أخرى لأهداف أمنية أو عسكرية[1]. و أصبحت الهجمات السيبرانية من التحديات والتهديدات الرئيسة التي يتحتم على الدول مواجهتها في العصر الراهن.

١.الوثيقة الإستراتيجية للدفاع السيبراني، منظمة الدفاع غير الحكومية، مركز الدفاع السيبراني التابع للجمهورية الإسلامية الإيرانية، ص ٢٤، منشور على الموقع الرسمي التالي:(آخر زيارة بتاريخ ٢٠١٦/٨/١٥)

http://d-padafand.farsp.ir/upload/96/att-pdf.

أولاً: تعريف الهجمات السيبرانية

إنّ تعريفات الهجمات السيبرانية القائمة والمفاهيم ذات الصلة واسعة جداً، إلا إنّ هناك اتجاهين رئيسيين مختلفين[٢] في تعريف هذا النمط من الهجمات و هما الاتجاه الضيق والاتجاه الواسع. يركز الإتجاه الضيق على موضوع الهجوم، وهذا ما تبنته الولايات المتحدة الأمريكية و حلفاؤها. ومن أمثلة التعريفات في هذا الاتجاه،ما ورد في معجم الاستخدامات العسكرية الذي نشرته هيئة الأركان المشتركة عام ٢٠١١ بعد تأسيس «القيادة السيبرانية الأمريكية»[٣]، حيث عرف الهجوم السيبراني بأنه: «نشاط عدائي باستخدام الكمبيوتر أو الشبكات أو الأنظمة ذات الصلة، يهدف إلى تعطيل أو تدمير أنظمة الخصم السيبرانية الحرجة أو ممتلكاته أو وظائفه. إن النتائج المرجوة من الهجوم السيبراني لا تقتصر بالضرورة على أنظمة كمبيوترية مستهدفة أو البيانات نفسها، وإنّ تفعيل أو تأثير الهجوم السيبراني قد يفصل زمنياً أو مكانياً عن النشاط السيبراني»[٤].

وعلى النقيض من الاتجاه الضيق الذي تبنته الولايات المتحدة رسمياً، فقد تبنت منظمة شنغهاي للتعاون[٥] نهجاً أكثر توسعاً بشأن الهجمات السيبرانية. حيث أعربت هذه المنظمة عن قلقها بشأن التهديدات التي تشكلها إمكانية استخدام وسائل المعلومات والاتصالات الحديثة و تقنياتها لأغراض تتنافى مع ضمان الأمن والاستقرار الدوليين على الصعيدين العسكري والمدني[٦]. فينظر أعضاء هذه المنظمة– أي مؤيدي الاتجاه الواسع – إلى نشر المعلومات الضارة للأنظمة الاجتماعية و السياسية و الاقتصادية، فضلاً عن المجالات الروحية والأخلاقية والثقافية للدول

2.Oona A. Hathaway، Rebecca Crootof، Philip Levitz، Haley Nix، Aileen Nowlan، William Perdue & Julia Spiegel، "The law of Cyber-Attack"، California law review، 2012، p.824.

3."United States Cyber Command".

4. James E. Cartwright، Memorandum for Chiefs of the Military Serve. Commanders of the Combatant Commands، Dirs. Of the Joint Staff Directories on Joint Terminology for Cyberspace Operations 5 (No. 2011).

٥. منظمة شنغهاي للتعاون(SCO) تأسست في مدينة شنغهاي بتاريخ ١٥ حزيران ٢٠٠١ و أصبحت منظمة رسمية حسب مبادئ القانون الدولي في عام ٢٠٠٢ و تتألف من الصين، روسيا و معظم جمهوريات الاتحاد السوفيتي السابق في آسيا الوسطى فضلاً عن مراقبين بما فيهم إيران،الهند و باكستان.من أهدافها مكافحة الإرهاب،مواجهة التطرف و الحركات الانفصالية والتصدي لتجارة الأسلحة، إلا إن بعضهم يرى أنها حلف عسكري لمواجهة حلف الشمال الأطلسي ((NATOينظر إبتسام محمد العامري، منظمة شنغهاي للتعاون الإقليمي، ص١-٧، ١٤/ آذار/٢٠١٣. متاح على الموقع:

http://lcis.Uobaghdad.edu.iqLuploads/ workshop/

6.OonaHathaway،op،cit p.825.

الأخرى بوصفها أيضاً من التهديدات الرئيسية للأمن السيبراني[٧].

إنّ التعارض في محتوى هذين الاتجاهين –مفهوم الهجمات السيبرانية–يظهر الحاجة الماسة إلى وضع تعريف واضح ومتفق عليه دولياً بشان تلك الهجمات.

إنّ الهجوم السيبراني تصرف يدور في عالم رقمي قائم على استخدام بيانات رقمية ووسائل اتصال تعمل إلكترونياً، ومن ثم تطور ليتضمن مفهوماً أوسع يقوم على تحقيق أهداف عسكرية أو أمنية ملموسة ومباشرة، جرّاء اختراق مواقع إلكترونية حساسة، عادة ما تقوم بوظائف تصنف بأنها ذات أولوية، كأنظمة حماية محطات الطاقة النووية أو الكهربائية أو المطارات و وسائل النقل الأخرى[٨].ولذلك نرى أنّ التعريف الذي أورده « شميت « المتخصص في القانون الدولي الإنساني والعضو البارز في مركز الدفاع السيبراني التعاوني التابع لحلف الشمال الأطلسي(NATO) في دليل تالين هو الأقرب لمفهوم الهجمات السيبرانية إذ عرفها بالقول : «الهجوم السيبراني هو أي تصرف إلكتروني دفاعياً كان أم هجومياً يتوقع منه وعلى نحو معقول في التسبب بجرح أو قتل شخص أو إلحاق أضرار مادية أو دمار بالهدف المهاجم»[٩].

وهذا التعريف يتوافق مع ما جاءت به اتفاقية مجلس أوربا المتعقلة بالجريمة السيبرانية لعام ٢٠٠١ حيث نصت المادة الخامسة (٥) منها على: « تعتمد كل دولة طرف، ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الفعل التالي في قانونها الوطني، إذا ما ارتكبت عمداً وبغير حق، الإعاقة الخطيرة لعمل منظومة الكمبيوتر عن طريق إدخال أو إرسال أو إتلاف أو محو أو تغيير أو تبديل أو تدمير بيانات الكمبيوتر»[١٠].

7.Shanghai Cooperation Agreement، Annex I، p. 203.

٨. أحمد عبيس نعمة الفتلاوي،»الهجمات السيبرانية مفهومها و المسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر»،مجلة المحقق الحلي للعلوم القانونية و السياسية،جامعة بابل،السنة الثامنة،العدد الرابع،٢٠١٦،،ص٦١٦.

9.MichealN.Schmitt. William H.Boothby. Wolff Heintschel Von Heinegg. Thomas C.Wingfield. Eric Talbot Jensen. Seen Whatts. Louise Arimatsu. Genevieve Bernatchez. Penny Cumming. Robin Geiss. Terry D.Gill. Derek Jinks. JannKleffner. Nils Melzer& Kenneth Whatkin، "Tallinn Manual on the International Law Applicable to Cyber warfare"، Cambridge University Press، First Publishes، 2013، p. 92.

١٠.مجلس أوربا، «اتفاقية مجلس أوروبا المتعلقة بالجريمة الالكترونية، مجموعة المعاهدات الأوربية رقم ١٨٥، بودابست، ٢٠٠١، المادة رقم (٥).

ثانياً: طبيعة الهجمات السيبرانية

لدى التعرض إلى تعريف الهجمات السيبرانية، فإنّ تساؤلات عدة تطرح بخصوص طبيعة هذه الهجمات، فهل يصح اعتبارها هجوماً بالمعنى الاصطلاحي؟ وهل يمكن عدّ الهجوم السيبراني وسيلة قتالية أو أنه يشكل طريقة قتالية؟.

للإجابة عن هذه التساؤلات لا بدّ من الرجوع إلى أحكام الصكوك الدولية ذات الصلة بتنظيم النزاعات المسلحة التقليدية، ف(الهجمات) كما وردت في القانون الدولي الإنساني هي أعمال العنف ضد الخصم سواء تم القيام بها على سبيل الهجوم أو الدفاع و بغض النظر عن المنطقة التي تنفذ فيها تلك الأعمال، و هذا ما نص عليه البروتوكول الإضافي الأول لاتفاقيات جنيف لعام ١٩٧٧ في الفقرة الأولى من المادة (٤٩) بأنها: «تعني «الهجمات» أعمال العنف الهجومية والدفاعية ضد الخصم»[١١].

أما فيما يخص النشاطات السيبرانية موضوع البحث فإنها بموجب هذا التعريف لا تُعدّ هجوماً إذ إنّ القرصنة واختراق البيانات الإلكترونية وإنْ وُجّهت إلى الخصم للهجوم أو الدفاع، إلا إنها لا تنطوي على أعمال عنف، وعليه إذا أخذنا بنص هذه الفقرة بمعزل عن باقي أحكام البروتوكول فلا يمكن إضفاء صفة الهجوم على النشاطات السيبرانية ذات الآثار المدمرة الواسعة.

لكنّ هذا أمر غير صائب، إذ لا يمكن قراءة نص الفقرة الأولى من المادة (٤٩) بمعزل عن باقي أحكام البروتوكول الذي نص في مواد أخرى على القواعد الأساسية التي تحكم الهجمات و التي يمكن أن تنطبق إلى حد ما على الهجمات السيبرانية كالقاعدة الواردة في المادة (٤٨) التي توجب على الأطراف المتنازعة التمييز دوماً بين المدنيين و المقاتلين و بين الأعيان المدنية و الأعيان العسكرية، أي: وبعبارة أخرى تحظر شن الهجمات العشوائية[١٢].

وهذا ما أكدته القاعدة السابعة الواردة في القانون الدولي الإنساني التي تنص على «يميز أطراف النزاع في جميع الأوقات بين الأعيان المدنية و الأهداف العسكرية»[١٣]، و أيضاً ما أوردته

١١.اللجنة الدولية للصليب الأحمر، «الملحقان» البروتوكولان الإضافيان إلى اتفاقية جنيف المعقودة في ١٢ آب/أغسطس ١٩٤٩» جنيف، سويسرا، ط٤، ١٩٩٧، ص٤٠.

١٢.المصدر السابق، ص٤٠.

١٣.جون–ماري هنكرتس و لويزدوزوالد–بك، القانون الدولي الإنساني العرفي،اللجنة الدولية للصليب الأحمر، المجلد الأول(القواعد)،ص ٢٣.

المادة (٥١) في الفقرة الثانية بخصوص حظر الهجمات ضد السكان المدنيين الرامية أساساً إلى نشر الرعب بينهم[١٤].

وكذلك حظر الهجمات على المنشآت التي تحتوي على قوات خطيرة قد تسبب ضرراً للبيئة الطبيعية و بالتالي تعرض صحة السكان و سلامتهم للخطر الوارد في المواد (٥٢ و٥٦) من البروتوكول نفسه.[١٥]

مما سبق يتبين أنَّ أعمال العنف المسلح يحكمها أمران[١٦]: فهي إما أن تكون: مباشرة وتؤدي بطبيعتها إلى إلحاق أذى مادي بالأهداف العسكرية والمدنية أو غير مباشرة، أي: تلحق الأذى بعد وقوع الهجوم أياً كانت الوسيلة أو الطريقة.

وعلى وفق ما تقدم فإن التركيز على آثار النشاط السيبراني وجسامته سيبين أنَّ وصف الهجوم متحقق فيه،على سبيل المثال عندما تتعرض الحواسيب أو الشبكات في دولة ما للهجوم السيبراني، فقد يؤدي ذلك إلى حرمان المدنيين من الاحتياجات الأساسية كمياه الشرب والرعاية الطبية والكهرباء.

ويمكن أن تتدخل النشاطات السيبرانية في تعطيل خدمات إنقاذ الأرواح كالمستشفيات أو أن تعطل البنى التحتية الحيوية مثل السدود والمفاعلات النووية وأنظمة التحكم في الطائرات، وجرّاء كل هذا قد يتضرر مئات الآلاف من السكان (١٧). فهذه النشاطات وعلى وفق جسامتها وآثارها سواء المباشرة منها أو غير المباشرة، تعد هجوماً سيبرانياً أي ينطبق عليها وصف (الهجوم).

١٤. اللجنة الدولية للصليب الأحمر، ''الملحقان'' البروتوكولان الإضافيان إلى اتفاقية جنيف المعقودة في ١٢ آب/أغسطس ١٩٤٩،مصدر سابق، ص٤٠.

١٥.المصدر السابق، ص ٤١ و ٤٢.

١٦.احمد عبيس نعمة الفتلاوي، مصدر سابق، ص٦١٧.

١٧.لوران جيزيل، ما هي القيود التي يفرضها قانون الحرب على الهجمات السيبرانية، اللجنة الدولية للصليب الأحمر، ٢٠١٣/٦/٢٨. متاح على الموقع الرسمي:(آخر زيارة بتاريخ ٢٠١٦/٨/٥) https://www.ICrc.org.Cyber-warefare.

تكييف الهجمات السيبرانية

من أهم جوانب مكافحة هذه التهديد المتنامي هو تكييف هذه الهجمات، و تحديد مسؤولية الدول، سواء التي ترتكبها بشكل مباشر عن طريق أجهزتها الأمنية والعسكرية أم تلك التي تنفذها عن طريق دعم جماعات أخرى غير مرتبطة بها رسمياً. وعليه فلابد من تكييف الهجمات السيبرانية في ظل كل من قانون الحرب (Jus ad Bellum) الذي يوجد بين ثنايا القانون الدولي العام، و القانون في الحرب (Jus in Bello) أو القانون الدولي الإنساني، ذلك لأن القانون الدولي يميز بين أسباب النزاع المسلح والنزاع المسلح نفسه وهذا التمييز يشكل عنصراً حاسماً في كفالة احترام كلا القانونين[١٨]، فالغاية من القانون الدولي الإنساني أو القانون في الحرب هي حماية ضحايا النزاعات المسلحة بغض النظر عن انتمائهم لأطراف النزاع أو مدى شرعية النزاع، فهو يقتصر على تنظيم جوانب النزاع ذات الأهمية الإنسانية و تسري أحكامه على الأطراف المتحاربة بغض النظر عن مدى عدالة القضية التي يدافع عنها هذا الطرف أو ذاك، بخلاف قانون الحرب الذي يبحث في مدى شرعية النزاع المسلح و يسعى إلى تقييد اللجوء إلى القوة فيما بين الدول، وهذا هو السبب في أهمية التمييز واستقلال قانون الحرب عن القانون في الحرب[١٩].

ومن ناحية أخرى إن اختلاف الفقهاء بشأن مفهوم هذه الهجمات يؤدي إلى تباين آرائهم في القوانين الواجبة التطبيق عليها.فهناك من يرى بأن القوانين والصكوك الدولية التي تنظم النزاعات المسلحة وضعت في مدة ما قبل تأثير الأنظمة الإلكترونية على وسائل وطرق القتال ولم يأخذ واضعو هذه الأنظمة التطورات التكنولوجية بالحسبان ومن ثم فإن الهجمات السيبرانية لا تخضع لهذه الصكوك والقواعد. وعلى العكس من هذا الرأي ذهب فريق آخر إلى أنّ هذه القواعد مرنة ويمكن تطبيقها على الهجمات السيبرانية[٢٠].

١٨.فرانسوا بونيون، الحرب العادلة وحرب العدوان والقانون الدولي الإنساني، المجلة الدولية للصليب الأحمر، مختارات من أعداد عام ٢٠٠٢، ص٣٦-٤١.

١٩.اللجنة الدولية للصليب الأحمر، القانون الدولي الإنساني (إجابات عن أسئلتك)، ديسمبر ٢٠١٤، ص٨-٩.

٢٠.برويز حسيني و حسين ظريف منش، هيكلية الدفاع السيبراني في الدول دراسة مقارنة، دورية بجوهشهاي حفاظتي-أمنيتي، جامعة إمام حسين (ع)، طهران/إيران، السنة الثانية، العدد٥، ٢٠١٣.ص٥٢.

أولاً:الهجمات السيبرانية في ظل قانون الحرب (Jus ad Bellum)

إن قانون الحرب يشير إلى الظروف التي يمكن للدول فيها اللجوء إلى النزاع المسلح أو استخدام القوة المسلحة بشكل عام، أي:وبعبارة أخرى يبحث في مشروعية اللجوء إلى استخدام القوة المسلحة [٢١]. ومن أجل بناء عالم يسوده السلام،أكّد ميثاق الأمم المتحدة على تسوية النزاعات بالطرق السلمية و حظر أعمال العدوان ومنع التهديد باستخدام القوة ضد أي دولة [٢٢].

إنّ الهجمات السيبرانية تشكل تهديداً للمبادئ الرئيسية في القانون الدولي كاحترام سيادة الدول، لما فيها من اختراق لمعلومات أمنية وعسكرية تصنف بالسرية، وتقوض واجباً أساسياً، وهو الامتناع عن استخدام أو التهديد باستخدام القوة نظراً إلى أضرارها البالغة على سير عمل الحكومة والخدمات في الدولة التي تتعرض لمثل هكذا هجمات[٢٣]. وبناء على ما تقدم سنبحث في تكييف الهجمات السيبرانية على وفق قانون الحرب في ظل مبادئه الأساسية في الفرعين الآتيين:

الفرع الأول: مبدأ السيادة

تعد فكرة السيادة والاعتراف بها للدول من المبادئ المتفق عليها في ميثاق الأمم المتحدة والاتفاقيات الدولية التي تصب في هذا الصدد. إذ أشارت الفقرة الأولى من المادة الثانية من ميثاق الأمم المتحدة إلى مبدأ المساواة في السيادة بين جميع أعضائها بالنص: « تقوم الهيئة على مبدأ المساواة في السيادة بين جميع أعضائها»[٢٤].

وفي ظل التغيير التكنولوجي و ظهور الفضاء السيبراني، فقد تغير المفهوم التقليدي للسيادة من خلال ظهور مفاهيم جديدة منها ما يعرف بالسيادة الرقمية التي تعرف بأنها «بسط الدولة لسيطرتها وولايتها القضائية على الفضاء الرقمي المتمثل بالإنترنت الذي يجتاز حدود الدولة وينشئ مجموعة أشخاص افتراضية ضمن شبكات إلكترونية ما وراء أي انتماء وطني»[٢٥]. وهنا ظهر

٢١.اللجنة الدولية للصليب الأحمر، القانون الدولي الإنساني (إجابات عن أسئلتك)،ديسمبر ٢٠١٤. ص٨.

٢٢.ميثاق الأمم المتحدة، الفصل الأول، المواد ١-٢، على الموقع الرسمي: www.un.org>charter-united-nations

٢٣. محمد علي رعايتكننده فلاح، الحرب السيبرانية و تهديد الأمن القومي للجمهورية الإسلامية، أطروحة دكتوراه، جامعة آزاد إسلامي،كلية الآداب و العلوم الإنسانية، قم/إيران، إيران ٢٠١٢.، ص ٧٢-٧٦.

٢٤.ميثاق الأمم المتحدة، الفصل الأول، المواد (٢) ف ١.

٢٥.سراب ثامر احمد، الهجمات على شبكات الحاسوب في القانون الدولي الإنساني، أطروحة من متطلبات نيل درجة الدكتوراه في القانون العام، جامعة النهرين، كلية الحقوق، ٢٠١٥، ص١٠١.

التحدي الحقيقي، إذ لا تستطيع الدولة فرض سيطرتها على مواطنيها في الفضاء السيبراني عن طريق الجنسية مثلاً، كما لا يقتصر الفضاء السيبراني على الإحاطة بالمفاهيم الجغرافية التقليدية بل يمتد ليشمل ظاهرة تغييب الهوية الوطنية[٢٦].

وإنّ مستخدمي شبكات الكمبيوتر والإنترنت، أي: الأفراد الذين يكونون الفضاء السيبراني ينتمون إلى مجتمعات سياسية متعددة وفي حال ارتكاب جريمة ما ضمن هذا الفضاء وقيام الدولة بتتبع مصدر الجريمة، فقد تنتهك في سبيل ذلك مفهوم السيادة الوطنية إذ قد يكون مصدر الجريمة ينتمي أو واقعاً ضمن نطاق سيادة دولة أخرى. وبناءً على ما سبق فيمكن القول بأن سيادة الدولة التقليدية ومقوماتها بدأت تتقلص بوجود وسائل الاتصال الإلكترونية التي تجعل الحدود الإقليمية للدول والانتماءات الوطنية تتضاءل شيئاً فشيئاً، مما تثير التساؤل بشأن نطاق سيادة الدولة في الفضاء السيبراني[٢٧].

إنّ اضمحلال الحدود الجغرافية في الفضاء السيبراني، جعل بعضهم يرى بأن ذلك يخرج الفضاء السيبراني عن نطاق سيطرة وسيادة الدولة، ويؤدي إلى غياب حكم القانون فيه، إلا إنّ ذلك ليس صحيحاً إطلاقاً لعدة أسباب منها:

١-إن استخدام الفضاء السيبراني يتطلب أجهزة ومعدات مادية التي من دونها لا يستطيع المستخدمون الولوج فيه، وبما إن هذا الهيكل المادي يقع ضمن أراضي الدولة فمن الطبيعي أنْ يقع ضمن اختصاص تلك الدولة، وبالتالي تفرض سيطرتها وسيادتها عليه. ومن ناحية أخرى إنّ الفضاء السيبراني بحد ذاته يتطلب التنظيم والرقابة فيما يتعلق بأسماء المستخدمين و عناوينهم و نطاق انطلاق إشارة الاتصال الإلكترونية[٢٨] و هذا التنظيم يخضع لسيطرة الدولة و رقابتها.

٢-إنّ العلاقات المالية التي تنشأ من خلال الفضاء السيبراني تحتاج إلى قوانين تنظمها، وإلا أصبحت ضعيفة وغير موثوقة[٢٩].

٢٦.ينظر نبيل علي وفادية حجازي، الفجوة الرقمية رؤية عربية لمجتمع المعرفة، سلسلة عالم المعرفة، العدد ٣١٨، (الكويت، المجلس الوطني للثقافة والفنون والآداب، ٢٠٠٥)، ص١٢.

٢٧.مصطفى عصام نعوس، سيادة الدولة في الفضاء الإلكتروني،مجلة الشريعة و القانون،جامعة الإمارات العربية المتحدة،كلية القانون،السنة السادسة و العشرون،العدد ٥١، يوليو ٢٠١٢.، ص ١٣٦-١٣٩.

28.See Joshua E. Kastenberg، Non Intervention and Neutrality in cyberspace: An Emerging principle in the National Practice of International Law، 64 Air Force Law Review.

29.Jack L. Goldsmith & Tim Wu، Who controls the internet? Illusions of a borderless world، (Oxford Univ. Press، 2006).

٣-إنّ المحتويات والمعلومات المرسلة من خلال الفضاء السيبراني لها أهميتها في العالم الحقيقي، أي إنّ للدولة مصلحة معلنة للسيطرة على المعلومات التي تتدفق عبر هذا الفضاء و بالذات في حماية مواطنيها من البيانات التشهيرية أو حماية النظام والآداب العامة من المواد الإباحية، فإن هذه المعلومات يجب أن تخضع لقوانين الدولة التي تقع فيها لحماية مصالحها[٣٠].

٤-إن القدرة على التسبب بالأضرار أو خلق الفوضى أو نشر خطابات العنف أو الكراهية (Speech of Hate) من خلال الفضاء السيبراني، تشبه إلى حد كبير مخاطر العالم الحقيقي و دائماً ما تصور الدول بأن الفضاء السيبراني من المسائل المتعلقة بالأمن القومي الأمر الذي يتطلب إيجاد الوسيلة الممكنة لفرض السيطرة والحد من مخاطره[٣١].

إنّ الأسباب المذكورة تدحض القول بأنّ الفضاء السيبراني، بمنأى عن سيادة الدول ولذلك شرعت الدول بمعالجة مشاكل السيادة، لتلافي المخاطر المستقبلية نتيجة استخدام الفضاء السيبراني، سواء على الصعيد الوطني أم الدولي. فقامت أغلبيتها بتطوير تشريعاتها الوطنية لاستيعاب الجرائم التي تحدث في نطاق إقليمها و قامت بالتنسيق مع الدول الأخرى عن طريق إبرام اتفاقيات تعني بتنظيم الجرائم السيبرانية وحل مشكلة السيادة من خلال الاتفاق على آليات تتبع مصادر الجريمة والقوانين واجبة الإتباع في حال حدوثها كالتوصية الصادرة من مجلس أوروبا بشأن المشاكل الإجرائية المرتبطة بتكنولوجيا المعلومات[٣٢]، واتفاقية بودابست عام ٢٠٠١[٣٣]، وبروتوكول ستراسبورغ عام ٢٠٠٣[٣٤]، والاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠[٣٥].

وعلى العموم فإن مبدأ السيادة الإقليمية ينطبق على الفضاء السيبراني ويشمل البنية التحتية الإلكترونية سواء كانت على إقليم الدولة أم مياهها الداخلية أم بحرها الإقليمي أم حتى مياهها الأرخبيلية، فيحق للدولة أن تمارس الرقابة على أنشطة البنية التحتية السيبرانية، كنظم الحواسيب و

30. Jack L. Goldsmith & Tim Wu، Who controls the internet? Illusions of a borderless world،op. cit، P. 147-61.

31.Patrick W. Franzese، Sovereignty in Cyberspace: can it exist? University of Pennsylvania Law 20/6/2014 available at: http://www.law.upenn.edu/live/files/3473-Franzese-p-sovereignty-in-cyberspace-can-it-exist. (last visit at 29/8/2016).

٣٢.التوصية الصادرة عن مجلس أوروبا رقم R(٩٥)١٣ بتاريخ ١١/سبتمبر ١٩٩٥.

٣٣.مجلس أوروبا، اتفاقية مجلس أوروبا المتعلقة بالجريمة الإلكترونية، مجموعة المعاهدات الأوربية رقم ١٨٥، بودابست عام ٢٠٠١.

٣٤.البروتوكول الإضافي لاتفاقية الجريمة المعلوماتية بشأن تجريم الأفعال ذات الطبيعة العنصرية وكراهة الأجانب المرتكبة عبر أنظمة الكمبيوتر، ٢٨ يناير ٢٠٠٣، على الموقع: http://Conventions.Coe.int/treaty/fr/Treaties/Html/189.htm

35. www.lawjo.net>showthread>26439.

شبكات الاتصال والمعلوماتية وقطاعات الطاقة و النقل و...، في تلك المناطق، مع الأخذ بنظر الاعتبار أن ممارسة تلك السيادة يمكن أن تنظم وفقاً ة تلك السيادة يمكن أن تتقيدق إشارة الإتصال الإلكترونيا»للقواعد العرفية أو المقننة للقانون الدولي[٣٦].

وقد ذهب الخبراء في حلف الشمال الأطلسي إلى أبعد من ذلك حيث أكدوا أنّ على الدول واجبَ منع استخدام البنى التحتية السيبرانية الواقعة في إقليمها أو التي تخضع لسيطرتها الكاملة (Overall Control) في نشاطات تمس الحقوق السيادية للدول الأخرى[٣٧].

و من خلال ما تقدم يمكن القول أنّ سيادة الدولة على البنى التحتية السيبرانية لا تقتصر على تلك الواقعة أو المشيدة على إقليم الدولة، بل تمتد إلى كل البنى التحتية السيبرانية التي تخضع لسيطرتها بشكل كامل وإنْ كانت في إقليم دولة أخرى[٣٨].

وفي ضوء ما سبق، فإن الهجمات السيبرانية التي توجه من قبل دولة معينة ضد البنى التحتية السيبرانية التابعة لدولة أخرى، يمكن أن تمثل خرقاً لسيادة دولة الإقليم خاصة إذا تسببت تلك الهجمات بإحداث آثار مدمرة[٣٩].

الفرع الثاني: حظر استخدام أو التهديد باستخدام القوة

إنّ المادة الثانية من ميثاق الأمم المتحدة تنص في الفقرة الرابعة منها على: «يمتنع أعضاء الهيئة جميعاً في علاقاتهم الدولية عن التهديد باستخدام القوة أو استخدامها ضد سلامة الأراضي أو الاستقلال السياسي لأية دولة، أو على أي وجه آخر لا يتفق ومقاصد الأمم المتحدة[٤٠].

ويتمم هذا الحظر بقاعدة عدم التدخل الواردة في القانون الدولي العرفي التي تحظر الدول من التدخل في الشؤون الداخلية للدول الأخرى[٤١].

36. Wolff Heintscble Von Heinegg، Territorial Sovereignty and Neutrality in cyberspace، U. S. Naval war college، 2013 volume 89، p. 128.

37.Tallinn Manual on the International law applicable to cyber warfare، charter.1، section. 1، Rule. 5.

38. Tallinn manual on the international law applicable to cyber warfare، op. cit.، p.27.

٣٩.سراب ثامر أحمد، مصدر سابق، ص ١١٨.

٤٠.ميثاق الأمم المتحدة، المادة ٢ (رابعاً).

41.General Assembly. Res.37/10، U.N. Doc.A/RES/37/10 (Nov.، 15، 1982) – also General Assembly Rec. 25/2625، U.N. Doc.A/RES/25/2625 (Oct. 24، 1970).

لقد أكدت محكمة العدل الدولية (ICJ) في قضية الأنشطة العسكرية وشبه العسكرية (نيكاراغوا ضد الولايات المتحدة) بأنه متى ما اتخذ التدخل شكل استخدام أو التهديد باستخدام القوة فإن قاعدة عدم التدخل الواردة في القانون الدولي العرفي تتطابق مع المادة (٢ / رابعاً) من ميثاق الأمم المتحدة[٤٢].

إنّ نطاق الحظر الوارد في ميثاق الأمم المتحدة لاستخدام أو التهديد باستخدام القوة كان موضوع نقاش دولي مكثف. وقد ذهب فقهاء القانون الدولي إلى اتجاهين مختلفين في تحديد نطاق الحظر الوارد في المادة (٢/ رابعاً): الفريق الأول يرى بأن الحظر الوارد في الميثاق هو حظر واسع ولا يشمل فقط استخدام القوة العسكرية، بل يشمل كل أنواع الإكراه السياسي والاقتصادي وهذا ما تؤيده أغلب الدول النامية[٤٣].

أمّا الفريق الآخر فيعتمد على المفهوم الضيق في تفسير هذه الفقرة، ويحصر الحظر في القوة المسلحة فقط، وهذا ما تحبذه القوى العظمى وبالخصوص تلك التي تدعم مفهوم المسؤولية عن الحماية[٤٤].

إنّ ممّا يترتب على هذا الاختلاف صورتين: الأولى عند الأخذ بالرأي الضيق أي اعتبار الحظر يشمل القوة المسلحة فقط فيؤدي ذلك إلى عدم إمكانية الدولة التي توجَّه ضدها ضغوط غير مسلحة سواء أكانت سياسية أو اقتصادية مهما كانت درجتها، اللجوء إلى استخدام القوة بحجة الدفاع عن النفس.

أما الصورة الثانية فتوسع من مفهوم القوة و تعطي الحق للدولة المستهدفة بالرد على هذه التدخلات بالوسائل كلها، بما فيها استخدام القوة دفاعاً عن النفس بصورة فردية كانت أم جماعية[٤٥].

42.)ICJ،Military and paramilitary activities in and against Nicaragua (Nicar.v. U.S.)، 1986، ICJ. 14، (June 27)، para. 209.

43.Daniel B. Silver، Computer Network Attack as a Use of Force Under article 2(4) of United Nations Charter، in computer network attack and international law 73، 80-82 (Michael N. Schmitt & Brain T. O'Donnell eds. 2002).

44.Ibid.

٤٥.سراب ثامر احمد، مصدر سابق، ص١١١.

أما ممارسات المجتمع الدولي فتؤكد أخذها بالمفهوم الضيق للقوة، فقد جاء في حكم محكمة العدل الدولية في قضية نيكاراغوا سابقة الذكر: «إن مجرد الضغط الاقتصادي أو السياسي لا يمكن أن يشكل استخداما للقوة بالمعنى الوارد في ميثاق الأمم المتحدة في المادة (/٢ رابعاً)»[٤٦].

إنّ حظر استخدام القوة الوارد في المادة (٢/ رابعاً) ليس مطلقاً بل يخضع لاستثناءين: الاستثناء الأول هو في موضوع الأمن و السلم الدوليين الوارد في المادة (٣٩) من ميثاق الأمم المتحدة التي تمنح السلطة لمجلس الأمن لتحديد وجود أي تهديد أو خرق للسلم أو عمل من أعمال العدوان، ومن ثم له أن يقرر الإجراءات واجبة الاتخاذ للحفاظ على أو استعادة السلم والأمن الدوليين[٤٧]، و ينص الميثاق على سلطة مجلس الأمن في اتخاذ التدابير التي لا تتضمن استخدام القوة المسلحة[٤٨]، أو له العمل عن طريق القوات البرية والبحرية والجوية[٤٩].

إنّ إجراءات الأمن الجماعي بموجب المادة (٣٩) قد تكون صعبة سياسياً لأنها تتطلب الترخيص من قبل مجلس الأمن الذي غالباً ما تكون حركاته بطيئة بسبب طبيعة المصالح بين الدول الدائمة العضوية[٥٠].

أما الاستثناء الثاني على المادة (٢/ رابعاً) فهو بشأن حق الدفاع الشرعي الذي ورد في المادة (٥١) من ميثاق الأمم المتحدة، حيث نصت هذه المادة على: «ليس في هذا الميثاق ما يضعف أو ينقص من الحق الطبيعي للدول فُرادى أو جماعات في الدفاع عن أنفسهم إذا اعتدت قوة مسلحة على أحد أعضاء الأمم المتحدة، وذلك إلى أن يتخذ مجلس الأمن التدابير اللازمة لحفظ السلم والأمن الدوليين»[٥١].

إنّ هذه المادة تشترط على الدول لاستخدام حقها في الدفاع الشرعي أن تكون قد تعرضت لاعتداء مسلح، ومن ثم إن الأشكال الأخرى من استخدام القوة التي لا تكون بمثابة هجوم مسلح لا تعطي الحق في الدفاع الشرعي.

46.ICJ،Military and paramilitary activities in and against Nicaragua (Nicar.v. U.S.)، 1986، ICJ. 14، (June. 27)، paras 188-190.

٤٧.ميثاق الأمم المتحدة، المادة ٣٩.

٤٨.المصدر السابق، المادة ٤١.

٤٩.المصدر السابق، المادة ٤٢.

50.Oona Hathaway، op.cit.، p. 814. (4)

٥١.ميثاق الأمم المتحدة، المادة (٥١).

وبموجب هذه الاستثناءات، يعتمد جواز استخدام القوة المسلحة على وقوع العدوان،إذ جاء تعريف العدوان في قرار صادر من الجمعية العامة للأمم المتحدة بأنه: «استخدام القوة المسلحة بواسطة دولة ضد السيادة أو السلامة الإقليمية أو الاستقلال السياسي لدولة أخرى أو بأي شكل آخر لا يتفق مع ميثاق الأمم المتحدة»[٥٢].

ومما تقدم قد يتبادر إلى الذهن السؤال الآتي : هل تشكل الهجمات السيبرانية هجوماً مسلحاً أم شكلاً آخر من أشكال القوة؟، وهل تعرض دولة ما لهجوم سيبراني يمنحها الحق في الدفاع الشرعي؟.

للإجابة عن هذه التساؤلات لابد من التطرق إلى النظريات الرئيسة التي برزت لتحديد متى يمكن عد الهجوم السيبراني هجوماً مسلحاً ومن ثم يرتب الحق في الدفاع الشرعي، وهذه النظريات تقوم على المناهج الآتي ذكرها:

١-النهج القائم على الوسيلة (Instrument-Based Approach)

تبنى أصحاب هذا النهج معيار الوسيلة المستخدمة في الهجوم وبموجب هذه النظرية، إنّ الهجوم السيبراني بمفرده، لن ينشئ لمفهوم هجوم مسلح يستوجب حق الدفاع الشرعي الوارد في المادة (٥١) من ميثاق الأمم المتحدة لأنه «يفتقر إلى الخصائص الفيزيائية المرتبطة بالإكراه العسكري». و بعبارة أخرى لأنه بشكل عام لا يحتوي طاقة حركية (Kintinc) مثل ما هو معروف في الأسلحة التقليدية[٥٣].

وما يدعم هذه النظرية ما ذهبت إليه الأمم المتحدة باعتبار القطع الكلي أو الجزئي للتلغراف والراديو ووسائل الاتصال الأخرى، تدابير لا تتطلب استخدام القوة[٥٤].

وإنّ تعريف العدوان الوارد في قرار صادر عن الجمعية العامة للأمم المتحدة قد أدرج في الفقرة الثالثة منه، عدداً من الأعمال التي من شأنها أن تشكل «العدوان، بموجب المادة (٣٩) من الميثاق»[٥٥]، وكل تلك الأعمال وإنْ جاءت على سبيل المثال وليس الحصر، تتضمن استخدام

52.General Assembly، Res. 3314، U.N. Doc. A/RES/3314، (Dec. 14، 1974).

53.Michael N. Schmitt، Computer network attack and the use of force in International Law: Thoughts on normative framework، International Review of the Red Cross،No.846، 30/6/2002.

٥٤.ميثاق الأمم المتحدة، المادة ٤١.

55. UN.General Assembly.Res. 3314، Dec،14،1974.

الأسلحة التقليدية أو القوة العسكرية، و مع ذلك يحق لمجلس الأمن أن يعتبر فعلاً ما عدواناً ولو لم يرد شكل هذا العدوان في الفقرة الثالثة من هذا القرار[٥٦].

إنّ حلف الشمال الأطلسي أيضاً قد أشار إلى تأييده لهذه النظرية من خلال النص في منهج الدفاع السيبراني المشترك التابع له عام ٢٠١٤ على: «إن الهجوم السيبراني سيلزم الدول الأعضاء بالتشاور» مع بعضها البعض بموجب المادة (٤) من معاهدة حلف الشمال الأطلسي... إلا إنّ الهجوم السيبراني لا ينشئ هجوماً مسلحاً يلزم الدول الأعضاء لمساعدة بعضها البعض بموجب المادة (٥) من هذه المعاهدة»[٥٧]. وهذا تطور ملفت للنظر خصوصا بعد الهجوم السيبراني الذي تعرضت له جمهورية إستونيا عام ٢٠٠٧، حيث اجتمع حلف الشمال الأطلسي رداً على ذلك الهجوم وفقاً للمادة (٥) من ميثاق حلف الشمال الأطلسي، أي المادة التي تتيح استخدام القوة المسلحة ضد أي اعتداء على دولة طرف فيه.

إنّ هذه النظرية وإنْ كانت سهلة التطبيق نظراً لسهولة تحديد الأسلحة والقوة العسكرية، إلّا إنها تتغاضى عن الهجمات السيبرانية ذات القدرة البالغة على إحداث الأضرار من دون استخدام الأسلحة العسكرية التقليدية[٥٨].

٢-النهج القائم على الأهداف(Target-Based Approach)

بموجب هذه النظرية يكفي أن يستهدف الهجوم السيبراني نظاماً الكترونياً مهماً للغاية، لكي يصنف هجوماً مسلحاً و يركز أصحاب هذه النظرية على طبيعة الهدف الذي يتم استهدافه، فالهجوم السيبراني يحتاج إلى اختراق نظام رئيسي، على سبيل المثال البنى التحتية الوطنية الحرجة للدولة كالنظم المصرفية، لتسويغ الردود العسكرية التقليدية في مواجهته والتي يمكن أن تشعل حرباً تقليدية (Conventional War)[٥٩]،وقد انتقدت هذه النظرية بسبب تجاهلها لمفهوم البنى التحتية الحرجة المتعددة الأغراض للدولة في العصر الراهن، فضلاً عن جسامة الهجوم السيبراني و آثاره[٦٠].

٥٦.بدر محمد هلال ابو هويمل، جريمة العدوان في القانون الدولي، دراسة لاستكمال متطلبات النجاح في مساق القانون الدولي، جامعة آل البيت، كلية الدراسات العليا، الأردن، ٢٠١٢، ص١٢.

57.NATO Agrees common Approach to cyber Defense، Fe. 25، 2014، available at: http://www.euractiv.com/en/infosociety/nato-agrees-common-approach-cyber-defence.article. 171377.

58.Oona Hathaway، op. cit.، p. 846.

59.Matthew J. Sklerov، solving the Dilemma of state Responses to cyber Attacks: A Justification for the use of Active Defenses against states who Neglect their Duty to prevent، 201 MIL. L. REV.،

60.Gray Sharp، in Stephanie G. Handler، The new cyber Face of the Battle، Developing a Legal Approach to Accommodate Emerging Trends in Warfare، Stanford Journal of International Law، vol. 48، 2012، p. 12.

٣-النهج القائم على الآثار(Effects-Based Bpproach)

يعد هذا الاتجاه نهجاً وسطاً بين النهج القائم على الوسيلة و النهج القائم على الأهداف. إذ يصنف أصحاب هذه النظرية الهجوم السيبراني كهجوم مسلح على أساس خطورة آثاره[٦١]. وقد ذهب بعض الفقهاء المؤيدين لهذه النظرية إلى تحديد العوامل التي يمكن القياس عليها لتصنيف الهجوم السيبراني كهجوم مسلح ومن هذه العوامل الخطورة، الفورية و المباشرة والقابلة للقياس[٦٢]،كما يرى أصحاب هذه النظرية أنّ كل نشاط مشبوه يمكن معاقبته على وفق آثاره على الدول الأخرى[٦٣].

وقد ذهب دانيل سيلفر (Daniel B. Silver) المستشار العام السابق لوكالة الاستخبارات المركزية ووكالة الأمن القومي الأمريكية بأنّ: «الهجوم السيبراني يسوغ الدفاع الشرعي إلاني يبرر الدفاع عن النفس فقط واذا كانت نتيجته المتوقعة، إحداث إصابات جسدية أو أضرار مادية تماثل النتائج المرتبطة بالإكراه المسلح»[٦٤].

و بموجب هذه النظرية فإن الهجوم السيبراني على سبيل المثال ضد نظام مراقبة الملاحة الجوية، والتسبب بحوادث الطائرات، سيعد هجوماً مسلحاً لأنه من المتوقع أنّ هجوماً كهذا سيتسبب في خسائر كبيرة سواء في الأرواح أم الأموال.

وقد أيد ماركو روسيني(Marco Roscini) هذا التوجه بقوله «... من الممكن عدُ الهجمات السيبرانية بمثابة خرق واضح لأحكام الفقرة (٤) من المادة (٢) من ميثاق الأمم المتحدة، شريطة أن تتسبب بتعطيل أو دمار واسع للبنى التحتية الضرورية في حياة الإنسان، وفيما لو تحقق ذلك فللدولة المعتدى عليها، الحق في اللجوء الى استخدام القوة بموجب المادة (٥١) من الميثاق نفسه، والتي تنص على الحق في الدفاع عن النفس»[٦٥].

مما سبق يمكن القول:إنّ هذا الاتجاه وإنْ كان هو الاتجاه الأكثر أهميةً وقبولاً من النظريات السابقة، إلا إنّه لا ينطبق إلّا على مجموعة صغيرة من الهجمات السيبرانية الضارة، أي: تلك التي

61.Daniel. B. Silver،.، Computer Network Attack as a Use of Force Under article 2(4) of United Nations Charter، in computer network attack and international law 73،2002،p. 13.
62.it.، p. 914.
63.Sean P. Kanuck، Recent Development: Information warfare: New Challenges for public International Law، 37 Harvard International Law Journal،l. 272، 290،1996.
64.Daniel B. Silver، op. cit.، p. 89.
65.Marco Roscini، "World Wide Warfare- Jus ad Bellum and the Use of Cyber Force"، Max Planck yearbook of United Nations law، vol. 14، 2010، p 85-130.

لها آثار تماثل آثار الهجوم باستخدام أسلحة تقليدية أو أسلحة الدمار الشامل[٦٦].

أما مجموعة الخبراء في دليل تالين فقد ذهبوا بالقول إنه: «أي هجوم سيبراني يكون باستخدام أو تهديداً باستخدام القوة ضد السلامة الإقليمية أو الاستقلال السياسي لأية دولة أو بأي شكل يتعارض مع مقاصد الأمم المتحدة، يعد عملاً غير مشروع»[٦٧]. و استندوا في ذلك إلى الرأي الاستشاري الصادر عن محكمة العدل الدولية بشأن شرعية استخدام أو التهديد باستخدام الأسلحة النووية[٦٨]، الذي ذكر في في إحدى فقراته بأن حظر استخدام القوة أو التهديد بها الوارد في المادة (٢/ رابعاً) من ميثاق الأمم المتحدة وحق الدفاع الشرعي الوارد في المادة (٥١) من الميثاق نفسه، ينطبقان على «أي استخدام للقوة بغض النظر عن طبيعة الأسلحة المستخدمة»[٦٩].

وتأسيساً على ما تقدم يمكن القول أن الهجمات السيبرانية متى ما كانت آثارها شبيهة بآثار الهجوم المسلح التقليدي من ناحية الإصابات الجسدية والأضرار المادية فإنها تكيّف كاستخدام للقوة المسلحة المعروفة، وبالتالي للدولة المتضررة اللجوء إلى استخدام حقها في الدفاع عن النفس[٧٠].

من ناحية أخرى إنّ المادة (٢/ رابعاً) لم تحظر استخدام القوة المسلحة فقط، بل حظرت التهديد باستخدامها ضد الدول الأخرى وقد تم تعريف التهديد باستخدام القوة بأنه: «التهديد الصريح أو الضمني، شفاهاً أو عملاً، باستخدام غير الشرعي للقوات المسلحة ضد دولة أو عدة دول والذي تحقيقه يتعلق بإرادة الدولة التي قامت بعمل التهديد»[٧١].

بناءً على ما نصت عليه محكمة العدل الدولية في رأيها الاستشاري بشأن شرعية استخدام الأسلحة النووية أو التهديد باستخدامها في الفقرة ال٤٧ بأن (مفهوما»التهديد» بالقوة و «استعمال» القوة وفقا للفقرة ٤ من المادة ٢ من ميثاق الأمم المتحدة متلازمان من حيث إنّه إذا كان استعمال القوة في حالة ما غير مشروع _لأي سبب من الأسباب_ فإن التهديد باستعمال

66.Oona Hathaway، op. cit.، p. 848.
67.Tallinn Manualon the international law applicable to cyber warfare،op.cit، Chapter II، section 1، Rule 10.
68.Ibid، p. 42.
69.ICJ Nuclear weapons advisory opinion، legality of threats or use of Nuclear weapons. Advisory opinion، 1996، I.C.J. 226 (8 July)، para 39.
70. Tallinn manual on the international law applicable to cyber warfare، op. cit.، p. 54.
71.Marco Roscini، "Threats of Armed Force on contemporary International Law". Netherlands International Law Review، No. 54، 2007، p. 235.

هذه القوة هو أيضا غير مشروع)[٧٢]، فبالتالي إنّ التهديد باستخدام الهجوم السيبراني يكون مرتبطاً في شرعيته بمدى شرعية الهجوم السيبراني ذاته.

الجدير بالذكر إنّ الهجمات السيبرانية التي ترقى إلى مستوى الهجوم المسلح، وإنْ كانت تسوغ حق الدفاع عن النفس، إلّا أنّ هذا الحق ليس مطلقاً. فاستخدام الدولة للقوة المسلحة رداً على الهجوم السيبراني، يجب أن يتفق ليس فقط مع ميثاق الأمم المتحدة بل وقواعد القانون الدولي العرفي، وما تضمنته مبادئ استخدام القوة المسلحة كمبدأي الضرورة العسكرية ومبدأ التناسب في استخدام القوة المسلحة أيضاً[٧٣].

فمن متطلبات شرعية اللجوء إلى القوة، وجوب استخدام القوة كملاذ أخير حينما تكون الوسائل السلمية كالتسوية الدبلوماسية غير مجدية في تحقيق الهدف العام للدولة[٧٤]. كما إنه بموجب مبدأ التناسب، يُحظر استخدام القوة التي تكون مفرطة في الشدة والنطاق بالنسبة إلى الخطر الفعلي أو الوشيك الصادر عن قوات عسكرية تابعة لدولة أخرى[٧٥].إنّ السؤال الذي يثار هنا: هو إذا لم تكن الهجمات السيبرانية ذات آثار جسيمة تبلغ مستوى النزاع المسلح،فهل يمكن القول بأنها غير منظمة؟ وكيف للدولة المتضررة الرد على مثل هذه الهجمات؟

للإجابة لابد من القول بأنّ الهجمات السيبرانية التي لا يمكن عدُ استخدامها للقوة محظوراً بموجب المادة (٢/ رابعاً) من ميثاق الأمم المتحدة، يمكن عدُها شبيهة بأعمال الضغط السياسي والاقتصادي، وفي هذه الحالة تخرق قاعدة (عدم التدخل) الواردة في القانون الدولي العرفي[٧٦].

وعلى هذه الشاكلة يمكن القول:إن المادة (٢ رابعاً) من ميثاق الأمم المتحدة تشير إلى استخدام القوة المسلحة، إلا إن مبدأ (عدم التدخل) ينطبق على الأشكال الأخرى لاستخدام القوة[٧٧].

72.ICJ Nuclear weapons Advisory opinion، op. cit.، para 47.
73.Oona Hathaway، op.cit،p.849.
74.R. Y. Jennings، The Caroline and Macleod Cases، 32 the American Journal of International law L.82،89، 1938.
75.Robert D. Slane،the Cost of Conflation :Preserving the Dualism of Jus ad Bellum and Jus in Bello in the Contemporary law of war،34 the Yale Journal of International Law l.47، 2009.
76.General Assembly. A/RES/37/10 ، op. cit.
77.)A. Randelzhofer، "Article 2(4)"، in: Simma، B. (ed)، The Charter of the United Nations: A commentary. Vol. 1، 2002، p. 118.

وفي سبيل رد تلك الهجمات يمكن للدولة المتضررة فيما إذا تمكنت من الوصول إلى معرفة هوية مرتكبي الهجمات السيبرانية ونسبتها إلى دولة معينة اتخاذ الطرق التالية:

١- اللجوء إلى مجلس الأمن بالاستناد إلى المادة (٣٥) من ميثاق الأمم المتحدة التي نصت على: «لكل عضو من أعضاء الأمم المتحدة أن ينبّه مجلس الأمن أو الجمعية العامة إلى أي نزاع أو موقف من النوع المشار إليه في المادة الرابعة والثلاثين». ولمجلس الأمن أن يوصي بالتدابير المناسبة لحل النزاع وإذا قرر مجلس الأمن بأن النزاع المذكور يشكل تهديداً للسلم والأمن الدوليين فله استعمال صلاحياته في إصدار التوصيات والتحرك لإعادة السلم والأمن الدوليين، وفيما إذا كل هذه الإقدامات لم تَفِ بالغرض فله اللجوء إلى صلاحياته في استخدام القوات البرية والبحرية والجوية»[٧٨].

٢-اللجوء إلى محكمة العدل الدولية وفقاً للمادة (٣٤) من نظامها الأساسي لأجل تحميل الدولة مسؤولية الهجمات و للحصول على التعويض المناسب عن الأضرار الناشئة عن الهجوم السيبراني. وإنْ كانت عملية تحديد ميزان الخسائر الناشئة عن الهجوم السيبراني، عملية صعبة للغاية وذلك بسبب تردد و تكتم المؤسسات المالية الحكومية بشأن الإعلان عن المعلومات الدقيقة حول الخسائر[٧٩].

و يذهب بعضهم إلى أنه يمكن اللجوء إلى هذه المحكمة للحصول على رأي استشاري تطلبه الأجهزة الرئيسة للأمم المتحدة،بشأن مشروعية الهجمات السيبرانية[٨٠]. إن الآراء الاستشارية للمحكمة وإنْ كانت غير ملزمة، إلا إنها تساعد في تشكيل قاعدة دولية عرفية[٨١].

٣-للدولة المتضررة أن تلجأ إلى التدابير المضادة أو المقابلة بالمثل لرد الهجمات السيبرانية بشرط أن لا تبلغ الهجوم المسلح[٨٢]. و ذلك حسبما ورد في مشروع مواد مسؤولية الدول عن

٧٨.ميثاق الأمم المتحدة، المواد: ف١/٣٥، ف١/٣٦، ٣٩، ٤١، ٤٢.

٧٩.علي قاسمي و ويكتور بارين جهار بخش،الهجمات السيبرانية والقانون الدولي،ص١٢٩، دراسة منشورة بتاريخ (٢٠١٢/٥/٢) على الموقع التالي:(آخر زيارة بتاريخ ٢٠١٦/٨/٣) www.SID.ir/pdf

٨٠.ميثاق الأمم المتحدة، المادة ٩٦.

81.B. Conforti، The Law and Practice of the United Nations، Leiden Martins Nijhoff، 2005، p. 276.

٨٢.ميثاق الأمم المتحدة، (م ٤٩/اولًا).

الأفعال غير المشروعة لعام ٢٠٠١ و بالذات المواد (٤٩-٥٤) منه [٨٣].

ثانياً: الهجمات السيبرانية في ظل القانون في الحرب (Jus in Bello)

على الرغم من أنّ الهجوم السيبراني القائم بذاته لا يشكل نزاعاً مسلحاً، إلا إن الهجمات السيبرانية قد يتم استخدامها أثناء النزاعات المسلحة للرد على استفزازات تقليدية أو لتمهيد الطريق لهجوم تقليدي بهدف تحقيق التفوق والميزة العسكرية[٨٤].

إنّ توظيف الهجمات السيبرانية في النزاع المسلح كما جاء في تقرير اللجنة الدولية للصليب الأحمر عام ٢٠١١ يجب أن يتوافق مع جميع مبادئ القانون الدولي الإنساني و قواعده كما هو الحال مع أي سلاح أو وسيلة أو أسلوب حرب آخر، جديداً كان أم قديماً[٨٥].

وما يؤيد ذلك ما أشارت إليه محكمة العدل الدولية إنّ :» مبادئ وقواعد القانون الدولي الإنساني المنطبق في النزاع المسلح، تنطبق على «جميع أشكال الحروب وعلى جميع أنواع الأسلحة.. بما في ذلك تلك المستقبلية»[٨٦].

وبناءً على ذلك فإن القانون الدولي الإنساني أو القانون في الحرب (Jus in Bello) ينطبق على الهجمات السيبرانية التي تحدث في أثناء نزاع مسلح دائر.

كما أكّد الخبراء في الأمم المتحدة على انطباق المبادئ القانونية المستقرة كمبادئ الإنسانية والضرورة العسكرية والتناسب في استخدام القوة والتمييز بين المدنيين و المقاتلين على الهجمات السيبرانية التي تقع أثناء النزاع المسلح[٨٧].

83.A. Randelzhofer،op.cit.p.118.

٨٤.مايكل ن.شميث، الحرب بواسطة شبكات الاتصال: الهجوم على شبكات الكمبيوتر (الحاسوب) و القانون في الحرب، المجلة الدولية للصليب الأحمر، مختارات من أعداد ٢٠٠٢،ص ٩٠-٩٤.

٨٥.اللجنة الدولية للصليب الأحمر، القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة، تقرير تشرين الأول/أكتوبر ٢٠١١، متاح على الموقع الرسمي:

www.icrc.org/eng/assets/files/red-cross-crescent-movement/31st international-conference/31-int. conference-ihl-challenges-report-11-5-1-2-en.Pdf.

86.ICJ Nuclear weapons Advisory opinion، op. cit.، para 86.

٨٧.ينظر تقرير الخبراء الحكوميين بشأن التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، رقم التقرير A/٧٠/١٧٤ ٢٢ تموز/يوليو ٢٠١٥. متاح على الموقع الرسمي:(آخر زيارة بتاريخ ٢٠١٦/٩/٥)

www.un.org/ga/search/viewdoc.asp?symbol=A/70/174،para.28.

أولاً: مبدأ الضرورة العسكرية:

إنّ مبدأ الضرورة العسكرية يتعلق بميزة عسكرية محددة يمكن تحقيقها من عمل عدائي خاص. فيما يثير موضوع تكييف العلاقة بين مبدأ الضرورة العسكرية والنزاع المسلح، خلافاً فقهياً. ففريق من الفقهاء يرى أنّ الضرورة العسكرية هي ركن من أركان النزاع المسلح وأنّ الحرب العادلة تنبع من ضرورة تدفع لشنها وهي الضرورة العسكرية، ومن مؤيدي هذا الاتجاه الفقيه دي فورتس حيث ذهب إلى القول: «إنّ الضرورة العسكرية لا تنفك عن كونها عنصراً رئيساً في العمليات القتالية»[٨٨]. وقد أيّد الفقيه هنري ميروفتز(Henri Meyrowitz) هذا الاتجاه و استند في ذلك إلى حيثيات مؤتمر بروكسل للسلام عام ١٨٧٤الذي علق فيه الوفد الروسي آنذاك قائلاً: «إنّ الضرورة العسكرية تقوم متى ما قامت النية على تحقيق الهدف العسكري المشروع»[٨٩].أما الفريق الآخر على العكس تماماً إذ ذهبوا إلى أنّ الضرورة العسكرية ما هي إلا استثناء على القاعدة ولا يمكن اللجوء إليها، إلا في ظروف معينة ووفق شروط محددة[٩٠].

أما على صعيد القانون الدولي فقد تمت الإشارة إلى مبدأ الضرورة العسكرية في صكوك دولية عدة منها ديباجة إعلان سان بيترسبورغ عام ١٩٦٨، التي نصت على «... أن الهدف المشروع الوحيد الذي يجب أن تسعى إليه الدول في أثناء الحرب هو إضعاف القوات العسكرية للعدو...»[٩١].

وأكدت اتفاقية لاهاي لعام ١٩٠٧ المتعلقة بسير العمليات العسكرية على أن: «ترى الأطراف السامية المتعاقدة أنّ هذه الأحكام التي استمدت صياغتها من الرغبة في التخفيف من آلام الحرب كلما سمحت بذلك المقتضيات العسكرية، هي بمثابة قاعدة عامة للسلوك يهتدي بها

88.Rebeca Grant، "In Determining Military Necessity and proportionality، The commander's judgment is more critical than even، in search of lawful targets"، Airforce magazine، Feb.، 2003، p. 40.

89.Henri Meyrowitz، "The principle of superfluous injury or unnecessary suffering–from declaration of st. Petersburg of 1868 to Additional protocol 1 of 1977"، extract printofIRRC،no.299،March-April1994،p. 106.

90.Richard P.DimegLio، "The Evolution of the Just war tradition: Defining Jus Post bellum"، Military Law Review، vol. 186، winter 2005، p. 120.

٩١.اللجنة الدولية للصليب الأحمر، «القانون الدولي المتعلق بسير العمليات العسكرية، مجموعة اتفاقيات لاهاي وبعض المعاهدات الأخرى»، جنيف، ط ثانية، سبتمبر/أيلول ٢٠٠١، ص١٦٩.

المتحاربون مع بعضهم ومع السكان»[٩٢].

وقد نصت هذه الاتفاقية في المادة (٢٣) الفقرة (٢/ز) على «يمنع بالخصوص... تدمير ممتلكات العدو أو حجزها، إلا إذا كانت ضرورات الحرب تقتضي حتماً هذا التدمير أو الحجز»[٩٣].

وفي السياق نفسه أشارت المادة (٥٢) من البروتوكول الإضافي الأول عام ١٩٧٧ في الفقرة الثانية إلى أن: «تقتصر الهجمات على الأهداف العسكرية فحسب... والتي يحقق تدميرها التام أو الجزئي أو الاستيلاء عليها أو تعطيلها، في الظروف السائدة حينذاك، ميزة عسكرية أكيدة»[٩٤].

وقد ذهبت لجنة القانون الدولي بمناسبة تعرضها إلى المشروع الخاص بالمسؤولية الدولية بالقول: «لابدّ من التذكير بعدم جواز اللجوء إلى الضرورة العسكرية، إلا إذا لم تستطع الدولة بلوغ أهدافها العسكرية المشروعة إلا بالقيام بعمل طارئ وضروري لتحقيق ذلك الهدف حماية لمصالح الدولة العليا»[٩٥].

واستناداً إلى ما سبق يمكن القول إن اللجوء إلى الهجمات السيبرانية يجب أن يكون ضرورياً لتحقيق الهدف العسكري المشروع، وأما مسألة تحديد الأهداف والمنشآت العسكرية في الفضاء السيبراني فتثير تحدياً واسعاً أمام المجتمع الدولي، وذلك لأنّ المنشآت التي تقدم خدمة للجهد العسكري هي في الوقت نفسه قد تخدم القطاع المدني.

إنّ عدم تحديد معايير منظمة لاستخدام الفضاء السيبراني للأغراض العسكرية الهجومية سيعني إمكانية اللجوء لاستخدامها بداعي الضرورة العسكرية[٩٦]. وقد أشار إلى هذا التحدي ريكس هيوز (Rex Hughes) مدير شبكة الابتكار السايبيري في جامعة كامبردج بالقول: «إنّ الهجمات الرقمية تنشئ تحدياً واضحاً أمام تطبيق مبدأ الضرورة العسكرية ولحل هذه المعضلة لابد من تضافر الجهود بين خبراء القانون الدولي ومهندسي الصناعات الإلكترونية لتحديد ما يمكن

٩٢. اللجنة الدولية للصليب الأحمر، «القانون الدولي المتعلق بسير العمليات العسكرية، مجموعة اتفاقيات لاهاي وبعض المعاهدات الأخرى»، ص١٣.

٩٣. المصدر السابق، ص٢١.

٩٤. اللجنة الدولية للصليب الأحمر، «الملحقان، البروتوكولان الإضافيان إلى اتفاقيات جنيف الأربعة لعام ١٩٤٩، مصدر سابق، ص٤٣.

95. UN، "Year book of the International Law commission" vol. II، part 1، 1980، Article 3.

٩٦. أحمد عبيس نعمة الفتلاوي، مصدر سابق، ص٦٣٠-٦٣١.

أن يوصف بهدف...»[٩٧].

ثانياً: مبدأ التناسب في استخدام القوة المسلحة

إنّ من شروط تحقيق مبدأ التناسب في استخدام القوة في النزاع المسلح ما ورد في البروتوكول الإضافي الأول لعام ١٩٧٧ في الفقرة (٥/ب) من المادة (٥١) إذ نصت بأنه : «الهجوم الذي يتوقع منه إحداث خسائر عرضية في أرواح المدنيين، إصابة المدنيين، الإضرار بالأعيان المدنية أو مزيجاً منها،الذي سيكون مفرطاً فيما يتعلق بالميزة العسكرية المباشرة والملموسة المرتقبة»[٩٨].

وأكدت المادة (٥٧) من البروتوكول نفسه على: «يُلغى أو يُعلق أي هجوم، إذا تبين أنّ الهدف المقصود ليس هدفاً عسكرياً، أو أنّه مشمول بحماية خاصة، أو أنّ الهجوم قد يتوقع منه أنْ يحدث خسائر في أرواح المدنيين أو إلحاق الإصابة بهم، أو الإضرار بالأعيان المدنية أو أنْ يحدث خلطاً من هذه الخسائر أو الأضرار وذلك بصفة عرضية تفرط في تجاوز ما ينتظر أنْ يسفر عنه ذلك الهجوم من ميزة عسكرية مباشرة»[٩٩].

ونظراً لمضمون هذه المواد فإن تطبيق مبدأ التناسب يتطلب من صُناع القرار العسكري التفكير ملياً بالإصابات المدنية المحتملة أو تدمير الممتلكات المدنية مقابل تحقيق أهداف عسكرية. أما بشأن الهجمات السيبرانية فنظراً إلى طبيعة الضرر الذي تحدثه هذه الهجمات، فإنّ تحقيق مبدأ التناسب فيها يشكل تحدياً فريداً من نوعه أمام التنظيم الدولي وذلك لأن آثار الهجوم السيبراني عادة ما تكون غير مباشرة[١٠٠]. على سبيل المثال إنّ الهجوم السيبراني الذي يوقف تدفق المعلومات عبر الإنترنت قد يبدو مجرد إزعاج في بادئ الأمر، إلا إنّ ذلك سيؤدي على سبيل المثال إلى شل قدرة المستشفيات على نقل المعلومات الحيوية، ومن ثم يؤدي إلى خسائر بالأرواح وإصابات بالغة[١٠١].

97.Rex Hughes، "A Treaty for cyber space"، International Affairs Journal، vol. 86، No. 2، 2010، p. 537.

٩٨.اللجنة الدولية للصليب الأحمر، «الملحقان» «البروتوكولان الإضافيان إلى اتفاقية جينيف المعقودة في ١٢ آب أغسطس ١٩٤٩»، مصدر سابق، ص٤٢.

٩٩.اللجنة الدولية للصليب الأحمر، «الملحقان» «البروتوكولان الإضافيان إلى اتفاقية جينيف المعقودة في ١٢ آب أغسطس ١٩٤٩»، مصدر سابق، ص٤٢.

١٠٠.علي قاسمي و ويكتور بارين جهار بخش، مصدر سابق، ص١٣٤.

101.Oona Hathaway، op. cit.، p. 851.

وفي هذا الشأن ذهب شين (Shin) بالقول: «يمكن تطبيق مبدأ التناسب على الهجمات السيبرانية... لكنّ علينا أنْ نسأل فيما إذا كانت الهجمات السيبرانية يمكن عدها عدواناً لا يختلف عن الهجوم باستخدام الصواريخ على سبيل المثال»[١٠٢].

ويضيف قائلاً : «إن مبدأ التناسب في استخدام القوة السيبرانية لا يزال غامضاً ويحتاج إلى أجوبة أهمها كيف يمكن إحراز التناسب في الرد على الهجمات السيبرانية»[١٠٣].

وهذا ما أيده هيوز حيث ذهب بالقول: «إذا تم توجيه هجمات سيبرانية ضد بنى تحتية ثنائية الاستعمال (مدنية–عسكرية) وعن بعد فلا يبدو أنّ الميزة العسكرية ستكون واضحة، ما يجعل من تطبيق مبدأ التناسب في أثناء الهجمات السيبرانية أمراً في غاية الصعوبة»[١٠٤].

إنّ تحقيق التناسب في الهجمات السيبرانية قد يكون مستحيلاً، وذلك لأن تكنولوجيا المعلومات والاتصالات غير متساوية في الدول، ومن ثم قد تكون الدولة الضحية غير متطورة من ناحية تكنولوجيا الهجوم السيبراني لرد الهجمات السيبرانية الموجهة ضدها[١٠٥]، و إنّ تطبيق مبدأ التناسب يتطلب توقع النتائج المحتملة للنشاط العدائي، وفيما يتعلق بالهجمات السيبرانية و الغموض الذي يكتنف نوع آثار هذه الهجمات و شدتها نتيجة اللامحدودية التي يتمتع بها العقل البشري فإنّ توقع النتائج المحتملة لهذه الهجمات يجعل تطبيق هذا المبدأ يتسم بصعوبة بالغة بالنسبة للقادة العسكريين الذين عليهم في سياق الهجمات السيبرانية مواجهة المزيد من الشكوك والغموض بشأن شرعية الهجمات التي سينفذونها[١٠٦].

ثالثاً: مبدأ التمييز بين المدنيين و المقاتلين

إنّ هذا المبدأ الذي يتطلب من أطراف النزاع التمييز بين الأشخاص المدنيين والمقاتلين، و من ثم توجيه الهجمات للأهداف العسكرية دون المدنية، يقدم تحدياً آخر أمام القانون الدولي. فبموجب هذا المبدأ على القادة العسكريين استخدام الوسائل التي بإمكانها الاستهداف الدقيق

102.Shin Beomchul،، "The Cyber warfare and the Right of Self-Defense: legal perspectives and the case of the United States، IFANS، Vol. 19، No. 1، June2011،p.118.
103،ibid، p118.
104.Rex Hughes، op. cit.، p. 538.
105.Greenberg، L. T.، Information warfare and International Law، Mishawaka: National Defense University Press، 1998، p. 32.
106.Oona Hathaway، op.cit،p.851.

(غير عشوائية الأثر)، للتمييز بين السكان المدنيين والمقاتلين، وأيضاً بين الأعيان المدنية والأهداف العسكرية»[١٠٧].

لقد عرّفت الفقرة الأولى من المادة (٥٠) من البروتوكول الإضافي الأول لعام ١٩٧٧، المدنيين بأنهم: «الأشخاص الذين لا ينتمون إلى القوات المسلحة»[١٠٨]. وقد حدد هذا البروتوكول الأهداف العسكرية في الفقرة الثانية من المادة (٥٢) إذ نص : «تقتصر الهجمات على الأهداف العسكرية فحسب، وتنحصر الأهداف العسكرية فيما يتعلق بالأعيان على تلك التي تسهم مساهمة فعالة في العمل العسكري، سواء كان ذلك بطبيعتها أم بموقعها أم بغايتها أم باستخدامها، والتي يحقق تدميرها التام أو الجزئي أو الاستيلاء عليها أو تعطيلها في الظروف السائدة حين ذلك ميزة عسكرية أكيدة»[١٠٩].

وقد تأكد هذا المبدأ في القانون الدولي العرفي من خلال محكمة العدل الدولية في رأيها الاستشاري بشأن شرعية التهديد أو استعمال الأسلحة النووية، حيث جاء في قرارها: «ينبغي على الدول، ألّا تجعل المدنيين هدفاً للهجوم، وعليه يجب ألّا تستخدم الأسلحة التي لا تميّز بين الأهداف المدنية والعسكرية»[١١٠]، وقد ذهبت المحكمة إلى أبعد من ذلك، فكيّفت هذا المبدأ كقاعدة آمرة بالقول: «مبدأ التمييز هو أحد المبادئ الرئيسة في القانون الدولي الإنساني وأحد مبادئ القانون الدولي العرفي التي لا يجوز انتهاكها»[١١١].

وقد أكدت المحكمة الجنائية الدولية الخاصة بيوغسلافيا السابقة هذا التكييف واعتبرت مبدأ التمييز من القواعد الأساسية في القانون الدولي الإنساني وواجب التطبيق على جميع النزاعات المسلحة الدولية وغير الدولية دون استثناء[١١٢].

١٠٧.اللجنة الدولية للصليب الأحمر، «الملحقان «البروتوكولان الإضافيان لاتفاقية جينيف المعقودة في ١٢ آب أغسطس ١٩٤٩»، مصدر سابق، المادة (٤٨)، ص٤٠.

١٠٨.المصدر السابق،المادة ٥٠،ص٤٠.

١٠٩.المصدر السابق، المادة ٥٢، ص٤٠.

110.ICJ Nuclear weapons Advisory opinion. Op. cit، para 78.

111.Ibid، para 79.

112. ICTY، case II-95-11-R61، 8 March 1996، prosucort v. Matric، para 11.

أمّا في نطاق الهجمات السيبرانية و طبقا لهذا المبدأ فيحظر على أطراف النزاع شن هجمات توجَّه ضد أهداف غير عسكرية يقصد بها أو يتوقع منها أن تتسبب بالموت أو الإصابة أو التلف أو الدمار.

لقد أكد الخبراء في دليل تالين في المادة (٣٨) منه على ما جاء في المادة (٥٢) من البروتوكول الإضافي الأول وأضافوا عليه نصاً يقول فيه :»إنّ الأهداف العسكرية قد تكون الكمبيوترات، شبكات الكمبيوتر والبنى التحتية السيبرانية»[١١٣].

إنّ تطبيق مبدأ التمييز على الهجمات السيبرانية في بعض الحالات قد يكون سهلاً فعلى سبيل المثال إنّ الهجوم السيبراني، الذي يستهدف نظام مراقبة الحركة الجوية العسكرية وبالتالي التسبب في حوادث نقل القوات العسكرية، سيكون شرعياً وغيرَ مخالفٍ لمبدأ التمييز[١١٤].

أما الهجوم السيبراني على المستشفيات و المتاحف و دور العبادة أو القطاع المصرفي المدني أو الشبكات التي تديرها، فيعد هجوماً غيرَ مشروعٍ إذ يخرق بوضوح مبدأ التمييز الوارد في القانون الدولي الإنساني[١١٥].

إنّ تطبيق مبدأ التمييز على الهجمات السيبرانية يتسم بكثير من التعقيد، وذلك لتشابك الاستخدام المدني والعسكري لنفس الشبكات حيث إن خمسةً وتسعين بالمئة (٩٥٪) من الاتصالات العسكرية تستخدم الشبكات المدنية في بعض المستويات، لذا من الممكن أن تكون الشبكات المدنية أهدافاً عسكرية جذابة[١١٦].

و بموجب الفهم التقليدي للأعيان ذات الاستخدام المزدوج(Dual-Uses) فإنه متى ما أُستخدمت عينٌ معينة لأغراض مدنية وعسكرية على حدٍ سواء فإن تلك العين تصبح هدفاً عسكرياً مشروعاً، إذا أسهمت مساهمة فعالة في العمل العسكري أو تحقق تدميرها ميزة عسكرية

113.Tallinn manual on the International Law Applicable to cyber warfare، op. cit.، p. 125.

114.Michael N. Schmitt، wired warfare: Computer Network attack and the Jus in Bello، in computer Network attack and International Law 187، 195 (Michael N. Schmitt 8 Brian To' Donnell eds.، 2002).

115.Oona Hathaway، op. cit.، p. 852.

116.Vida M. Antolin-Jenkins، Defining the parameters of cyberwar operations: Looking for law in all the wrong places? 51 Naval، REV، 132، 140، (2005).

أكيدة بشرط أن تراعي مبدأ التناسب بشأن الأضرار التي تلحق بالمدنيين[١١٧].

أمّا في الفضاء السيبراني فإن كثيراً من الأعيان التي تشكل بنيته الأساسية هي مزدوجة الاستخدام، ما يجعل منها أهدافاً عسكرية غير مشمولة بالحماية سواء من الهجمات الحركية أم السيبرانية، إلا إنّ ذلك يبقى محكوماً بحظر الهجمات العشوائية و بقواعد التناسب واتخاذ الاحتياطات المستطاعة في أثناء الهجوم، ولأن الشبكات الإلكترونية المدنية والعسكرية مترابطة إلى حد بعيد، فيجب توقع الضرر المدني العرضي في معظم الحالات[١١٨].

أما التحدي الأصعب في تطبيق مبدأ التمييز على الهجمات السيبرانية، فهو تمييز المدنيين عن المقاتلين، وذلك لعدة أسباب منها، إن الهجوم السيبراني غالباً ما يتم عن طريق أشخاص قد يبعدون عن محل الهجوم مسافات قد تتجاوز مئات الأميال، وهذا ما يجعل التمييز بين المقاتل والمدني صعباً للغاية إنْ لم يكن مستحيلاً[١١٩].

وقد تقوم الدول بتقويض مبدأ التمييز من خلال استخدامها المدنيين في تنفيذ الهجمات السيبرانية، حيث بفعلها هذا تضع أولئك المدنيين خارج نطاق الحماية التي يتمتعون بها بموجب القواعد الدولية، وذلك لمشاركتهم في الأعمال القتالية[١٢٠].

والدول تقوم بذلك إمّا لكون أولئك المدنيين يمتلكون خبرات تقنية لا تمتلكها الحكومات أو لإخفاء أو إنكار تورطها في تنفيذ الهجمات السيبرانية خوفاً من تعرضها لهجمات مضادة أو اعتبار استخدامها لتلك الهجمات استخداماً غير شرعي للقوة[١٢١].

١١٧.حماية الأعيان المدنية في القانون الدولي الإنساني، ٢٠٠٨ بحث منشور على الموقع: (آخر زيارة بتاريخ ٢٠١٦/٩/١)

http://www.mezan.org/uploads/files/8798.pdf

١١٨.اللجنة الدولية للصليب الأحمر، تقرير عن القانون الدولي الإنساني والنزاعات المسلحة المعاصرة، المؤتمر الدولي الثاني والثلاثون للصليب الأحمر والهلال الأحمر (قوة الإنسانية)، جنيف، سويسرا ٨-١٠ كانون الأول/ديسمبر ٢٠١٥. رقم الوثيقة 32IC/15XXX.

١١٩.أحمد عبيس نعمة الفتلاوي، مصدر سابق، ص٦٣٢.

120.Oona Hathaway، op. cit.، p. 854.

121.Geffrey Carr، Inside Cyber Warfare 2010، p. 46.

رابعاً: مبدأ مارتنزMartinus Clause

جاءت تسمية (مارتنز) نسبة إلى الدبلوماسي الروسي فيدور فيودوف جمارتنز أحد مندوبي روسيا في مؤتمر السلام عام ١٨٩٩، الذي صرح فيه: «في الحالات غير المشمولة بالأحكام، يظل السكان المتحاربون تحت حماية وسلطان مبادئ قانون الأمم كما جاءت من تقاليد استقر عليها بين الشعوب المتمدنة وقوانين الإنسانية ومقتضيات الضمير العام»[١٢٢].

و يطلق على الشرط تسمية «المبدأ البديل أو الاحتياطي» كونه يطبق في حال عدم وجود نص يحمي الشخص المعني، بخصوص حالة لم يرد بها نص صريح.تتجسد أهمية هذا المبدأ في تضييق نطاق أيّ تفسير، تتعمد الدول من خلاله إضفاء الشرعية على استخدام الهجمات السيبرانية دون قيد أو شرط بحجة عدم الاتفاق على ما يقيدها بموجب القانون الدولي الإنساني رغم حظر الأخير صراحة استعمال طرق القتال و وسائله التي لا تميز بين المدنيين والمقاتلين، فضلاً عن إحداث إصابات مفرطة الضرر، فجاء شرط مارتنز ليؤكد أصالة هذه المبادئ، ومن ثم لا يمكن الاحتجاج مطلقاً بشرعية إطلاق استعمالها.

وقد ورد هذا الشرط في مقدمة اتفاقيات لاهاي لعامي ١٨٩٩ و ١٩٠٧ المتعلقة بقواعد وأعراف الحرب البرية وكذلك في اتفاقيات جنيف لعام ١٩٤٩ كما تم إدراجها في البروتوكول الإضافي الأول لعام ١٩٧٧، حيث نصت الفقرة الثانية من المادة الأولى بأنه: «يظل المدنيون والمقاتلون في الحالات التي لا ينص عليها في هذا البروتوكول، أو أي اتفاق دولي آخر، تحت حماية وسلطان مبادئ القانون الدولي، كما استقر عليه العرف ومبادئ الإنسانية وما يمليه الضمير العام[١٢٣].

وقد أكد عليه البروتوكول الإضافي الثاني لعام ١٩٧٧ في ديباجته حيث ورد: «في الحالات التي لا تشملها القوانين السارية، يظل شخص الإنسان في حمى المبادئ الإنسانية وما يمليه الضمير العام»[١٢٤].

122.Antonio Gessese، "The Martens Clouse: Half a loaf or simply pien the sky? " EJIL (2000)، Vol. III، No. 1، p. 187-194.

١٢٣.اللجنة الدولية للصليب الأحمر، «الملحقان، البروتوكولان الإضافيان إلى اتفاقيات جينيف الأربعة لعام ١٩٤٩، مصدر سابق، ص١١٨.

١٢٤. المصدر السابق، ص٩٣.

أمّا في سياق الهجمات السيبرانية فيمكن الاستناد إلى ما أورده القاضي شهاب الدين في الرأي الاستشاري الصادر عن محكمة العدل الدولية عام ١٩٩٦ بخصوص شرعية التهديد واستعمال الأسلحة النووية حيث أكد على: «يمنح شرط مارتنز سلطة معالجة مبادئ القانون الإنساني وما يمليه الضمير العام بوصفهما مبادئ من القانون الدولي، تاركاً المحتوى الدقيق للمعيار الذي ستلزمه مبادئ القانون الدولي على ضوء الظروف المتغيرة، بما في ذلك التغيرات في وسائل الحرب ومستويات مظهر المجتمع الدولي وتسامحه»[١٢٥]. كما ذهبت المحكمة في رأيها الاستشاري بأن شرط مارتنز «أثبت أنه وسيلة فعالة لمواجهة التطور السريع في التكنولوجيا العسكرية»[١٢٦]، وعلى هذا الأساس أكدت المحكمة أنّ المبادئ الأساسية للقانون الإنساني تظل منطبقة على جميع الأسلحة الجديدة بما فيها الأسلحة النووية، وذكرت إنه لا توجد دولة تجادل في ذلك[١٢٧].

وبشأن دحض القول بعدم وجود تنظيم قانوني للهجمات السيبرانية يذهب إيركيكودار(ErkiKodar) وكيل وزارة الدفاع للشؤون القانونية والإدارية في جمهورية إستونيا وأحد واضعي دستورها إلى القول: «إنّ مبدأ مارتنز يشير إلى أنه في حالة عدم وجود ذكر واضح في الاتفاقيات الدولية المعاصرة أو العرف، فإن مبادئ التقييد التي تضمنها قانون النزاعات المسلحة ستبقى المطبقة في هذه الحالة»[١٢٨].

وقد أشار شميت (Schmitt) إلى انطباق هذا الشرط على الهجمات السيبرانية بقوله: «يعد مبدأ مارتنز المبدأ الأكثر قرباً لكونه يغطي أوضاعاً غير منظمة في الاتفاقيات الدولية، ولا يكون ذلك ممكناً إلا باللجوء إلى القانون الدولي الإنساني العرفي، ذلك المصدر المهم الذي أشارت إليه المادة (٣٨) من النظام الأساس لمحكمة العدل الدولية»[١٢٩].مما سبق يتبين أن عدم وجود قواعد دولية محددة –عرفية كانت أم تعاهدية – تنظم الهجمات السيبرانية، لا يعني الإقرار ضمناً بجواز اللجوء إليها، لأنها تتنافى بطبيعتها مع القوانين الإنسانية وما يمليه الضمير العام العالمي في حال أنها استهدفت منشآت تحوي قوى خطرة كالمحطات النووية وأنابيب النفط أو أعيان مدنية ضرورية لبقاء

125.ICJ Nuclear weapons Advisory opinion، op. cit.، Dissenting opinion of Judge Shah abuddeen، pp. 22-23.

126.ICJ Nuclear weapons Advisory opinion، para 78.

127.Ibid، para 86.

128.ErkiKodar، Applying the law of Armed conflict to cyber Attacks: from the Martens clause to Additional protocol I"، ENDC Proceeding، volume 15، 2012، p. 110.

129.Michael N. Schmitt، wired warfare: Computer Network attack and the Jus in Bello، op. cit.، p. 369.

الإنسان كشبكات الكهرباء والمياه[١٣٠].

خلاصة القول إن شرط مارتنز يعد صمّام الأمان الذي يمنع الدول وغيرها من الأطراف المتنازعة من استخدام و استحداث وسائل قتال جديدة كما يقطع الطريق أمام الدول للتهرب من المسؤولية بحجة عدم وجود قواعد قانونية تحكم الوسائل والأساليب الجديدة التي لم يتطرق إليها القانون الدولي الإنساني، و هو ما يمكن التعويل عليه في تحريك المسؤولية الدولية الناشئة عن الهجمات السيبرانية، لسد الذريعة بعدم وجود أحكام دولية صريحة تحظر استخدامها.

الدول ومسؤوليتها عن الهجمات السيبرانية

قبل ظهور وسائل الاتصال الإلكترونية (Digital Instructions)،كانت القوة والقيادة من نصيب أصحاب التفوق العسكري والهيمنة الاقتصادية. أما اليوم فقد غيرت وسائل الاتصال الإلكترونية جذرياً من هذا التوازن في القوة، فأصبحت تمثل واحدة من أكثر التحديات المهمة التي تواجه السلام العالمي. وأصبحت المسألة الكبرى كفالة الدول عدم استعمال البنية التحتية الحرجة للاتصالات سلاحاً ضد المدنيين والأعيان المدنية[١٣١].

إنّ تكنولوجيا المعلومات والاتصالات تثير تحدياً غير مسبوق أمام البلدان بشأن أمنها القومي. فأصبح بموجب هذا التطور بإمكان الأفراد إحباط السلطة، وتنفيذ هجمات سيبرانية قد تؤدي إلى شلّ البنية التحتية بأكملها وتعطيل الاتصالات وإحداث أضرار جسيمة في الأرواح والممتلكات، وأصبح بإمكان الدول الأضعف بقليل من الخبرات التقنية أن تمثل تهديداً لأمن أكبر الدول[١٣٢].

إنّ الأساس الحالي لشبكة الاتصالات في الفضاء السيبراني وبروتوكول التحكم بالإرسال وبروتوكول الإنترنت يعود تاريخه إلى عام ١٩٨٢، وهذا نظام اتصال قديم صُمّم أساساً لمجموعة صغيرة من الباحثين والأكاديميين لتبادل المعلومات فيما بينهم في بيئة منخفضة المخاطر من ناحية التعرض للانتهاك، وخطر الانتهاك يمثل صميم مشكلة تتبع الهجمات السيبرانية[١٣٣]، إلا إن هذه

١٣٠.احمد عبيس نعمة الفتلاوي، مصدر سابق، ص٦٣٤.
١٣١.علي قاسمي و ويكتور بارين جهاربخش، مصدر سابق، ص ١١٦.
١٣٢.المصدر السابق، ص ١١٦.
133.Lipson، H.F.، Tracking and Tracing cyber-attacks: Technical challenges and Global policy Issues، CERT Coordination center، 2002، p. 14.

ليست المشكلة الوحيدة بل نقاط ضعف النظام تشكل صعوبات مضاعفة عندما نأخذ بنظر الاعتبار البرمجيات العديدة الموجودة حالياً.

فعلى سبيل المثال، إنّ تحديد مصدر الهجوم الذي يظهر هو غير موثوق بحد ذاته بسبب إمكانية التلاعب به، ومن ثم إنكاره[١٣٤]، ومثال على ذلك ما حصل في الهجمات السيبرانية التي وقعت عام ١٩٩٩ ضد وزارة النقل الأمريكية عن طريق خوادم (servers) في مريلاند التي تدار من قبل أتباع حركة فالون غونغ موفمنت(Falun Gong movement) لإظهار أن تلك الهجمات قد تمت من قبل تلك الحركة لجعلها تتحمل مسؤولية الفعل، إلا إن الحقيقة هي أن تلك الهجمات كانت تهدف إلى تخريب خواديم كلاً من مريلاند ووزارة النقل الأمريكية غير أن الولايات المتحدة الأمريكية لم تتمكن من تحديد المسؤول عن ذلك بصورة قطعية إلى وقتنا الراهن [١٣٥]. ولأجل البحث في تحديات تحريك المسؤولية الدولية بشأن الهجمات السيبرانية سنتطرق إلى الشروط واجبة الإتباع لتحريك المسؤولية وهي:

أولاً: إسناد الهجوم السيبراني

بشأن المسؤولية الدولية عن الهجمات السيبرانية ً، إنّ من شروط قيام المسؤولية الدولية عموماً هو إسناد التصرف إلى الدولة. أما فيما يخص الهجمات السيبرانية فهناك صعوبات بالغة في إسنادها و ذلك يرجع إلى صعوبة تتبع مصدر الهجمات المتطورة التي ينفذها قراصنة محترفون سواء كانوا يعملون بشكل خاص أو مدعومين من قبل دولة[١٣٦]. إنّ إسناد الهجوم السيبراني إلى الدولة، هو أحد العناصر الأساسية إنْ لم يكن الوحيد في بناء النظام القانوني الذي يعنى بمكافحة الهجمات السيبرانية، فقوانين الحرب تتطلب تعريف الدولة عن نفسها عند مهاجمتها دولة أخرى على الرغم من عدم امتثال الدول لهذا التقليد في أغلب الأحيان[١٣٧].

134.Michael N. Schmitt، Heather A. Harrison and Thomas C. Wingfield، computers and war: Legal Battle space background paper prepared for informal high-level expert meeting on current challenges to international humanitarian law، Cambridge، June 25-27-2004، p.99.

١٣٥.سراب ثامر احمد، مصدر سابق، ص١٢٨.

136.Scott J. Shackelford، State responsibility for cyber attacks: Competing standards for a growing problem، University of Cambridge، Dept of Politics and International Studies، Cambridge. U.K. 2009، p. 201.

137.Brenner S.W. &Grescenzi A.C.، State-Sponsored crime: The futility of the Economic Espionage Act، Houston Journal International Law، 28، 2006، (pp 389-464)، p. 398.

إنّ المسؤولية إما أنْ تكون مباشرة أو غير مباشرة، وتتحرك المسؤولية المباشرة للدولة عن الهجمات السيبرانية في حال قيام أيٍّ من هيئاتها كالوكالات الاستخبارية أو الجيش أو الأمن الداخلي مثلاً، بأنشطة سيبرانية تؤدي إلى خرق التزام قانوني دولي ولا يهم كون الفعل محل النقاش قد تم بالتطبيق لتعليمات صريحة من الدولة أو من دونها طالما أن تلك الهيئة تتصرف بصفة رسمية بوصفها أداة للتعبير عن إرادة الدولة[١٣٨]. وكذلك بموجب مشروع مواد مسؤولية الدول لعام ٢٠٠١، فإن الأشخاص والكيانات التي هي ليست من هيئات الدولة، إلا إنها تحمل تخويلاً رسمياً بموجب القانون الداخلي، عند قيامها بأنشطة سيبرانية غير مشروعة تثير مسؤولية الدولة التي زودتها بالتخويل. على سبيل المثال قيام حكومة دولة معينة بتزويد شركة خاصة بتخويل رسمي للقيام بتنفيذ هجمات سيبرانية ضد دولة أخرى أو تزويد كيان خاص بسلطة رسمية تخوله القيام بعمليات إلكترونية لجمع المعلومات الاستخبارية (Computer Network Exploitation) فإن ذلك يثير مسؤولية الدولة في حال خرق تلك الكيانات، قواعد القانون الدولي[١٣٩].

وهنا يتبادر إلى الذهن تساؤلٌ بشأن أفراد أو جماعات ينفذون هجمات سيبرانية ضد البنى التحتية المعلوماتية أو الحيوية التابعة لدولة أخرى وهم ليسوا من أجهزة الدولة أو ممن لديهم تخويل من الدولة فكيف يمكن مساءلتهم؟ و بعبارة أخرى كيف تتم عملية إثبات مسؤولية الدولة غير المباشرة عن أعمال تلك المجموعات؟

إنّ الإجابة تكمن في مدى سيطرة الدول على تلك المجموعات أو الأفراد ونوع الرابطة بينهم، إذ إنّ المسؤولية غير المباشرة للدولة تقوم عند قيام الدولة بدعم جماعات مسلحة لتنفيذ هجمات سيبرانية خارج إقليمها أما مقدار هذا الدعم فهو الذي يحدد مسؤولية الدولة عن أفعال تلك الجماعات وسنبين ذلك في ضوء معياري السيطرة الكاملة (Overall Control) والسيطرة الفعالة (Effective Control).

١- بموجب معيار السيطرة الكاملة (Overall Control)

إنّ هذا المعيار تم ذكره لأول مرة من قبل محكمة العدل الدولية في قضية الأنشطة العسكرية و شبه العسكرية في أو ضد نيكاراغوا عام ١٩٨٦حيث ذهبت إلى تحديد مفهوم السيطرة الكاملة بأنه : «معيار يحدد إسناد تصرفات الأفراد أو المجموعات المسلحة أو الكيانات إلى الدولة بذاتها»

١٣٨. عبد الكريم علوان، الوسيط في القانون الدولي العام، دار الثقافة، عمان، ٢٠١٠، ص١٦٣.
١٣٩.سراب ثامر احمد، مصدر سابق، ص١٣٠.

و بينت ذلك بالقول : « إنّ مثل هذه التصرفات لابدَّ أنْ تكون تحت رقابة صارمة من الدول و يعامل الطرف الآخر، وكأنّه جهاز تابع لها، و في حال ثبوت ذلك يمكن تحريك المسؤولية الدولية ضد الدولة عن انتهاكات الأفراد أو المجموعات المسلحة أو الكيانات «[١٤٠].

و قد ذهبت المحكمة الجنائية الدولية الخاصة بيوغسلافيا السابقة في قضية تاديتش(Tadic) في تحديد مسؤولية الدولة عن ما ينسب إليها من انتهاكات ارتكبتها مجموعات مسلحة مدعومة من قبلها بالقول :»... كان للدولة دور في التنظيم والتنسيق، فضلاً عن تزويد المجموعة المسلحة بالدعم، ما يعني أنّ لها السيطرة الكاملة عليها، وما يصدر عن المجموعات المسلحة تلك، يعني أنه صادر عن الدولة نفسها»[١٤١].

و قد ذهب الفقهاء إلى اعتبار تلك المجموعات بحكم الجهاز التابع للدولة فعلى سبيل المثال ذهب ديريك جنكز(Derek Jinks) إلى القول:» على الرغم من أنّ الدولة كقاعدة عامة لا يمكن مساءلتها عن تصرفات كيانات لا توصف بأنها دولة (non-State Actors)، إلا إنّ الفقه حاول معالجة هذه المعضلة، من خلال عدَ التصرفات التي تقوم بها تلك الكيانات بمثابة تصرفات صادرة عن الدولة نفسها، على وفق مبدأ (الواقع القانوني)[١٤٢]، و بعبارة أخرى عدِّها أجهزة تابعة للدولة بحكم الواقع القانوني، ما يعني إمكانية توجيه المسؤولية ضد الدولة، تحت طائلة ممارسة السلطة العامة و إنْ كانت ظاهرياً كيانات تمارس تصرفات خاصة و مستقلة عن الدولة»[١٤٣].

إنّ اعتماد معيار السيطرة الكاملة في تقرير مسؤولية الدول عن أعمال مجموعات مسلحة مدعومة من قبلها قد يكون الخيار الأرجح فيما يتعلق بالهجمات السيبرانية وذلك لصعوبة إثبات ارتباط الدولة ومدى سيطرتها على منفذي الهجمات السيبرانية بشكل قطعي بموجب معيار السيطرة الفعالة الذي سنتطرق إليه بالبحث لاحقاً، وقد ذهب سكوت شاكلفورد (Scott Shackelford) إلى تأييد ذلك بقوله: «إذا كان على القانون الدولي الاكتفاء بتطبيق معيار

140.ICJ،Military and Parmilitary Activities in and against Nicaragua (Nicar v. U.S)op.cit، para.109
141.ICTY، Prosecutor v. Tadic، 1995، para 70

١٤٢.إن مصطلح بحكم الواقع(De Facto) هو مصطلح قانوني يستخدم عادة للتعامل مع تصرف قانوني، و كأنه واقعة قانونية، دون البحث في مشروعيتها القانونية،ينظر قاموس المعاني القانونية،على الرابط الإلكتروني،آخر زيارة ٢٠١٦/٦/١٨:

http://legal-dictionary.thefreedictinary.com/de+facto

143.DerekJinks،"State Responsibility for the Acts of Private Armed Groups"، Forthcoming، 4 CHICAGO J.INT'L L.، 2003، p.1.

واحد على الحرب السيبرانية فمن الضروري أن يتم الاعتماد على معيار السيطرة الكاملة كجزء من نظام دولي مستقبلي في الفضاء السيبراني[١٤٤].

٢- بموجب معيار السيطرة الفعالة (Effective Control)

إنّ هذا المعيار تم التطرق إليه أولاً عند محكمة العدل الدولية في قضية نيكاراغوا ضد الولايات المتحدة سابقة الذكر[١٤٥] تحديداً، وقد ذهبت المحكمة إلى أنّ معيار السيطرة الفعالة على العمليات هو المعيار المناسب للتطبيق على الأقل بشأن القوات شبه العسكرية[١٤٦].

إنّ مضمون هذا المعيار هو إذا كانت الجهات شبه العسكرية أو غير الحكومية تعتمد في تصرفاتها بشكل كبير على دولة ما ومع ذلك تحتفظ باستقلاليتها فإن أعمال تلك المجموعة قد تنسب إلى تلك الدولة بشرط إثبات ذلك الارتباط. وهذا ما ذهب إليه غالبية الفقهاء في حكم محكمة العدل الدولية في قضية نيكاراغوا ضد الولايات المتحدة[١٤٧]. وبالمثل فإن ذات المعيار قد ينطبق على الهجمات السيبرانية، فقد تقدم دولة ما على الاتفاق مع شركة أو أحد المواطنين أو مجموعة منهم للقيام بعمليات سيبرانية ضد دولة أخرى، فضلاً عن قيام الدولة بالمساعدة في تمويل المهارات والخبرات، لأجل التخطيط للقيام بهجمات سيبرانية، فإن ذلك كله يؤدي إلى إثارة مسؤولية الدولة على أساس السيطرة الفعالة التي لا تقتصر على مجرد التمويل المادي أو التجهيز بل يمتد إلى الاشتراك بالتخطيط والإشراف، مع أنّ تلك المجموعة تبقى تتمتع بدرجة عالية من الاستقلال عنها[١٤٨].

وفي هذه الحالة إنّ دعم الدولة للهجمات السيبرانية لا يثير مسؤوليتها، إلا إذا ثبتت سيطرتها الفعالة على مُنفِّذي الهجمات بشكل قطعي ولا يَدَعُ مجالاً للشك ونظراً للصعوبات التقنية البالغة في إثبات هوية مصدر الهجمات السيبرانية، فإن هذا المعيار يقدم بطاقة دخول مجانية إلى الدول

144.Scott Shackelford، op. cit.، p. 203.

145.ICJ، Nicaragua Judgment، op. cit.، para 115.

146.Capaldo G. Z.، providing a right of Self-Defense Against Large Scale Attack by Irregular Forces: The Israeli-Hezbollah Conflict،Harvard International Law Journal Online،48،2007،(pp.101-112)،p.104

147.R. J. P. Pronk. ICTY Issues final judgment against DusanTadic in first international war crimes tribunal since world war II، Human rights brief، center for human rights and humanitarian law، 1997.

148.Antonio Cassese،"The Martens Clouse: Half a loaf or simply pien the sky? " EJIL (2000)، Vol. III، No. 1، p. 652.

الداعمة لتلك الهجمات[١٤٩].إنّ اعتماد معيار السيطرة الفعالة دون أيّ تقنيات جديدة في تتبع مصادر الهجمات قد يجعل البحث في مسؤولية الدول عن الهجمات السيبرانية غير ذي جدوى ولذلك الحين يمكن القول:إنّ فقدان أو إتلاف البيانات قد يكون كافياً لإثبات سيطرة الدولة وإنزال المسؤولية عليها[١٥٠].

لقد ذهبت محكمة العدل الدولية في أحدث قضية لها بشأن تحديد المسؤولية الدولية، وهي قضية الإبادة الجماعية في البوسنة[١٥١]، إلى الأخذ بمعيار السيطرة الفعالة لكن بشكل أكثر تقييداً. وقد انتقد القاضي أنطونيو كاسيزي هذا الحكم واعتبره «غير واقعي» ذلك لأنه «يتطلب مستوى عالياً من الإثبات» وهذا المستوى يكاد يكون من المستحيل تحقيقه في سياق الهجمات السيبرانية[١٥٢].

إنّ هذين المعيارين وإنْ كانا يوفران بعض الدعم اللازم لتقرير مسؤولية الدولة عن انتهاكات القانون الدولي عن طريق استخدام الهجمات السيبرانية، إلا إن الاستناد اليهما كلياً من دون وضع اتفاقية دولية تعنى بهذه الهجمات قد يكون أمراً غير واقعي[١٥٣] وذلك لصعوبة تحديد هوية المهاجم لاتخاذ الإجراءات اللازمة لتحريك المسؤولية الدولية ضد الدولة التابع لها والمسؤولية الجنائية الدولية ضد مرتكب الهجمات ذاته، فضلاً عن صعوبة كبح أيّ توجهات لارتكاب هجمات مماثلة في المستقبل وذلك لأنّ هذه الهجمات تتخذ من الفضاء السيبراني مجالها الرحب لكونها تصرفات غير مادية ولا يمكن إثباتها بالطرق العادية[١٥٤].

149.Scott Shackelford، op. cit.، p. 202.
150.Ibid، p.202.
151.ICJ، Case of: Bosnia and Herzegovina. V. Serbia and Montenegro، 2007.
152.C. Tosh، Genocide Acquittal provokes legal Debate، Institute for War and Peace Reporting، March 2، 2007.
153.H. F. Lipson،Tracking and Tracing cyber-attacks: Technical challenges and Global policy Issues، CERT Coordination center،p.3.
١٥٤.ينظر أحمد عبيس نعمة الفتلاوي، مصدر سابق، ص٦٣٨-٦٣٩.

ثانياً: الهجوم السيبراني غير المشروع

إنّ الشرط الثاني لقيام مسؤولية الدول هو الفعل غير المشروع والضار أما في سياق الهجمات السيبرانية فإنها لا تشكل عملاً غير مشروعٍ إلا في الحالات الآتية:

١-خرق مبادئ ميثاق الأمم المتحدة كأن يرقى الهجوم إلى مستوى استخدام القوة من خلال الوسائل الإلكترونية في حال إسنادها إلى دولة معينة.

٢-خرق الالتزامات الدولية التي يفرضها القانون الدولي الإنساني كاستهداف الأعيان المدنية بهجمات سيبرانية، كالنظم المعلوماتية التي تتحكم في الإمداد بالطاقة الكهربائية، إذا ما أسندت إلى دولة معينة.

٣-خرق القواعد الدولية في وقت السلم وخارج سياق النزاع المسلح كخرق مبدأ عدم التدخل في شؤون دولة معينة[١٥٥].

ومن ناحية أخرى إنَّ الهجوم السيبراني يعد غير مشروع بموجب القانون الدولي إذا ألحق بالدولة المستهدفة ضرراً ما، يخولها اللجوء إلى التدابير المضادة بما فيها الإلكترونية لوقف الدولة مصدر الهجوم عن خرق قواعد القانون الدولي بشرط إنذار الدولة مصدر الهجوم مسبقاً باتخاذها تلك التدابير[١٥٦]. إلا في حالة الضرورة حيث يجوز للدولة المتضررة اتخاذ التدابير المضادة دون إنذار مسبق وذلك لحفظ حقوقها[١٥٧]. إنّ التدابير المضادة ترمي إلى إرغام الدولة مصدر الهجوم على إيقاف خرقها للقواعد الدولية وبالتالي يجب أنْ لا تتعارض تلك التدابير مع:

«١-الالتزام بالامتناع عن استخدام القوة أو التهديد بها طبقاً لميثاق الأمم المتحدة وعدم وصول تلك الاجراءات المضادة إلى مستوى الهجوم المسلح.

٢-الالتزامات المتعلقة بحماية حقوق الإنسان الأساسية.

١٥٥.سراب ثامر احمد، مصدر سابق، ص١٢٨.

١٥٦. الجمعية العامة للأمم المتحدة، «تقرير لجنة القانون الدولي عن أعمال دورتها الثالثة والخمسين»، مصدر سابق، المادة (٤٣).

١٥٧.المصدر السابق، المادة (٥٢/ف٢) ينظر كذلك:

Tallinn manualon the international law applicable to cyber warfare، op. cit.، Chapter I، section II، rule 6.

٣-الالتزامات ذات الطابع الإنساني التي تمنع الأعمال الانتقامية.

٤-جميع الالتزامات الأخرى التي تتفق مع المعايير العامة في القانون الدولي»[١٥٨].

وإنّ التدابير المضادة يجب أن تتناسب مع الفعل الضار، أي: أنْ يكون رد فعل الدولة المتضررة مناسباً للفعل غير المشروع لأجل أن لا يخلَّ بمبدأ التناسب[١٥٩]. على سبيل المثال، عند قيام الدولة (ب) بتنفيذ هجمات سيبرانية ضد محطة توليد الكهرباء في السد التابع لدولة (أ) لإجبار الأخيرة على زيادة تدفق المياه إلى النهر الذي يمر عبر الدولتين، فإن رد الدولة (أ) بعمليات سيبرانية ضد أنظمة التحكم بالري التابعة لدولة (ب) يكون تدبيراً مضاداً قانونياً متناسباً مع الهجوم[١٦٠].

وتأكيداً على ذلك ذهبت محكمة التحكيم في قضية تفسير الاتفاق الجوي بين فرنسا والولايات المتحدة الأمريكية بالقول: «... إنّ الاجراءات المعاكسة (المضادة) تهدف إلى توطيد أركان الشرعية بين الفرقاء المعنيين»[١٦١].أما إذا كانت آثار الهجوم السيبراني من الجسامة والشدة مما يبلغ مستوى الهجوم المسلح، فعند ذاك يجوز للدولة المستهدفة اللجوء إلى حق الدفاع الشرعي بموجب المادة (٥١) من ميثاق الأمم المتحدة.

١٥٨.المصدر السابق، أ. ب. ج. د/ ف١/م٥٠.

١٥٩.الجمعية العامة للأمم المتحدة، «تقرير لجنة القانون الدولي عن أعمال دورتها الثالثة والخمسين»، مصدر سابق،، المادة (٥١) ينظر كذلك:

Tallinn manualon the international law applicable to cyber warfare، op. cit، Chapter I، section II، rule 9.

160.Tallinn manual on the international law applicable to cyber warfare، op. cit، p. 37.

١٦١. قرار محكمة التحكيم بين فرنسا والولايات المتحدة الأمريكية في ٩ كانون الأول ١٩٨٧.

الخاتمة

إنّ الهجمات السيبرانية هي إحدى أهم التحديات المعاصرة التي تواجه المجتمع الدولي، لما لها من تداعياتٍ على الأمن القومي للدول و تهديدٍ للسلم و الأمن الدوليين. لكنها مازالت من المفاهيم الحديثة التي لا يوجد اتفاق دولي بشأن تعريفها مما يؤدي إلى صعوبة تكييفها و تحديد المسؤولية الدولية عنها.

– تكمن الميزة النسبية للهجمات السيبرانية في انخفاض تكاليفها و سهولة اللجوء إليها إذ لا تتطلب حشوداً من المقاتلين العسكريين و الآلاف من الأسلحة والوسائل كالنزاعات المسلحة التقليدية،بل يكفي لتنفيذها شخص أو مجموعة صغيرة ممن لديهم الخبرة و المهارة في التكنولوجيا السيبرانية وثغرات البرامج والأنظمة الكمبيوترية لاستخدامها ضد دولة أو دول أخرى، إلا إن هذه الميزة تتحول إلى 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.

– فيما يخص الهجمات السيبرانية التي تحدث في أثناء النزاع المسلح التقليدي فقد أجمع الفقهاء الدوليون على خضوعها للقانون الدولي الإنساني؛ إلا إن التحدي الأكبر هو تلك الهجمات التي تحدث في وقت السلم و مدى إمكانية عدها هجوماً مسلحاً يثير حق الدفاع الشرعي، ومتى تعد خرقا لمبدأ «عدم التدخل» الذي يسمح فقط باستخدام التدابير المضادة و الطرق السلمية الأخرى في مواجهتها.

– إنّ تحديد مسؤولية الدولة عن الهجمات السيبرانية يتسم بصعوبات بالغة، و ذلك لصعوبة إسناد الهجوم إلى الدولة لأن المهاجمين السيبرانيين غالباً ما يستخدمون برامج تَخَفٍ، تؤدي إلى صعوبة بل استحالة الوصول إلى مصدر الهجوم في أغلب الأحيان. و حتى لو تم الوصول إلى مصدر الهجوم فمن الصعب جداً إثبات ارتباطه مع الدولة خاصة في حالة كون المصدر من الجهات غير الحكومية ما يؤدي إلى صعوبة مضاعفة في إثبات دعم الدولة لتلك الجهة و مقدار هذا الدعم.

– على الرغم من كون الهجمات السيبرانية مفهوماً حديثاً نسبياً و يتطور بسرعة بالغة، إلا إنها لا تحدث في فراغ قانوني و يمكن الاستناد في ذلك إلى آراء و قرارات محكمة العدل الدولية كرأيها بشأن مشروعية التهديد بالأسلحة النووية أو استخدامها، و حكمها في قضية الأنشطة العسكرية

و شبه العسكرية في أو ضد نيكاراغوا، و قضية الإبادة الجماعية في البوسنة، كما يمكن الاستناد إلى قرار المحكمة الجنائية الدولية الخاصة بيوغسلافيا السابقة.

-هناك جهود دولية بذلت في سبيل تنظيم الأنشطة السيبرانية كاتفاقية بودابست ودليل تالين وقرارات صادرة عن الأمم المتحدة، وإنّ هناك قوانين وإنْ كانت سابقة لظهور الهجمات السيبرانية إلا إنها تنظم وسائل وأدوات قد تستخدم في تنفيذها مما يمكن الرجوع إليها، مع ذلك هذه الجهود لم ترْقَ إلى مستوى تنظيم شامل لهذه الهجمات

- تُعدُّ العلاقة بين القانون والتكنولوجيا، علاقة تبادلية فالتطورات التكنولوجية المختلفة تفترض مواكبة التشريعات القانونية لها، سواء على الصعيد الداخلي للدولة أو على الصعيد الدولي، إلا إنّ الأنشطة السيبرانية (خاصة الهجوم السيبراني) تفتقد إلى الأطر القانونية الصارمة للتعامل معها. والتنظيمات والقوانين الدولية المعاصرة وإنْ كانت تنطبق على الهجمات السيبرانية إلا إنها لا تغطي كل أشكال وتحديات الهجمات السيبرانية، فلذلك لابد من عقد اتفاقيات دولية بشأن تنظيم هذه الهجمات بشكل تفصيلي وذلك لحماية المجتمع الدولي من العواقب الإنسانية الوخيمة سواء الدموية منها أم المادية أم البيئية.

-إنَّ عملية وضع تنظيم شامل لهذه الظاهرة الخطيرة تتسم بصعوبات شتى وذلك لأن المصالح الدولية للقوى العظمى تقف حجر عثرة أمامها، كالصعوبات التي واجهت المجتمع الدولي عند وضع اتفاقية بشأن الأسلحة النووية والجدل حول تقييدها أو حظر استخدامها كلياً.