ملخص البحث

يشهد العالم في الفترة الراهنة نوعاً جديداً من سباق التسلح ، لا على غرار المعروفة منها في حقل الأسلحة التقليدية وغير التقليدية، ويقوم هذا السباق على استحداث أو تطوير برامج الكترونية معدة لأغراض عسكرية تعرف اختصاراً بالسايبر (Cyber).

لقد بدأ الباحثون منذ مدة لا تتجاوز خمس سنوات ماضية بالبحث والتحليل القانوني على هذا الموضوع، في ضوء معطيات مؤكدة بأن تهديداً ستتسبب به الهجمات السيبرانية على صعيد السلم و الأمن الدوليين و بمستوى لا يقل جسامة عن اخطر التهديدات المعروفة دولياً.

المقدمة

لأن موضوع الهجمات السيبرانية يحتل مرتبة متقدمة في الجهد القانوني وبالذات عند المؤسسات الدولية المتخصصة من جهة ، ولقلة الأبحاث العربية والعراقية منها بالذات من جهة أخرى، دفعنا ذلك لاختياره ليكون موضوعاً لدراستنا هذه، معولين في إتمامها على تحليل أحكام القانون الدولي العام و الجهود الدولية ذات الصلة بتنظيم استخدامها بالحظر أو التقييد، فضلاً عن أهم الاجتهادات القضائية والفقهية والتي تناولت موضوع الهجمات السيبرانية من زوايا مختلفة.

أن عدداً من الإشكاليات ستثار لدى البحث والتحليل في موضوع الدراسة من أهمها: ما هي السيبرانية وكيف نشأت ؟ هل يمكن أن تصنف ضمن وسائل وطرائق القتال ؟ وإذا كانت كذلك هل ستنطبق عليها أحكام الاتفاقيات الدولية والقواعد العرفية ذات الصلة بسير العمليات القتالية؟

من جانب آخر، نسأل كيف تعامل المجتمع الدولي مع مشكلة الفراغ القانوني الذي يشهده موضوع التنظيم الدولي للسيبرانية ؟ و هل من بارقة أمل ببدء مفاوضات دولية متعددة الأطراف أو ثنائية تنهي الجدل حول شرعية اللجوء إليها في ضوء أحكام القانون الدولي الإنساني والقواعد العرفية المستقرة بين الأمم المتحضرة؟

و ماذا لو استمر إخفاق المجتمع الدولي في التوصل إلى إبرام اتفاقية دولية تعنى بتنظيم السيبرانية للأغراض العسكرية ؟ هل مفتاح الحل يكمن في تدخل الدول الرائدة في مجال تكنولوجيا المعلومات وبالأخص الولايات المتحدة وروسيا والصين أم تتدخل دول أخرى لتقريب وجهات النظر؟

كل هذه الإشكاليات سنحاول الإجابة عنها في ضوء خطة البحث المقسمة على مبحثين: الأول نسلط فيه الضوء على مفهوم الهجمات السيبرانية ، من حيث مصدر كلمة سايبر في اللغة والاصطلاح، فضلاً عن تصفح التاريخ الذي بدأ فيه استخدام الوسائل الالكترونية على هيئة هجمات مسلحة هذا من جهة.

ومن جهة أخرى سنبحث في ابرز النماذج السيبرانية التي وثقتها المؤسسات الرسمية وغير الرسمية ، والتي ستمنح فرصة للاطلاع على حقيقة استخدام التكنولوجية الالكترونية في المجال العسكري والأمني وتحديد آثارها المستقبلية على السلم و الأمن الدوليين.

أما المبحث الثاني فسنركز فيه على التنظيم الدولي المعاصر للهجمات السيبرانية، والتكييف القانوني لها في ضوء مبدأي الحق في اللجوء إلى الحرب (Jus in bellum) و سلوكيات الحرب (Jus ad bello).

وسواء أكان اللجوء إلى السيبرانية محظوراً أم مقيداً وفقاً لأحكام القانون الدولي العام والإنساني منه بالذات ،سنتطرق إلى المسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي الراهن، فضلاً عن البحث والتحليل في الجهود الدولية المعنية بإبرام اتفاقية دولية متعددة الأطراف تحظر أو تقييد الاستخدام الالكتروني للأغراض العسكرية، بالمقارنة مع التشريعات الوطنية لمكافحة الجريمة السيبرانية واتفاقية مجلس أوربا لعام ٢٠٠١.

<u>خطة البحث</u>

المبحث الأول : مفهوم الهجمات السيبرانية.

المطلب الأول: السيبرانية في اللغة والاصطلاح.

الفرع الثاني:مصدر كلمة سايبر (Cyber) في اللغة.

الفرع الثاني : تعريف سايبر (Cyber) اصطلاحاً.

المطلب الثاني: الهجمات السيبرانية : نشأتها ونماذج عنها.

الفرع الأول: نشأة الهجمات السيبرانية.

الفرع الثاني: نماذج منتخبة بشأن الهجمات السيبرانية.

المبحث الثاني: الهجمات السيبرانية في ضوء التنظيم الدولي المعاصر.

المطلب الأول: التكييف القانوني للهجمات السيبرانية.

الفرع الأول: مبدأ الحق في اللجوء إلى الحرب (Jus in bellum).

الفرع الثاني: مبدأ سلوكيات الحرب (Jus ad bello).

المطلب الثاني: المسؤولية الدولية الناشئة عن الهجمات السيبرانية.

الفرع الأول: التنظيم الدولي المعاصر و موقفه من المسؤولية الدولية.

الفرع الثاني: الموقف الدولي من إبرام الاتفاقية الدولية.

المبحث الأول

مفهوم الهجمات السيبرانية

لم تكن الهجمات السيبرانية معروفة إلا في وقت قريب، ما يشكل إحدى أهم التحديات الراهنة التي يواجهها المختصون في القانون الدولي العام ، وبالخصوص في تحديد طبيعتها أو عناصرها، فضلاً عن نطاق هذه الهجمات في ضوء القانون الدولي الإنساني وما يترتب عليها من تبعات المسؤولية الدولية الجنائية كانت أم المدنية .

وما يزيد في اتساع التحدي الذي يواجهه المختصون في القانون الدولي العام، والإنساني على وجه الخصوص، إنما يتجسد في الغموض التي اكتنف مفهوم الهجمات السيبرانية وعدم الاتفاق على تعريف محدد ، يمكن الاستدلال في ضوئه لتنظيم استخدامها بالحظر أو التقييد لمواجهة عواقبها الخطرة على الصعيد الإنساني.[١]

ومن أجل الوقوف على مفهوم الهجمات السيبرانية، سنبحث في نطاق تعريفها لغةً واصطلاحاً في ضوء المعاجم اللغوية، وما درج عليها المختصون في القانون الدولي العام، و خبراء تكنولوجيا المعلومات، فضلاً عن الأحكام الواردة الاتفاقيات الدولية و القوانين الجزائية الوطنية ذات الصلة، وذلك في مطلبين، يتناول الأول تعريف الهجمات السيبرانية في اللغة والاصطلاح، فيما سيركز المطلب الثاني على نشأة الهجمات السيبرانية والنماذج الأكثر حضوراً على المستوى الدولي.

المطلب الأول

السيبرانية في اللغة والاصطلاح

سيتم البحث في فرعين: الأول يركز على المصدر اللغوي لكلمة السيبرانية، فيما سيركز الثاني على مصدر كلمة السيبرانية اصطلاحا في ضوء الاجتهادات الفقهية والممارسات الدولية.

الفرع الأول

مصدر كلمة سايبر (Cyber) في اللغة

تذكر المراجع العلمية بأن عالم الرياضيات نوربرت وينر (Norbert wiener) ، هو أول من استخدم مصطلح السيبرانية وذلك في عام ١٩٤٨، في أثناء دراسته لموضوع القيادة والسيطرة والاتصال في عالم الحيوان، فضلاً عن حقل الهندسة الميكانيكية .[٢]

أما فيما يتصل بالبحث عن مصدر كلمة سايبر (Cyber) في المعاجم اللغوية، فيتضح أنها يونانية الأصل و ترجع إلى مصطلح (kybernetes) ، الذي ورد بداية في مؤلفات الخيال العلمي و يعني القيادة أو التحكُم عن بُعد.[٣]

وبالرجوع إلى قواميس اللغة ، فلم تشر في الغالب إلى مصدر كلمة سايبر (Cyber)، سوى ما وجدناه في قاموس (المورد) إذ يعرفها بالقول:" السيبرانية : هي علم الضبط ، ومصدرها (Cybernetics)"[٤]، وهو مصدر يتطابق مع مفهوم الهجمات السيبرانية ، أي ضبط الأشياء عن بعد والسيطرة عليها.

وما يؤكد ما طرح سلفاً، إن معظم القواميس المتخصصة في المصطلحات العسكرية، لم ترجع كلمة سايبر إلى مصدرها، بل عرفت في نطاق استخدامها الفعلي أي العسكري، كقاموس المصطلحات العسكرية الأمريكية إذ يعرفها :" أي فعل يستخدم عن طريق شبكات الكترونية بهدف السيطرة أو التعطيل لبرامج الكترونية أخرى".[٥]

فيما عرف قاموس مصطلحات الأمن ألمعلوماتي ، مصطلح السيبرانية بالقول: هجوم عبر الفضاء الالكتروني يهدف إلى السيطرة على مواقع الكترونية أو بنى محمية الكترونياً لتعطيلها أو تدميرها أو الأضرار بها".[٦]

أما في اللغة العربية وبالرجوع إلى المختصين فيها ، فنجد أن تحدياً يواجهونه في اختيار مصطلح مقارب لمصطلح (Cyber) في اللغة الانكليزية، ولا أدل على ذلك من أن الترجمة العربية لعنوان اتفاقية مجلس أوربا المتعلقة بالجريمة السيبرانية كانت ترجمة غير صائبة، إذ تُرّجِمَ العنوان (Convention on

Cybercrime) إلى اللغة العربية (الاتفاقية المتعلقة بالجريمة الالكترونية) ويعود السبب في ذلك إلى عدم وجود مصطلح مناظر في اللغة العربية.[٧]

أما سبب اختيار الدراسة لمصطلح السيبرانية ، فيعود إلى المصطلح الذي استخدمه نوربرت وينر في كتابه آنف الذكر وهو (Cybernetic) ، لعدم وجود مصطلح متفق عليه في اللغة العربية من جهة، و لأن الوثائق الصادرة عن الأمم المتحدة باللغة العربية، استخدمت مصطلح السيبرانية نفسه من جهة أخرى.[٨]

الفرع الثاني

تعريف سايبر (Cyber) اصطلاحاً

في هذه الدراسة استخدمنا مصطلح الهجمات السيبرانية (Cyber Attack)،على عكس ما درج عليه البعض من المختصين ، فمنهم من تبنى مصطلح الفضاء السيبراني (Cyber Space)، بالاستناد إلى المحيط الذي تجري فيه العمليات السيبرانية (Cyber Operations) الناشئة عن أداء أنظمة الكترونية مهمتها متابعة وجمع المعلومات التي تعمل الكترونياً وتحليلها ومن ثم اتخاذ إجراءات محددة لمهاجمتها عن طريق أنظمة الكترونية أخرى مخصصة لهذا الغرض.[٩]

و تبنى آخرون مصطلح الحرب السيبرانية (Cyber Warfare)، بالاستناد إلى أيدلوجية أمنية أو عسكرية، تضع منهاجاً لتحقيق أهداف على الصعيد الأمني أو العسكري تجاه (العدو المفترض).[١٠]

أما البعض الآخر فاختار مصطلح الهجمات السيبرانية (Cyber Attacks)، كوصف واقعي يجمع بين كل ما ذكر آنفا[١١]، فهو تصرف يدور في عالم افتراضي قائم على استخدام بيانات رقمية و وسائل اتصال تعمل الكترونياً ، ومن ثم تطور ليتضمن مفهوماً أوسع يقوم على تحقيق أهداف عسكرية أو أمنية ملموسة ومباشرة، جراء اختراق مواقع الكترونية حساسة، عادةً ما تقوم بوظائف تصنف بأنها ذات أولوية ، كأنظمة حماية محطات الطاقة النووية أو الكهربائية أو المطارات و وسائل النقل الأخرى .[١٢]

ولأن مصطلح الحرب هو مصطلح غير محبذ في وقتنا الراهن على مستوى التنظيم القانوني الدولي،[١٣] فيكون مصطلح الهجمات السيبرانية أكثر قرباً للموضوع الذي تتناوله هذه الدراسة ، ولا سيما أن تصرفات دولية عدة أشارت إلى مصطلح الهجمات، وعدتها بمثابة التصرف الذي يوضع في الحسبان في أثناء النزاعات المسلحة ، طبقاً للقانون الدولي الإنساني. [١٤]

وفي الموضوع ذاته عادةً ما ينصب اهتمام المختصين في القانون الدولي الإنساني على وصف الوسيلة والأثر، وبعبارة أخرى التركيز على وسيلة الهجوم وطريقة تنفيذها وما سينجم عنها من آثار، أكثر من التركيز على ما تحتويه وسائل وطرائق القتال ذاتها.

و يؤيد هذا التوجه كل من توماس رد (Thomas Rid) وبيتر ماكبورني (Peter Mcburney) المختصان في القانون الدولي الإنساني، إذ ذهبا إلى تفضيل اصطلاح الهجوم السيبراني، بدلاً من الحرب السيبرانية على أساس أن الأخير أوسع نطاقاً من الأول.[١٥]

لقد تعرض مصطلح الهجوم السيبراني إلى تعاريف عدة، ومن زوايا مختلفة، وإن كانت مشتركة على مضمون متقارب في المعنى، وهو استهداف مواقع الكترونية من خلال وسائل اتصال الكترونية أخرى.[١٦]

ومن تلك التعاريف ما ذهب إليها خبراء ومختصين في القانون الدولي الإنساني، و أولهم شين (Shin) إذ يذهب بالقول: " ....استخدام الطيف الالكتروني أو الكهرومغناطيسي لتخزين وتعديل وتبادل البيانات وجهاً لوجه مع أنظمة تحكم في بنى تحتية مرتبطة بها".[١٧]

فيما عرفه فيورتس (Fuertes) بالقول:" هجوم عبر الانترنت يقوم على التسلل إلى مواقع الكترونية غير مرخص بالدخول إليها، بهدف تعطيل أو إتلاف البيانات المتوفرة فيها أو الاستحواذ عليها، وهي عبارة عن سلسلة هجمات الكترونية تقوم بها دولة ضد أخرى".[١٨]

فيما عرفه شمت (Schmitt) بالقول :" مجموعة من الإجراءات التي تتخذها الدولة للهجوم على نظم المعلومات المعادية بهدف التأثير والإضرار بها، وفي الوقت نفسه للدفاع عن نظم المعلومات الخاصة بالدولة المُهاجِمة".[١٩]

وقد عرفه زيمت وباري (Zimet & Barry) بالقول:" مجموعة من العمليات القائمة على الحرب الالكترونية و الخداع النفسي، فضلاً عن استهداف شبكة تواصل العدو العسكرية وعملياته الأمنية الالكترونية".[٢٠]

وأخيراً يذهب ماركو روسيني (Marco Roscini) إلى تعريفها بالقول: " تطويع الإمكانيات الالكترونية العسكرية لأجل التأثير في مواقع الكترونية أخرى وتعطيلها أو تدميرها سواء أكانت تقدم خدمات مدنية أو عسكرية .[٢١]

وفي رأينا أن التعريف الذي ذهب إليه ميشيل (Michael) هو الأقرب لمفهوم الهجمات السيبرانية التي عرّفها روسيني (Roscini)، ، إذ يعرفها بالقول:" الهجوم السيبراني، هو أي تصرف دفاعياً كان أم

هجومياً، يتوقع منه و على نحو معقول في التسبب بجرح أو قتل شخص أو إلحاق أضرار مادية أو دمار بالهدف المُهاجم".[٢٢]

أن المثال الأكثر توافقاً مع ما ذكر آنفاً، هو أن تهاجم طائرة حربية مواقع حساسة لدولة ما، كمراكز البنى التحتية المعلوماتية (Information Infrastructure Installations) تابعة لها فتطلق صواريخ موجهة تبث أطيافاً كهرومغناطيسية تتسبب في تعطيل منظومات الاتصال الالكترونية، فضلاً عن التدمير المادي لأجهزتها.[٢٣]

وهو ما يتوافق مع مفهوم استخدام الوسائل الالكترونية للأغراض العسكرية، ففي عام ٢٠٠٧ عرفت القيادة الإستراتيجية الأمريكية (US. Strategic Command) الهجمات السيبرانية بالقول: "تطويع عمليات نظام الكمبيوتر بهدف منع الخصوم من الاستخدام الفعَّال لها ، فضلاً عن التسلل إلى أنظمة المعلومات وشبكات الاتصال بهدف جمع و حيازة وتحليل البيانات التي تحتويها ".[٢٤]

أن التعريف آنف الذكر، يتوافق مع مضمون المادة (٥) من اتفاقية مجلس أوربا المتعلقة بالجريمة السيبرانية، والتي نصت:" تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الفعل التالي في قانونها الوطني،إذا ما ارتكب عمداَ وبغير حق الإعاقة الخطيرة لعمل منظومة الكومبيوتر عن طريق إدخال أو إرسال أو إتلاف أو محو أو تغيير أو تبديل أو تدمير بيانات كومبيوتر".[٢٥]

وفي هذا الشأن نطرح تساؤلاً له صلة باستخدام التقنيات الالكترونية في الإطار العسكري: هل يمكن عد النشاط الالكتروني إذا استخدم لإغراض عسكرية، هجوما بالمعنى الاصطلاحي ؟ وهل هو وسيلة أم طريقة قتالية، وبعبارة أخرى هل يمكن عده سلاحاً، وإذا كان كذلك، هل هو سلاح تقليدي ؟

بداية لا بد من تعريف الهجوم المسلح، إذ ورد في الفقرة (١) من المادة (٤٩) من البروتوكول الإضافي الأول لعام ١٩٧٧، الملحق باتفاقيات جنيف الأربعة لعام ١٩٤٩ بالنص:" تعني "الهجمات" أعمال العنف الهجومية والدفاعية ضد الخصم" .[٢٦]

ومن قراءة النص المتقدم وتطبيقه على الهجوم السيبراني، فالظاهر أنه بعيد عن مصطلح الهجوم الوارد في الفقرة (١) السالفة ، لكون – الهجوم السيبراني- لا يصاحب أعمال عنف مسلح ملموسة ومباشرة في أثناء الاستخدام.

و لا يمكن القبول بفرضية أن كل تصرف سيبراني ينشأ عنه قرصنة أو اختراق لبيانات الكترونية هو بمثابة أعمال عنف مسلح، و علينا أن نسأل هل الفرضية المتقدمة مقنعة في ضوء الآثار التي تتسبب بها الهجمات السيبرانية على حياة الإنسان بالذات؟

أن قراءة نص الفقرة (١) من المادة (٤٩) السابقة الذكر ، بمعزل عن باقي أحكام البروتوكول الإضافي الأول، هو أمر غير صائب، بدليل تكشف عنه أحكام البروتوكول نفسه، إذ أن أعمال العنف المسلح ، يحكمها أمران: إما أن تكون مباشرة وتؤدي بطبيعتها إلى إلحاق أذى مادي في الأعيان العسكرية أو المدنية، أو غير مباشرة بعد وقوع الهجوم أياً كانت الوسيلة أو الطريقة.

وفي ضوء ما تقدم فأن الأصح هو التركيز على نوع الآثار وجسامتها ، فكلما ثبت أن المدنيين على سبيل المثال سيتأثرون جراء أي نشاط سيبراني عسكري، كاستهداف منظومة السيطرة والتحكم الالكترونية لمفاعل نووي لتوليد الطاقة الكهربائية، سيعني أن وصف (هجوم) متحقق فيه.

ولا أدل على ذلك ما أشارت إليه الفقرة (٢) من المادة (٥١) من البروتوكول الإضافي الأول لعام ١٩٧٧، بالنص:" لا يجوز أن يكون السكان المدنيون بوصفهم هذا وكذا الأشخاص المدنيون محلاً للهجوم. وتحظر أعمال العنف أو التهديد به الرامية أساساً إلى بث الذعر بين السكان المدنيين".[٢٧]

أما بخصوص تعريف وسائل القتال وطرائقها، فقد عرفها موريس اوبير (Murice Aubert) بالقول:" وسائل القتال هي الأسلحة ذاتها، بينما طرائقها فتعني كيفية استخدامها".[٢٨]

فيما تعرف الأسلحة التقليدية، بأنها: "أسلحة ليست أسلحة تدمير شامل جرى فهمها على أنها تتضمن أجهزة مصممة للقتل أو الجرح أو إلحاق الضرر، عادةً لا حصراً، بواسطة تأثيرات المواد شديدة الانفجار أو الطاقة الحركية أو العوامل المحرقة ونُظم إيصالها".[٢٩]

وقد أطلق البعض من المختصين ومنهم رادويج (Harry D. Raduege)،[٣٠] مصطلح التعطيل الشامل (Mass Disruption) لوصف الهجوم السيبراني، وهي تقابل مصطلح الدمار الشامل (Mass Destruction) المعروفة بها الأسلحة النووية والكيميائية والبيولوجية.

أن للوصف مغزى قانونياً وفنياً في آن واحد، إذ يعكس هدف الهجوم السيبراني وهو التعطيل التام أو الجزئي للمنظومات الالكترونية العسكرية أو المدنية للعدو المفترض، فضلاً عن التأثير على مجمل العمليات العسكرية التقليدية الأخرى.

ومن خلال قراءة التعاريف المتقدمة ومضامينها، ومقارنتها مع خصائص الهجمات السيبرانية، يتضح أنها وسيلة و طريقة في الوقت نفسه، وبعبارة أخرى يعتمد ذلك على الهدف من استخدامها ، فقد تسهم في توجيه العمليات العسكرية الأخرى كالصواريخ بعيدة المدى أو الطائرات بدون طيار(Drawn) لتحديد أهداف عسكرية منتخبة وتدميرها أو لتعطيل أجهزة الكشف المبكر للهجمات التي يقوم بها سلاح جو معادي أو وقف عمليات الاتصال في المطارات العسكرية أو المدنية.

أن التعريف المتقدم ذكره، يتجسد – على سبيل المثال - في الهجوم الذي قامت به إسرائيل عام ٢٠٠٧ ضد سوريا، إذ توقفت أجهزة الرادار وباقي منظومات الاتصال في المطارات العسكرية والمدنية عن العمل ، في أثناء الهجوم الذي نفذه سلاح الجو التابع لها على مواقع سورية زعمت إسرائيل أنها منشآت لمفاعل نووي[٣١]، و في هذه الحالة يعد الهجوم السيبراني طريقة قتالية، إذ يدخل ضمن الخطط العسكرية وبالتالي هو طريقة قتالية.

وعلى العكس قد تكون الهجمات السيبرانية وسيلة قتالية ، من خلال استخدامها بذاتها، للتسلل إلى أنظمة الكترونية معدة لحماية أو لتنظيم سير عمل منشآت حيوية، كمحطات توليد الطاقة النووية أو السدود أو وسائل النقل كالمطارات، بهدف تطويعها والسيطرة عليها، لتدمير ذاتها بذاتها من خلال تغذيتها بمعلومات خاطئة لأجهزة التحكم والحماية الالكترونية.

والمثال على ذلك، استهداف نظام الحماية أو التحكم بعمليات حساسة في محطة نووية ما، وتسخيرها للدولة المهاجمة، فضلاً عن إدخال بيانات خاطئة عن عمل المحطة كدرجة الحرارة في أجهزة الطرد المركزية (Centrifuge)، ما قد يؤدي إلى تعرضها للانفجار أو التعطيل الكلي أو الجزئي أو تأخير مهامها المعتادة والطبيعية. [٣٢]

وأجلى تطبيق على ما ذكرناه آنفا ما تعرضت إليه محطة (نطانز) النووية الإيرانية من هجوم سيبرآني، أعلنت عنه الولايات المتحدة في عام ٢٠١١، إذ استخدمت برنامجاً ويدعى (Stuxnet) عطل بعضاً من العمليات الحساسة والحق أضراراً جزئية في عمليات تخصيب اليورانيوم، وهو ما يمكن معه عدَّ هذا الهجوم سابقة في حقل الهجمات السيبرانية.[٣٣]

وبالعودة إلى المعنى الاصطلاحي ، يذهب البعض إلى القول، بعدم صحة تصنيف الهجمات السيبرانية بكونها وسيلة قتالية، بحجة أنها لا تشترك في أهم صفة تُعرف بها الأسلحة التقليدية وهي الطاقة الحركية (kinetic)، إذ لا يمكن – حسب رأيهم- تحسس الهجوم على نحو مادي، فضلا عن أن (وسيلة) الهجمات السيبرانية لا تحوي على مواد شديدة الانفجار، وبالتالي يرون أنها مستبعدة بحكم طبيعتها من طائفة الأسلحة وتنظيمها دولياً.[٣٤]

وفي هذا الشأن ، نقول أن استبعاد الهجمات السيبرانية -على هذا النحو- من فئة الأسلحة هو أمر غير صائب، إذ لا يشترط في الأسلحة عموماً، احتوائها على طاقة حركية، فالأسلحة الكيميائية أو البيولوجية لا يشترط احتوائها على طاقة حركية أو مواد شديدة الانفجار، كما لا يشترط في استخدامها وسيلة حركية، وبعبارة أخرى يمكن استخدامها دون الحاجة إلى الصواريخ أو القذائف.

أن المعيار الأصح في التمييز بين وسائل وطرائق القتال، إنما يعتمد على الهدف من استخدامها و النتيجة التي ستؤديها، فكلما كانت تتسبب بطريق مباشر أو غير مباشر بقتل أو جرح أو تدمير أو تعطيل كلي أو جزئي ، فتعد وسيلة قتالية، أما إذا استخدمت كجزء من مخطط عسكري فتعد طريقة قتالية تخضع للنظام القانوني الدولي[٣٥]، وهو ما تتصف به الهجمات السيبرانية في الاثنين معاً.

وما يؤكد ذلك، ما ذهب إليه توماس رد و بيتر مكبورني بالقول:" أن وصف أي سلاح يتوقف على عنصرين: الأول هو البعد المعنوي أو النفسي ويقوم على رغبة المهاجم بإيقاع إصابات في الهدف العسكري للعدو، أما العنصر الثاني فهو العملي أو التطبيقي، ويقوم على توجيه السلاح فعلاً ضد أهداف عسكرية منتخبة، وهو ما يتوافر في السلاح السيبراني".[٣٦]

المطلب الثاني

الهجمات السيبرانية : نشأتها ونماذج عنها

شهد العقد الأخير تطورات سريعة في مجال تكنولوجيا المعلومات ما أفضى إلى متغيرات بعيدة المدى في جميع مجالات الحياة تقريباً، ولا سيما في المجالين العسكري والأمني اللذين شهدا نشوء أبعاد جديدة في طريقة القتال وأسلوب بناء قدرات القوات المسلحة .ويعزى ذلك جزئياً إلى المستجدات التي طرأت على أنماط التفكير الاستراتيجي، وعلى بلورة عقيدة قتالية تتلاءم مع الواقع المتغيّر.[٣٧]

وعلى صعيد الدراسات والأبحاث القانونية المهتمة بهذا المجال ، فيعد جون اركويلا (John Arquila) و ديفيد رونفيلد (David Ronfeld) أول من بحثا في مسألة الهجمات السيبرانية عام ١٩٩٧، في كتابهم الموسوم "الحرب السيبرانية قادمة" (Cyber war is Coming)، إذ أشارا فيه إلى أنظمة الاتصال الالكترونية ودورها في النزاعات المسلحة مستقبلاً.[٣٨]

أما على صعيد الردود الدولية الرسمية، فقد بقت الدول المعنية ببرامج لتطوير قدراتها السيبرانية متكتمة عليها بادئ الأمر، وعدتها بمثابة عنصر مهم من عناصر الأمن القومي، إلا أن الأمر لم يبق على هذا النحو، فسرعان ما أبدى قادة دول ومسؤولون ، عن دعمهم لبناء القدرات السيبرانية تحت إطار مبدأ الدفاع عن النفس (Self- Defense).[٣٩]

وفي هذا الصدد ، سنشير إلى عدد من الردود تلك، فعلى سبيل المثال اقترح رئيس قسم الحرب الالكترونية الصينية، داي كوينجمن (Dai Qingmin) في عام ٢٠٠٣ ، بأنه :" ...على الصين أن تتهيأ لحرب سيبرانية تتضمن سلسلة هجمات الكترونية، ما يدعوها إلى الإعداد و التنسيق في العمليات العسكرية لصد الهجمات السيبرانية المضادة....".[٤٠]

فيما صرح الرئيس الأمريكي باراك اوباما عام ٢٠٠٩بالقول: " .... وبالتالي فأن الفضاء السيبراني هو حقيقة و مخاطرهُ قادمةٌ معه لا محالة....."."[٤١]

وتأكيداً للمخاطر المحدقة بأمن الولايات المتحدة صرح اوباما أيضاً:" لم نستعد كما يجب ، بل فشلنا في تأمين الحماية الكافية للبنى التحتية الرقمية الخاصة بنا".[٤٢]

أن إستراتيجية الهجمات السيبرانية الأمريكية كانت ولا تزال، متأثرة بالأولويات الجديدة للصناعة العسكرية الإسرائيلية، المصنفة بالبالغة السرية، والتي تستهدف تباعاً الصناعة النووية الإيرانية والصناعات الدفاعية الأوربية المفترض أنها تعود لبلدان حليفة.[٤٣]

وفي الجهة الأخرى من العالم كانت هنالك توجهات للخصم التقليدي، ونقصد به روسيا الاتحادية، فقد كانت الأسبق في نطاق الاستعداد للهجمات السيبرانية.[٤٤]

إذ يذهب كل من جادي (Gady) و أوستن (Austin) إلى تحليل ما صرح به الرئيس فلاديمير بوتين عام ٢٠٠٠، و إعلانه عن تعاليم أمن المعلومات (**Information Security Doctrine**) والتي تتلخص بالآتي:" زيادة المخاطر السيبرانية التي تتعرض لها روسيا مقابل تخصيصات مالية قليلة حالياً مخصصة لدعم برامج الدفاع السيبراني"، ومن ثم وضع بوتين برنامج طويل الأمد لتطوير قدرات روسيا وبما يتناسب وحاجتها لمنظومات الاتصال الالكترونية وتسخيرها في الجانب العسكري والأمني".[٤٥]

فيما صرح العضو الأسبق في مجلس النواب الروسي (الدوما) ، نيكولاي كوريانوفج (Nikolai Kuryanovich) بالقول: " في القريب العاجل ستحدث الكثير من النزاعات المسلحة، ولكن لا على ارض المعركة التقليدية، بل من عدد هائل من جنود المعلومات، والتي يمكن أن تحقق أهدافاً أمنية وعسكرية أكثر بكثير مما يحققه الآلاف من الجنود المقاتلين في جبهات القتال".[٤٦]

وبالمقابل صرح زعيم حزب المحافظين في بريطانيا، ديفد كاميرون عام ٢٠١٠،بالقول:" سيكون الأمن السيبراني الجزء الأهم ضمن إستراتيجية الحزب على الصعيد القومي".[٤٧]

وبعد أن بينا الجانب الأهم من ردود الأفعال الدولية حيال الهجمات السيبرانية سنسلط الضوء فيما يلي من البحث ، متصفحين تاريخها وكيف نشأت ، فضلاً عن ذكر أهم الأحداث التي شهدتها الساحة الدولية وتحليلها في ضوء أحكام القانون الدولي العام والإنساني منها بالذات.

الفرع الأول

نشأة الهجمات السيبرانية

ترتبط الهجمات السيبرانية مباشرة بحدثين مهمين: الأول باستحداث أجهزة الكمبيوتر في منتصف الخمسينيات من القرن المنصرم كأداة لمعالجة وحفظ المعلومات رقمياً (Digital)، رافقه تضافر جهود عدد من الشركات الخاصة والعامة، توج بتطوير وحدة المعالجة المركزية (CPU) وذلك لتسهيل المهام الموكلة له، وقد تطور ذلك بصورة جذرية في العقود اللاحقة ، حتى أصبح جهاز الكمبيوتر ، أساساً في عمل الكثير من المؤسسات الخاصة والعامة، فضلاً عن الحياة اليومية للأفراد. [٤٨]

أما الحدث الثاني فهو بظهور الشبكة العنكبوتية (الانترنت) والذي احدث انقلاباً مثيراً في حياة البشرية من خلال التواصل ونقل المعلومات بسرعة فائقة عن طريق سيل من البيانات المرسلة عبر الأثير.[٤٩]

وفي سياق متصل، يصف البعض أن نشوء الثورة المعلوماتية الحالية، هو بمثابة الجيل الثالث للثورات التقنية التي غيرت في أسلوب الحياة وإمكانيات البشرية، وبعبارة أخرى الثورتان الزراعية والصناعية وأخيراً الثورة المعلوماتية.[٥٠]

لقد سارعت الدول في وتيرة استخدام الكمبيوتر لتحقيق قفزات نوعية في المجال الأمني والعسكري، وذلك في مطلع التسعينيات من القرن المنصرم[٥١] حتى أطلق البعض عليها مصطلح الحرب السيبرانية الباردة (Cyber Cold War) أو سباق التسلح السيبراني (Cyber arms race) .[٥٢]
و في بادئ الأمر لم يكن للهجمات السيبرانية صدى على المستوى الدولي ، إذ نشأت الجريمة السيبرانية أولا على هيئة جرائم طالت المؤسسات المالية والمصرفية، فضلاً عن الشركات المتخصصة ببرمجة نظم الاتصالات، وقد دأبت الدول على اتخاذ التدابير التشريعية لتجريم الأفعال وتحديد العقوبات.[٥٣]

وقد عالجت الدول ومنها العربية كالعراق و الإمارات و عمان والأردن وسوريا الجرائم السيبرانية من خلال تشريعات جزائية وأخرى تنظيمية في تجريم الدخول غير المشروع إلى المواقع الالكترونية والأنظمة المعلوماتية المملوكة من الغير.[٥٤]

و فيما يخص الدول واستخدامها للتكنولوجيا المتقدمة لأهداف عسكرية ، فعادةً ما تلجأ إليها لأجل تحقيق مكاسب محددة ، في أقل تقدير للهيمنة على واقع النزاع المسلح، وللظفر بالنصر بأقل خسائر، هذا في النزاعات المسلحة التقليدية، أما فيما يخص موضوع بحثنا، فيبدو الموضوع مختلف نوعا ما، فلا يشترط وجود طرفين متحاربين في أثناء إعداد أو تنفيذ الهجمات السيبرانية، فضلاً عن أنها في الغالب تحمل طابعاً وقائياً ضد الخصم المستهدف من الهجوم.

أن الأثر المترتب في اللجوء إلى الهجمات السيبرانية، يختصره الخبير الروسي ديمتري كريجوروف (Dmitry I. Grigoriev) بأنه يتجسد في التهديد على المستوى العسكري والسياسي،فضلاً عن التهديدات الإجرامية والإرهابية التي يمكن لمجموعات من غير الدول تبنيها لأجل الحصول على مزايا سياسية أو اقتصادية.[٥٥]

لقد تنبه إلى هذا الموضوع الكثير من المختصين،[٥٦] فركزوا عليه بالبحث والتحليل في نطاق النزاعات المسلحة عموماً، وهو ما سنتعرض إليه فيما يلي للبحث في دراسة نماذج منتخبة للهجمات السيبرانية .

الفرع الثاني

نماذج منتخبة بشأن الهجمات السيبرانية

يسجل لنا التاريخ المعاصر، نماذج للهجمات السيبرانية اخترنا منها بعضاً مما ذكره المختصون في هذا الشأن : وأولها الهجوم السيبراني الذي نفذته الولايات المتحدة الأمريكية وصرحت به عام ١٩٨٢ ضد منظومة التحكم العالية صناعياً في أنبوب نفط (Chelyabinsk) التابع للإتحاد السوفيتي السابق، و الذي نجم عنه انفجار كبير طال ثلاثة كيلومترات من الأنبوب وأدى إلى خسائر بالغة فيه، وهو ما نفاه الاتحاد السوفيتي السابق آنذاك. [٥٧]

أما النموذج الآخر، فهو ما تعرضت له أنظمة الاتصال الالكترونية التابعة لوزارة الدفاع الأمريكي (Pentagon) و وكالة الفضاء الأمريكية (NASA) و وكالة الطاقة الأمريكية (Energy Department) لهجمات سيبرانية بين الأعوام ١٩٩٨- ٢٠٠٠، والذي أدى إلى الاستحواذ على الآلاف من الملفات المصنفة بأنها عالية السرية ، وقد وجهت الولايات المتحدة التهمة رسمياً إلى روسيا الاتحادية، في حين أنكرت الأخيرة -آنذاك- مسؤوليتها عن هذا الهجوم.[٥٨]

و يرى آخرون أن أول مرة نفذت فيها الهجمات السيبرانية، كانت في حرب كوسوفو عام ١٩٩٩، من خلال استهداف سلاح الجو التابع لحلف الشمال الأطلسي (NATO) لشبكات الهاتف في يوغسلافيا السابقة. [٥٩]

وفي النزاع المسلح ذاته، وبعد استهداف طيران حلف شمال الأطلسي للسفارة الصينية في بلغراد، قام عدد من القراصنة الصينيين - وكردة فعل - بمهاجمة مواقع الكترونية رسمية منتخبة تابعة للولايات المتحدة الأمريكية، وبالذات الموقع الالكتروني للبيت الأبيض ، نجم عنها الاستحواذ على الآلاف من البيانات الرقمية ، المصنفة – آنذاك - بأنها عالية السرية. [٦٠]

أما النموذج الآخر للهجمات السيبرانية، فيتلخص بردة الفعل الصينية تجاه الولايات المتحدة، فبعد أن استهدفت الأخيرة مواقع الكترونية عسكرية ، والاستحواذ على معلومات ذات صلة بتطوير المقاتلات طراز (EP-3) و طراز (Fighter Jet) الصينيتين، قام عدد من المهاجمين الذين يعتقد أنهم صينيون، بمهاجمة مواقع الكترونية أمريكية ، نجم عنها خسائر كبيرة قدرت بملياري دولار أمريكي. [٦١]

لقد وجهت الولايات المتحدة، التهمة رسمياً إلى الصين محملة إياها عواقب هذا الهجوم، بعد أن ظهرت رسالة على شاشات الأجهزة الالكترونية مذكور فيها عبارة: (تمت القرصنة بواسطة صينيون) (Hacked by Chinese).[٦٢]

أن مسلسل الهجمات هذه لم ينته، ففي عام ٢٠٠٧ تعرضت استونيا،إحدى جمهوريات الاتحاد السوفيتي السابق، إلى هجمات سيبرانية متلاحقة أدت إلى تعطيل كامل لشبكات الاتصال الالكترونية فيها، وبالذات المواقع الرسمية الحساسة لرئيس الوزراء ورئيس البرلمان، فضلاً عن المواقع الرسمية الأخرى لمكاتب الوزراء الاستونيين، وقد وجه الاتهام رسمياً إلى روسيا الاتحادية ، إذ عدتها استونيا هجمات انتقامية بسبب قيامها بنقل نصب تذكاري يخلد الجيش الروسي من العاصمة (تالين) إلى مكان آخر مجهول .[٦٣]

ويمكن القول أن الهجوم السيبراني الذي تعرضت له استونيا عام ٢٠٠٧، يمثل أنموذجاً متميزاً لاختبار ردة فعل حلف شمال الأطلسي الذي تنتمي إليه استونيا ، و تحسب ردة الفعل في أمرين اثنين: الأول بالطلب الذي تقدمت به استونيا لعقد اجتماع أمني طارئ للدول الأعضاء في الحلف. [٦٤]

أما الثاني ففي تكييف الهجمات السيبرانية التي تعرضت لها استونيا، وعدها بمثابة هجوم مسلح يهدد دول الحلف جميعاً بالاستناد إلى المادة (٥) من اتفاقية حلف الشمال الأطلسي لعام ١٩٤٩والتي تنص: (يتفق الأطراف، على أن أي هجوم ، أو عدوان مسلح ضد طرف منهم أو عدة أطراف في أوربا أو أمريكا الشمالية، يُعدّ عدواناً عليهم جميعاً، وبناءً عليه فإنهم متفقون على أنه في حالة وقوع مثل هذا العدوان المسلح، فإن على كل طرف منهم ، تنفيذاً لما جاء في المادة ٥١ من ميثاق الأمم المتحدة عن حق الدفاع الذاتي عن أنفسهم بشكل فردي أو جماعي.....).[٦٥]

وفي مكان آخر من العالم وفي العام نفسه، تعرض موقع سوري يشتبه بأنه مفاعل نووي، إلى هجمات نفذها سلاح الجو الإسرائيلي في السادس من أيلول/ سبتمبر من عام ٢٠٠٧،والذي تزامن معه قيام إسرائيل بهجمات سيبرانية وصفت بأنها عالية الدقة ، استهدفت أنظمة الاتصالات في وزارة الدفاع السورية أدت إلى تعطيلها بالكامل، فضلاً عن تفادي الخسائر أو الأخطاء في استهداف المفاعل، وهو ما يعد خير مثال على قدرة الهجمات السيبرانية على تحسين أداء العمليات العسكرية التقليدية و توفير الدعم اللازم في انجازها.[٦٦]

والمثال الآخر على الأثر الذي تؤديه الهجمات السيبرانية في المعارك التقليدية، ما تجسد في النزاع المسلح الروسي الجورجي عام ٢٠٠٨، فقبل بدء العمليات القتالية وبالتحديد بيوم واحد ، تعطل نظام الاتصال الالكتروني(IT) للقوات الجورجية بالكامل، ولاسيما في إقليم اوسيتيا الجنوبية الذي شهد حالة من التوتر بسبب إعلانه الانفصال عن جورجيا. [٦٧]

لقد أسهم الهجوم السيبراني في حدوث إرباك اضعف قدرة وسائل الدفاع الجوي الجورجية ، فضلاً عن تعرض مواقع الكترونية أخرى لهجمات سيبرانية مماثلة، طالت مواقع حساسة كوسائل الإعلام والبني التحتية وأهمها قطاع المواصلات.[٦٨]

وفي مثال آخر، أكدت التقارير الاستخبارية الأمريكية في عام ٢٠٠٩، بقيام بعض من المجموعات المسلحة في أثناء احتلال العراق ، باختراق مواقع الكترونية كانت تستقبل بيانات غاية في الأهمية تنقلها الطائرات بدون طيار لتحديد تحركات هذه المجموعات، ما ساعد الأخيرة في مراقبة التحركات العسكرية الأمريكية الموجهة ضدهم.[٦٩]

ومن النماذج الأخرى الدالة على قدرة الهجمات السيبرانية وبالذات في تعطيل أو تدمير بنى تحتية تحتوي قوى خطرة، الهجوم السيبراني الذي تعرض له المفاعل النووي الأمريكي ديفيد بيس (David - Besse) لتوليد الطاقة الكهربائية في أوهايو في الثاني من حزيران عام ٢٠٠٣ ، بفعل أنظمة اختراق وتعطيل لشبكات السيطرة والتحكم الالكترونية في المفاعل نفسه.[٧٠]

وحسب تصريحات المسؤولين الأمريكيين، أنه لولا وجود وسائل الحماية في المفاعل، و مبادرتها بإطفاء المفاعل ذاتياً، لكانت الكارثة تتعدى توقف المفاعل النووي عن العمل، و لأدى إلى كارثة انفجاره ، لدرجة يصعب فيها تخيل الأضرار والخسائر البشرية الناجمة عن ذلك الهجوم، ولم تكن هذه الهجمات السيبرانية هي الأخيرة بعد هذا الحدث، إذ لا تزال محطات توليد الطاقة الكهربائية النووية الأمريكية تتوقف عن التشغيل مرة أو مرتين منذ عام ٢٠٠٦ بفعل هذه الهجمات.[٧١]

ولم يتوقف الهجوم السيبراني على المفاعلات النووية للأغراض السلمية فقط، بل تعرضت بنى تحتية أخرى للهجمات ذاتها، ففي ابريل نيسان من عام ٢٠٠٩، تعرضت شبكة التحكم والسيطرة الكهربائية في الولايات المتحدة، إلى هجمات سيبرانية مماثلة، أدت إلى التسلل في نظام السيطرة والتحكم به و وقف تشغيله عن بُعد، وقد وجهت الولايات المتحدة التهمة رسمياً إلى الصين وروسيا الاتحادية وحملتهما مسؤولية هذا الهجوم وتبعاته ، وهو ما أنكرته الدولتان في وقتها. [٧٢]

وقد تكون أكثر الهجمات حداثةً، ما تقوم به الولايات المتحدة وإسرائيل بشأن البرامج النووية الإيرانية ، إذ أعدت برامج خاصة لمهاجمة المواقع الحساسة الإيرانية منذ عام ٢٠٠٦، من خلال نظام رئيس يسمى

اللهب (Flame) ، فضلاً عن برنامجي (DUQU) و (Stuxnet) للتأثير في نشاط اليورانيوم و أجهزة الطرد المركزي والمرافق التابعة له في منشأة (نطانز) النووية بالذات.[٧٣]

ويعد هجوم برنامج (Stuxnet) هو الأخطر على صعيد الهجمات السيبرانية لمنشآت مدنية أو عسكرية على الإطلاق،إذ تعرضت المواقع النووية الإيرانية إلى أسلوب ومنهج يقوم على شقين: الأول باستهداف أجهزة الطرد المركزية وخروجها عن السيطرة من جهة، أما الثاني فبالتحايل على أجهزة التحكم والإيحاء لها، أن عمليات تشغيل المنشأة النووية تعمل بصورة طبيعية، إلا أنها في الواقع معطلة.[٧٤]

وفي هذا الخصوص ، يسوق لنا الخبير في أمن الحاسوب رالف لانكنر (Ralph Langner) دليلاً على وقوف دول بعينها في تطوير (Stuxnet)، فيقول:" .. أنه ليس ببرنامج للقرصنة، فبالنسبة لي يبدو أن مصادر استحداثه وتطويره تحتاج إلى قدرات دولة بعينها لا مجرد قدرات ذاتية لأفراد".[٧٥]

أن برنامج (Stuxnet) يمثل الدليل الدامغ على قدرة الهجمات السيبرانية الفعلية في تدمير أعيان مدنية أو عسكرية، كمنشآت توليد الطاقة و محطات المياه و وحدات الصناعة، وأكثر من ذلك إذ يمكن عده بداية لهجمات سيبرانية ستجر الويل على العالم لا تقل خطورة عن الأسلحة التقليدية أو غير التقليدية من حيث حجم الدمار ونطاق آثاره.

أن النماذج التي ذكرت في هذه الدراسة ،ما هي إلا بداية لتطور مفهوم النزاعات المسلحة ، فضلاً عن المسؤولية الدولية الناشئة عن خرق المبادئ الدولية المنظمة لسير العمليات القتالية، وهو ما يستدعي تحركاً دولياً سريعاً لدرء مخاطرها على صعيد السلم والأمن الدوليين. وهذا ما سنسلط عليه الضوء في المبحث الثاني من هذا البحث.

المبحث الثاني

الهجمات السيبرانية في ضوء التنظيم الدولي المعاصر

تعرض باحثون كثر إلى موضوع الهجمات السيبرانية، فطرحوا عدداً من الإشكاليات القانونية سنقف عندها بالبحث والتحليل و أهمها: هل ينطبق القانون الدولي العام، والإنساني بالذات على الهجمات السيبرانية ؟ وبعبارة أخرى، ما هو الموقف منها في ظل وجود فراغ قانوني يعتقد به البعض من المختصين ؟[٧٦]

و من جهة أخرى يطرح باحثون آخرون إشكاليات من زاوية مختلفة، منها: ما هو الموقف من مبدأي الشرعية والمشروعية في موضوع الهجمات السيبرانية ، بالتركيز على مبدأ الضرورة العسكرية ومبدأ التناسب ومبدأ وجوب التمييز في استخدام القوة.[٧٧]

ويرى آخرون أن الهجمات السيبرانية يمكن أن تكيف لا في ظل أحكام القانون الدولي الإنساني المدونة فحسب، بل وفي أحكام القانون الدولي العام ككل، على أساس أن الصورة الأولية تظهر أن الهجمات تلك يمكن أن ترتكب أثناء النزاعات المسلحة الدولية أو غير الدولية، و في أوقات السلم أيضاً، ما يلوح في الأفق مواضيع أخرى، يطرحها هؤلاء وأهمها: المسؤولية الدولية الناشئة عن الهجمات السيبرانية في وقت السلم، ومفهوم السيادة والولاية القضائية .[٧٨]

وأخيراً الإشكالية المتمثلة في التصور الآتي: أن اغلب الهجمات السيبرانية لا تعلن الدول رسمياً عن تبنيها لها، إنما قد يعلن فرد أو مجموعة من الأفراد المسؤولية عنها، فكيف يمكن للقانون الدولي أن يتصدى لهذا الموضوع ، وبعبارة أخرى أيهما سيطبق معيار السيطرة الكاملة (Overall Control) أم السيطرة الفاعلة (Effective Control)،[٧٩] أم الاثنان معاً لتقرير المسؤولية الدولية؟

وللإجابة عن هذه الإشكاليات سنبحث في مطلبين: الأول، نسلط فيه الضوء على التكييف القانوني للهجمات السيبرانية، فيما سيكون الثاني معنياً ببحث المسؤولية الدولية الناشئة عنها في ضوء أحكام القانون الدولي العام، فضلاً عن أهم الجهود الدولية ذات الصلة بتنظيمها.

المطلب الأول

التكييف القانوني للهجمات السيبرانية

ذكرنا فيما سبق ، أن مفهوم الهجمات السيبرانية ما زال يواجه اختلافاً بيناً، ما أدى إلى معضلة وتحدي أكبر يواجهه المختصون في القانون الدولي، ويتجسد ذلك في تكييف الهجمات السيبرانية ، فضلاً عن البحث في مصدر التكييف وأساسه، هل نجده منظماً في مبادئ القانون الدولي العام أم المبادئ والقواعد المنطبقة في القانون الدولي الإنساني ؟

والمعضلة ستكون كبيرة فيما لو تم الإقرار بوجود فراغ قانوني – عدم وجود قواعد قانونية محددة - ينظم الهجمات السيبرانية ، ليطرح التساؤل الآتي: ما هي القواعد الواجبة التطبيق؟ ولا سيما أن نطاق استخدامها يزداد يوماً بعد يوم ومخاطرها تلوح في الأفق مهددةً بذلك السلم والأمن الدوليين.

أن الاطلاع على آراء المختصين ذات الصلة بموضوع الدراسة، تدل على هذا التحدي، فمنهم من يرى أن المبادئ والقواعد التي أرساها القانون الدولي الإنساني تنطبق على تلك الهجمات.[٨٠]

وعلى العكس يرى آخرون بأن المدة التي جرى فيها تقنين القواعد القانونية ذات الصلة باستخدام وسائل و طرائق القتال، لم يكن لاستخدام الأنظمة الالكترونية للأغراض العسكرية وجود يذكر، ما يعني أنها غير مقننة أصلاً ، و أنها غير منظمة وفقاً للقواعد الدولية العرفية ما يفهم أنها خارج التنظيم القانوني الدولي.

ويشير الفريق الثاني، إلى مدة إبرام الاتفاقيات وذلك في منتصف القرن الثامن عشر وما بعدها ولاسيما اتفاقيات لاهاي لعام ١٨٩٩ -١٩٠٧ واتفاقيات جنيف الأربعة لعام ١٩٤٩ والبروتوكولان الإضافيان لعام ١٩٧٧، والتي لم يكن للهجمات السيبرانية خلال إبرامها وجود يذكر،[٨١] ويدعو أولئك إلى إعادة النظر في تقويم القانون الدولي الإنساني، وتطويره بهدف استيعاب مفهوم الهجمات السيبرانية وتنظيمها في إطار قانوني دولي صريح.[٨٢]

أن تكييف استخدام الهجمات السيبرانية يدور في فرضيتين اثنتين: الأولى في عدم القدرة على إثبات الدليل المادي الناجم عن استخدام الهجمات السيبرانية ، وهي العائق الأكبر الذي يواجهه المختصون ،على عكس وسائل وطرق القتال الأخرى المعروفة، و التي تترك أثراً مادياً ملموساً مباشراً أم غير مباشر بعد الهجوم، كالدمار أو التعطيل الجزئي أو الكلي الذي تتعرض له الأعيان العسكرية أو المدنية أو القتل أو الجرح الذي يصيب المقاتلين أو المدنيين.[٨٣]

أما الفرضية الثانية فعلى العكس، إذ تثبت أن الهجمات السيبرانية قد تؤدي إلى آثار مادية ملموسة على المستويات الاقتصادية والأمنية والعسكرية كافة.[٨٤]

ولدى قراءة ديباجة القرار الصادر عن الجمعية العامة للأمم المتحدة رقم (٣٦/ ٥٥) لعام ٢٠٠٠ الموسوم (مكافحة إساءة استعمال تكنولوجيا المعلومات)، يتضح أن آثار الهجمات السيبرانية هي غير محدودة ويمكن أن تطال بالدمار نواحي الحياة أجمعها، ومع ذلك لا يزال البحث في خطورتها يناقش على المستوى الأدنى من التنظيم الدولي، وبعبارة أخرى تأكيد خطورة الهجمات السيبرانية دون المبادرة إلى تحديد آثارها في ضوء اتفاقية دولية معنية بالحظر أو التقييد.[٨٥]

و قد يعود السبب في عدم التصريح بتلك الآثار، إلى تكتم الدول وتفردها بهذا الاستخدام ، فهي لا تحبذ أن يطرح موضوع التنظيم على المنابر الدولية، حتى لا تحيد عن الموقع المهم بين الدول المهيمنة على هذا القطاع المهم والحيوي لكونه يديم أمنها القومي.

أن تأخر الدول في التوصل إلى اتفاقية دولية معنية بالهجمات السيبرانية، يعيد بالذاكرة إلى الوراء بالذات كما حصل في موضوع تأخر التنظيم الصريح والمحدد في استخدام الأسلحة النووية بالحظر أو التقييد

حتى وقتنا الحالي، حيث مانعت الدول الحائزة تنظيم هذا الموضوع ، فاستبدلته باتفاقية حظر الانتشار النووي لعام (١٩٦٨) واتفاقية الحظر الشامل للتجارب النووية لعام (١٩٩٦).[٨٦]

ومن خلال ما تقدم يبدو أن العائق في تكييف الهجمات السيبرانية كإحدى وسائل أو طرائق القتال، إنما يعود لمصالح بعض الدول الرائدة في مجال استخدامها ، فضلاً عن قدرة الأنظمة الالكترونية في تحويل تلك الأوامر(برامج الكترونية عدائية) إلى آثار مادية ملموسة، وبعبارة أخرى لها حركة و قابلة لإحداث خسائر في أهداف منتخبة مسبقاً في الدولة الضحية للهجوم السيبراني وهو ما يطلق عليه عادة (Kinetic Effect) أي الأثر الحركي.[٨٧]

وفي ما يلي من البحث سنتطرق إلى مبدأين طالما أشير إليهما في تكييف استخدام طرق أو وسائل القتال وهما الحق في الحرب (Jus ad Bellum) و سلوكيات الحرب (Jus in Bello).

الفرع الأول

مبدأ الحق في اللجوء إلى الحرب (Jus in bellum)

عرف الفقيه ميتشل والزر(Michael Walzer) هذا المبدأ بالقول: "أنه قانون الحرب في إطار نظرية العدوان (Theory of Aggression) أي الحق في رد العدوان".[٨٨]

وفي سياق متصل يطرح التساؤل الآتي، هل يمكن للدولة اللجوء إلى الهجمات السيبرانية كحق وخيار مطروح للدفاع عن النفس ؟

للإجابة سيتم البحث في ثلاث مسائل: الأولى حظر استخدام القوة أو التهديد بها في ضوء تحليل حكم الفقرة (٤) من المادة (٢) من ميثاق الأمم المتحدة ، أما الثانية فبحث الاستثناءات الواردة على حظر استخدام القوة أو التهديد بها ، وأخيراً الثالثة فبتسليط الضوء على قواعد القانون الدولي الإنساني ذات الصلة بمبدأ الضرورة العسكرية و مبدأ وجوب التمييز بين المدنيين والمقاتلين و مبدأ التناسب في استخدام القوة المسلحة.

وفيما يخص المسألة الأولى: فتنص الفقرة (٤) من المادة (٢) من الميثاق بأنه: (يمتنع أعضاء الهيئة جميعاً في علاقاتهم الدولية عن التهديد باستعمال القوة أو استخدامها ضد سلامة الأراضي أو الاستقلال السياسي لأية دولة أو على أي وجه آخر لا يتفق ومقاصد " الأمم المتحدة ").

أن قراءة نص هذه الفقرة قراءة مستفيضة، يتضح أنها تحظر التدخل في الشؤون الداخلية فيما بين الدول الأعضاء سواء أكان التدخل بصورة التهديد في استخدام القوة أو في استخدامها فعلاً، وقد يكون طرح هذه الفقرة وفي موضوع البحث يثير تساؤلاً: ما علاقة نص هذه الفقرة بالهجمات السيبرانية؟

أشار عدد من الباحثين لدى دراستهم موضوع الهجمات السيبرانية إلى جدلية تكييف تلك الهجمات إن وقعت بمثابة خرق واضح لحكم الفقرة (٤) من المادة السالفة ، ومن أولئك شين (SHIN) و ماركو روسيني (Marco Roscini) .[٨٩]

ولدى استقراء الآراء الفقهية الأخرى، فقد جرى تفسير الفقرة (٤) من المادة (٢)، على نحويين مختلفين: الأول يؤكد أن نص هذه الفقرة ، إنما ينطبق على التهديد أو الاستخدام الفعلي للقوة المسلحة فحسب، وهو منحى تحبذه الدول التي عرفت بدعمها للمجموعات المسلحة أو ما يعرف بالتدخل الإنساني أو التدخل لأجل المسؤولية.[٩٠]

أما الثاني : وهو ما تؤيده اغلب الدول النامية، فيذهب إلى مفهوم أوسع نطاقاً،أي أن التهديد باستخدام القوة أو استخدامها فعلاً، لا يعني أنها الوسيلة الوحيدة للتدخل في شؤون الدول الداخلية التي أشار إليها حكم الفقرة نفسها، فالتدخل في الشؤون السياسية أو الاقتصادية يعد كذلك بمثابة تدخل قد يهدد استقرار الدولة وسيادتها.[٩١]

ويستند الفريق الثاني إلى ما أشارت إليه صراحة محكمة العدل الدولية وفي مناسبات عدة، ولاسيما في قضية الأنشطة العسكرية وشبه العسكرية (نيكاراغوا ضد الولايات المتحدة الأمريكية) (Nicar.v.US) عام ١٩٨٦.[٩٢]

أن طرح قضية التدخل في نيكاراغوا كمثال على حظر الهجمات السيبرانية له ما يبرره ، إذ أن الهجمات تلك عادةً ما تستهدف استقرار الدول وأنظمتها السياسية، بل في حالة استخدام الهجمات السيبرانية قد تكون تهديداً مباشراً للسيادة والأمن الداخلي للدول.

أن المثال على ذلك يتجسد في صورة استهداف شبكات الاتصال الالكترونية والكهرومغناطيسية، فضلاً عن البنى التحتية الضرورية لحياة المواطنين، كمحطات توليد الطاقة الكهربائية، وقد يكون الاستهداف مباشراً قبيل إعلان حالة النزاع المسلح، كاستهداف البنى التحتية العسكرية أو المدنية ، بأسلحة موجهة عن بعد و دون سابق إنذار.[٩٣]

وعلى الرغم من أن الرأي المستقر لدى فقهاء القانون الدولي العام، يشير إلى أن التهديد لا يقوم إلا بقوة عسكرية مادية[٩٤] ، إلا أن شين (Shin) ذهب إلى اتجاه مغاير بالقول:" من الصعب الإقرار بشرعية الهجمات السيبرانية فذلك لا يعفي الدول من مسؤولية التدخل وفقاً للفقرة (٤) من المادة (٢) من ميثاق

الأمم المتحدة، في حال أدت الهجمات السيبرانية إلى آثار مادية ملموسة في الأعيان المدنية أو العسكرية".[٩٥]

وقد ذهب إلى هذا الاتجاه ماركو روسيني (Marco Roscini) بالقول:" ... ومن الممكن أن تعد 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 إلى استخدام القوة تحت طائلة المادة (٥١) من الميثاق نفسه، والتي تتيح الحق في الدفاع عن النفس"، ثم يذكر روسيني بالقول :" يمكن للقواعد العرفية الدولية أن تؤدي دوراً متميزاً في تكييف الهجمات تلك، ولاسيما في ظل عدم وجود اتفاقيات دولية تنظم صراحة موضوع الهجمات السيبرانية".[٩٦]

وتأسيساً على ما تقدم يمكن القول بوقوع خرق لأحكام القانون الدولي الإنساني العرفي، ولكن لا على سبيل الطرق المعتادة للتدخل، ويعود ذلك إلى أن الدول عادةً ما تخفي نشاطها في هذا المجال، إذ تعهد مسؤولية الهجمات السيبرانية إلى كيانات من غير الدول(مجموعات من الأفراد) ، لتتجنب المسؤولية الدولية ضدها أو لتوخي تلقيها هجمات مضادة كردة فعل، وهو ما يؤكده سانجيف تومار (Sanjiv Tomar) من خلال تقييمه لنشاطات الصين الاقتصادية في أفريقيا على وجه التحديد إذ يذهب بالقول: استخدمت الصين ما يمكن الاصطلاح عليه بالقوة الناعمة للسيطرة على الثروات الطبيعية في أفريقيا من خلال توسيع نطاق النزاعات المسلحة غير الدولية على أسس عرقية أو قومية، وبعبارة أخرى فإنها دعمت حروبا بالوكالة عنها (Proxy War) وبمختلف الإمكانيات، ومنها دعم مجموعات مسلحة شنت هجمات سيبرانية ضد مصالح اقتصادية أمريكية كبيرة في أفريقيا .[٩٧]

وفي هذا الشأن يذهب توماس فرانك (Thomas M.Franck) إلى القول بأنه: "تخفي الدول عادة تورطها في هجمات سيبرانية، خشية أن يؤسس ذلك إلى استخدام مماثل لهجمات سيبرانية غير قانونية مضادة...".[٩٨]

أما المسألة الثانية، فسنتطرق إلى إمكانية استخدام الهجمات السيبرانية كاستثناء من الحظر الوارد في الفقرة (٤) من المادة (٢) من ميثاق الأمم المتحدة.

أن مراجعة ميثاق الأمم المتحدة وبالذات المادة (٣٩) منه والتي نصت: (يقرر مجلس الأمن ما إذا كان قد وقع تهديد للسلم أو إخلال به أو كان ما وقع عملاً من أعمال العدوان، ويقدم في ذلك توصياته أو يقرر ما يجب اتخاذه من التدابير طبقاً لأحكام المادتين ٤١ و ٤٢ لحفظ السلم والأمن الدولي أو إعادته إلى نصابه)، يتضح أنها الاستثناء الأول على حظر استخدام القوة، وإن كان اللجوء إليها صعباً ومعقداً للغاية

بسبب الإجماع الذي تقتضيه من أعضاء مجلس الأمن الدائمين لإصدار قرار وفقاً للمادة (٤٢) من الميثاق نفسه لتشكيل هيئة أركان حرب.[٩٩]

أما الاستثناء الآخر فهو ما نجده في المادة (٥١) من الميثاق والتي نصت: (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 " الأمم المتحدة.....).[١٠٠]

و وفقاً لحكم هذه المادة فللدولة الحق في استخدام القوة للدفاع عن نفسها في مواجهة أي هجوم، سواء أكان هجوما وفق ما هو معروف ضمن وسائل استخدام القوة أو طرائق تنفيذها، أو باستخدام تكنولوجيا المعلومات الحديثة للأغراض العسكرية.

أن ما طرح آنفا يدفعنا إلى التساؤل الآتي: ما هو المعيار الذي يقوم عليه الدفاع عن النفس؟ وهل ينطبق هذا الأمر على الهجمات السيبرانية والتي تأخذ صورة التسلل إلى مواقع الكترونية ومن ثم السيطرة والتحكم فيها عن بعد، وبعبارة أخرى هل ترقى الهجمات السيبرانية إلى مرتبة تصرف عدائي (Aggressive behavior) ؟

أن السوابق القضائية لمحكمة العدل الدولية ذهبت بأن نطاق الهجوم المكاني وآثاره، معنيان في تحديد ردة فعل الدولة المعتدى عليها، وبعبارة أخرى هل لها الحق في استخدام القوة أم لا ؟

لقد قضت المحكمة - على سبيل المثال- :".... أن وقوع الحادثة على حدود الدولة، استخدم في أثنائها وسائل قتالية، لا يمكن أن تكيف لوحدها كهجوم مسلح، ولا تبرر القيام بعمليات قتالية مضادة، فهي لا تعدو كونها حادثة حدودية وقعت (Frontier incidents) كما أنها لم تكن على نطاق واسع (Significant scale).[١٠١]

وبالرجوع إلى الموضوع نفسه، يرى ميشيل شميت (Mecheal Schmitt) أن الهجمات السيبرانية تقوم على عدة عناصر: منها ما يتعلق بنوع الهجوم ونطاق آثاره (Severity) ، والتزامن، أي الوقت الذي يستغرقه الهجوم وآثاره الآنية (Immediacy)، فضلاً عن النطاق المكاني الذي تعرض للهجوم (Invasiveness).

وأخيراً، مدى إمكانية تقدير الأضرار الناشئة عن الهجوم (Measurability) ، و يؤكد ميتشل بالقول:" أن الهجوم السيبراني يمثل خروجاً عن القواعد القانونية المألوفة في تنظيم وسائل و طرائق القتال".[١٠٢]

وفي ضوء ما تقدم من معطيات ،يمكن القول أن الركون إلى مسألة الدفاع عن النفس واللجوء إليها كمبرر للقيام بهجمات سيبرانية مضادة ،هو أمر صعب ومعقد، لكون الأخيرة غير متفق على مفهومها

على صعيد القانون الدولي العام والإنساني بالذات، بدليل أثبتته الوقائع، إذ لم يسجل إلى وقت إعداد هذه الدراسة ، أن قامت دولة بعمليات قتالية تحت عنوان الدفاع عن النفس لمجرد تعرضها لهجمات سيبرانية.

أن المعيار في تكييف الهجمات السيبرانية في ضوء مبدأ الحق في اللجوء إلى الحرب (Jus ad Bellum)، وفيما إذا كانت من قبيل التصرف العدائي أو كونه تصرفاً لرد العدوان، إنما يعتمد بدرجة أساس على القواعد القانونية ذات الصلة وبالذات حكم الفقرة (٤) من المادة (٢) والمادة (٥١) من ميثاق الأمم المتحدة، والتي ترتب آثار قانونية عند اللجوء إليها، وبعبارة أخرى فهي تكيف على صورتين:

الأولى: قيام المسؤولية الدولية جراء العدوان باستخدام الهجمات السيبرانية وما ينجم عنها من أضرار مادية مباشرة أو غير مباشرة واسعة و ملموسة لحقت بمصالح دولة أخرى أو أمن مواطنيها ومقاتليها.

ثانياً: تبرير حق الدفاع عن النفس و استخدام القوة المسلحة لرد العدوان وبما يتوافق والمبادئ الدولية ذات الصلة ، وأهمها مبدأي الضرورة العسكرية والتناسب في استخدام القوة.

و لتأكيد هذا التوجه يذهب ديلوكا (Deluca) إلى أنه :" ... من الممكن وصف الهجمات السيبرانية التي تعرضت لها استونيا عام ٢٠٠٧، بأنها عدوان يخضع إلى مبدأ الحق في اللجوء إلى الحرب (Jus ad bellum)،لأن البنى التحتية في استونيا كمحطات إطفاء الحريق و المستشفيات و الصحف اليومية و البنوك، كانت هي المستهدفة مباشرة من الهجوم، ما يعني أن المدنيين وفي هذه الحالة وقعوا ضحية هذا الهجوم ".[١٠٣]

وما يؤيد ما ذكر في أعلاه ، إعلان وزارة الدفاع الأمريكية (البنتاغون) الصريح في عام ٢٠١١، بأن توجيه هجمات سيبرانية ضد الولايات المتحدة، وما ينجم عنها من أضرار ملموسة في مصالحها الأمنية أو العسكرية أو الاقتصادية، سيعني تبرير استخدام القوة العسكرية اللازمة، للرد على هذا الاعتداء في ضوء ما يمكن الاصطلاح عليه بالحرب العادلة (Just war) أو الحرب المبررة (Casus belli).[١٠٤]

و على العكس مما تقدم، هنالك من انتقد هذا التوجه ، على أساس أن من الصعب التمييز بين آثار الهجمات السيبرانية المسببة لأضرار مادية، عن آثار الهجمات المسلحة التقليدية كالصواريخ الموجهة، ما يعني أن تحديد مفهوم هذه الهجمات، هو نقطة البداية لتقنين التصرفات المخالفة لأحكام أي اتفاقية دولية تبرم مستقبلاً ، يكون موضوعها حظر أو تقييد استخدام الوسائل أو الطرق السيبرانية للأغراض العسكرية.[١٠٥]

أن التوجه الحالي، يدفع نحو انطباق المبادئ الدولية على سير الهجمات السيبرانية، وهذا ما نجده في تحليل أعدته لجنة الهجمات السيبرانية التابعة للمجلس الوطني الأمريكي للأبحاث عام ٢٠٠٩، بالقول:"

نعتقد أن مبادئ النزاعات المسلحة، فضلاً عن ميثاق الأمم المتحدة ذات الصلة بشرعية اللجوء إلى استخدام القوة أو تلك المعنية بسير العمليات القتالية هما المعنيان بتنظيم الهجمات السيبرانية ...."."[١٠٦]

الفرع الثاني

مبدأ سلوكيات الحرب (Jus ad bello)

فيما سبق من الدراسة، تم البحث في علاقة الهجمات السيبرانية بمبدأ الحق في اللجوء إلى الحرب، و لا بد من طرح الموضوع ذاته في ضوء مبدأ سلوكيات الحرب، وبعبارة أخرى أهم المبادئ الدولية التي تحكم سير العمليات القتالية وهذا ما سنتناوله في هذا الفرع .

١. مبدأ الضرورة العسكرية

قبل الخوض في مفهوم هذا المبدأ ، نطرح تساؤلاً :هل يمكن توجيه الهجمات السيبرانية ضد أهداف عسكرية أو مدنية أو خليط من ذلك ، بحجة توافر أسباب مقنعة دفعت بالطرف المحارب إلى تبنيها كخيار عسكري ضروري؟

قبل الإجابة لابد من تفحص أحكام الصكوك الدولية المعنية بتنظيم مبدأ الضرورة العسكرية، ومن بعد ذلك أهم الآراء التي قيلت بشأنه.

لقد تم التطرق إلى مبدأ الضرورة العسكرية في عدة صكوك دولية منها ما جاء واضحاً في إعلان سان بيترسبورغ لعام ١٨٦٨ بالقول : "ضرورات الحرب يجب أن تخضع لمتطلبات الإنسانية ".[١٠٧] كذلك نجده في حكم الفقرة (٢\ز) من المادة (٢٣) من اتفاقية لاهاي بشان الحرب البرية لعام ١٩٠٧ ، بأنه: " يمنع بالخصوص ..... تدمير ممتلكات العدو أو حجزها، إلا إذا كانت ضرورات الحرب تقتضي حتماً هذا التدمير أو الحجز".[١٠٨]

وفي الشأن ذاته أشارت الفقرة (٢) من المادة (٥٢) من البروتوكول الإضافي الأول لعام ١٩٧٧ إذ قضت بأنه: " تقتصر الهجمات على الأهداف العسكرية فحسب ، وتنحصر الأهداف العسكرية فيما يتعلق بالأعيان ،على تلك التي تسهم مساهمة فعَّالة في العمل العسكري ، سواء كان ذلك بطبيعتها أم بموقعها أم بغايتها أم باستخدامها ، و التي يحقق تدميرها التام أو الجزئي أو الاستيلاء عليها أو تعطيلها ، في الظروف السائدة حينذاك ، ميزة عسكرية أكيدة".[١٠٩]

من جانب آخر، نجد حكم الفقرة (رابعاً) من المادة (٥١) من البروتوكول الإضافي الأول لعام ١٩٧٧ يؤكد عدم جواز استعمال وسائل و طرق قتال، من شأنها أن تؤدي إلى هجمات عشوائية و من بينها :

أ- تلك التي لا توجه إلى هدف عسكري محدد.

ب- أو تلك التي تستخدم طريقة أو وسيلة للقتال لا يمكن أن توجه إلى هدف عسكري محدد.

ت- أو تلك التي تستخدم طريقة أو وسيلة للقتال لا يمكن حصر آثارها على النحو الذي يتطلبه هـذا ألملحق " البروتوكول "، ومن ثم فإن من شأنها أن تصيب في كل حالة كهذه الأهداف العسكرية و الأشخاص المدنيين أو الأعيان المدنية دون تمييز.[١١٠]

وبناء على ما تقدم يفهم أن مبدأ الضرورة العسكرية يتيح مهاجمة الأعيان العسكرية كخيار ضروري بالمرتبة الأولى ، إلا أن ذلك لا يمنع - كضرورة - من مهاجمة أعيان مدنية إذا كانت تُسهم بطريقة غير مباشرة في تحقيق ميزة عسكرية أكيدة .

ولكن علينا أن نسأل إذا كان بالإمكان التمييز بين الأهداف العسكرية والمدنية في النزاعات المسلحة التقليدية، فلأمر ليس كذلك بالنسبة للهجمات السيبرانية التي من الممكن أن تستهدف منشآت تقدم خدمة للجهد العسكري وفي الوقت نفسه للمدنيين.

يجيبنا عن هذا السؤال ركس هوجيس (Rex Hughes) بالقول:" أن الهجمات الرقمية (Digital) تنشئ تحدياً واضحاً أمام تطبيق مبدأ الضرورة العسكرية، ولحل هذه المعضلة لابد من تضافر الجهود بين خبراء القانون الدوليين ومهندسي الصناعات الالكترونية لتحديد ما يمكن أن يوصف بهدف ....".[١١١]

أن عدم تحديد معايير منظمة لاستخدام تكنولوجيا المعلومات للإغراض العسكرية الهجومية، سيعني إمكانية اللجوء في استخدامها بداعي الضرورة العسكرية، وهو ما نجده جلياً في تصريحات متبادلة بين الولايات المتحدة الأمريكية وروسيا.

إذ أصدرت وزارة الدفاع الأمريكية بياناً وضحت فيه أن خبراء من روسيا نشروا دراسة قانونية تفيد بأنه:" لروسيا الحق باستخدام الأسلحة النووية في حال تعرضها لهجوم سيبراني".[١١٢]

فيما أعلنت روسيا بأنه:" أن توجيه هجمة سيبرانية ضد منشآت الاتصال الالكترونية الأمريكية، سيعني حكماً وقوع نتائج كارثية توازي استخدام أسلحة الدمار الشامل"،[١١٣]

ومن تحليل هذه التصريحات يتضح أن مبدأ الضرورة العسكرية هو مبدأ حاضر بقوة في أي هجمات سيبرانية متبادلة بين هاتين الدولتين، فالولايات المتحدة تركز على ردة فعل روسيا في حال تعرضها لهجوم سيبراني أمريكي.

فيما يتضح من جانب آخر نوايا روسيا في عدم استخدام المجال الالكتروني لمهاجمة الولايات المتحدة خشية تعرضها لهجوم آخر مضاد، باستخدام أسلحة دمار شامل قد تلجأ إليها الولايات المتحدة كضرورة عسكرية وهذا واضح من خلال استخدام عبارة نتائج كارثية (Catastrophic Consequences).

٢. مبدأ وجوب التمييز بين المقاتلين والمدنيين

وفقاً لهذا المبدأ يتوجب على أطراف النزاع المسلح التمييز بين المقاتلين والمدنيين،إذ أشارت المادة (٤٨) من البروتوكول الإضافي الأول لعام ١٩٧٧بالقول: " تعمل أطراف النزاع على التمييز بين السكان المدنيين و المقاتلين وبين الأعيان المدنية و الأهداف العسكرية ومن ثم توجه عملياتها ضد الأهداف العسكرية دون غيرها ، وذلك من أجل تأمين احترام و حماية السكان المدنيين والأعيان المدنية".[١١٤]

وهو ما نصت عليه الفقرة (٢) من المادة (٥١) من البروتوكول نفسه بالقول: " لا يجوز أن يكون السكان المدنيون بوصفهم هذا، وكذا الأشخاص المدنيون محلاً للهجوم وتحظر أعمال العنف أو التهديد به الرامية أساساً إلى بث الذعر بين السكان المدنيين".[١١٥]

وفي الجانب القضائي الدولي يعد الرأي الذي ذهبت إليه محكمة العدل الدولية بشأن شرعية التهديد باستعمال أو استعمال الأسلحة النووية عام ١٩٩٦ الجانب التطبيقي الأكثر تأكيدا إلى هذا المبدأ بأنه: " يهدف إلى حماية السكان المدنيين والأعيان المدنية ويؤسس التمايز بين المقاتلين وغير المقاتلين ، وينبغي على الدول ، ألا تجعل المدنيين هدفاً للهجوم ، ويجب بالتالي ألا تستخدم الأسلحة التي لا تميز بين الأهداف المدنية والعسكرية".[١١٦]

لقد كيفت المحكمة ضمن فقرات الرأي الاستشاري السابق، هذا المبدأ كقاعدة آمرة بالقول: " القواعد الأساسية (للقانون الدولي الإنساني) يجب أن تمتثل إليها الدول سواء كانت قد صدقت أو لم تصدق على الاتفاقيات التي تحتويها ، ذلك أنها تمثل مبادئ القانون الدولي العرفي غير القابلة للانتهاك".[١١٧]

وقد ذهبت المحكمة الجنائية الدولية الخاصة بيوغسلافيا السابقة لعام ١٩٩٣إلى التأكيد على ما ذكر سلفاً، من خلال تسليط الدائرة التمهيدية الأولى ، الضوء على أهمية هذا المبدأ وانطباقه على النزاعات المسلحة الدولية و غير الدولية دون استثناء ، بالقول: " القاعدة التي تنص على أن السكان المدنيين ، بصفتهم هذه فضلاً عن المدنيين الأفراد ، لن يكونوا هدفا للهجوم ، هي قاعدة أساسية في القانون الدولي الإنساني ، الواجب تطبيقه على جميع النزاعات المسلحة".[١١٨]

وبناءً على ما تقدم من معطيات، فإن تطبيق مبدأ وجوب التمييز بين المقاتلين والمدنيين على الهجمات السيبرانية هي مسألة في غاية التعقيد -على عكس الهجمات التقليدية- إذ سيكون المهاجم في الأغلب بعيداً عن المكان المستهدف من الهجوم ولمسافة قد تتجاوز المئات من الكيلومترات، ما يعني أن التمييز بين المقاتلين والمدنيين هو أمر صعب إذا لم يكن مستحيلاً، وهو ما دفع بالمحامين الدوليين للمطالبة بتطبيق هذا المبدأ على الهجمات التي تقوم بها الطائرات بدون طيار (Drown)، وفي مناسبة أخرى في

تحميل روسيا الاتحادية مسؤولية الهجمات السيبرانية التي تعرضت لها استونيا عام ٢٠٠٧ بسبب عدم تمييزها بين المقاتلين والمدنيين.[١١٩]

وفي هذا الشأن دعا فقهاء كماركو روسيني (Marco Roscini) إلى أن يتحرك المحامون الدوليون لأجل البحث في مدى مواءمة الطابع السري الذي تتميز به الهجمات السيبرانية في ضوء أحكام القانون الدولي الإنساني وبالذات مبدأ سلوكيات الحرب (Jus ad bellum) ، خصوصاً بعد تنامي ادعاءات الدول بتعرضها إلى هجمات غير معروفة المصدر.[١٢٠]

٣. مبدأ التناسب في استخدام القوة المسلحة

استخدم مصطلح مبدأ التناسب أول مرة في عام ١٩٢٢ في أثناء تقنين قواعد الحرب الجوية في لاهاي ، وبالذات في الفقرة (١) من المادة (٤) بالنص: " لا يكون القصف الجوي مشروعاً إلا عندما يوجه فقط ضد الأهداف التالية: القوات العسكرية ، الأشغال العسكرية و المؤسسات أو المستودعات العسكرية ، المصانع التي تعتبر مراكز هامة و معروفة لإنتاج الأسلحة أو الذخيرة أو الإمدادات العسكرية المتميزة ، خطوط الاتصال أو النقل المستعملة لأغراض عسكرية ".[١٢١]

واستمر التنظيم الدولي في الإشارة إلى هذا المبدأ، في الفقرة (٥ \ب) من المادة (٥١) من البروتوكول الإضافي الأول لعام ١٩٧٧ بأنه: " يحظر الهجوم الذي قد يتوقع منه أن يسبب بصورة عارضة خسائر في أرواح المدنيين أو إصابات بينهم ، أو أضراراً بالأعيان المدنية أو مجموعة من هذه الخسائر أو الأضرار ، ويكون مفرطاً في تجاوز ما ينتظر أن يسفر عنه من ميزة عسكرية ملموسة ومباشرة ".

و هو مضمون أكدته الفقرة (ب ٢١) من المادة (٥٧) من البروتوكول الإضافي الأول لعام ١٩٧٧ ، بالنص على :" يلغى أو يعلق أي هجوم ، إذا تبين أن الهدف المقصود ليس هدفاً عسكرياً ، أو أنه مشمول بحماية خاصة ، أو أن الهجوم قد يتوقع منه أن يُحدِثَ خسائر في أرواح المدنيين أو إلحاق الإصابة بهم ، أو الأضرار بالأعيان المدنية أو أن يحدث خلطاً من هذه الخسائر أو الأضرار وذلك بصفة عرضية، تفرط في تجاوز ما ينتظر أن يسفر عنه ذلك الهجوم من ميزة عسكرية مباشرة ".[١٢٢]

أن السؤال الجوهري الذي يطرح بمناسبة التعرض إلى هذا المبدأ تتلخص بالآتي: هل يمكن تأكيد احترام مبدأ تناسب قبل التخطيط لاستخدام وسائل أو طرائق سيبرانية معدة لإغراض هجومية؟

لدى الاطلاع على آراء بعض المختصين، نراهم حذرين عند تعرضهم للمبدأ في ضوء الآثار الناجمة عن الهجمات السيبرانية، إذ يذهب شين (SHIN) إلى القول :" يمكن تطبيق مبدأ التناسب على الهجمات السيبرانية"، ثم يقول: "ولكن علينا أن نسأل فيما إذا كانت الهجمات السيبرانية يمكن عدَّها عدواناً لا يختلف عن الهجوم باستخدام الصواريخ على سبيل المثال"[١٢٣]، في الإشارة إلى تصريح وزارة الدفاع

الأمريكية عام ٢٠١١، والتي لم تفرق بين الهجوم الذي قد تتعرض له أكان بالصواريخ أو الهجمات السيبرانية و عدّها مبرراً للرد باستخدام القوة المسلحة المناسبة.[١٢٤]

ويضيف شين (Shin) بالقول :"أن مبدأ التناسب في استخدام القوة السيبرانية لا يزال غامضاً و يحتاج إلى أجوبة أهمها كيف يمكن ضمان مبدأ التناسب في الرد على الهجمات السيبرانية".[١٢٥]

ويتفق ركس (Rex) مع ما ذهب إليه شين (Shin) بقوله:" إذا تم توجيه هجمات سيبرانية ضد بنى تحتية ثنائية الاستعمال (مدنية –عسكرية) وعن بُعد، فلا يبدو أن المنفعة العسكرية ستكون واضحة، ما يجعل من تطبيق مبدأ التناسب في أثناء الهجمات السيبرانية أمراً في غاية الصعوبة".[١٢٦]

ونحن نؤيد الرأي أعلاه، إذ ثبت من الواقع المرير للنزاعات المسلحة التي يشهدها العالم اليوم،استخدام أسلحة أدت إلى آثار لا إنسانية سواء في صفوف المدنيين أو العسكريين لا تتناسب والهدف الرئيس من استخدام القوة ،وهو رد العدوان بمثله، ما يعني أن عدم وجود أحكام صريحة تنظم استخدام الهجمات السيبرانية،فضلاً عن موقف مبدأ التناسب منها ، هو إقرار ضمني بعجز هذا المبدأ على ضبط الآثار المتوقع حدوثها سواء في أثناء التخطيط أو بعد تنفيذ الهجوم السيبراني.

٤. مبدأ مارتنز

قبل أن نخوض في مفهوم هذا المبدأ، و البحث في قدرته على سد الفراغ الذي يعتقده البعض من المختصين في القانون الدولي، وبعبارة أخرى عدم وجود أحكام محددة تنظم الهجمات السيبرانية، نطرح التساؤل الآتي، هل يمكن التوسع في تطبيق هذا المبدأ على الهجمات السيبرانية كما جرى في سوابق قضائية دولية مماثلة ؟

سنحاول الإجابة من خلال البحث في مفهوم مبدأ مارتنز ،ذلك المبدأ الذي يعد صمام الأمان في معالجة القضايا الدولية المستحدثة و غير المنظمة صراحة وفقا لأحكام القانون الدولي العام ، ومن ثم استقراء آراء الفقهاء فيما يخص تطبيقه على الهجمات السيبرانية.

لقد سبق القول أن التنظيم الدولي المعاصر يواجه معضلة كبيرة في موضوع الهجمات السيبرانية والتي لم تنظم صراحة على صعيد القانون الدولي العام ولا الإنساني (المقنن) بوجه خاص، فكيف يمكن التصدي لهذا الفراغ القانوني، ولاسيما أن اغلب المبادئ الدولية التي تطرقنا إليها بالبحث لا يمكن تطبيقها بسهولة على هذه الهجمات؟

أن نشأت هذا المبدأ تعود إلى فيودور فيودوفج مارتنز (Fyodor F. Martens) احد مندوبي روسيا في مؤتمر السلام عام ١٨٩٩[١٢٧] والذي صرح فيه:" أنه في الحالات غير المشمولة بالأحكام ، يظلُ السكان

المتحاربون تحت حماية و سلطان مبادئ قانون الأمم كما جاءت ، من تقاليد التي استقر عليها الحال بين الشعوب المتمدنة وقوانين الإنسانية ومقتضيات الضمير العام".[١٢٨]

وتكرر ذكر هذا المبدأ في ديباجة اتفاقية لاهاي الثانية المتعلقة بقوانين و أعراف الحرب البرية لعام ١٨٩٩، إذ نصت: " حتى تصدر مدونة بقوانين الحرب أكثر اكتمالاً ، ترى الأطراف المتعاقدة من المناسب أن تعلن أنه في الحالات التي لا تشملها هذه اللائحة التي اعتمدتها ، يظل السكان المدنيون والمقاتلون تحت حماية مبادئ الأمم الناتجة عن العادات الراسخة بين الشعوب المتحضرة و قوانين الإنسانية ، وما يمليه الضمير العام".[١٢٩]

وفيما يخص السوابق القضائية فيعد الرأي الاستشاري الذي أدلت به محكمة العدل الدولية عام ١٩٩٦ ، و الخاص بشرعية التهديد أو استعمال الأسلحة النووية ، الأكثرُ قُرباً لموضوع الدراسة، إذ أكدت المحكمة ، بالقول " يمنح شرط مارتنز سلطة معالجة مبادئ القانون الإنساني وما يميله 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".[١٣٠]

ولدى قراءة حيثيات هذه الفتوى قراءة مستفيضة يتضح أن عدم وجود قواعد دولية محددة سواء أكانت عرفية أم تعاهدية تنظم الهجمات السيبرانية ، لا يعني الإقرار ضمناً بجواز اللجوء إليها من دون سند قانوني صريح ،لكونها – في الأغلب- تتنافى بطبيعتها مع القوانين الإنسانية و ما يمليه الضمير العام العالمي في حال أنها استهدفت منشآت تحوي قوى خطرة أو أعيان مدنية ضرورية لبقاء الإنسان كمحطات الكهرباء والسدود.

لقد أشار شميت (Schmitt) في معرض بحثه عن المبدأ المناسب و القابل للتطبيق على الهجمات السيبرانية بالقول:" 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".[١٣١]

وقد يُطرح السؤال الآتي : أن اغلب الهجمات السيبرانية هي هجمات عادةً ما يعلن أفراد أو مجموعات مسلحة من غير الدول مسؤوليتها عنها ، فهل ينطبق شرط مارتنز على النزاعات المسلحة كافة ، الدولية منها وغير الدولية ؟

لقد أشارت الفقرة (٢) من المادة (١) من البروتوكول الإضافي الأول لعام ١٩٧٧ إلى شرط مارتنز وانطباقه على النزاعات المسلحة الدولية بالقول : " يظل المدنيون و المقاتلون في الحالات التي ينص

علها هذا الملحق " البرتوكول " أو أي اتفاق دولي آخر تحت حماية و سلطان مبادئ القانون الدولي كما استقر عليها العرف ومبادئ الإنسانية وما يمليه الضمير العام "[١٣٢]. بينما أشارت ديباجة البروتوكول الإضافي الثاني لعام ١٩٧٧الى انطباق المبدأ على النزاعات المسلحة غير الدولية وذلك بالقول: " وإذ تذكر أنه في الحالات التي لا تشملها القوانين السارية يظل شخص الإنسان في حمى المبادئ الإنسانية وما يمليه الضمير العام".[١٣٣]

أن الفراغ القانوني الذي يشهده موضوع تنظيم الهجمات السيبرانية، وبعبارة أخرى عدم وجود اتفاقية دولية تنظمه، يفنده البعض من الفقهاء ويعدونها حجة مصطنعة ،إذ يذهب ايركي كودار (Erki Kodar) إلى القول: أن مبدأ مارتنز يشير 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".[١٣٤]

ومما تقدم تتضح الأهمية التي يوليها القانون الدولي العام والإنساني بالذات في مسألة انتهاك المبادئ الدولية السابقة، وتتجلى الأهمية في تقرير مسؤولية الدولة عن الأضرار التي تلحق بدول أخرى ومصالحها والتعويض عما لحق بها ،هذا في حالة عدم وقوع ضحايا ، أما في حالة وقوع ضحايا (قتلى أو جرحى) فيمكن أن توجه المسؤولية الجنائية الفردية لكل من القادة ومرؤوسيهم على حد سواء و وفقاً لما هو ثابت في القانون الدولي الإنساني العرفي وما أقرته المحاكم الجنائية الدولية، وهو ما سنسلط عليه الضوء فيما يلي من البحث.

المطلب الثاني

المسؤولية الدولية الناشئة عن الهجمات السيبرانية

كثرت في الآونة الأخيرة الدراسات القانونية المتخصصة [١٣٥] للبحث في إمكانية توجيه المسؤولية الدولية ضد دولة أو مجموعة من غير الدول (Non-State Actors)، نسبت ضدها تهم بارتكاب هجمات سيبرانية.

ولأجل الوقوف على أبعاد المسؤولية الدولية الناشئة عن الهجمات السيبرانية، سنبحث في مفهوم المسؤولية الدولية في ضوء التصرفات الدولية المعاصرة كقرارات المحاكم الدولية، فضلاً عن آراء وتعليقات كبار فقهاء القانون الدولي العام بشأنها.

الفرع الأول

التنظيم الدولي المعاصر و موقفه من المسؤولية الدولية

تعرض موضوع المسؤولية الدولية إلى متغيرات عدة ، بدءً من طرح النظريات ذات الصلة بها والمتمثلة بنظريتي الخطأ والمخاطر، فضلاً عن النظرية الموضوعية، و انتهاءً بالتنظيم الدولي المعاصر والمتمثل بتدخل لجنة القانون الدولي لإعداد مسودة بشأن المسؤولية الدولية عن الأفعال غير المشروعة.

ولأن ما يهم هو بيان مفهوم المسؤولية الدولية في ضوء الهجمات السيبرانية، فسنبحث في التعريف الوارد في مشروع المسؤولية الدولية عن الأفعال غير المشروعة لعام ٢٠٠١ ، و المادة (١) منه بالذات والتي نصت: (كل فعل غير مشروع دولياً تقوم به الدولة يستتبع مسؤوليتها الدولية).[١٣٦]

ويصح القول أنه لا يمكن قيام المسؤولية الدولية، إلا إذا ثبت أن السلوك كان مخالفاً لأحكام القانون الدولي العرفية أو التعاهدية ، ولكن هل يشترط أن يرتب السلوك ضرراً؟

أن مراجعة حكم المادة (١) من مشروع المسؤولية الدولية بشأن العمل غير المشروع لعام ٢٠٠١، يتضح أنها لم تشترط وقوع الضرر لتحريك المسؤولية الدولية.١٣٧

أن المفهوم نفسه، الذي جاءت به المادة (١) آنفة الذكر هو مفهوم مغاير لما استقر عليه في الاجتهاد الدولي القضائي والفقهي، الذي اشترط تحقق عنصر الضرر لقيام المسؤولية الدولية.[١٣٨]

أما على الصعيد الفقهي، فيعرفها محمد حافظ غانم بأن:" المسؤولية الدولية تترتب قِبل الدولة وقِبل أي من أشخاص القانون الدولي، إذا ما أتى ذلك الشخص أمراً يستوجب المؤاخذة وفقاً للمبادئ والقواعد القانونية السائدة في المجتمع الدولي".[١٣٩]

وفيما يخص القانون الدولي الإنساني ولكونه الأقرب إلى موضوع البحث، سنتناول المسؤولية الدولية الناشئة عن الهجمات السيبرانية .

من المعروف أن معظم أحكام الاتفاقيات و القواعد العرفية الدولية ذات الصلة ، حددت وبطريقة واضحة المسؤولية التي تقع على الدولة سواء أرتكب التصرف من مؤسسات الدولة الرسمية أو شبه الرسمية، شريطة أن يكون لها القدرة على ضبط تصرفاتها، وهو ما أشارت إليه المادة (٣) من اتفاقية لاهاي بشأن الحرب البرية لعام ١٨٩٩ المعدلة في عام ١٩٠٧، بالنص :" يكون الطرف المتحارب الذي يخل بأحكام اللائحة المذكورة ملزماً بالتعويض إذا دعت الحاجة, كما يكون مسئولاً عن جميع الأعمال التي يرتكبها أشخاص ينتمون إلى قواته المسلحة..[١٤٠]

ولو تمعنا في النظر حيال المسؤولية الدولية الناشئة عن الهجمات السيبرانية، سنجد أنها تختلف من ظرف لآخر، فلو كان الهجوم السيبراني، منصباً على تعطيل وسائل الاتصال العسكرية أو المدنية في أثناء النزاع المسلح، فالأمر وببساطة يخضع إلى أحكام القانون الدولي الإنساني وبالذات الأحكام التي تضبط تصرفات المقاتلين وطرائق العمليات العسكرية والتي ذكرنا جزءاً منها في ما سبق من الدراسة.

و في الشأن نفسه ، يضيف محمد حافظ غانم قيداً آخر ، على ما سبق ذكره فيقول : "... وإذا كان العرف الدولي قد استقر على ضرورة الإعلان عن الحرب قبل وقوع العمليات العدائية، فإن وقوع هذه العمليات دون إعلان قد يخلق حالة الحرب طالما كانت ظروف الحال تؤيد ذلك".[١٤١]

ومما يتقدم نستنتج أنه ، كلما كانت الهجمات السيبرانية بالأساس منتهكة لقاعدة دولية تعاهديه أو عرفية في أثناء النزاع المسلح ، فإن المسؤولية الدولية المترتبة على ذلك الأثر، ستكون في نطاق المبادئ الدولية المنظمة لسير العمليات العدائية وهي:

١. مبدأ أن حق أطراف النزاع في اختيار وسائل و طرائق القتال ليس حقا مطلقاً، المتفرع إلى مبدأين دوليين آخرين وهما:

أ- مبدأ وجوب التمييز بين المدنيين والمقاتلين.

ب-مبدأ الإصابات المفرطة الضرر أو العشوائية الأثر أو الآلام التي لا مبرر لها.

٢. مبدأ الضرورة العسكرية.

٣. مبدأ التناسب في استخدام القوة.

٤. مبدأ (شرط مارتنز).

أما الظرف الثاني فهو القيام بهجمات سيبرانية في حالة السلم، كالتجسس والتواصل مع مجموعات مسلحة لا تعود بجنسية أفرادها للدولة المتدخلة ، ففي هذه الحالة تقوم المسؤولية الدولية بناءً على خرق مبدأ عدم جواز التدخل في الشؤون الداخلية للدول ، وعليه لابد من بحث هذا الموضوع بشيء من التفصيل.

أن تحديد مسؤولية الدولة حيال دورها في التدخل يضبطه أمران اثنان: الأول ما نجده في المادة (٤) من مسودة لجنة القانون الدولي حول المسؤولية الدولية عن الأفعال غير المشروعة ، والتي تطرقت إلى مسؤولية الدولة في التصرفات الدولية الخاطئة، والمادة (٨) والتي تطرقت إلى مسؤولية الدولة عن تصرفاتها وتصرفات المجموعات المسيطرة عليها.[١٤٢]

ومن تحليل حكم المادة آنفة الذكر، يتضح أن مسؤولية الدولة، تقوم متى ما نسب لإحدى أجهزتها التنفيذية أو التشريعية أو القضائية تصرفاً خاطئاً ، تسبب في أضرار تجاه مصالح دولة أخرى أو ضد أحد رعاياها.

أن معيار السيطرة والقدرة على ضبط تصرفات أجهزة الدولة أو احد موظفيها أو المجموعات المسلحة المدعومة من قبلها ، يمثل الأساس الذي يمكن من خلاله تحريك المسؤولية الدولية، على أن معيار السيطرة أكان متحققاً أم لا ؟ ، فيترك إلى المحاكم المختصة للبحث فيه والتحقق من وجوده .

وبالنسبة لموضوع البحث وفي هذه النقطة بالذات، فغالباً ما تعلن مجموعة من غير الدول أو أفراداً بعينهم المسؤولية عن الهجمات السيبرانية، فكيف نظم القانون الدولي العام مثل هذه الأوضاع القانونية ؟

للإجابة عن هذا السؤال وبالركون إلى السوابق القضائية الدولية ذات الصلة بالموضوع، يتضح أن مفهوم السيطرة (Control Concept)، هو المرتكز الذي قامت عليه في توجيه المسؤولية الدولية و أهمها في قضية الأنشطة العسكرية أو شبه العسكرية في أو ضد نيكاراغوا عام ١٩٨٦،إذ ذهبت محكمة العدل الدولية في قرارها بأنه : ".....إلى أن معيار المسؤولية الدولية عن التصرفات الخاطئة ، إنما يتجلى في قدرة الدولة للسيطرة على القوات شبه العسكرية... ".[١٤٣]

أن قراءة نصوص القرار السابق، سيساعد في فهم توجهات المحاكم الدولية ، إذ ذهبت محكمة العدل الدولية إلى تكييف واقعة التدخل بالقول :" وبما أنه ثبت للمحكمة دور الولايات المتحدة في تدريب وتسليح المجموعات المسلحة الكونترا (Contras) في نيكاراغوا وتجهيزها بوسائل اتصال متقدمة"[١٤٤]، فقد حملت محكمة العدل الدولية الولايات المتحدة مسؤولية التدخل في الشؤون الداخلية لنيكاراغوا، فضلاً عن تحملها تبعات تصرفاتهم المخالفة للقانون الدولي العام.

أما المناسبة الثانية التي تطرقت إلى مسؤولية الدولة عن ما ينسب إليها من انتهاكات ارتكبت من مجموعات مسلحة مدعومة من قبلها ، فهي قضية تادتش (Tadic) في المحكمة الجنائية الدولية الخاصة بيوغسلافيا السابقة ، إذ ركزت المحكمة في قرارها على معيار السيطرة الكاملة (Overall Control)، بالقول: " ... كان للدولة دور في التنظيم والتنسيق، فضلاً عن تزويد المجموعة المسلحة بالدعم، ما يعني أن لها السيطرة الكاملة عليها، وما يصدر عن المجموعات المسلحة، يعني أنه صادر عن الدولة نفسها".[١٤٥]

وتأسيساً على ما تقدم يصح القول ، أن مسؤولية الدولة تقوم متى ما ثبت أن لها السيطرة الكاملة (Overall Control) على أجهزتها الحكومية، وبالذات العسكرية والأمنية منها ، ليقرر بعد ذلك المسؤولية الدولية عن الهجمات السيبرانية.

ولا أدل على ما ذكرناه، هو أن اقرب قضية تطرقت إلى المسؤولية الدولية الناشئة عن دعم المجموعات المسلحة، ما أشارت إليه محكمة العدل الدولية في قضية الإبادة الجماعية في البوسنة عام ٢٠٠٧.

لقد وجهت البوسنة التهمة رسمياً ضد صربيا وأقامت دعوى أمام محكمة العدل الدولية، عن جريمة الإبادة الجماعية التي ارتكبتها قوات صرب البوسنة.

وتتلخص القضية باتهام وجهته البوسنة ضد صربيا لدعمها قوات صرب البوسنة بارتكاب إبادة جماعية ضد البوسنيين، ما وضع المحكمة في بحث دائم عن العلاقة المحتملة بين هذين الطرفين أي علاقة قوات صرب البوسنة بصربيا.[١٤٦]

وبعد تحقيق مطول أجرته محكمة العدل الدولية، أصدرت قراراها بعدم مسؤولية صربيا عن جريمة الإبادة الجماعية في البوسنة، فضلاً عن عدم وجود علاقة بينها وبين قوات صرب البوسنة.[١٤٧]

وفي هذا الشأن علق القاضي الأسبق للمحكمة الجنائية في يوغسلافيا السابقة، انطونيو كاسيزي (Antonio Cassese) على قرار محكمة العدل الدولية بالقول :" فبعد اتهام كل من الجنرال ملادك (Mladic) وبقية الضباط ومنهم راديسلاف كرستيتش (Radislav Krstić) ، بارتكاب الإبادة الجماعية في سربرنيتسا (Srebrenica)[١٤٨] ، ناقشت المحكمة موضوع فيما لو كان هؤلاء وبحكم الواقع تابعين أو مدعومين من دولة أخرى، فطبقت على وضعهم ، مفهوم السيطرة الفعالة (Effective Control) أي المعيار ذاته المطبق في قضية الأنشطة العسكرية وشبه العسكرية (نيكاراغوا ضد الولايات المتحدة) ، على أساس أن ذلك يتوافق مع حكم المادة (٨) من مشروع المسؤولية الدولية عن الأفعال غير المشروعة لعام ٢٠٠١، والتي تطرقت إلى مسؤولية الدولة حول تصرفاتها المباشرة أو تصرفات مجموعات أو أشخاص مسيطرة على تصرفاتهم.[١٤٩]

ويضيف أنطونيو كاسيزي بالقول:" ولأن مضمون المسؤولية الدولية وفقاً للمادة سالفة الذكر تقضي بتحميل الدولة تبعات التصرفات التي يقوم بها أفراد أو مجموعات يعملون في ضوء تعليماتها ، أو تحت إدارتها المباشرة ،أو تحت سيطرتها والذي لم يثبت للمحكمة وجوده في القضية، فقد أصدرت المحكمة قرارها بعدم تحميل صربيا المسؤولية عن الإبادة الجماعية ،لعدم تحقق المعايير التي تضمنتها المادة (٨) من مشروع المسؤولية الدولية على وقائع الدعوى".[١٥٠]

في حين يرى الفقيه سكوت شاكلفورد (Scott Shackelford)،:" أن السيطرة الفعالة يمكن أن تطبق كمعيار على التصرفات التي تضطلع بها مجموعات مسلحة غير نظامية"، ويشير في ذلك إلى التوجه السابق لمحكمة العدل الدولية في قضية نيكاراغوا ضد الولايات المتحدة ، وبالذات في دعم العمليات شبه العسكرية، التي قامت بها مجموعات حليفة للولايات المتحدة الأمريكية.[١٥١]

وفي رأي آخر لسكوت شاكلفورد يقول فيه:" أن معياري السيطرة الفعالة والكاملة تطبقان على تصرفات الدولة الخاطئة معاً ، ويستدل في ذلك على قضية نيكاراغوا ضد الولايات المتحدة، إذ ذهبت المحكمة إلى التمييز بين الانتهاك الجسيم والانتهاك غير الجسيم.[١٥٢]

ومما تقدم فإن شاكلفورد قد وضع معادلة تتلخص بأنه:" كلما كان الانتهاك جسيماً، فيعني توفر الدليل على وجود دعم تلقته تلك المجموعات المسلحة ونفذت الهجوم على أساسه، والعكس صحيح"، وهي معادلة قابلة للانتقاد.

إذ يرى بعض الفقهاء أن هذا التوجه سيشجع على انتهاك أحكام القانون الدولي العام[١٥٣]، فيما يرى آخرون أنها مقدمة لتدويل نزاعات مسلحة غير دولية.[١٥٤]

أن الاستناد إلى هاذين المعيارين، في تقرير مسؤولية الدولة عن انتهاكات القانون الدولي العام، والإنساني بالذات قد يكون غير واقعي، خصوصاً في الهجمات السيبرانية،إذ من الصعب تحديد هوية المهاجم، وهو ما يمثل عائقاً أمام ادعاءات الدولة المستهدفة من الهجوم، ومن ثم اتخاذ الإجراءات لملاحقة المسؤول عنها ، فضلاً عن كبح أية توجهات لارتكاب هجمات مماثلة في المستقبل، وبعبارة أخرى تعطيل الإجراءات الرادعة، وهو ما يخل بهدف القانون الجنائي الدولي لكونه المعني بملاحقة منتهكي القانون الدولي الإنساني وفقاً لمفهوم المسؤولية الجنائية الفردية.

وما يؤكد هذا الطرح، ما صرح به انطونيو كاسيزي، إذ وجه انتقاداً للمحكمة ذاتها بعد أن تبنت معيار السيطرة الفعالة، في قرارها الخاص بقضية الإبادة الجماعية في البوسنة، وقال:" .... أنه معيار غير واقعي في الإثبات".[١٥٥]

ومن جانب آخر ذهب ماركوف (Markoff) وكرامر (Kramer) بخصوص تحديد مسؤولية الدول عن الهجمات السيبرانية بالقول :" يمكن أن يكون معيار السيطرة الفعالة مجدياً في تحديد جزء من المسؤولية الدولية لا كلها، ويعتمد ذلك في تبني اتفاقية دولية تشارك فيها كل من الولايات المتحدة و روسيا ، لتحديد المسؤولية الدولية الناشئة عن الهجمات السيبرانية".[١٥٦]

ولتأكيد أهمية موضوع الملاحقة الجنائية ضد مرتكبي الهجمات السيبرانية خصوصاً في ما تعلق بحفظ السلم والأمن الدوليين ، يذهب القاضي ستين جولبيرج (Stein Schjolberg) بالقول :" إن عدم وجود محاكم دولية أو جنائية مختصة بملاحقة المسؤولين عن ارتكاب الجرائم السيبرانية الخطرة على المستوى العالمي، سيعني أن عدداً غير قليل من منفذي الهجمات السيبرانية الخطرة سيكونون بمنأى عن العقاب".[١٥٧]

أن الثابت في تحديد مسؤولية الدول عن إسهاماتها في النزاعات المسلحة التقليدية قد يكون أكثر يسراً، بالاستناد إلى معياري السيطرة الكاملة أو الفعالة، للتحقيق في هجمات قامت بها مجموعات مسلحة عابرة للحدود استخدمت أسلحة أو طرق تقليدية أو غير تقليدية كالأسلحة الجرثومية أو الكيميائية.

وعلى العكس سيكون الأمر صعباً للغاية في إثبات المسؤولية الدولية الناشئة عن هجمات سيبرانية مزعومة ، والتي تتخذ من الفضاء مجالها الرحب ، لكونها تصرفات غير مادية ولا يمكن إثباتها بالطرق العادية ، وهو ما يعد العقبة التي تقف بوجه التنظيم الدولي ذات الصلة بالهجمات السيبرانية.

وبعبارة أخرى أن إبرام اتفاقية متعددة الأطراف تحظر على الدول الأطراف تقديم الدعم إلى مجموعات مسلحة، سيمهد الطريق تجاه المحاكم الجنائية الدولية للتحرك وملاحقة المتهمين في ارتكاب انتهاكات جسيمة تسببت فيها الهجمات السيبرانية.

أن التصور الذي ذكرناه سيعني تحريك المسؤولية الجنائية إلى القادة والرؤساء المسؤولين عن الانتهاكات الجسيمة ،وفقاً المادة (٨٦) من البروتوكول الإضافي الأول لعام ١٩٧٧، والتي تنص على:

أ- تعمل الأطراف السامية المتعاقدة وأطراف النزاع على قمع الانتهاكات الجسيمة واتخاذ الإجراءات اللازمة لمنع كافة الانتهاكات الأخرى للاتفاقيات ولهذا اللحق "البروتوكول"، التي تنجم عن التقصير في أداء عمل واجب الأداء .

ب- لا يعفي قيام أي مرؤوس بانتهاك الاتفاقيات أو هذا اللحق "البروتوكول" رؤساءه من المسؤولية الجنائية أو التأديبية، حسب الأحوال، إذا علموا، أو كانت لديهم معلومات تتيح لهم في تلك الظروف، أن يخلصوا إلى أنه كان يرتكب، أو أنه في سبيله لارتكاب مثل هذا الانتهاك، ولم يتخذوا كل ما في وسعهم من إجراءات مستطاعة لمنع أو قمع هذا الانتهاك.[158]

أنّ أساس المسؤولية الجنائية في القانون الدولي، فضلاً عن الأنظمة الجنائية الوطنية إنما يقوم على فرضية الذنب الشخصي، وبعبارة أخرى لا يمكن أن يكون شخص مسؤولاً جنائياً عن أفعال أو إجراءات لم يكن مشاركا فيها شخصياً، أو لم يشارك فيها بطريقة أخرى كالتحريض أو الإعداد ما قبل التنفيذ انسجاماً مع مبدأ لا جريمة ولا عقوبة إلا بقانون.[١٥٩]

إذ يذهب ويليامسون (J.A.Williamson) إلى ذلك بالقول:" أن مسؤولية القيادة أمر ضروري للتمكين من الملاحقة القضائية لأشخاص يقفون وراء المرتكبين المباشرين للجرائم .فبدون هذا الشكل من أشكال المسؤولية، يمكن للأرفع مقاماً إعفاء أنفسهم من أي فعل آثم بحجة أن مرؤوسيهم، على سبيل المثال، لم يكونوا ينفذون أوامرهم عندما ارتكبوا الجرائم، أو أنهم لم يكونوا موجودين أبداً في موقع الانتهاكات .أما

اليوم فالقانون واضح :الشخص ملزم بوصفه قائداً بالتدخل عندما تشكل أفعال مرؤوسيه - أو من شأنها أن تشكل – انتهاكات للقانون الدولي الإنساني، وعليه منع هذه الأفعال أو قمعها".[١٦٠]

وقد يسأل البعض، كيف نظمت الدول في تشريعاتها الوطنية، موضوع ملاحقة المسؤولين عن السلوكيات الإجرامية والتي تتخذ من الأنظمة الالكترونية مجالها الطبيعي، كعمليات القرصنة التي تتعرض لها البنوك وتحويل الأرصدة منها، فضلاً عن غيرها من التصرفات التي جرمت وفقاً للتشريعات الجزائية و الاتفاقيات الدولية المعنية بتنظيم الجرائم الالكترونية.

و تطرح أسئلة لا تقل أهمية عما ذكر آنفاً، منها : هل من الممكن تحديد مكان تنفيذ الهجوم (الموقع الالكتروني المهاجم) ؟ ما هي الوسائل المتوافرة لإثبات هوية الجاني على نطاق القانون الجنائي الوطني؟ وهل يمكن أن يساعد ذلك في إبرام اتفاقية معنية بحظر أو تقييد وسائل و طرائق سيبرانية على المستوى الدولي ؟

كل هذه الأسئلة سنحاول الإجابة عنها في معرض البحث والتحليل في الجهود الدولية الرامية لتنظيم استخدام الهجمات السيبرانية موضوع الدراسة وذلك في الفرع الثاني.

الفرع الثاني: الموقف الدولي من إبرام الاتفاقية الدولية.

إن هدف أي قانون يتجسد في السعي إلى تحقيق مصالح محددة من خلال التعرض لها و تنظيمها وفق نهج منطقي يحمي المصالح المستهدفة من التشريع.

أن القانون الدولي العام يرمي إلى الهدف ذاته وهو تنظيم العلاقات بين أشخاص القانون الدولي العام، رغم عدم الاتفاق على وجود سلطة تشريعية عالمية كما هو حال النظم القانونية الداخلية للدول.[١٦١]

وفي ظل التصور الذي طرح آنفا ،علينا أن نسأل: كيف نظم القانون الدولي مسألة الهجمات السيبرانية ؟

وإذا كان السؤال المطروح آنفاً هو تصور عام، فيمكن بيان حدوده في تفرعات أخرى أهمها : هل من قواعد دولية عرفية يمكن الاستناد إليها في سد النقص الذي قد يشوب التقنين الدولي الحالي، و هل من جهود دولية لأجل تنظيم هذا الموضوع بصيغة اتفاقية دولية، تتصدى بالحظر أو التقييد بوجه أي تطور لهجمات سيبرانية لا يحمد عقباها على المستوى الدولي؟

كل هذه الأسئلة سنسلط عليها الضوء، محاولين الإجابة عنها في ضوء الجهود الدولية فضلاً عن تحليل أحكام الاتفاقيات الدولية والدراسات القانونية ذات الصلة بموضوع البحث.

إن أي محاولة لتقويم أحكام الصكوك الدولية ومدى انطباقها على الهجمات السيبرانية يستدعي أولاً البحث فيها، ولاسيما الأحكام ذات الصلة بتنظيم استخدام وسائل القتال و طرائقه.

ولقد سبق الذكر ، أن معظم الاتفاقيات الدولية ذات الصلة بتنظيم استخدام وسائل و طرائق القتال ، أبرمت في زمن لم يكن معروفاً خلالها، استخدام الانترنت أو وسائل الاتصال الالكترونية كما هو الحال في الوقت الراهن ، ومن الطبيعي أن لا نجد حكماً قانونياً ينظم استخدام الهجمات السيبرانية بشكل صريح ومباشر. [١٦٢]

أن الطرح المتقدم لا يعني أيضاً أن يترك الباب مفتوحاً أمام الهجمات السيبرانية دون تنظيم قانوني، وهو الأمر نفسه يذكرنا بعدد من الأسلحة التي تم تنظيمها لا وفقاً لقواعد ومبادئ قانونية مدونة، إنما وفقاً لقواعد دولية عرفية راسخة في التنظيم الإنساني الدولي ، كشرط مارتنز الذي تم البحث فيه سابقاً من الدراسة، الذي يقضي أنه: (في الحالات غير المشمولة بالأحكام، يظلُ السكان المتحاربون تحت حماية و سلطان مبادئ قانون الأمم كما جاءت، من تقاليد التي استقر عليها الحال بين الشعوب المتمدنة وقوانين الإنسانية ومقتضيات الضمير العام).

وعلى سبيل المثال حُظر استخدام الأسلحة المسببة للعمى (Blend Laser Weapons) عام ١٩٩٥ في البروتوكول الإضافي لاتفاقية الأمم المتحدة للأسلحة التقليدية لعام ١٩٨٠ ، لا لحكم صريح ورد في الاتفاقيات الدولية ذات الصلة، بل بالاستناد إلى مبادئ دولية مقننة وأخرى عرفية، أشارت إلى عدم شرعية استخدامها [١٦٣]، لأنها أسلحة وصفت بالعمياء، وهو ما يمكن أن ينطبق على الهجمات السيبرانية، لكونها لا تميز بين هدف مدني و آخر عسكري إن استخدمت على نطاق واسع.

وفي السياق نفسه، يمكن الاستناد إلى ما أصدرته محكمة العدل الدولية من فتوى بشأن شرعية التهديد أو استخدام الأسلحة النووية في عام ١٩٩٦، في ضوء المبادئ الدولية، كمبدأ أن حق أطراف النزاع في اختيار وسائل و طرائق القتال ليس حقاً مطلقاً، ما يعني أن الفرصة سانحة أمام المجتمع الدولي لتنظيم هذا الموضوع بالاستناد إلى المبادئ نفسها، فضلاً عن الاسترشاد بالاتفاقيات الدولية والتشريعات الداخلية التي نظمت موضوع مكافحة الجرائم السيبرانية.

وقد يتساءل البعض ، لمَ لا يتوصل المجتمع الدولي - في الوقت الراهن - إلى إبرام اتفاقية دولية تحظر استخدام الهجمات السيبرانية أو تقييد استخدامها في اقل تقدير؟

أن الإجابة عن هذه الإشكالية، تتطلب تفحص المصالح الدولية التي تقف حائلاً دون إبرام مثل هكذا اتفاقيات دولية، وبعبارة أخرى مصالح الدول التي تحتكر أو تهيمن على قطاع البرامج الالكترونية للأغراض العسكرية؟

أن التفوق الذي تتميز به بعض الدول كالولايات المتحدة وروسيا الاتحادية في حقل الأنظمة الالكترونية العسكرية والمهيمنة على الساحة الدولية، أدخل موضوع الهجمات السيبرانية ضمن دائرة الصراع

التقليدي الذي كان دائرا بينها في أثناء زمن الحرب الباردة، وبعبارة أخرى الرجوع إلى مفهوم الهيمنة من أجل النفوذ وتحقيق كل منهما مكاسب محددة سلفاً، قبل الخوض في مسألة تنظيمه بصيغة اتفاقية دولية متعددة الأطراف.

أن الاختلاف في وجهات النظر والمواقف بين الدولتين، هو ذاته المتبع في قضايا دولية سابقة كتنظيم استخدام الأسلحة النووية والذي سبق أن تطرقنا إليه في هذه الدراسة، إذ استغرقت المفاوضات بشأنها عقوداً من الزمن نجم عنها الاستئثار بحق الحيازة مقابل حرمان الدول الأخرى من حيازة التكنولوجية النووية للأغراض العسكرية.

وفي هذا الشأن نطرح مقاربة أدلى بها المختص بالقانون الدولي الإنساني ،سكوت شاكيلوفرد (Scott J. Shackelford) مفادها:" أن الاختلاف في وجهات النظر حول حظر تكنولوجيا المعلومات في النزاعات المسلحة هي ذاتها القائمة بين الدول الحائزة للأسلحة النووية،إذ لا يزال الغموض يكتنف موقف المجتمع الدولي من حظرها على مستوى اتفاقية متعددة الأطراف".[١٦٤]

وكالعادة فإن التحدي الأكبر الذي يواجه تنظيم الهجمات السيبرانية هو عدم وجود إرادة دولية على الصعيدين الدبلوماسي (المفاوضات) والقانوني (قرارات مجلس الأمن) ، يقابله تسارع وتيرة استحداث وتطوير أنظمة الكترونية قادرة على التسلل والاختراق لأنظمة الكترونية تابعة لدولة أخرى ، ومن ثم إلحاق الضرر بها على نحو يمكن وصفه هجوماً وعدواناً مباغتاً للمنشآت الحيوية.

لقد أدى هذا التحدي إلى إثارة نوع من الضبابية حول قدرة أو عدم قدرة القانون الدولي العام والإنساني بالذات على كبح آثار الهجمات السيبرانية، ولا سيما وأن القانون الدولي الإنساني، يذهب إلى تنظيم استخدام الأسلحة ، في حين لا يبدو أن الهجمات السيبرانية – في وقتنا الراهن - تصنف على هذا النحو، إذ يذهب قاضي مشاة البحرية الأمريكي فيدا انتولين (Vida M.Antolin) ، بالقول: ".... أن أغلب الهجمات السيبرانية تقوم على عمليات لا تلتقي والمعايير التي يهدف القانون الدولي إلى تنظيمها....."[١٦٥]

أن الرأي الذي طرحه القاضي فيدا انتولين ، لم يكن دقيقاً وفقاً لفلسفة القانون الدولي الإنساني القائمة بالأصل على المنع والحظر على أية تصرفات تتناقض والمبادئ الإنسانية الراسخة بين الشعوب المتحضرة ، ولاسيما وأن النماذج التي ذكرناها في هذا البحث ، تثبت و بدليل قاطع وجود مخاطر محدقة بالبشر على الصعيد الإنساني جراء استخدام الهجمات السيبرانية.

ويمكن القول أن طريقة استخدام تكنولوجيا المعلومات وهدفها، لا يقتصر على ما هو معروف من آثار استخدام هذه التكنولوجيا لأغراض عسكرية أو أمنية، وبعبارة أخرى، بقائها في طي الحقل غير المادي

كالاستحواذ على ملفات أو تعطيل مواقع الكترونية، بل تغير الهدف منها لدرجة بات من الممكن تدمير منشآت حيوية محمية وفقاً للقانون الدولي العام، وهو ما تحظره المبادئ الدولية التي تضمنتها الاتفاقيات الدولية، فضلاً عن العرف الدولي.

أن الخطورة الكامنة في اللجوء إلى الهجمات السيبرانية، دفع بالجمعية العامة للأمم المتحدة إلى إيلاء اهتمام كبير بحث الدول قُدماً نحو بدء مفاوضات دولية و تنظيم استخدامها وفقا لأحكام القانون الدولي الإنساني، من خلال سلسلة من القرارات صدرت عنها، وبقيت في طي الوثائق دون أن تجد لها صدى في المحافل الدولية المعنية ببدء المفاوضات الدولية.[١٦٦]

ومن التحديات الكبرى التي تواجه المجتمع الدولي ،هو استخدام تكنولوجيا المعلومات لا من الدول فقط ، بل من مجموعات من غير الدول، ما يجعل أي تنظيم دولي لهذه المسألة قاصراً، إذ غالباً ما تعلن تلك المجموعات مسؤوليتها عن هجمات سيبرانية ألحقت أضراراً جسيمة في قطاعي الاتصالات والاقتصاد، فضلاً عن مخاطرها الإنسانية الأخرى، إذ يذهب كريستوفر ديلوكا (Christopher D.Deluca) إلى القول:" أن هذا النوع الجديد من الحرب دفع بالدول والكيانات من غير الدول (Non-States Actors) ، إلى امتلاك تكنولوجيا المعلومات لأجل إلحاق الضرر بالبنى التحتية الضرورية لحياة الإنسان".[١٦٧]

أن هذا الواقع وإن كان يمثل بحد ذاته تحدياً أمام التنظيم الدولي ، إلا أنه لا يمثل مانعاً في إبرام اتفاقية دولية تحظر تصرفات معينة سواء ارتكبتها دول أو مجموعات من غير الدول، وهو السبيل الذي اتبعته الكثير من الاتفاقيات الدولية المعنية بتنظيم استخدام وسائل و طرائق القتال والذي سبق البحث فيه.[١٦٨]

أن جل المبادرات الدولية المعنية بتنظيم استخدام تكنولوجيا المعلومات لإغراض عسكرية، ما زالت في طي الطرح والنقاش الحذر، كما هو حال معظم المسائل ذات الصلة بتنظيم استخدام الأسلحة التقليدية وغير التقليدية وطرائق استحداثها أو تطويرها أو إنتاجها، إذ تخضع في العادة إلى الموازنة بين المصالح القومية والدفاع عن النفس وبين الآثار غير الإنسانية التي قد تتسبب بها.

أن المعادلة التي تقوم عليها مسألة تنظيم تكنولوجيا المعلومات في الاستخدام العسكري والأمني غاية في الصعوبة، لكونها حديثة النشأة وتحتاج إلى تضافر جهود دولية حثيثة، تشترك فيها الدول والمنظمات الدولية الحكومية كالأمم المتحدة والاتحاد الأوربي، فضلاً عن المنظمات الدولية غير الحكومية كاللجنة الدولية للصليب الأحمر.

أن المشكلة الدولية الراهنة هي ذاتها التي واجهتها الدول في أثناء الإعداد لتدابير تشريعية لكبح وملاحقة المسؤولين عن الجريمة الالكترونية على المستوى الوطني، إذ كان التحدي الأكبر يتجسد في تحديد

السلوكيات المجرمة (الإلكترونية)، وبعبارة أخرى تحديد الركن المادي للجريمة، فضلاً عن الركن المعنوي.[١٦٩]

وفي إطار التنظيم الجنائي لم يعد مقبولاً التوسع في تجريم سلوك، عبر التوسع في تفسير القواعد الجزائية بالاعتماد على القياس أو التفسير الذي تتبناه المحاكم الجزائية الوطنية، وبعبارة أخرى التفسير أو القياس غير المستند على نص قانوني محدد يتناول الجريمة السيبرانية، تطبيقاً للمبدأ الجزائي القائل : لا (جريمة ولا عقوبة إلا بنص).[١٧٠]

لقد دأبت الدول ومنذ أكثر من عقد على سن تشريعات وطنية،[١٧١] حددت الأطر القانونية للسلوك الالكتروني المُجرَّم، فضلاً عن الجزاءات الواجب إيقاعها على المتهم بارتكابها، بالاسترشاد على أحكام اتفاقية مجلس أوربا المتعلقة بالجريمة السيبرانية لعام ٢٠٠١.

وفي هذا الشأن يمكن القول أن التصدي لآثار الهجمات السيبرانية على المستوى الدولي، لابد أن ينطلق من النقطة ذاتها التي بدأتها الدول في مكافحة الجريمة الالكترونية على المستوى الوطني، فضلاً عن القواعد الدولية العرفية ذات الصلة.

وما يؤكد إمكانية التوصل إلى إبرام الاتفاقية الدولية، ما ذهب إليه المختص في العلاقات الدولية جيفري كيلسي (Jeffrey Kelsey) بالقول:" ...لعقد من الزمن أو ما يزيد بقي تهديد الحرب السيبرانية من دون حل، وقد وصل المجتمع الدولي إلى توافق بشأن تنظيمه وفقا لأحكام القانون الدولي الإنساني، ولكن لا عن طريق أحكام قانونية دولية صريحة إنما بالقياس على تصرفات أخرى حظرها القانون الدولي الإنساني".[١٧٢]

و بناءً على ما تقدم ينبغي أن تطرح المسألة أولاً على طاولة النقاش لدراسة الآثار المتوقعة من استخدام تكنولوجيا المعلومات على هيئة هجمات سيبرانية، خصوصاً في ظل انعدام التوافق الدولي بشأنها، امتثالاً لحكم المادة (٣٦) من البروتوكول الإضافي الأول التي نصت بأنه: " يلزم أي طرف متعاقد عند دراسة أو تطوير أو اقتناء سلاح جديد أو أداة للحرب أو إتباع أسلوب للحرب ، أن يتحقق فيما إذا كان ذلك محظوراً في جميع الأحوال بمقتضى هذا الملحق " البروتوكول " أو أية قواعد أخرى من قواعد القانون الدولي ، التي يلتزم بها الطرف السامي المتعاقد ".[١٧٣]

لقد سعت بعض الدول إلى تنظيم استخدام تكنولوجيا المعلومات في ظل اتفاقيات دولية إقليمية ،حددت الإطار القانوني للسلوك الإجرامي والعقوبات الواجب إيقاعها على كل من يستخدم تكنولوجيا المعلومات، لأجل الحصول على منافع مادية أو معنوية أو بهدف زعزعة أمن المجتمع واستقراره و بمختلف جوانبه الاقتصادية والصحية و وحدة مجتمعه.[١٧٤]

ويصح القول أن هذه الاتفاقيات، قد تكون حجر الأساس لإبرام اتفاقيات دولية لا لأجل تنظيم استخدام تكنولوجيا المعلومات في النطاق الداخلي للدولة الطرف في الاتفاقية فحسب، بل أكثر من ذلك وهو كبح استخدامها بهدف تهديد السلم والأمن الدوليين.

ومن الراجح في ظل التحرك الدولي البطيء، أن يتجه المجتمع الدولي نحو تقييد استخدام تكنولوجيا المعلومات بصورة هجمات سيبرانية بدلاً من حظرها، ولنا في اتفاقية الأمم المتحدة لحظر أو تقييد استخدام الأسلحة التقليدية لعام ١٩٨٠ خير دليل على التعقيدات التي صاحبت إبرامها.[١٧٥]

أن السبب في تأخر إبرام معظم الاتفاقيات ذات الصلة بوسائل و طرائق القتال، يعود إلى عدم رغبة الدول المعروفة بصناعتها العسكرية المتقدمة في الدخول إلى اتفاقيات دولية، قد تحظر عليها وسائل تساعد في حفظ أمنها تحت مسميات الضرورة العسكرية، وهو ما سنراه جلياً لدى استعراض تصريحات لمسؤولين في الولايات المتحدة وروسيا الاتحادية لاحقاً في هذه الدراسة.

وهو ما يعني إن تنظيم استخدام الهجمات السيبرانية يواجه معضلة كبيرة تتجسد بأمرين اثنين هما: عدم وجود أحكام دولية صريحة تنظمها من جهة، يقابله تسارع الاعتماد عليها في العمليات العسكرية والأمنية من جهة أخرى.[١٧٦]

إن المعضلة هذه دفعت بالأمم المتحدة و بعض الدول للإعلان صراحةً عن نيتها بدعم أي توجه دولي يفضي إلى حظر أو تقييد استعمال أنظمة الكترونية معدة للاستخدام العسكري أو الأمني،و وفقاً لما استقر عليه القانون الدولي العام المقنن، فضلاً عن العرف الدولي والسوابق القضائية وآراء كبار فقهاء القانون.

و يعد الأمين العام للأمم المتحدة بان كي مون (Ban Ki-Moon) أول مسؤول أممي، دعا لإبرام اتفاقية دولية متعددة الأطراف، تنظم مسألة الهجمات السيبرانية.[١٧٧]، فيما أيدت وزارة الخارجية الأمريكية هذا التوجه ، وصرحت أن النموذج الأفضل والواجب الاقتداء به في إبرام الاتفاقية الدولية، هو اتفاقية مجلس أوربا المتعلقة بالجريمة السيبرانية لعام ٢٠٠١.[١٧٨]

وفي هذا الشأن يطرح شميت ، رأياً عند تناوله لموضوع إبرام الاتفاقية فيقول:" لابد أن تتم المعالجة عن طريق اختبار المبادئ الدولية المعنية بتنظيم النزاعات المسلحة ومدى انطباقها على الهجمات السيبرانية، وبالذات في ضوء مبدأ الآثار المدوية (Reverberating Effects)".[١٧٩]

أن الرأي الذي يطرحه شميت، كأساس لتنظيم الهجمات السيبرانية هو ذاته المعتمد لدى الكثير من الفقهاء،وإن استخدم شميت مصطلحاً مغايراً لما سبق ذكره في هذه الدراسة أي مصطلح الطاقة الحركية (Kinetic) والتي تعني تغيير الطيف الالكتروني (الأوامر والمعلومات) إلى طاقة ملموسة يمكن أن تؤدي

الأثر ذاته بالنسبة لوسائل القتال الأخرى، كالقنابل والصواريخ وبعبارة أخرى التسبب بالتدمير أو التعطيل الكلي أو الجزئي في الهدف المحتمل. [١٨٠]

وبناءً على ما تقدم يتضح للقارئ أن الصعوبة التي تكتنف تحديد مسؤولية المهاجم السيبراني، قد تجد لها حلاً فيما لو أبرمت اتفاقية دولية تحدد صور إسهام الدول في الهجمات السيبرانية لا على سبيل الحصر ، تجنباً لأي تطور قد يشهده هذا القطاع، كتحديد نقطة انطلاق البيانات (نواة الهجوم) ،فضلاً عن نوعها و آثارها في أثناء الهجوم أو ما بعده وهذا ما سنتناوله في هذه الدراسة لاحقاً.

أن الولايات المتحدة الأمريكية تحبذ السير على النهج ذاته المتبع في اتفاقية مجلس أوربا المتعلقة بالجريمة السيبرانية لعام ٢٠٠١، لإبرام اتفاقية دولية تنظم استخدام الهجمات السيبرانية على صعيد النزاعات المسلحة، وهو ما يدفعنا باتجاه البحث والتحليل في أحكام هذه الاتفاقية ولاسيما في ثلاث مسائل مهمة وهي:

١. **نطاق الهجمات الإجرامية السيبرانية (Cybercrime Offences)**[١٨١].
٢. **إجراءات التحقيق (Investigative Procedures).**
٣. **التعاون الدولي (International Corporation).**

وفيما يخص نطاق السلوك الإجرامي السيبراني، فقد ألزمت الاتفاقية الدول الأطراف بأن تتخذ التدابير اللازمة كتشريع قوانين على المستوى الداخلي، تجرم سلوكيات محددة تمس خصوصية وتجانس وتوافر بيانات الكومبيوتر ومنظوماته.

فعلى سبيل المثال، ورد في المادة (٢) من الاتفاقية ما نصه: (تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الفعل التالي في قانونها، إذا ما ارتكب عمداً وبغير حق.....). ومن تلك الجرائم:

١. **الدخول على كامل أو جزء من منظومة كومبيوتر.**[١٨٢]
٢. **الاعتراض باستخدام وسائل فنية، لعمليات إرسال غير عمومية لبيانات كومبيوتر إلى أو من أو خلال منظومة كومبيوتر، بما في ذلك ما ينبعث من منظومة كومبيوتر من موجات كهرومغناطيسية تحمل هذه البيانات.**[١٨٣]
٣. **إتلاف أو محو أو إفساد أو تعديل أو تدمير بيانات موجودة على الكومبيوتر.**[١٨٤]
٤. **الإعاقة الخطيرة لعمل منظومة الكومبيوتر عن طريق إدخال أو إرسال أو إتلاف أو محو أو تغيير أو تبديل أو تدمير بيانات كومبيوتر.**[١٨٥]

٥. الإنتاج أو البيع أو الحصول بغرض الاستخدام أو الجلب أو التوزيع لجهاز صمم أو طوع بغرض ارتكاب أي من الجرائم المنصوص عليها المواد (٢-٥) من الاتفاقية.[١٨٦]

٦. المساعدة أو التحريض على ارتكاب أي من الجرائم المنصوص عليها في المواد (٢-٥) من الاتفاقية.[١٨٧]

أما فيما يخص إجراءات التحقيق (Investigative Procedures) وطرائق إثبات وقوع الجريمة وتحديد هوية مرتكبها، فقد عالجت الاتفاقية هذا الموضوع في مواد عدة ، منها ما ورد في نص المادة (١٤) بالنص: (تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لإقرار الصلاحيات والإجراءات الواردة بهذا القسم وذلك لأغراض تحقيقات وإجراءات جنائية محددة).

إن تحديد المكان والزمان وهوية مرتكب الجريمة السيبرانية، هو بمثابة المفتاح لتحريك المسؤولية الدولية، وهو ما نظمته الاتفاقية بشكل محكم تقريباً في الفقرتين (١) و (٢) من المادة (١٦) منها، إذ تبدأ إجراءات التحقيق أولاً في تتبع سير البيانات المخزنة والتحفظ عليها لمدة لا تزيد عن تسعين يوماً لإتاحة الفرصة أمام السلطات المختصة باتخاذ إجراءاتها وللكشف عن منفذيها.[١٨٨]

ومن المؤكد إن أكثر ما يخشى عليه في تحريك المسؤولية الجنائية، هو إخفاء البيانات أو تدميرها بعد تنفيذ الهجوم، لهذا سعت الاتفاقية إلى تنظيم هذه المسألة الحساسة والخطرة من خلال المادة (١٧) والتي دعت الدول الأطراف للسعي سريعاً في التحفظ على خط سير البيانات وفقاً لإجراءات تحقيقية محكمة.

فيما توجهت المادة (١٨) من الاتفاقية إلى تنظيم موضوع آخر وهو آلية التعامل مع أي شخص بحوزته جهاز كومبيوتر يحتوي على بيانات محددة وموجودة فيه، استخدمت في تنفيذ الجريمة، فضلاً عن إلزام مقدم خدمة الانترنت (Server) في إقليم الدولة الطرف لغرض تقديم التسهيلات اللازمة والمعلومات الخاصة بالمشترك بالخدمة (المتهم)، كالإفصاح عن هويته وعنوانه البريدي أو موقعه الجغرافي ورقم هاتفه وغير ذلك من أرقام الدخول الأخرى الخاصة به، فضلاً عن أية معلومات أخرى خاصة بموقع تركيب أجهزة ومعدات الاتصالات والتي تتوافر بموجب اتفاق الخدمة أو الترتيبات الخاصة بذلك.

من جانب آخر ألزمت المادة (٢٠) من الاتفاقية الدول الأطراف باتخاذ التدابير التشريعية، كسن قوانين تقضي بمنح الجهات الحقيقية تخويلاً بالتجميع الفوري لبيانات الكومبيوتر وإلزام مقدم الخدمة وفي نطاق قدرته الفنية بالتعاون مع السلطات المختصة ومساعدتها بجمع وتسجيل لخط سير البيانات المرتبطة باتصالات معينة في إقليم الدولة الطرف والمحافظة على سرية المعلومات التي تحتويها البيانات تلك.

أما فيما يخص الولاية القضائية والقانون الواجب التطبيق على المتهمين بارتكاب مثل هذه الجرائم فقد قضت الفقرة (١) من المادة (٢٢) من الاتفاقية بأنه :" يعتمد كل طرف ما قد يلزم من تدابير تشريعية

وتدابير أخرى وذلك لإقرار الاختصاص بشأن أي جريمة تنص عليها المواد (٢ إلى ١١) من هذه الاتفاقية وذلك عندما ترتكب الجريمة :

أ- في إقليمه، أو

ب- على متن إحدى السفن ترفع علم ذلك الطرف، أو

ت- على متن إحدى الطائرات المسجلة بموجب قوانين ذلك الطرف،أو

ث- من جانب أحد مواطنيه، إذا كانت الجريمة معاقب عليها بموجب القانون الجنائي بمكان ارتكابها، أو في حالة ارتكاب الجريمة خارج الاختصاص القضائي الإقليمي لأية دولة.

وأخيراً تناولت الاتفاقية موضوع التعاون الدولي (International Corporation) بشأن مكافحة الجرائم السيبرانية وذلك في القسم الثالث منها، إذ نصت المادة (٢٣) بأنه:" يتعاون الأطراف مع بعضهم البعض، وفقاً لنصوص هذا الباب ومن خلال تطبيق الاتفاقيات الدولية ذات الصلة والخاصة بالتعاون الدولي في الشؤون الجنائية والترتيبات المتفق عليها بمقتضى التشريعات والمتبادلة بالمثل، والقوانين الوطنية لأقصى درجة ممكنة لأغراض إجراءات التحقيقات التي تتعلق بجرائم نظم وبيانات الكومبيوتر، أو من أجل تجميع أدلة الجريمة الجنائية في شكل الكتروني"، كما تناولت المادة (٢٤) من الاتفاقية مسائل ضرورية لإتمام التحقيقات من ضمنها مسألة تسليم المجرمين.

ومن أجل بناء شبكة من التواصل بين الدول الأطراف، قضت المادة (٣٥) من الاتفاقية بإنشاء وسيلة للتواصل تدعى بشبكة (٧/٢٤) بالنص:" يعين كل دولة طرف نقطة اتصال تكون متاحة مدة أربع وعشرين ساعة يومياً ولمدة سبعة أيام أسبوعياً وذلك لضمان توافر المساعدة الفورية لأغراض التحقيقات أو الإجراءات الخاصة بالجرائم الجنائية التي تتعلق بنظم بيانات الكومبيوتر، أو من أجل جمع الأدلة الخاصة بجريمة جنائية في شكل الكتروني....".

وعلى الرغم من أن الاتفاقية تعد وسيلة فعالة لمكافحة الجريمة السيبرانية، إلا أن المنظمات المعنية بحقوق الإنسان وجهت انتقادات واسعة ضدها ، لكونها ستمنح الحكومات حق مراقبة التواصل الالكتروني للأفراد[١٨٩].

ومن جانبه وجه مكتب الأمم المتحدة لمكافحة المخدرات والجريمة توصية إلى الدول الأطراف، بضرورة توخي الحذر في تطبيق هذه الاتفاقية بالقول:" أن التطور الذي شهده العالم في مجال إبرام اتفاقية لمكافحة الجريمة السيبرانية لابد أن يكون موضوعياً وحذراً في الوقت نفسه".[١٩٠]

وبالمقابل كانت هنالك ردود فعل مؤيدة لإبرام هذه الاتفاقية، فقد ذهب كل من ميشيل فاتس (Michael A. Vatis) وستبتو جونسن (Steptoe E. Johnson)، بالقول:" تتجسد أهمية الاتفاقية بكونها الأكثر واقعية في مكافحة الجريمة السيبرانية ، والأكثر قبولاً من أطراف دولية متعددة في الوقت الراهن".[١٩١]

وبالرجوع إلى أصل الدراسة و موضوعها، ترى روسيا الاتحادية وعلى النقيض من التأييد الأمريكي للاتفاقية، أن اتفاقية مجلس أوربا لا يمكن الاعتماد عليها في مسألة تنظيم الهجمات السيبرانية لوحدها ، بل لا بد من إبرام اتفاقية دولية معنية بالهجمات السيبرانية، تأخذ في الحسبان القواعد الدولية المنظمة لسير النزاعات المسلحة، وعلى أن تصنف الاتفاقية ضمن مجموعة الاتفاقيات الدولية المعنية بالحد من التسلح وعنوانها المقترح هو الاتفاقية الدولية المعنية بالحد من الأسلحة السيبرانية (International Cyber Arms Control Treaty) .[١٩٢]

ومما تقدم من مواقف يبدو جلياً توجهات أكبر دولتين مهتمتين بالمجال العسكري السيبراني، فالولايات المتحدة تدعو إلى ما يمكن الاصطلاح عليه بنزع الأسلحة السيبرانية ،فيما تتجه النوايا الروسية إلى ابعد من ذلك وهو الحد منها.

أن المقترح الروسي هذا يعود للعام ١٩٩٨، عندما دعت الأخيرة الأمم المتحدة لآجل كبح الهجمات السيبرانية.[١٩٣]وهو ما دفع بالجمعية العامة للأمم المتحدة عام ٢٠٠٠ لإصدار قرار يدعو إلى دراسة التهديدات التي تصاحب استخدام المنظومات الالكترونية لإغراض عسكرية، وإمكانية السير باتجاه تبني معايير دولية للحد من مخاطرها على المستوى الدولي.[١٩٤]

وكحال أية مبادرات دولية معنية بالحد من التسلح أو نزعه، تناوبت روسيا الاتحادية والولايات المتحدة الأمريكية الأدوار، عن طريق طرح عدد من المقترحات لأجل إبرام اتفاقية دولية متعددة الأطراف يضمن مصالح كل واحدة منهما، وهو ما يمكن بيانه لدى تحليل موقفهما من مشروع الاتفاقية وكالآتي :

١. موقف روسيا الاتحادية:

و يركز على تبني اتفاقية دولية تضع في الحسبان مبدأ الامتناع (Refrain) في:

أ- تطوير أو استحداث أو استخدام وسائل التأثير أو الإضرار في الأنظمة والمصادر المعلوماتية للدول الأخرى.
ب- الاستخدام المتعمد للمعلومات بهدف التأثير أو الإضرار في المنشآت الحيوية للدول الأخرى.
ت- الدخول غير المصرح به في أنظمة المعلومات و الاتصالات ومصادرها، فضلاً عن استخدامها.
ث- مساعدة أو تشجيع المجموعات الإرهابية أو الأفراد الخارجين عن القانون لتهديد الدول عن طريق استخدام أنظمتها الالكترونية و وسائل الاتصال الأخرى.[١٩٥]

ج- حظر استخدام كلمات المرور الخبيثة (Embedding malicious code) في أثناء سير العمليات القتالية.

ح- حظر مهاجمة الأنظمة غير القتالية أو العمل على الخداع في عملها.[١٩٦]

٢. موقف الولايات المتحدة الأمريكية:

لو راجعنا موقف الولايات المتحدة من المقترح الروسي آنف الذكر، لاتضح تأييدها له في بداية الأمر، ولكن سرعان ما تبدل هذا التأييد ، لتمارس الولايات المتحدة مناورة اعتادت على إتباعها فيما يخص موضوعا نزع السلاح و الحد منه.[١٩٧]

لقد أعلنت إدارة باراك اوباما (Barack Obama) مؤخراً عن رغبة الولايات المتحدة في السعي لإبرام اتفاقية دولية لا تحظر استخدام المنظومات الالكترونية في نطاق العمليات الأمنية أو العسكرية، بل بتقييد استخدامها (Restriction) مع قبول الولايات المتحدة بدء محادثات ثنائية مع روسيا الاتحادية بشأن تحديد المبادئ العامة للاتفاقية في إطار لجنة الأمم المتحدة لنزع السلاح والأمن الدولي.[١٩٨]

أن الرغبة الثنائية في مسألة تنظيم الهجمات السيبرانية على هيئة اتفاقية دولية، قد حدث بالفعل عام ٢٠١٠ من خلال محادثات جمعت الجانبين الأمريكي والروسي، وصفت بأنها الأولى من نوعها على صعيد الموضوع وهو تنظيم استخدام الهجمات السيبرانية.[١٩٩]

أن التوجه الأمريكي يمكن تحديده من خلال الرأي الذي أبداه مدير وكالة الأمن القومي كيث الكسندر (Keith Alexander) عام ٢٠١٠،بالقول: "نحن ماضون في تبني قواعد بشأن الحرب السيبرانية ونحن نعتقد بأن روسيا قد بدأت بالفعل تبني قواعد في المحادثات الدولية...".

ويضيف قائلاً: " نحن ماضون لجمع تأييد دولي واسع ، لأجل تبني قواعد تحدد آلية تعامل الحكومات مع الحرب السيبرانية ،مع تأكيد أن نجاح أي اتفاقية إنما يقوم على تحديد آليات ملزمة للدول الأطراف".[٢٠٠]

أن الرأي الذي طرحه كيث الكسندر، إنما يعكس توجهات الإدارة الأمريكية بخصوص الاتفاقية المستقبلية، وبعبارة أخرى التوجه نحو إجهاض المقترح الروسي الرامي أساساً إلى إبرام اتفاقية دولية تقوم على مبدأ الحظر التام لاستخدام الهجمات السيبرانية وليس التقييد الذي تحبذه الولايات المتحدة.[٢٠١]

في حين يطرح كل من جادي (Gady) و أوستن (Austin) المختصان في علم تكنولوجيا الحرب الرقمية، رأيا أكثر تفاؤلاً بالقول:" لم تتوصل روسيا والولايات المتحدة إلى تفاهم ثنائي مشترك حيال معظم جوانب الأمن السيبراني، على الرغم من أن عام ١٩٩٨ شهد إعلانهما قيادة المسألة السيبرانية على المستوى العالمي"، ويضيفان قائلين " أن الدولتان يعملان معاً لا كحلفاء ولا كأعداء في الوقت نفسه، إنما بمستوى متوازن وحذر".[٢٠٢]

وفي ضوء ما تقدم من مواقف دولية وبالخصوص الأمريكية، يتضح أن لا اتفاقية مجلس أوربا المتعلقة بالجريمة السيبرانية لعام ٢٠٠١، ولا المقترح الروسي القاضي بإبرام اتفاقية دولية تحظر الهجمات السيبرانية يسيران في اتجاه واحد، وإن مشوار المحادثات الثنائية سيستغرق وقتاً طويلاً كما هو حال باقي المحادثات التي جرت على قضايا الحد من الأسلحة أو نزعها، و تبقى الإرادة الدولية هي المهيمنة على الأوضاع القانونية الدولية ، والسبب الرئيس في بطئ تطور القانون الدولي العام والإنساني بالخصوص.

أن إبرام اتفاقية دولية تنظم الهجمات السيبرانية، سيشهد عقبات ستضعها الدول العظمى وبالخصوص الولايات المتحدة وروسيا الاتحادية والصين، كما هو حال معظم المواضيع الدولية ذات الصلة بالسلم والأمن الدوليين والتي شهدت التعطيل لفترات طويلة.

وفي هذا الشأن يختصر الفقيه الألماني ماركو جيركه (Marco Gercke) بطرحه تصوراً عن مستقبل الاتفاقية وبالذات فيما لو سارت على النهج نفسه المتبع في اتفاقية الجريمة السيبرانية لعام ٢٠٠١، بالقول :" أن عقداً من الزمن مضى على إبرام اتفاقية الجريمة السيبرانية في أوربا، دون أن تلقى اتفاقية مماثلة خارج حدودها ، ما يعني أنها لم تكن ذات دور مؤثر في مكافحة الجريمة السيبرانية على النطاق العالمي".[٢٠٣]

أن أكثر من سبب كان المؤثر في عدم إبرام اتفاقية دولية متعددة الأطراف، ومن أبرزها عدم اتخاذ معظم الدول ولاسيما النامية منها بالذات الإجراءات اللازمة كسن قوانين تتناول بالتجريم التصرفات الالكترونية ، فضلاً عن قواعد الإثبات ومسؤولية مزود الخدمة الالكترونية. [٢٠٤]

وقد يأتي اليوم الذي يخرج موضوع هذه الاتفاقية عن ولاية هذه الدول، فضلاً عن الأمم المتحدة، من خلال مبادرة دولية تدعو إلى بدء مسار تفاوضي جديد تقوده دول على غرار المسارين التفاوضيين اللذين نجم عنهما إبرام اتفاقيات دولية، كاتفاقية أوتاوا لحظر الألغام الأرضية عام ١٩٩٧ ونظام روما المؤسس للمحكمة الجنائية الدولية عام ١٩٩٨، وأخيراً اتفاقية ودبلن لحظر الذخائر العنقودية عام ٢٠٠٨.

الخاتمة

بعد بيان مفهوم الهجمات السيبرانية من التنظيم الدولي المعاصر يتضح أنه ليس من المستغرب أن يتربع موضوع الهجمات السيبرانية، الصدارة في الدراسات القانونية المتخصصة بالقياس إلى القضايا الدولية الأخرى المهددة للسلم والأمن الدوليين.

ومن خلال البحث والتحليل القانوني المقارن ، تتجلى عدة نتائج وتوصيات وعلى النحو الآتي ذكرها:

أولا: النتائج

١. ما زال مفهوم السيبرانية غير متفق عليه دولياً، ما يستدعي أن تتصدى الجهود الدولية لبيانه وتحديده لكونه الأساس لأي اتفاقية دولية تنظم استخدامه مستقبلاً.

٢. أما بالنسبة للجهود الدولية والمبادرات بشأن تنظيم استخدام الهجمات السيبرانية ، فيمكن القول أن من أهم المعضلات التي تقف حائلة دون التوصل إلى مبادئ مشتركة لانطلاق المفاوضات بين الولايات المتحدة الأمريكية وروسيا بخصوص السيبرانية ، هو ما يمكن الاصطلاح عليه بانعدام مبدأ الثقة المتبادلة بينهما[٢٠٥]، ذلك المبدأ الذي أدى أدوارا بارزة في تأخر إبرام عدة اتفاقيات دولية لمدة ناهزت العقد من الزمن أو أكثر، وبالخصوص في اتفاقية حظر الأسلحة البيولوجية لعام ١٩٧٢، واتفاقية حظر الأسلحة الكيميائية لعام ١٩٩٣، فيما أسهم انعدام الثقة إلى وقف المبادرات حول إبرام اتفاقية الحظر الشامل للأسلحة النووية لعقود من الزمن وكل ذلك بسبب عدم الاتفاق على مبادئ بناء الثقة والشفافية، فضلاً عن أحكام الامتثال لأحكام مشروع الاتفاقية.

٣. وفيما لو تم الاتفاق على انطلاق المفاوضات متعددة الأطراف رسمياً بشأن الهجمات السيبرانية، فإن المسائل الأكثر إلحاحاً بالتنظيم ستدور في أحكام نطاق الاتفاقية وبعبارة أخرى خيار الحظر أم التقييد في الاستخدام،فضلا عن الأحكام ذات الصلة بامتثال الدول الأطراف للاتفاقية، وخصوصاً في حظر دعم المجموعات من غير الدول (المجموعات الإرهابية أو المجموعات المسلحة غير النظامية) ما يعني أن نتوقع عقداً من الزمن أو أكثر من المفاوضات لأجل إبرامها على المستوى الدولي متعدد الأطراف.

٤. أن إبرام الاتفاقية على النحو الذي قصدناه آنفاً، سيعني تحريك المسؤولية الجنائية الفردية عن دعم أو تدريب أو تمويل أي مجموعات إرهابية يمكن أن تستخدم الوسائل الالكترونية للأغراض غير العسكرية تجاه دول أخرى.

٥. أن عدم السير باتجاه تبني منظومة دفاعية سيبرانية عربية أو عراقية سيمنح الفرصة للدول التي لها أهداف عدوانية بمهاجمة المنشآت الضرورية لبقاء الإنسان، وخصوصاً شبكات الاتصال ومحطات الكهرباء والماء وقطاع النقل والصحة التي تعمل الكترونياً بهدف تعطيلها أو تدميرها كلياً أو جزئياً.

٦. أن الدراسة هذه ما هي إلا محاولة للإحاطة بالسيبرانية والموقف الدولي منها، وقد يأتي اليوم الذي يتوصل فيه المجتمع الدولي إلى اتفاقية دولية متعددة الأطراف ، ولكن بعد أن يقر العالم أن الويلات المصاحبة لها لا يمكن السكوت عنها، بالضبط كما شهدت الأسلحة الكيميائية والبيولوجية من جدل استمر لأكثر من عقد من الزمن أفضى إلى حظرها التام.

ثانيا: التوصيات

١. ايلاء اهتمام أكبر من المؤسسات الأكاديمية العربية ،والعراقية منها بالذات للبحث في موقف الدول العربية و الإجراءات اللازم اتخاذها لدرء الخطر العابر للحدود ، والذي يتخذ من منظومة الاتصال الالكتروني أداة لمهاجمة المصالح الحيوية وبالخصوص البنى التحتية التي تعمل الكترونياً.
٢. تأسيس مركز وطني لإعداد متخصصين في تكنولوجيا الدفاع الالكتروني، لصد أي هجوم سيبراني محتمل ضد المنشآت العسكرية والمدنية العراقية.

الهوامش

[1] 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 , p.7.

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

[3] Julia Cresswell, "**Oxford Dictionary of word Origins: Cybernetics**", Oxford Reference Online, Oxford University Press, 2010.

[4] منير البعلبكي،" **المورد : قاموس انكليزي –عربي**"، دار العلم للملايين، بيروت، ٢٠٠٤،ص،٢٤٣.

[5] U.S. Department of Defense, **Dictionary of Military and Associated Terms**, Joint Publication 1-02, Nov. 8, 2010, as amended through Feb. 15, 2012

[6] Richard Kissel,"**Glassory of Key Information Security Terms**", National Institute of Standards and technology, U.S Department of Commerce ", Revision, 2, May, 2013, p.57.

[7] انظر: مجلس أوربا،" **اتفاقية مجلس أوربا المتعلق بالجريمة الالكترونية**"، مجموعة المعاهدات الأوروبية رقم ١٨٥، بودابست عام ٢٠٠١.

[8] انظر على سبيل المثال : مكتب الأمم المتحدة المعني بالمخدرات والجريمة: "**تقرير الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية، دراسة شاملة عن مشكلة الجريمة السيبرانية والتدابير التي تتخذها الدول الأعضاء والمجتمع الدولي والقطاع الخاص للتصدي لها**" ، فيينا عام ٢٠١٣ ، الوثيقة : UNODC/CCPCJ/EG.4/2013/2

[9] James A. Lewis, "**Sovereignty and the role of Government in Cyberspace**", Center for Strategic and International Studies Journal, Spring Summer, Vol: XVI, Issue II, 2010, P.56.

[10] Shin, Beomchul," **The Cyber Warfare and the Right of Self –Defense: Legal Perspectives and the Case of the United States**, IFANS, Vol.19, No1, June 2011, p.104.

[11] Scoot.j.Shckelford, ," **State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem**", University of Cambridge, Dept of politicos and International STUDIES, Cambridge, UK,2009.p.194.

[12] K.Saalbach," **Cyber War, Methods and Practice**", Version 9.0, University of Osnabruck-17 Jun 2014, p.6.

[13] دأبت المؤسسات الدولية، فضلاً عن الاتفاقيات الدولية المعاصرة على استخدام مصطلح " **نزاع مسلح** "، بدلاً من مصطلح " **الحرب"** ، وكانت المناسبة الأولى في اتفاقيات جنيف الأربعة الموقعة في ١٢ أب / أغسطس عام ١٩٤٩، انظر :

ICRC," Exploring humanitarian law: IHL Guide, A legal manual for EHL teacher", ICRC, Geneva, January 2009.p.7.

[14] انظر: الفقرة (٢) من المادة (٥٤) من البروتوكول الإضافي الأول لعام ١٩٧٧، والتي نصت بأنه:(يحظر مهاجمة أو تدمير أو نقل أو تعطيل الأعيان والمواد التي لا غنى عنها لبقاء السكان المدنيين.....) كذلك المادة (٥٦) من البروتوكول نفسه والتي نصت :(لا تكون الأشغال الهندسية أو المنشآت التي تحوي قوى خطرة ألا وهي السدود

والجسور والمحطات النووية لتوليد الطاقة الكهربائية محلاً للهجوم) كذلك الفقرة (٢) من المادة (١٣) من البروتوكول الإضافي الثاني، والتي نصت بأنه :(لا تكون الأشغال الهندسية أو المنشآت التي تحوي قوى خطرة،ألا وهي السدود والجسور والمحطات النووية لتوليد الطاقة الكهربائية محلا للهجوم حتى ولو كانت أهدافاً عسكرية، إذا كان من شأن هذا الهجوم أن يتسبب في انطلاق قوى خطرة ترتب خسائر فادحة بين السكان المدنيين).

[15] Thomas Rid and Peter Mcburney,"**Cyber – Weapons**", Routledge publisher, The RUSI Journal, February –March, 2012, Vol.157.NO.1.p.3.

[16] Jonathan A.OPHARD, "**Cyber Warfare and the Crime of Aggression**: **The Need for Individual Accountability on Tomorrow's Battlefield** ", DUKE Law & Technology Review, No.3, p.3.

[17] Shin.Beomchul, op.cit.p. 105.

[18] Micheal S.Fuertes, "**Cyber warfare, Unjust Actins in a just War** ", Florida International University, Full 2013, p.1.

[19] Schmitt, M.N," **Computer Network Attack and the Use of Force in International Law through on a Normative**", The Colombia Journal of Transitional Law, 1999, Vol.27, No.885-937, p.7.

[20] Zimet .E.and C. L. Barry," **Military services Overview, Cyber power and National Security**", National Defense University Press ,Washington, DC,USA,2009,P.291.

[21] Marco Roscini," World **Wide Warfare – Jus ad bellum and the use of Cyber Force**",Max Planck Yearbook of United Nations Law, Volume 14,2010,p.91.

[22] Micheal N.Schmitt," **Tallinn Manual on the International Law Applicable to Cyber Warfare** ", Cambridge University press, first publishes 2013.p.92.

[23] Ivan Goldberg, "**Institute for the Advanced Study of Information Warfare (LASIW)**, http/www.psycom.net/war .1.html.

[24] K.Saalbach, op.cit.p.8.

[25] انظر: مجلس أوربا، " **اتفاقية مجلس أوربا المتعلق بالجريمة الالكترونية**" مصدر سابق، المادة (٥).

[26] انظر اللجنة الدولية للصليب الأحمر،" **الملحقان "البروتوكولان الإضافيان إلى اتفاقيات جنيف المعقودة في ١٢ أب/ أغسطس ١٩٤٩** "،مرجع سابق، ص.٤٠.

[27] انظر المصدر نفسه، ص.٤١.

[28] Murice Abuert," **The ICRC and the problem of excessively injuries or indiscriminate weapons**", Extract print from ICRC, No.279, Nov-Dec, 1990, p.483, footnote.18.

[29] توليو ستيف وشمالبرغر توماس،" **قاموس مصطلحات تحديد الأسلحة ونزع السلاح وبنا الثقة**" ، معهد الأمم المتحدة لبحوث نزع السلاح ، منشورات الأمم المتحدة،٢٠٠٣،ص.٣٧.

[30] Tang Lan, Zhang Xin, Harry D. Raduege, Jr., Dmitry I. Grigoriev, Pavan Duggal, and Stein Schjølberg,"**Global Cyber Deterrence Views from China, the U.S., Russia, India, and Norway**", The EastWest Institute, Printed in the United States, 2010, p.3.

[31] Thomas Rid and Peter Mcburney, op.cit, P.6.

[32] Micheal Gervais,"**Cyber Attacks and the Laws of War**", Berkeley Journal of International Law", Vol: 30, Issue .2, Article 6, 2012, p.46.

[33] Ibid.

[34] Nils Melzer," Cyber warfare and International Law", IDEAS for Peace and Security, UNIDIR Researches, 2011, p.5.

[35] عرفت المادة (٥١) من البروتوكول الإضافي الأول لعام ١٩٧٧، الهجوم المسلح على نحويين اثنين، الأول في الفقرة (٥/أ) ويشير إلى الوسيلة القتالية بأنه: والهجوم قصفا بالقنابل أيا كانت الطرق والوسائل....) أما الثاني ويشير إلى طريقة القتال وذلك في الفقرة (٥/ب) بأنه:(والهجوم الذي يمكن أن يتوقع منه أن يسبب خسارة في أرواح المدنيين أو إصابة بهم أو أضرارا بالأعيان المدنية....)

[36] Nils Melzer,"Cyberwarfare and International Law, op.cit, pp.2-4.

[37] جيل برعام," **تأثير تطور تكنولوجيا الحرب السبرانية على بناء القوة في إسرائيل**", ترجمه للعربية يولا البطل ،مؤسسة الدراسات الفلسطينية ، ٢٠١٣،ص.١.

[38] Arquilla, J and D.Ronfeld," **In Athena's Camp: Preparing for Conflict in the Information Age**, Rand Publishing, Santa Monia, CA, USA, 1997, P.59.

[39] Yoram Dinstein," **Computer Network Attacks and Self-Defense**", International Law Studies Review. vol. 76 no.99, 2002, pp.114-115.

[40] Larry Wortzel, "**China's cyber-offensive**", Wall Street Journal, 1 Nov. 2009.

[41] The White House, Office of the Press Secretary, "**Remarks on securing the nations' cyber infrastructure**", Press Realse,29 May 2009,www.white house.gov/the _press _office/ Remarks-by President-on- Securing-Our-Nations-Cyber-Infrastructure.

[42]"President Obama's Remarks on Securing U.S. Cyber Infrastructure," May29, 2009, http://www.america.gov/st/texttrans-english/2009/May/20090529161700eaifas0.1335871.html.

[43] المركز الاستشاري للدراسات والتوثيق، " **التحولات في العقيدة العسكرية الأمريكية: دعائم الضعف السبع**"، أوراق إستراتيجية، سلسلة غير دورية تعنى بالشؤون الإستراتيجية، العدد:٢، أيلول ٢٠١٤، بيروت، ص, ١٧.

[44] Keir Giles, "**Information Troops a Russia Cyber Command?"** legal paper third international conference on Cyber Conflicts, Tallinn Estonia,2011,p.47.

[45] Franz-Stefan Gady and Greg Austin," **Russia, The United States, And Cyber Diplomacy Opening the Doors**", The East West Institute, Printed in the United States,2010,p.1.

[46] Brian Kerbs,"**Report: Russian Hacker Forum Fuelled Georgia Cyber Attacks**", the Washington Post, 16, Oct, 2008.

[47]David Cameron, '**How Britain can best address the threats of the twenty-first century'**, address at Chatham House, London, 15 Jan. 2010, http://www.chathamhouse.org.uk/events/view/-/id/1419/, accessed 20 Jan. 2010.

[48] Christopher c. joyner and Catherine Lotrionte," **Information Warfare as International Coercion: Elements of a Legal Framework**", European Journal for International Law, Vol.12.No.825-865.2001.p.825.

[49]Ibid.p.825.

[50] Ibid.

[51] Peter Sommer & Ian Brown," **Reducing Systemic Cyber security Risk**", OCED, Jan, 2011, pp.13-16.

[52] Tang Lan, Zhang Xin, Harry D. Raduege, Jr., Dmitry I. Grigoriev, Pavan Duggal, and Stein Schjølberg, op.cit.p.1.

[53] http://www.lawoflibya.com/forum/showthread.php?t=3624

[54] انظر على سبيل المثال: قانون التوقيع الالكتروني والمعاملات الالكترونية العراقي رقم (٧٨) لسنة ٢٠١٢و القانون الاتحادي رقم (٢) لسنة ٢٠٠٦ بشأن مكافحة جرائم تقنية المعلومات في الإمارات العربية المتحدة، والمرسوم السلطاني رقم (٢٠٠١/٢٧) حول تعديل بعض أحكام قانون الجزاء العماني بإضافة المادة (٢٧٦) مكرر حول جرائم الحاسوب،والقانون الصادر في ٢٠٠١/١٢/٣١ بشأن المعاملات الالكترونية في الأردن، والقانون رقم (٤) الصادر في ٢٠٠٩/٢/٢٥، بشان التوقيع الالكتروني وخدمات الشبكة في سوريا.

[55] Tang Lan, Zhang Xin, Harry D. Raduege, Jr., Dmitry I. Grigoriev, Pavan Duggal, and Stein Schjølberg, op.cit, p.5.

[56] K.Saalbach, op.cit, p.28.

[57] Diego Rafael Canabarro and Thiago Borne," **Reflection on the fog of Cyber War**", National Center for Digital Government, Policy working Paper No.13:001, March 1, 2013, footnote 11, p.10.

[58] Scott J.Shackelford," **Analogizing Cyber: from Nuclear War to Net War Attacks in International Law**", op.cit.footnote, 66, p.14.

[59] Thomas W. Smith," **The New Law of War: Legitimizing Hi-Tech and Infrastructural**," International Studies Quarterly, 2002, Vol.**46**, p.366.

[60] Ibid**.**

[61] Ibid**.**

[62] للمزيد حول هذا الموضوع انظر:

Kenneth Grees, Darien Kindlind, Ned Moran, Rob Rachwald," World War C: Understanding Nation-States Motives behind Today's Advanced Cyber Attaches". Fire Eyes report ,p.6.,at https://www.fireeye.com/resources/pdfs/fireeye-wwc-report.pdf

[63]Scott J.Shackelford," **Analogizing Cyber: from Nuclear War to Net War Attacks in International Law**", op.cit, p.205.

[64] Ibid.p.194.

[65] http://www.nato.int/cps/en/natolive/official_texts_17120.htm

[66]Eshel, David, 'Israel adds cyber-attack to IDF', Aviation Week's DTI, 9 Feb. 2010, http://www.military.com/ features/0,15240,210486,00.html, accessed 22 Feb. 2015.

[67]Jonathan A.OPHARD, op.cit.p.para.2.

[68]Ibid.

[69] Gorman, S., Dreazen, & Y. Cole, A., "**Insurgents Hack U.S. Drones**," Wall Street Journal, 17, Dec 2009.

[70] Brent Kesler," **the vulnerability of Nuclear Facilities to Cyber Attack**", Strategic Insight Journal, Vol.10, Issue, 1, spring, 2011, p.19.

[71] Gorman, S. Dreazen, & Y. Cole, A., "**Computer Spies Breach Fighter-Jet Project**," The Wall Street Journal, (21 Apr 2009).

[72] http://www.usccu.us/#The_Urgency_of_This_ Cyber-Security Work, accessed 3 Jan. 2010.

[73] Boldizsár Bencsáth. "**Duqu, Flame, Gauss: Followers of Stuxnet**," BME CrySyS Lab, RSA, 2012.

[74]Yaakov Katz,"**Stuxnet Virus Set Back Iran's Program by 2 years**", Jerusalem Post, Dec, 15, 2010, at http://www.jpost.com/IranianThreat/News/Article.aspx?id=199475.

[75] J Hilder,"**Computer Virus Used to Sabotage Iran's Nuclear Plan, Built by US and Israel** ", Australian review, 27 January 2011.

[76] Oona A.Hathway , Rebecca Crootof , Philip Levtiz , aley Nix, Aileen Nowlan ,William Perdue ,Julia Spiegel,op.cit.p.873.

[77] Shin.Beomchul,op.cit.p.103

[78] Peter Margulies," **Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility**", Melbourne Journal of International Law, Vol.14.2013, p.1.

[79] ذكر مصطلح السيطرة الكاملة والسيطرة الفاعلة في قرار محكمة العدل الدولية في قضية الانشطة العسكرية وغير العسكرية (نيكاراغوا ضد الولايات المتحدة الأمريكية) وذلك في عام ١٩٨٦، فمبدأ السيطرة الكاملة يشير إلى سيطرة الدولة على مجموعات مسلحة إما تابعة لها رسميا وبعبارة أخرى ضمن تشكيلاتها العسكرية الرسمية أو أنها تتواجد على إقليمها بشكل معترف منها وبرضاها التام، أما مصطلح السيطرة الفاعلة فيشير إلى سيطرة الدولة على مجموعات مسلحة لا تنتمي لها رسميا ولا تتواجد على إقليمها ومع ذلك تتلقى دعما ماديا أو لوجستيا كإمدادات الأسلحة أو التدريب ، أنظر قضية (نيكاراغوا ضد الولايات المتحدة) لعام ١٩٨٦،في :

ICJ, **Military and parliamentary activities in and against Nicaragua (Nicar .v.US.)**, Para, 195, 1986.

[80] Rwx HUGES,"**Atreaty for Cyberspace**", International Affairs journal, Vol.86.No.2, 2010, p.533.

[81] Ibid.

[82] صرح عدد من الباحثين، بان قواعد القانون الدولي الإنساني غير كافية في تنظيم أو تكييف الهجمات السيبرانية ويدعو هؤلاء إلى ضرورة إعادة النظر بتلك القواعد ، للمزيد حول هذا الموضوع ، أنظر:

Davis Brown, **"Proposal for an international convention to regulate the use of information System in Armed Conflict**", Harvard International Law review, Vol47, 2006, p.179.

[83]Emily Haslam, "**Information Warfare: Technological Changes and International Law**", Journal of Conflict and Security Law, Vol. 5, 2000, p. 157.

[84] Micheal Schmitt," **Bellum Americanum: The law of armed conflict into the next millennium**", Newport: Naval War College, 1998, p.408.

[85] The preambles of Resolutions A/RES/55/63 of 4 December 2000, A/RES/ 56/121 OF 19 December 2001.

[86] Matthew Evangelista, **"Cooperation theory and Disarmament Negotiations in the 1950s",** World political Journal, Vol.42, No.4, July 1990, P.515.

[87] Matthew C. Waxman," **Cyber –Attack and the Use of Force: Back to the Future of Article 2 (4)**", The Yale Journal of International Law, Vol.36, No.421, 2011, p.431.

[88] للمزيد حول هذا الموضوع ينظر:

Nathan E.Mueller," **Micheal Walzer on the Moral Legitimacy of states and the Morality of Killing in War**", Thesis submitted to the faculty of the Virginia Polytechnic Institute and State University in partial fulfillment of the requirements for the degree of Master of Arts in Philosophy, May 10, 2006.p.1

كذلك ينظر:

Carsten Stahn,"**Jus ad bellum', 'jus in bello', 'jus post bellum'? – Rethinking the Conception of the Law of Armed Force",** The European Journal of International Law Vol. 17 no.5, 2007, p.923, footnote, 8.

[89] Shin,Beomchul,op.cit,p.109,Marco Roscini,"**World Wide Warfare _Jus ad bellum and the Use of Cyber Force**" ,Max Planck Yearbook of United Nations Law, Volume 14,2010,85-130.

[90]Carsten Stahn, op.cit. p.930.

[91] Ibid, p.110.

[92] Scoot J Shackleford," **State Responsibility for Cyber Attacks: Competing Standards for Growing Problem"**, CCD COE Publications, C.Czosseck and K. Podins Eds, Tallinn, Estonia, 2010, p.202.

[93]Ibid.p.200.

[94] Oona A.Hathway , Rebecca Crootof , Philip Levtiz , aley Nix, Aileen Nowlan ,William Perdue ,Julia Spiegel,op.cit.p.28.

[95] Shin, Beomchul, op.cit.p.111.

[96]Marco Roscini,"**World Wide Warfare _Jus ad bellum and the Use of Cyber Force**", op.cit.p.130.

[97] Sanjiv Tomar," **Proxy Warfare**", Journal of Defense Studies, Vol.8.No, 2, April-June, 2014, p.152.

[98] Thomas M.Franck,"**Legitmacy after Kosovo and Iraq", in International Law and the Use of force at the turn of the centuries** ", Essays in Honor of V.D Degan Crinc-Grotic & Matulovic eds, 2005, p.73.

[99] http://www.un.org/ar/documents/charter/chapter7.shtml

[100] Ibid.

[101] ICJ, **Military and parliamentary activities in and against Nicaragua (Nicar .v.US.)**, Para, 195, 1986.

[102] Oona A.Hathway , Rebecca Crootof , Philip Levtiz , aley Nix, Aileen Nowlan ,William Perdue ,Julia Spiegel,op.cit.p.34.

[103] Christopher D. DeLuca," **The Need for International Laws of War to Include Cyber Attacks Involving State and Non-State Actors**", Pace International Law Review Online Companion, pace University School of Law,Vol.3,No.9,Winter,2013,p.298.

[104] Siobhan Gorman and Julian Barnes, "**Cyber Combat: Act of War**", Wall Street Journal, May 13, 2011.

[105] Gray Sharp," **Cyberspace and the Use of Force**", Aegis Research Corp, 1999, p.234.

[106] William A.Owens, Kennth W.Dam and Herbert S.Lin," **Tendency, policy, Law, and ethics regarding US acquisition and use of cyber attack capabilities**", National Academics Press, Washington DC, 2009, P.3.

107 جون- ماري هنكرتس و لويز دوزوالد – بك ،" **القانون الدولي الإنساني العرفي** "، المجلد الأول ، القواعد ، اللجنة الدولية للصليب الأحمر ، ، مطبعة برنت رايت للإعلان و الدعاية، القاهرة ، ٢٠٠٧ . ص .٤٤.

108 اللجنة الدولية للصليب الأحمر ،" **القانون الدولي المتعلق بسير العمليات العسكرية ، مجموعة اتفاقيات لاهاي وبعض المعاهدات الأخرى** " ، مصدر سابق ، ص.٢١.

[109] اللجنة الدولية للصليب الأحمر ،" **الملحقان "البروتوكولان الإضافيان إلى اتفاقية جنيف المعقـــودة فـــي ١٢ أب أغسطس ١٩٤٩** "، جنيف، سويسرا ، الطبعة الرابعة ، ١٩٩٧ ، ص.٤٣.

110 المصدر نفسه ، ص .٤١.

[111] Rex HUGHES, op.cit.p.537.

[112] DEP'T OF DEFENSE, **OFF. OF GEN. CoUNS., AN ASSESSMENT OF INTERNATIONAL LEGAL ISSUES IN INFORMATION OPERATIONS** Second Edition, 1999**,** p.20.

[113] Christopher C. Joyner & Catherine Lotrionte," **Information Warfare as International Coercion: Elements of a Legal Framework**", Europe journal of International law,vol,12,2001,p.831.

[114] اللجنة السابق،للصليب الأحمر ،" **اللحقان "البروتوكولان الإضافيان إلى اتفاقية جنيف المعقـــودة فـــي ١٢ أب أغسطس ١٩٤٩**" ، مصدر سابق ، ص، ٤٠.

[115] المصدر نفسه، ص.٤٢.

[116] ICJ Report 1996," **Legality of the threat or use of nuclear Weapons**", Para 78, p.257.

117 Ibid،note 6 ، p.257،para.79.

[118]ICTY،Case IT-95-11-R61،8 MARCH 1996،Prosucort V.Martic،Para .11.

[119] Rex HUGHES, op.cit, p.537, footnotes 62.

[120] Marco Roscini, op.cit, p.88.

121 اللجنة الدولية للصليب الأحمر ،" **القانون الدولي المتعلق بسير العمليات العسكرية ، مجموعة اتفاقيات لاهاي وبعض المعاهدات الأخرى** ،" جنيف ، الطبعة الثانية ، سبتمبر \ أيلول ٢٠٠١ ، ص.١٣٦.

[122] المصدر نفسه، ص.٤٢.

[123] Shin, Beomchul, op.cit.p.118.

[124] Siobhan Gorman and Julian Barnes,op.cit.

[125] Ibid.p.118.

[126] Rex HUGHES, op.cit.p.538.

[127] Antonio Gessese، " **The Martens Clouse: Half a loaf or simply pie in the sky?**"، EJIL {2000}، Vol ,III، No. 1, p.187.

[128]Ibid،pp.193-194

[129] بالإضافة إلى لائحة لاهاي الثانية لعام ١٨٩٩ ، أشارت عدة صكوك دولية إلى مبدأ مارتنز منهـــا : اتفاقيـــات جنيف الأربعة لعام ١٩٤٩ ، الاتفاقية الأولى مادة (٦٣) ، الاتفاقية الثانية (٦٢) ، الاتفاقية الثالثة المـــادة (١٤٢)،

الاتفاقية الرابعة المادة (١٥٨) ، كما أشار البرتوكول الإضافي الأول لعام ١٩٧٧ لهذا المبدأ في الفقرة (٢) من المادة (١)، و ديباجة البرتوكول الإضافي الثاني لعام ١٩٧٧.

130 ICJ،" **Legality of the threat or use of nuclear weapons**"، Dissenting opinion of judge Shahabuddeen ، op.cit.note 6،p.406. ، Also see : Doswald –Beck ، " **International humanitarian law and the advisory opinion of the international court of justice on the threat or use of nuclear weapons**" ، ICRC، Vol. 316 ، 1997، pp .35-55.

[131]Micheal N.Schmmitt," **Wired warfare: Computer network attack and jus in Bello**", IRRC, Vol.84, No.846, 2002.p.369.

132 اللجنة الدولية للصليب الأحمر ،" **الملحقان البروتوكولان الإضافيان إلى اتفاقية جنيف المعقودة فـــي ١٢ أب أغسطس ١٩٤٩** "، مصدر سابق ، ص. ١١.

133 المصدر نفسه ، ص. ٩٣.

[134] Erki Kodar," **Applying the law of armed conflicts to Cyber attacks: from the Martens Clouse to Additional Protocol I**", ENDC Proceeding, Volume 15, 2012, p.110.

[135]Jonathan A.Ophardt, op.cit.para 12-18.

[136] http://www.un.org/arabic/documents/GADocs/56/A_56_589.pdf

[137] للمزيد حول هذا الموضوع أنظر: أيمن عبد العزيز سلامة ،" **المسؤولية الدولية عن ارتكاب جريمة الإبادة الجماعية** "، رسالة دكتوراه ، كلية الحقوق جامعة الإسكندرية، ٢٠٠٥ ، ص. ٣٣٤ .

[138] لا تقوم المسؤولية الدولية إذا كان الفعل غير المشروع لم يؤدي إلى ضرر، مثال على ذلك قيام دورية تركية بملاحقة سفينة ايطاليا أدى إلى إيقافها وتفتيشها ثم تبين أنها غير مخالفة ولا تحمل ما يثير الشك في حمولتها، ورغم إن تركيا اعتذرت عن هذا الفعل و وجهت اللوم إلى قائد الدورية ، إلا أن ايطاليا طالبت بمبلغ للتعويض عن الفعل غير المشروع ، إذ قررت محكمة التحكيم برفض طلب التعويض، بسبب عدم قيام ضرر لحق بالشركة الايطالية صاحبت السفينة، للمزيد حول هذا الموضوع أنظر:

Ghazi, H. S," **Summary of the principles of public international law**", House of Culture for Publishing and Distribution, first edition, Oman, 2007.

[139] محمد حافظ غانم ،" **المسؤولية الدولية : دراسة لأحكام القانون الدولي وتطبيقاتها التي تهم الدول العربية**"، :محاضرات معهد الدراسات العربية العالية ،جامعة الدول العربية ، القاهرة ،١٩٦٢ ، ص. ١٤ .

[140] شريف عتلم و محمد ماهر عبد الواحد،" **موسوعة اتفاقيات القانون الدولي الإنساني، النصوص الرسمية للاتفاقيات والدول المصدقة عليها**"،إصدار بعثة اللجنة الدولية للصليب الأحمر بالقاهرة،الطبعة السابعة ،٢٠٠٧،ص.٤.

[141] محمد حافظ غانم،" **المسؤولية الدولية**"، معهد الدراسات العربية، القاهرة،١٩٦٢،ص.٦٦٦.

[142]UN," **Responsibility of States for International Wrongful Acts 2001**", UN, 2005, Articles 4 & 8.

[143] Nicaragua v. United States, 1986, p. 392.

[144] Ibid.

[145]Case: Prosecutor v. Tadic, 1995, Para. 70.

[146] للمزيد حول حيثيات القضية والقرار الصادر عن محكمة العدل الدولية، ينظر:
Application of the Convention on the Prevention and Punishment of the Crime of Genocide (**Bosnia and Herzegovina v. Serbia and Montenegro**), Judgment, I.C.J. Reports 2007, p. 43JUDGMENT OF 26 FEBRUARY 2007: http://www.icj-cij.org/docket/files/91/13685.pdf

[147] Ibid .Para 297.

[148] مذبحة سربرنيتسا، هي جريمة ابادة جماعية ارتكبت في البوسنة والهرسك في يولو/ تموز عام ١٩٩٥،وراح ضحيتها ما يقرب من ٧ الآف شخص من المسلمين اغلبهم من الرجال والصبيان، للمزيد انظر قضية المدعي العام للمحكمة الجنائية ضد راديسلاف كرستيتش في:
Judgment, Prosecutor v. Radislav Krstić, Case No. IT-98-33-T, 2 August 2001.

[149] Antonio Cassese," **The Nicaragua and Tadic tests Revisited in Light of the ICJ Judgment on Genocide in Bosnia**", The European Journal of International Law,Vol:18.no4,2007,p.650.
[150] Ibid.p.651.
[151] Scott J.Shackelford op.cit, P.4.
[152] Nicaragua v. United States, 1986, p. 101.
[153]Gray, C," **International Law and the Use of Force**", Oxford University Press, Oxford, 2000, p.141.
[154] Watkin, K,"**Contrloing the use of force: A role for human rights in Contemporary Armed Conflicts**", American Journal of International Law, Vol: 98, No.1-34, 2004, p.5.
[155] Scott J.Shackelford, op.cit, p.6.
[156] Markoff J, and Kramer A.E," In Shift, US. Talkes to Russia on Internet Security, New York Times, 2009, December 12.
[157] Judge Stein Schjolberg," **An International Criminal Tribunal for Cyberspace (ICTC) Prosecution for the Tribunal Police investigation for the Tribunal**", A paper for the East West Institute (EWI) Cybercrime Legal Working Group, 2012.p.3.

[158] انظر : اللجنة الدولية للصليب الأحمر ،" **الملحقان "البروتوكولان الإضافيان إلى اتفاقية جنيف المعقودة في ١٢ أب أغسطس ١٩٤٩** "، مصدر سابق، ص:٦٧-٦٨.
[159] ماركو ساسولي وانطونيو بوفييه،" **كيف يوفر القانون الحماية في الحرب: مختارات من القضايا الخاصة بممارسات معاصرة في القانون الدولي الإنساني**، اللجنة الدولية للصليب الأحمر، ،جنيف، الطبعة الأولى، ٢٠٠٩. ، ص،٣٦٨.
[160] جيمي آلان ويليامسون،" **بعض الاعتبارات حول مسؤولية القيادة والمسؤولية الجنائية**"، مختارات من المجلة الدولية للصليب الأحمر، المجلد ٩٠، العدد ٨٧٠،يونيو/حزيران ٢٠٠٨،ص.٥٦.

[161] محمد طي،" **شرعية التصدي لقرارات مجلس الأمن الدولي :حق الدول و ولاية القضاء**"،المركز الاستشاري للدراسات والتوثيق، الطبعة الأولى،٢٠١٣،ص،٥١-٥٢.
[162] Rex Hughes, "A treaty for cyberspace", The Royal Institute of International Affairs, International Affairs Journal No.86, Blackwell publishing Ltd, 2010, p.533.

[163] انظر: البروتوكول المتعلق بأسلحة الليزر المسببة للعمى، البروتوكول الرابع الملحق باتفاقية حظر أو تقييد استعمال أسلحة تقليدية معينة يمكن اعتبارها مفرطة الضرر أو عشوائية الأثر١٣ تشرين الأول/أكتوبر ١٩٩٥.

[164] Scott J. Shackelford, op.cit.p.216.

[165] Vida M.Antolin- Jenkins, "Defining the parameters of cyber war operations: Looking for law in all the wrong places", Naval Law Review No.51., 2005, p.134.

[166] انظر مضامين قرارات الجمعية العامة للأمم المتحدة بشأن الهجمات السيبرانية في :

A/ RES/55/28 of 20 November 2000, A/ RES/59/61 of 3 December 2004, A/ RES/61/54 of 6 December 2006, A/ RES/62/17 of 5 December 2007, A/ RES/63/37 of 2 December 2008, A/ RES/64/25 of 2 December 2009.

[167] Christopher D.Deluca," The need for International Laws of War to Include Cyber Attacks Involving State and Non-State Actors ", Pace International Law Review, vol.3, No.9, winter 2013, p.279.

[168] أيان أنطوني، "**تأملات في استمرار الحد من الأسلحة وتغيره** "، في: معهد ستوكهولم لأبحاث السلم الدولي، " **التسلح ونزع السلاح والأمن الدولي** "، الكتاب السنوي ٢٠٠٦ نشر مركز دراسات الوحدة العربية، بيروت الطبعة الأولى، تشرين ثاني /نوفمبر، ٢٠٠٦، ص ٨٧٦.

[169] انظر على سبيل المثال الورقة القانونية بشأن أدلة الإثبات في الجريمة السيبرانية في المملكة المتحدة، في:
Mike McGuire, "Cyber Crime: review of the evidence", Chapter 1: Cyber –dependent Crimes, October 2013, p.24.

[170] فخري عبد الرزاق صليبي الحديثي، " **شرح قانون العقوبات، القسم العام**"، بغداد، ١٩٩٢، ص، ٣٦-٣٧.

[171] انظر القانون الفرنسي رقم ٢٠٠٤/٥٧٥، الصادر في ٢٠٠٤/٦/٢١.

[172]Elsey, Jeffrey T.G., 'Hacking into international humanitarian law: The prince-les of distinction and neutrality in the age of cyber warfare' Michigan Law Review, 2008, p.106.

[173] انظر اللجنة الدولية للصليب الأحمر،" **الملحقان "البروتوكولان الإضافيان إلى اتفاقيات جنيف المعقودة في ١٢ أب/ أغسطس ١٩٤٩** "،مرجع سابق، ص.٣٣.

[174] ورد في الفقرة الثالثة من ديباجة الاتفاقية المتعلقة بالجريمة الالكترونية ما نصه :" واقتناعاً بضرورة الحاجة إلى إتباع سياسة جنائية مشتركة – كمسألة أولوية – تهدف إلى حماية المجتمع ضد الجريمة الالكترونية ، وذلك من خلال عدة أمور منها: إقرار التشريع الملائم ودعم التعاون الدولي"، انظر: مجلس أوربا،" **اتفاقية مجلس أوربا المتعلق بالجريمة الالكترونية**" مصدر سابق.

[175] استمرت المفاوضات حيال إبرام الاتفاقية زهاء العقد من الزمن بسبب إصرار معظم الدول على خيار التقييد في استخدام الأسلحة بدلا من حظرها ، للمزيد حول هذا الموضوع ، انظر: فريتس كالسهوفن وليزابيث تسغفلد، ،" **ضوابط تحكم خوض الحرب : مدخل لدراسة القانون الدولي الإنساني** "،اللجنة الدولية للصليب الأحمر، الأصل باللغة الانكليزية، ترجمة احمد عبد الحليم،جنيف،يونيو/حزيران ٢٠٠٤.، ص. ٣٤.

[176]Oona A.Hathway , Rebecca Crootof , Philip Levtiz , aley Nix, Aileen Nowlan ,William Perdue ,Julia Spiegel,op.cit.p.844.

[177] Ban Ki-moon, 'Pay more attention to cyber warfare, verification', remarks to Advisory Board on Disarmament Matters, United Nations, New York, 18 Feb. 2009, http://www.un.org/News/Press/docs/2009/sgsm12108 doc.htm, accessed 17 Dec. 2009

[178] REX HUGHES, op.cit.p.534, footnote, no.53.

[179]Schmitt,"Bellum Americanum,"op.cit.pp, 394—400.

[180] Nils Melzer,op.cit.p.5.

[181] مما يلحظ في هذه الاتفاقية أنها استخدمت مصطلح الهجمات الإجرامية السيبرانية (Cybercrime Offences) ولم تستخدم مصطلح الهجمات السيبرانية (Cyber Attacks)، ولهذا الاستخدام مغزى قانوني، فالمصطلح الأول يطلق على الهجمات الإجرامية السيبرانية ذات الصلة بالقطاعات المدنية كالقرصنة على حسابات المصارف ، فيما ينصب المصطلح الثاني على الهجمات السيبرانية ذات الصلة بالقطاعات الأمنية والعسكرية، ولا أدل على ذلك ما تضمنته الفقرة السابعة من ديباجة بالنص:" وإيمانا بأن المكافحة الفعالة للجريمة السيبرانية تستلزم زيادة وسرعة وتفعيل التعاون الدولي في المسائل الجنائية". انظر: انظر: مجلس أوربا، " **اتفاقية مجلس أوربا المتعلق بالجريمة الالكترونية**" مصدر سابق.

[182] المادة (٢) من الاتفاقية نفسها

[183] المادة (٣) من الاتفاقية نفسها.

[184] المادة (٤) من الاتفاقية نفسها.

[185] المادة (٥) من الاتفاقية نفسها.

[186] الفقرات (١و٢) من البند (أ) من المادة (٦) من الاتفاقية نفسها.

[187] المادة (١١) من الاتفاقية نفسها.

[188] الفقرتان (١ و٢) من المادة (١٦) من الاتفاقية نفسها.

[189]J. Pryce, "Convention on Cybercrime, Privacy & Security Law Report", BNA, Inc., October 16, 2006 Vol. 5, No.1, p.1451.

[190]United Nations Congress on Crime Prevention and Criminal Justice (Jan. 22, 2010) at 15, available at http://www.unodc.org/ documents

[191] Micheal A.Vatis and Stepote E.Johnson," The Council of Europe Convention on Cybercrime", National Academic of Scinces, US, 2011, p.13.

[192] يذهب ليي (GAMS lee) إلى تعريف مصطلح نزع الأسلحة (Disarmament)، بأنه :" مصطلح يشير إلى التخلي عن أنواع معينة من الأنظمة التسليحية، فضلاً عن ترسانات عسكرية محددة، وهدفه المتوقع هو شامل وليس محدداً ، أما مصطلح الحد من الأسلحة (Arms Control) فيعرفه بأنه : مجموعة من الخطوات التي تتخذها الدول

لأجل التخفيف من خطر اندلاع نزاعات مسلحة، كاتفاق مجموعة من الدول على وقف تطوير أو إنتاج أو استحداث أنظمة تسليحية معينة.للمزيد حول هذا الموضوع انظر:

GAMS lee, "Arms Control and disarmament", political and social affairs division, 1987, revised 15 February 1999, p.2.

[193] انظر الرسالة التي بعث بها ممثل روسيا الاتحادية الدائم سيرغي ايفانوف إلى الأمين العام للأمم المتحدة في ٢٣ سبتمبر ١٩٩٨،

http://www.un.org/ga/search/view_doc.asp?symbol= A/C.1/53/3&Lang=E; accessed June 7, 2010

[194] انظر القرار الصادر عن الجمعية العامة للأمم المتحدة في ٢٠ نوفمبر عام ٢٠٠٠ المرقم ٥٥/٢٨.

[195] Report of the U.N. Secretary General, Developments in the field of information and telecommunications in the context of international security (July 10, 2000) at 5, available at http://www.un.org/documents/ga/docs/55/a55140.pdf; accessed June7, 2010

[196] انظر المقترح الذي أدلى به نائب الممثل الدائم لروسيا الاتحادية لدى مجلس الأمن في الرابط الالكتروني:

www.nytimes.com/2009/06/28/world/28cyber.html?_r=1&scp=3&sq=Vladislav%20Shersty uk& st=cse; accessed June 7, 2010

[197] اعتادت الولايات المتحدة ممارسة المناورة في معظم المفاوضات الدولية ولاسيما بشأن إبرام الاتفاقيات ذات الطابع الإنساني، وهو أمر يمكن الاستدلال عليه لدى تفحص تصريح وزيرة الخارجية الأمريكية السابقة مادلين أولبرايت إذ ذكرت: " إن للولايات المتحدة الأمريكية خصوصية واستثناء من المعايير الدولية القانونية الناشئة عن الاتفاقيات الدولية....." ، وبحسب رأيها هذا "تملك الولايات المتحدة مجالاً استثنائياً في التعامل مع القضايا الدولية باعتبارها قوة عظمى وتتصرف من هذا المنطلق، وهو ما يحفظ للأمم المتحدة والمجتمع الدولي استقراراً " ، وما رفضها التوقيع على ميثاق روما المنشئ للمحكمة الدولية الجنائية، إلا ردة فعل (مبررة) للعمل بحرية في مواجهة الأزمات الدولية كما يفهم من سياق عبارتها آنفة الذكر، ا للمزيد حول هذا الموضوع نظر:

Forman, Stewart patric,"multilateralism", Amsterdam, Lynne Rienner Publishers, 2002, p.334.

[198] J. Markoff and A. Kramer, In Shift, U.S. Talks to Russia on Internet Security, N.Y. Times (December 12, 2009), available at http://www.nytimes.com/2009/12/13/science/13cyber.html; accessed June 7, 2010.

[199] http://www. america.gov/st/texttrans-english/2010/May/20100510144916xjsnommis0.4230245.html

[200] Transcript of Remarks by Gen. K. Alexander at the Center for Strategic and International Studies, Washington, D.C. (June3, 2010) at 11, available at

http://www.nsa.gov/public_info/_files/speeches_testimonies/100603_alexander_transcript.pdf;

Accessed June 7, 2010.

[201] Ibid. At 14 June 2010.

[202] Franz-Stefan Gady and Greg Austin, op.cit, p.i.

[203] Marco Gercke, "Computer Law Review International", Issue 5 15. October 2011, page, 129.

[204] Ibid.

المصادر

المصادر باللغة العربية:

أولا: الكتب:

١. أيان أنطوني، "تأملات في استمرار الحد من الأسلحة وتغيره "، في: معهد ستوكهولم لأبحاث السلم الدولي، " التسلح ونزع السلاح والأمن الدولي "، الكتاب السنوي ٢٠٠٦ نشر مركز دراسات الوحدة العربية، بيروت الطبعة الأولى، تشرين ثاني /نوفمبر، ٢٠٠٦.

٢. توليو ستيف وشمالبرغر توماس،" قاموس مصطلحات تحديد الأسلحة ونزع السلاح وبنا الثقة" ، معهد الأمم المتحدة لبحوث نزع السلاح ، منشورات الأمم المتحدة،٢٠٠٣.

٣. جون- ماري هنكرتس و لويز دوزوالد – بك ،" القانون الدولي الإنساني العرفي "، المجلد الأول ، القواعد ، اللجنة الدولية للصليب الأحمر ، ، مطبعة برنت رايت للإعلان و الدعاية، القاهرة ، ٢٠٠٧.

٤. جيل برعام," تأثير تطور تكنولوجيا الحرب السبرانية على بناء القوة في إسرائيل", ترجمه للعربية يولا البطل ،مؤسسة الدراسات الفلسطينية ، ٢٠١٣.

٥. شريف عتلم و محمد ماهر عبد الواحد،" موسوعة اتفاقيات القانون الدولي الإنساني، النصوص الرسمية للاتفاقيات والدول المصدقة عليها"،إصدار بعثة اللجنة الدولية للصليب الأحمر بالقاهرة،الطبعة السابعة ،٢٠٠٧.

٦. فخري عبد الرزاق صليبي الحديثي، " شرح قانون العقوبات، القسم العام"، بغداد، ١٩٩٢.

٧. فريتس كالسهوفن وليزابيث تسغفلد، ،" ضوابط تحكم خوض الحرب : مدخل لدراسة القانون الدولي الإنساني "،اللجنة الدولية للصليب الأحمر، الأصل باللغة الانكليزية، ترجمة احمد عبد الحليم،جنيف،يونيو/حزيران ٢٠٠٤.

٨. ماركو ساسولي وانطونيو بوفييه،" كيف يوفر القانون الحماية في الحرب: مختارات من القضايا الخاصة بممارسات معاصرة في القانون الدولي الإنساني، اللجنة الدولية للصليب الأحمر، ،جنيف، الطبعة الأولى، ٢٠٠٩.

٩. محمد حافظ غانم ،" المسؤولية الدولية : دراسة لأحكام القانون الدولي وتطبيقاتها التي تهم الدول العربية"، :محاضرات معهد الدراسات العربية العالية ،جامعة الدول العربية ، القاهرة ،١٩٦٢.

١٠.محمد حافظ غانم،" المسؤولية الدولية"، معهد الدراسات العربية، القاهرة،١٩٦٢.

١١.محمد طي،" شرعية التصدي لقرارات مجلس الأمن الدولي :حق الدول و ولاية القضاء"،المركز الاستشاري للدراسات والتوثيق، الطبعة الأولى،٢٠١٣.بيروت.

١٢.المركز الاستشاري للدراسات والتوثيق، " التحولات في العقيدة العسكرية الأمريكية: دعائم الضعف السبع"، أوراق إستراتيجية، سلسلة غير دورية تعنى بالشؤون الإستراتيجية، العدد:٢، أيلول ٢٠١٤، بيروت.

١٣.منير البعلبكي،" المورد : قاموس انكليزي –عربي"، دار العلم للملايين، بيروت، ٢٠٠٤,

ثانيا: البحوث والدراسات

١٤.جيمي آلان ويليامسون،" بعض الاعتبارات حول مسؤولية القيادة والمسؤولية الجنائية"، مختارات من المجلة الدولية للصليب الأحمر، المجلد ٩٠، العدد ٨٧٠،يونيو/حزيران ٢٠٠٨،ص.٥٦.

ثالثا: الرسائل والأطروحات

١٥.أيمن عبد العزيز سلامة ،" المسؤولية الدولية عن ارتكاب جريمة الإبادة الجماعية "، رسالة دكتوراه ، كلية الحقوق جامعة الإسكندرية، ٢٠٠٥.

رابعا: التشريعات و الصكوك والوثائق الدولية

١٦.التشريعات الوطنية

١٧.القانون الاتحادي رقم (٢) لسنة ٢٠٠٦ بشأن مكافحة جرائم تقنية المعلومات في الإمارات العربية المتحدة.

١٨.قانون التوقيع الالكتروني والمعاملات الالكترونية العراقي رقم (٧٨) لسنة ٢٠١٢.

١٩.القانون الصادر في ٢٠٠١/١٢/٣١ بشأن المعاملات الالكترونية في الأردن.

٢٠.القانون الفرنسي رقم ٢٠٠٤/٥٧٥، الصادر في ٢٠٠٤/٦/٢١.

٢١.القانون رقم (٤) الصادر في ٢٠٠٩/٢/٢٥، بشان التوقيع الالكتروني وخدمات الشبكة في سوريا.

٢٢.والمرسوم السلطاني رقم (٢٠٠١/٢٧) حول تعديل بعض أحكام قانون الجزاء العماني.

٢٣.الصكوك الدولية

٢٤.اتفاقيات جنيف الأربعة الموقعة في ١٢ أب / أغسطس عام ١٩٤٩.

٢٥.البروتوكول المتعلق بأسلحة الليزر المسببة للعمى، البروتوكول الرابع الملحق باتفاقية حظر أو تقييد استعمال أسلحة تقليدية معينة يمكن اعتبارها مفرطة الضرر أو عشوائية الأثر١٣ تشرين الأول/أكتوبر ١٩٩٥.

٢٦.اللجنة الدولية للصليب الأحمر،"القانون الدولي المتعلق بسير العمليات العسكرية، مجموعة اتفاقيات لاهاي وبعض المعاهدات الأخرى"،جنيف،الطبعة الثانية،سبتمبر/ أيلول، ٢٠٠١.

٢٧.اللجنة الدولية للصليب الأحمر ،" الملحقان "البروتوكولان الإضافيان إلى اتفاقية جنيف المعقودة في ١٢ أب أغسطس ١٩٤٩ "، جنيف، سويسرا ، الطبعة الرابعة ، ١٩٩٧.

٢٨.مجلس أوربا،" اتفاقية مجلس أوربا المتعلق بالجريمة الالكترونية"، مجموعة المعاهدات الأوروبية رقم ١٨٥، بودابست عام ٢٠٠١.

٢٩.

٣٠.الوثائق الدولية

٣١.مكتب الأمم المتحدة المعني بالمخدرات والجريمة: "تقرير الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية، دراسة شاملة عن مشكلة الجريمة السيبرانية والتدابير التي تتخذها الدول الأعضاء والمجتمع الدولي والقطاع الخاص للتصدي لها" ، فيينا عام ٢٠١٣ ، الوثيقة : UNODC/CCPCJ/EG.4/2013/2

٣٢.القرار الصادر عن الجمعية العامة للأمم المتحدة في ٢٠ نوفمبر عام ٢٠٠٠ المرقم ٥٥/٢٨.

References by Forging Language

First: Books:

1. **Arquilla, J and D.Ronfeld," In Athena's Camp: Preparing for Conflict in the Information Age, Rand Publishing, Santa Monia, CA, USA, 1997.**
2. **Boldizsár Bencsáth. "Duqu, Flame, Gauss: Followers of Stuxnet," BME CrySyS Lab, RSA, 2012.**
3. **DEP'T OF DEFENSE, OFF. OF GEN. CoUNS., AN ASSESSMENT OF INTERNATIONAL LEGAL ISSUES IN INFORMATION OPERATIONS Second Edition, 1999.**
4. **Forman, Stewart patric," multilateralism", Amsterdam, Lynne Rienner Publishers, 2002**
5. **Franz-Stefan Gady and Greg Austin," Russia, The United States, And Cyber Diplomacy Opening the Doors", The East West Institute, Printed in the United States,2010.**
6. **GAMS lee, "Arms Control and disarmament", political and social affairs division, 1987, revised 15 February, 1999.**

7. **Ghazi, H. S," Summary of the principles of public international law", House of Culture for Publishing and Distribution, first edition, Oman, 2007.**
8. **Gray, C," International Law and the Use of Force", Oxford University Press, Oxford, 2000.**
9. **ICRC," Exploring humanitarian law: IHL Guide, A legal manual for EHL teacher", ICRC, Geneva, January 2009.**
10. **Julia Cresswell, "Oxford Dictionary of word Origins: Cybernetics", Oxford Reference Online, Oxford University Press, 2010.**
11. **K.Saalbach," Cyber War, Methods and Practice", Version 9.0, University of Osnabruck-17 Jun 2014.**
12. **Marco Gercke, "Computer Law Review International", Issue 5 15. October 2011.**
13. **Marco Roscini,"World Wide Warfare _Jus ad bellum and the Use of Cyber Force" ,Max Planck Yearbook of United Nations Law, Volume 14,2010.**
14. **Micheal A.Vatis and Stepote E.Johnson," The Council of Europe Convention on Cybercrime", National Academic of Sciences, U.S, 2011.**
15. **Micheal N.Schmitt," Tallinn Manual on the International Law Applicable to Cyber Warfare ", Cambridge University press, first publishes 2013.**
16. **Micheal S.Fuertes, "Cyber warfare, Unjust Actins in a just War ", Florida International University, Full, 2013.**
17. **Micheal Schmitt," Bellum Americium: The law of armed conflict into the next millennium", Newport: Naval War College, 1998.**
18. **Norbert Wiener, "Cybernetic or control communication in the animal and the machine, M.I.T, Press, Second Edition, Cambridge, Massachusetts, 1948.**
19. **Peter Sommer & Ian Brown," Reducing Systemic Cyber security Risk", OCED, Jan, 2011.**
20. **Richard Kissel," Glossary of Key Information Security Terms", National Institute of Standards and technology, U.S Department of Commerce ", Revision, 2, May, 2013.**
21. **Scoot J Shackleford," State Responsibility for Cyber Attacks: Competing Standards for Growing Problem", CCD COE Publications, C.Czosseck and K. Podins Eds, Tallinn, Estonia, 2010.**
22. **Scoot.j.Shckelford, ," State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem", University of Cambridge, Dept of politicos and International STUDIES, Cambridge, UK,2009.**
23. **Tang Lan, Zhang Xin, Harry D. Raduege, Jr., Dmitry I. Grigoriev, Pavan Duggal, and Stein Schjølberg,"Global Cyber Deterrence Views**

from China, the U.S., Russia, India, and Norway", The EastWest Institute, Printed in the United States, 2010.

24. **U.S. Department of Defense, Dictionary of Military and Associated Terms, Joint Publication 1-02, Nov. 8, 2010, as amended through Feb. 15, 2012.**
25. **William A.Owens, Kennth W.Dam and Herbert S.Lin," Tendency, policy, Law, and ethics regarding US acquisition and use of cyber attack capabilities", National Academics Press, Washington DC, 2009.**
26. **Zimet .E.and C. L. Barry," Military services Overview, Cyber power and National Security", National Defense University Press ,Washington, DC,USA,2009.**

SECOND: Researches and Studies.

1. **Antonio Cassese," The Nicaragua and Tadic tests Revisited in Light of the ICJ Judgment on Genocide in Bosnia", The European Journal of International Law,Vol.18.no.4,2007.**
2. **Antonio Gessese، " The Martens Clouse: Half a loaf or simply pie in the sky?"، EJIL،، Vol.III، No. 1, ,2000.**
3. **Brent Kesler," the vulnerability of Nuclear Facilities to Cyber Attack", Strategic Insight Journal, Vol.10, Issue, 1, spring, 2011.**
4. **Brian Kerbs,"Report: Russian Hacker Forum Fuelled Georgia Cyber Attacks", the Washington Post,16 Oct, 2008.**
5. **Carsten Stahn,"Jus ad bellum', 'jus in bello', 'jus post bellum'? – Rethinking the Conception of the Law of Armed Force", The European Journal of International Law Vol. 17, no.5, 2007.**
6. **Christopher C. Joyner & Catherine Lotrionte," Information Warfare as International Coercion: Elements of a Legal Framework", Europe journal of International law,vol.12,2001.**
7. **Christopher c. joyner and Catherine Lotrionte," Information Warfare as International Coercion: Elements of a Legal Framework", European Journal for International Law, Vol.12.No.825-865,2001**
8. **Christopher D. DeLuca," The Need for International Laws of War to Include Cyber Attacks Involving State and Non-State Actors", Pace International Law Review Online Companion, pace University School of Law,Vol.3,No.9,Winter,2013.**
9. **Christopher D.Deluca," The need for International Laws of War to Include Cyber Attacks Involving State and Non-State Actors ", Pace International Law Review, vol.3, No.9, winter ,2013.**

10. **David Cameron, 'How Britain can best address the threats of the twenty-first century', address at Chatham House, London, 15 Jan. 2010, http://www.chathamhouse.org.uk/events/view/-/id/1419/, accessed 20 Jan. 2010.**
11. **Davis Brown, "Proposal for an international convention to regulate the use of information System in Armed Conflict", Harvard International Law review, Vol.47, 2006.**
12. **Diego Rafael Canabarro and Thiago Borne," Reflection on the fog of Cyber War", National Center for Digital Government, Policy working Paper No.13:001, March 1, 2013.**
13. **Doswald –Beck ، " International humanitarian law and the advisory opinion of the international court of justice on the threat or use of nuclear weapons" ، ICRC، Vol. 316 ، 1997.**
14. **Elsey, Jeffrey T.G., 'Hacking into international humanitarian law: The prince-les of distinction and neutrality in the age of cyber warfare' Michigan Law Review, 2008.**
15. **Emily Haslam, "Information Warfare: Technological Changes and International Law", Journal of Conflict and Security Law, Vol. 5, 2000.**
16. **Erki Kodar," Applying the law of armed conflicts to Cyber attacks: from the Martens Clouse to Additional Protocol I", ENDC Proceeding, Volume .15, 2012.**
17. **Eshel, David, 'Israel adds cyber-attack to IDF', Aviation Week's DTI, 9 Feb. 2010, http://www.military.com/ features/0,15240,210486,00.html, accessed 22 Feb. 2015.**
18. **Gorman, S. Dreazen, & Y. Cole, A., "Computer Spies Breach Fighter-Jet Project," The Wall Street Journal,21 Apr, 2009.**
19. **Gorman, S., Dreazen, & Y. Cole, A., "Insurgents Hack U.S. Drones" ,Wall Street Journal, 17, Dec 2009.**
20. **Ivan Goldberg, "Institute for the Advanced Study of Information Warfare (LASIW), http/www.psycom.net/war .1.html.**
21. **J Hilder," Computer Virus Used to Sabotage Iran's Nuclear Plan, Built by US and Israel ", Australian review, 27 January ,2011.**
22. **J. Pryce, "Convention on Cybercrime, Privacy & Security Law Report", BNA, Inc, Vol. 5, No.1, October 16,2006.**
23. **James A. Lewis, "Sovereignty and the role of Government in Cyberspace", Center for Strategic and International Studies Journal, Spring Summer, Vol. XVI, Issue. II, 2010.**
24. **Jonathan A.OPHARD, "Cyber Warfare and the Crime of Aggression:**

The Need for Individual Accountability on Tomorrow's Battlefield ", DUKE Law & Technology Review, No.3.2010.

25. **Judge Stein Schjolberg," An International Criminal Tribunal for Cyberspace (ICTC) Prosecution for the Tribunal Police investigation for the Tribunal", A paper for the East West Institute (EWI) Cybercrime Legal Working Group, 2012.**
26. **Keir Giles, "Information Troops a Russia Cyber Command?" legal paper third international conference on Cyber Conflicts, Tallinn Estonia,2011.**
27. **Kenneth Grees, Darien Kindlind, Ned Moran, Rob Rachwald," World War C: Understanding Nation-States Motives behind Today's Advanced Cyber Attaches". Fire Eyes report ,p.6.,at https://www.fireeye.com/resources/pdfs/fireeye-wwc-report.pdf**
28. **Larry Wortzel, "China's cyber-offensive", Wall Street Journal, 1 Nov, 2009.**
29. **Marco Roscini," World Wide Warfare – Jus ad bellum and the use of Cyber Force",Max Planck Yearbook of United Nations Law, Volume. 14,2010.**
30. **Markoff and A. Kramer, In Shift, U.S. Talks to Russia on Internet Security, N.Y. Times (December 12, 2009), available at http://www.nytimes.com/2009/12/13/science/13cyber.html; accessed June 7, 2010.**
31. **Markoff J, and Kramer A.E," In Shift, US. Talks to Russia on Internet Security, New York Times, December 12. 2009.**
32. **Matthew C. Waxman," Cyber –Attack and the Use of Force: Back to the Future of Article 2 (4)", The Yale Journal of International Law, Vol.36, No.421, 2011.**
33. **Matthew Evangelista, "Cooperation theory and Disarmament Negotiations in the 1950s", World political Journal, Vol.42, No.4, July, 1990.**
34. **Micheal Gervais," Cyber Attacks and the Laws of War", Berkeley Journal of International Law", Vol. 30, Issue .2, Article 6, 2012.**
35. **Micheal N.Schmmitt," Wired warfare: Computer network attack and jus in Bello", IRRC, Vol.84, No.846, 2002.**
36. **Mike McGuire, "Cyber Crime: review of the evidence", Chapter 1: Cyber –dependent Crimes, October, 2013.**
37. **Murice Abuert," The ICRC and the problem of excessively injuries or**

indiscriminate weapons", Extract print from ICRC, No.279, Nov-Dec, 1990.

38. **Nils Melzer," Cyber warfare and International Law", IDEAS for Peace and Security, UNIDIR Researches, 2011.**
39. **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.**
40. **Peter Margulies," Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility", Melbourne Journal of International Law, Vol.14.2013.**
41. **President Obama's Remarks on Securing U.S. Cyber Infrastructure," May29, 2009, http://www.america.gov/st/texttrans-english/2009/May/20090529161700eaifas0.1335871.html.**
42. **Rex Hughes, "A treaty for cyberspace", The Royal Institute of International Affairs, International Affairs Journal No.86, Blackwell publishing Ltd, 2010.**
43. **Rwx HUGES," A treaty for Cyberspace", International Affairs journal, Vol.86.No.2, 2010.**
44. **Sanjiv Tomar," Proxy Warfare", Journal of Defense Studies, Vol.8.No, 2, April-June, 2014.**
45. **Schmitt, M.N," Computer Network Attack and the Use of Force in International Law through on a Normative", The Colombia Journal of Transitional Law, Vol.27, No.885-937, 1999**
46. **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, June 2011**
47. **Siobhan Gorman and Julian Barnes, "Cyber Combat: Act of War", Wall Street Journal, May 13, 2011.**
48. **The White House, Office of the Press Secretary, "Remarks on securing the nations' cyber infrastructure", Press Realse,29 May 2009,www.white house.gov/the _press _office/ Remarks-by President-on- Securing-Our-Nations-Cyber-Infrastructure.**
49. **Thomas Rid and Peter Mcburney,"Cyber – Weapons", Routledge publisher, The RUSI Journal, , Vol.157.no.1 February –March, 2012.**
50. **Thomas W. Smith," The New Law of War: Legitimizing Hi-Tech and Infrastructural," International Studies Quarterly, 2002.**

51. **Transcript of Remarks by Gen. K. Alexander at the Center for Strategic and International Studies, Washington, D.C. (June3, 2010) at 11, available at http://www.nsa.gov/public_info/_files/speeches_testimonies/100603_alexander_transcript.pdf.**
52. **Vida M.Antolin- Jenkins, "Defining the parameters of cyber war operations: Looking for law in all the wrong places", Naval Law Review, No.51. 2005.**
53. **Watkin, K,"Contrloing the use of force: A role for human rights in Contemporary Armed Conflicts", American Journal of International Law, Vol. 98, No.1-34, 2004.**
54. **Yaakov Katz," Stuxnet Virus Set Back Iran's Program by 2 years", Jerusalem Post, Dec, 15, 2010, at http://www.jpost.com/IranianThreat/News/Article.aspx?id=199475.**
55. **Yoram Dinstein," Computer Network Attacks and Self-Defense", International Law Studies Review. vol. 76 ,no.99, 2002.**

Third: Thesis.

1. **Nathan E.Mueller," Micheal Walzer on the Moral Legitimacy of states and the Morality of Killing in War", Thesis submitted to the faculty of the Virginia Polytechnic Institute and State University in partial fulfillment of the requirements for the degree of Master of Arts in Philosophy, May 10, 2006.**
2. **Thomas M.Franck," Legitimacy after Kosovo and Iraq", in International Law and the Use of force at the turn of the centuries ", Essays in Honor of V.D Degan Crinc-Grotic & Matulovic eds, 2005.**

Forth: Documents.

1. **ICJ, Military and parliamentary activities in and against Nicaragua (Nicar .v.US.), 1986.**
2. **ICJ Report 1996," Legality of the threat or use of nuclear Weapons", Para 78, p.257.**
3. **ICJ،" Legality of the threat or use of nuclear weapons"، Dissenting opinion of judge Shahabuddeen.**
4. **UN," Responsibility of States for International Wrongful Acts 2001", UN, 2005.**

5. **Case: Prosecutor v. Tadic, 1995.**
6. **Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), Judgment, I.C.J. Reports 2007, p. 43JUDGMENT OF 26 FEBRUARY 2007: http://www.icj-cij.org/docket/files/91/13685.pdf**
7. **Judgment, Prosecutor v. Radislav Krstić, Case No. IT-98-33-T, 2 August 2001.**
8. **Ban Ki-moon, 'Pay more attention to cyber warfare, verification', remarks to Advisory Board on Disarmament Matters, United Nations, New York, 18 Feb. 2009, http://www.un.org/News/Press/docs/2009/sgsm12108 doc.htm, accessed 17 Dec. 2009.**
9. **United Nations Congress on Crime Prevention and Criminal Justice (Jan. 22, 2010) at 15, available at http://www.unodc.org/ documents.**
10. **Report of the U.N. Secretary General, Developments in the field of information and telecommunications in the context of international security (July 10, 2000) at 5, available at http://www.un.org/documents/ga/docs/55/a55140.pdf; accessed June7, 2010.**
11. **ICTY،Case IT-95-11-R61،8 MARCH 1996،Prosucort V.Martic**
12. **A/ RES/55/28 of 20 November 2000**
13. **The preambles of Resolutions A/RES/55/63 of 4 December 2000, A/RES/ 56/121 OF 19 December 2001.**
14. **A/ RES/59/61 of 3 December 2004**
15. **A/ RES/61/54 of 6 December 2006**
16. **A/ RES/62/17 of 5 December 2007**
17. **A/ RES/63/37 of 2 December 2008**
18. **A/ RES/64/25 of 2 December 2009.**

Fifth: WEB-SITES:

1. **http://www. america.gov/st/texttrans-english/2010/May/20100510144916xjsnomm is0.4230245.html**
2. **http://www.lawoflibya.com/forum/showthread.php?t=3624**
3. **http://www.nato.int/cps/en/natolive/official_texts_17120.htm**
4. **http://www.un.org/ar/documents/charter/chapter7.shtml**
5. **http://www.un.org/arabic/documents/GADocs/56/A_56_589.pdf**

6. **http://www.un.org/ga/search/view_doc.asp?symbol= A/C.1/53/3&Lang=E; accessed June 7, 2010**
7. **http://www.usccu.us/#The_Urgency_of_This_ Cyber-Security Work, accessed 3 Jan. 2010**
8. **www.nytimes.com/2009/06/28/world/28cyber.html?_r=1&scp=3&sq=Vladislav%20Sherstyuk& st=cse; accessed June 7, 2010**

Abstract

In the current period the world is witnessing, a new kind of arms race, not the well-known ones in conventional and non-conventional weapons field style, this race is based on the development of electronic programs intended for military purposes know as Cyber race.

Researchers have since begun a period not exceeding five years ago the legal research and analysis on this topic, in the light of the data confirmed that the threat would cause its cyber attacks at the level of international peace and security and the level of at least the most serious threats for the gravity of the internationally known.

And because the subject occupies a leading position in the legal effort, particularly when specialized international institutions on the one hand, and the lack of Arab and Iraqi ones in particular research on the other hand, these two facts paid to choice it and to be the subject of this study, dependents in analysis of the provisions of the Public International Law and related to the conventions which organization to use international efforts prohibition or restriction, as well as the most important judicial and jurisprudence, which addressed the issue of cyber attacks from different sides.

That a number of questions would be raised at the research and analysis on the subject of the study like: What are the cyber attacks and hwo originated in accordance to Public international law? You could be classified within the means and methods of fighting? And if so do you apply the provisions of international conventions and customary rules related to the conduct of combat operations?

On the other hand, how the international community deal with the legal vacuum which witnessed the subject of international regulation of cyber problem? And is a glimmer of hope from the start of multilateral or bilateral international negotiations to end the controversy about the legitimacy of resorting to it in light of the provisions of international humanitarian law and customary rules of stable between civilized nations?

And what if the failure of the international community continued to arrive at the conclusion of an international convention on organized cyber military purposes? The key to the solution lies in the intervention of the leading IT countries, particularly the United States, Russia, China or other countries to interfere with the convergence of views?

All of these problems we will try to answer in the light of the research plan divided on two sections: the first shed the light on the concept of cyber attacks, in terms of the word Cyber source in the language and terminology, as well as browse the date on which began using electronic means to this body armed attacks on the one hand.

On the other hand we will look at the most prominent models cyber documented by formal and informal institutions, which would give a chance for the fact that the use of electronic technology in the military and security field and identify future implications for international peace and security.

The second section will focus on the contemporary international regulation of cyber attacks, in the light of the principles of the right to resort to war (Jus in bellum) and the behavior of War ((Jus ad Bello.

Whether resorting to cyber prohibited or restricted in accordance with the provisions of international law and humanitarian in particular, we will look to emerging about the international responsibility in light of the current international regulation, as well as research and analysis in the international effort on the conclusion of a multilateral international convention prohibiting or restricting mail use for military purposes in comparison with national legislation to combat cyber crime like Convention of the Council of Europe in 2001 known (Convention against Cyber crimes).

مجلة المحقق الحلي للعلوم القانونية والسياسية العدد الرابع/ السنة الثامنة ٢٠١٦

Cyber attacks: its concept and arising international responsibility In the light of contemporary international organization

BY

A.P.Dr.Ahmed Oubais Al-Fatlawi