الوضع القانوني للحرب السيبرانية على ضوء قواعد القانون الدولي

ختال هاجر

كلية الحقوق والعلوم السياسية، جامعة باجي مختار – عنابة، Khettel.h@gmail.com

تاريخ الإيداع: 2016/04/10 **تاريخ المراجعة:** 2017/02/20 **تاريخ القبول:** 2017/06/12

ملخص

تطورت وسائل وأساليب الحرب منذ اتفاقيات جنيف لعام 1949، وتشكل الأسلحة السيبرانية مثالا متقدما للتكنولوجيا الحديثة، إذ تتم العمليات الحربية ضمن وعبر فضاء افتراضي وهو الفضاء السيبراني (الالكتروني). وفي ظل حداثة هذا النوع الجديد من الأسلحة وما نتج عن استخدامه من آثار مأساوية ضد الإنسانية، استوجب معه البحث في مشروعية هذا السلاح الجديد ومدى مطابقته لقواعد القانون الدولي خاصة في ظل غياب اتفاق دولي يحظر أو يقيد استخدام الأسلحة السيبرانية.

الكلمات المفاتيح: أسلحة سيبرانية، فيروسات، طائرات من دون طيار، نزاع مسلح، حاسوب، دليل تالين.

Legal situation of the cyber warfare in the light of the rules of international law

Abstract

The means and methods of warfare have evolved since the Geneva Conventions of 1949. Cybernetic weapons constitute an advanced example of modern technology where military operations take place in and through a virtual space; this is the cybernetic space (electronics). In the light of this modern weapon, the harmful consequences of its use against humanity impose the need to undertake research on its legitimacy and its conformity with the rules of international law. Such studies are required particularly in the absence of an international agreement in order to prohibit or restrict such warfare.

Key words: Cybernetic weapons, viruses, drones, armed conflict, computer, Tallinn manual.

Statut juridique de la guerre cybernétique à la lumière des règles du droit international

Résumé

Les moyens et méthodes de la guerre ont évolué depuis les conventions de Genève de 1949. Les armes cybernétiques constituent un exemple avancé de la technologie moderne, où les opérations militaires se déroulent dans et à travers–un espace virtuel, il s'agit de l'espace cybernétique (électronique). A la lumière de cette arme moderne, les conséquences néfastes de son utilisation contre l'humanité imposent la nécessité d'entreprendre une recherche sur sa légitimité et sa conformité avec les règles du droit international, en particulier en l'absence d'un accord international visant à interdire ou à la restreindre.

Mots-clés: Armes cybernétiques, virus, drones, conflit armé, ordinateur, manuel de Tallinn.

المؤلف المرسل: ختال هاجر، Khettel.h@gmail.com

مقدمـــة

إن للحروب في كل عصر أدواتها التي تستخدمها تتناسب مع ذلك العصر ودرجة تقدمه، ونحن نعيش اليوم عصرا أصبحت فيه المعلومات ظاهرة بارزة، إذ يجري توظيفها في أدوات الفتك والتدمير بشكل فاق بمراحل عديدة توظيفها في التنمية والبناء، حتى أصبحت اليوم تكنولوجيا المعلومات تلعب دورا أساسيا في النزاعات المسلحة يتساوى في أهميته إن لم يكن متفوقا على القنابل والصواريخ وغيرها.

وقد شهد العقد الأخير تطورات سريعة في مجالي الحوسبة وتكنولوجيا المعلومات بما أفضى إلى تغييرات بعيدة المدى في جميع مجالات الحياة تقريبا، ولا سيما في المجالين العسكري والأمني اللذين شهدا تغييرات عديدة تتعلق بطريقة القتال وأسلوب بناء قوة الجيوش.

فكما ظهرت القوة الجوية كثورة في الشؤون العسكرية في أوائل القرن العشرين، قد تشكل الحرب السيبرانية أو كما يسميها آخرون الالكترونية أو المعلوماتية الثورة التالية في الألفية الجديدة. حيث حدثت تطورات تكنولوجية متقدمة في مجال الحرب السيبرانية أدت إلى تغيرات نوعية في خصائص ميدان القتال وكذلك في أنماط قتال الجيوش الحديثة. ونظرا لحداثة هذا المجال، فإن معرفة طبيعته وتأثيراته لا تزال في بداياتها. مما يدفعنا للتساؤل حول **مدى إمكانية تطبيق القواعد القانونية الدولية الحالية على الحرب السيبرانية ومدى حاجتنا اليوم إلى وضع إطار تنظيمي خاص يتماشى مع طبيعة حرب الفضاء السيبراني؟**

وللإجابة عن ذلك ارتأينا تقسيم الدراسة إلى ثلاثة مباحث: نتعرض في الأول إلى مفهوم الحرب السيبرانية. وفي المبحث الثاني إلى التكييف القانوني للهجوم بالفيروسات المعلوماتية، على أن نخصص المبحث الثالث إلى حكم استخدام الأسلحة السيبرانية في القانون الدولي الإنساني.

المبحث الأول: مفهوم الحرب السيبرانية

استخدمت الحرب السيبرانية في صور عديدة، بدءا باستخدام الاتصال اللاسلكي في الحرب العالمية الأولى، مرورا باستخدام الرادار في الحرب العالمية الثانية، حتى استخدام نظم الاتصالات الالكترونية المتطورة المحمولة جوا بالأقمار الصناعية اليوم[1].

تختلف الحرب السيبرانية عن غيرها من الحروب التقليدية، حيث تنفذ العمليات العدائية عبر فضاء افتراضي غير مادي وهو الفضاء السيبراني، لذا فمن الأهمية بمكان البحث في مفهوم هذه الحرب وذلك أولا بتعريف الحرب السيبرانية، والتطرق ثانيا إلى بعض أشكالها.

المطلب الأول: تعريف الحرب السيبرانية

يمكن وصف الفضاء السيبراني[2] بأنه عالم افتراضي يتشابك مع عالمنا المادي، يتأثر به ويؤثر فيه بشكل معقد، حيث تقوم العلاقة بين العالمين على نظرة تكاملية تحمل بين طياتها الكثير من المخاطر، فهناك من عرف مجال الفضاء السيبراني بوصفه " الذراع الرابعة للجيوش الحديثة " إلى جانب القوات البرية والبحرية والجوية.

والفضاء الالكتروني شأنه شأن ظاهرة الفضاء التقليدية التي تتألف من أربعة مكونات رئيسية: المكان والمسافة والحجم والمسار، ويتميز الفضاء الالكتروني بغياب الحدود الجغرافية وغياب عنصر الزمن[3].

وقد عرف الفضاء السيبراني بأنه: "البيانات الالكترونية، والشبكات الالكترونية المتصلة، والأشخاص الذين يستخدمونها"[4]، حيث تعد هذه العناصر العامل المشترك في جميع محاور استخدام الفضاء السيبراني.

أما بالنسبة لتعريف الحرب السيبرانية فلا يوجد تعريف عالمي متفق عليه حول هذا النوع من الحرب[5]. غير أنه انطلاقا من تعريف الفضاء السيبراني يمكن تعريف الحرب السيبرانية أو المعلوماتية، بأنها فرع من العمليات المعلوماتية أي "الأعمال التي تنفذ للتأثير على معلومات العدو ونظم معلوماته، وفي نفس الوقت حماية المعلومات ونظم المعلومات الخاصة بالمهاجم"، وتشمل هذه العمليات في الواقع أي إجراءات تتخذ بغير رضا متبادل بهدف اكتشاف البيانات المخزنة في أحد أجهزة الحاسوب أو تغييرها أو تدميرها أو تشويشها أو تحويلها. ويمكن أن يحدث ذلك وقت السلم كما في وقت الأزمات على حد سواء. أو على المستويات الإستراتيجية أو العملياتية أو التكتيكية من النزاع المسلح [6].

أما حرب المعلومات فهي أضيق من ذلك فهي: " عمليات معلوماتية تجرى أثناء الأزمات او النزاعات لتحقيق أو تعزيز أهداف معينة إزاء عدو أو أعداء محددين " لذلك تختلف حرب المعلومات عن العمليات المعلوماتية الأخرى من حيث السياق الذي تجرى فيه، وهو الأزمات أو المنازعات. فعمليات التجسس الروتينية التي تحدث في أوقات السلم لا تعد حرب معلومات إلا إذا جرت أثناء عمليات عدائية[7].

كما يمكن وصف العمليات السيبرانية بوجه عام بأنها عمليات تشن ضد أو عبر حاسوب أو نظام حاسوبي بواسطة تيار البيانات. وقد تهدف هذه البيانات إلى تحقيق أغراض مختلفة تضم على سبيل المثال اختراق نظام معين وجمع أو نقل أو تدمير أو تغيير أو تشفير البيانات، أو إجراء تعديل العمليات التي يتحكم فيها الجهاز الحاسوبي المخترق أو التلاعب بهذه العمليات. ويمكن على هذا النحو استخدام هذه الوسائل لتدمير أو تعديل أو تعطيل مجموعة متنوعة من الأهداف في العالم الحقيقي، كالبنى الأساسية. حيث تثير النتائج المحتملة لهذه العمليات مخاوف كبيرة على الصعيد الإنساني[8].

ونخلص من هذا كله إلى أن حروب المعلومات يمكن تعريفها بأنها: أي فعل أو نشاط يستهدف حرمان أو استغلال أو إفساد أو تدمير معلومات العدو ووظائفها. وفي الوقت نفسه حماية النفس ضد مثل هذه الأنشطة أو الأفعالّ[9].

المطلب الثاني: أشكال الحرب السيبرانية

لا يتوفر اليوم بصورة رسمية نظام لتصنيف أنواع العمليات ضمن وعبر الفضاء الالكتروني. فقد دفع التطور في مجال الفضاء الالكتروني إلى بروز ترسانة غير تقليدية لأسلحة الكترونية متعددة كالفيروسات، وهجمات إنكار الخدمة والاختراق وسرقة المعلومات والتشويش[10] غير أنه يمكن التفصيل في النوعين الآتيين الشائعي الاستعمال:

أولا: الحرب الفيروسية وهي مهاجمة الكترونية لشبكات الاتصال بواسطة فيروسات معلوماتية متنوعة.

ثانيا: الحرب عن طريق التحكم عن بعد بأسلحة سواء جوية أو برية أو بحرية.

الفرع الأول: الحرب الفيروسية المعلوماتية

يستحيل ذكر جميع أنواع الفيروسات، بل ويستحيل تصنيفها بصورة دقيقة بالنظر إلى تكاثرها وظهور أنواع جديدة في كل يوم[11]، ولكن يمكن التطرق إلى البعض منها[12]:

1- الفيروس البرمجي 2- الفيروس النظامي 3- الفيروس المتعدد الأطراف 4- الفيروس المترجم 5- الديدان 6- الآلي 7- فيروس فلايم.

ويوصف الفيروس المعلوماتي فلايم[13] بأنه سلاح معلوماتي يرمي الى اختلاس الوثائق على شكل pdf والبيانية كما صرحت بذلك شركة كاسبرسكي لاب الروسية لبرمجيات أمن الانترنت على لسان مديرها أوجين كاسبيرسكي.

وقد دعا الخبير الروسي إلى العمل الفوري على منع انتشار الأسلحة السيبرانية، وخاصة أن بعض الفيروسات والبرامج الخبيثة قادرة على سبيل المثال، على إحداث شلل تام لدولة بحجم الولايات المتحدة الأمريكية[14].

ويكون تأثير استخدام الفيروسات مضاعفا نتيجة لما ينطوي عليه من توجيه جيش يضم مجموعة كبيرة من أجهزة الكمبيوتر المرتبطة بشبكة واحدة المحملة بالفيروسات يتم التحكم فيها عن بعد لمهاجمة النظام المستهدف بعدد من الأوامر والطلبات في نفس الوقت ونشر الفيروسات فيه بهدف شله[15] وفي السنوات الماضية تمكنت فيروسات "سارس" و"لف" من الانتشار في نصف مليون جهاز كمبيوتر في أقل من أربع ساعات، وأصبحت هذه الهجمات تستخدم في النزاعات المسلحة الدولية حيث استخدمت في حرب الناتو على صربيا وفي حرب كوسوفا وفي حرب العراق وفي الصراع العربي الاسرائيلي[16].

الفرع الثاني: منظومات الأسلحة التي يتم التحكم بها عن بعد

يتم التحكم بهذه الأسلحة عن طريق الفضاء السيبراني أو الالكتروني، وتتمثل إحدى السمات الرئيسية لمنظومات الأسلحة التي يتم التحكم فيها عن بعد في أنها تتيح للمقاتلين الغياب جسديا عن منطقة العمليات الحربية. ويمكن لهذه التكنولوجيا الجديدة أن تساعد المقاتلين على توجيه هجماتهم إلى الأهداف العسكرية توجيها أكثر دقة، كما يمكن لهذه التكنولوجيا أن تعرض السكان المدنيين والممتلكات المدنية لقدر أكبر من الأضرار العرضية الناجمة عن ذلك[17].

وتعد الطائرات بلا طيار (drones) مثالا بارزا على منظومات الأسلحة التي يتم التحكم بها عن بعد. ويمكن تعريفها بأنها نظام المركبة الهوائية الموجهة التي يتم السيطرة عليها وعلى ما تحمله من معدات وعلى سطوح التحكم في أدائها من بعد، ويتم التحكم إما بشكل مباشر عن طريق إرسال أوامر محددة لها لتنفيذها أو بالخزن المسبق لبرامج معينة لتنفيذ مهمة محددة بحاسبات الطائرة بحيث يتم التنفيذ آليا كما يمكن التحكم بالطائرة بالطريقتين معا[18].

فقد عززت هذه الطائرات إمكانيات المراقبة الجوية الآنية تعزيزا كبيرا، مما أدى إلى زيادة أشكال التدابير الاحتياطية التي يمكن اتخاذها قبل شن الهجوم. وتنطوي منظومات الأسلحة التي يتم التحكم فيها عن بعد مع ذلك على مخاطر، إذ أظهرت الدراسات أن التحديات الخاصة بالتشغيل المسؤول لهذه المنظومات تتضمن قدرة المشغل المحدودة على معالجة كم كبير من البيانات، بما فيها البيانات المتناقضة في وقت معين (فيض المعلومات)، والإشراف على أكثر من منظومة في وقت واحد، مما يثير تساؤلات بشان مدى قدرة المشغل على التقيد التام بقواعد القانون الدولي الإنساني في مثل هذه الظروف[19].

وقد برهنت الطائرة بلا طيار أنها محورية في القيادة والسيطرة والاستطلاع خلال حربي أفغانستان والعراق والتدخل في ليبيا[20]. مثل طائرة "جلوبال هوك" التي استخدمت في حرب أفغانستان عام 2001، وطائرة "بريديتور" التي بدأ استخدامها بنجاح في حرب البلقان وافغانستان والعراق، وقد حظيت هاتان الطائرتان باهتمام القادة العسكريين، لأنهما وفرتا لهم صورا حية بالفيديو عن أنشطة العدو على الأرض في وقت قياسي، كما وفرتا فرصة تحديد الهدف وإطلاق صواريخ "هيلفاير" المحملة عليهما، مما دفع الخبراء إلى تصميم أجيال من الطائرات

المماثلة التي لا تنفذ عمليات الاستطلاع فحسب بل تهاجم المواقع المعادية أيضا[21]. وكما هو الحال بالنسبة إلى بريديتور، ترتبط "جلوبال هوك" بأشخاص على الأرض، لكنها تعمل بشكل مستقل أساسا بدلا من أن تتم قيادتها عن بعد وباستخدام فأرة حاسوب، يكتفي المشغل بالنقر لإبلاغ الطائرة بالتحرك ثم الإقلاع، ثم تحلق الطائرة بمفردها، وتقوم الطائرة بتنفيذ مهمتها، وتلقي التوجيهات بشأن أماكن تحليقها من إحداثيات يحددها النظام العالمي لتحديد المواقع بعد إنزالها من أحد الأقمار الصناعية[22].

تمتلك طائرات الحرب الالكترونية بدون طيار، المنتجة في الغرب بالمقارنة مع الطائرات العادية إمكانيات على المناورة أفضل، الأمر الذي يزيد من الحيوية والقدرة العملياتية وتمكنها من الاستخدام في المناطق التي تتمتع بحماية متماسكة من قبل وسائط الدفاع الجوي وفي ظروف الرؤية المختلفة ولا تحتاج إلى مطارات مجهزة للهبوط أو الإقلاع[23]. وتمثل الطائرة الشبح (x-47) الطراز الجديد من الطائرات من دون طيار، تم إطلاقها عام 2013 وتمثل هذه الطائرة المقاتلة – بالإضافة إلى أنواع أخرى مشابهة لها – تقدما في تكنولوجيا الأسلحة، إذ يتم تصميمها لتطير أسرع ولمسافات أطول، كما أنها تستطيع الإقلاع والهبوط ذاتيا، وتنفذ مجموعة من المهام بشكل ذاتي، وإعادة التزويد بالوقود في الهواء ذاتيا[24].

وهناك محاولات حثيثة لتطوير طائرة بلا طيار تستطيع التعرف على العناصر أو الأفراد المستهدفين، من خلال ملامحهم الشخصية أو البَيومِتْرِيَّة (Biométrique)، والمبادرة إلى قتلهم على الفور اعتمادا على برامج حاسوبية تلقائية القرار، وليس اعتمادا على أوامر المشغلين الجالسين خلف شاشات الحواسب في أماكن تبعد عشرات آلاف الكيلومترات عن مكان الاغتيال.

كما تم ابتكار العديد من الأسلحة الهجومية الالكترونية في حرب الخليج الثانية خاصة تلك المعتمدة على الطاقة الموجهة الحديثة ومنها أسلحة الميكروويف عالية القدرة (High –power Microwave Weapons)، والمعروفة اختصارا بـ (HPM) وهي من أهم الأسلحة الجديدة في مجال الحروب الالكترونية، ويمكن استخدامها لاختراق الأهداف عالية التحصين لتدمير وشل أسلحة الدفاع الجوي والرادارات وأجهزة الاتصال والحاسبات التي تعمل ضمن منظومة القيادة والسيطرة[25]. حيث أظهرت الولايات المتحدة خلال حرب الخليج مستوى التطور الحاصل في مجال الحرب الالكترونية[26]، وحققت قوات التحالف نجاحات باهرة في هذا المجال، وأثبتت أن اختراق المجال الجوي المعادي أصبح حاليا وبشكل رئيسي إحدى وظائف الحرب الالكترونية[27].

وكانت قد طرحت على طاولة النقاش من خلال مؤتمر سان ريمو المنعقد في سبتمبر 2011 المتعلق بالتحديات الحالية أو المعاصرة للقانون الدولي الإنساني مسألة التكنولوجيا الجديدة للأسلحة والقانون الدولي الإنساني، حيث ناقش الخبراء مشروعية بعض الأسلحة الجديدة كالطائرات من دون طيار، والروبوتات، والأسلحة الذاتية التشغيل أو التحكم، وتكنولوجيا الأقمار...، غير أن البعض من هذه الأسلحة تم استعمالها في ساحات المعركة الحديثة – كالأسلحة السيبرانية والطائرات من دون طيار– أما البعض الأخر منها تم إنتاجه ولكن لم يستعمل بعد ويبقى فقط مجرد علم خيالي، يمكن أن يتم توظيفها في المستقبل كالروبوتات الذاتية التشغيل[28].

المبحث الثاني: التكييف القانوني للهجوم بالفيروسات المعلوماتية

لقد اختلف حول تحديد الوصف القانوني للهجوم بالفيروسات المعلوماتية على شبكات الاتصال، فهناك رأي وصف هذا الهجوم بأنه عدوان تنطبق عليه خصائص الفعل العدواني واتجاه آخر رأى عكس ذلك وهو ما سنحاول

البحث فيه من خلال أولا تعريف العدوان ومدى انطباق الهجوم بالفيروسات على أعمال العدوان، وثانيا إمكانية إدراج مفهوم جديد للعدوان الفيروسي.

المطلب الأول: العدوان ومدى انطباقه على الحرب الفيروسية المعلوماتية

من خلال تحديد المقصود بالعدوان، سنحاول إسقاط خصائص هذا الأخير على الهجومات التي تتم بواسطة فيروسات معلوماتية.

الفرع الاول: تعريف العدوان

عرفت المادة الثامنة مكرر فقرة 2 من النظام الأساسي للمحكمة الجنائية الدولية[29] فعل العدوان بأنه: "استعمال القوة المسلحة من جانب دولة ما ضد سيادة دولة أخرى أو سلامتها الإقليمية أو استقلالها السياسي أو بأي طريقة أخرى تتعارض مع ميثاق الأمم المتحدة وينطبق فعل العدوان على أي من الأفعال الآتية وذلك وفقا لقرار الجمعية العامة للأمم المتحدة 3314 المؤرخ سنة 1974:

أ- الغزو بواسطة القوات المسلحة لدولة ما لإقليم دولة أخرى، أو الهجوم عليه أو أي احتلال عسكري، وإن كان مؤقتا ناتجا عن مثل هذا الغزو أو الهجوم، أو أي ضم لإقليم دولة أخرى أو جزء منه بواسطة استعمال القوة.

ب- إلقاء القنابل بواسطة القوات المسلحة لدولة ما ضد إقليم دولة أخرى، أو استعمال أي نوع من الأسلحة من قبل دولة ضد إقليم دولة أخرى.

جـ- ضرب حصار على موانئ أو ساحل دولة ما بواسطة القوات المسلحة لدولة أخرى.

د- هجوم القوات المسلحة لدولة ما على القوات المسلحة البرية أو البحرية أو الجوية أو الأسطولين البحري أو الجوي لدولة أخرى.

هـ- قيام دولة ما باستعمال قواتها المسلحة الموجودة داخل إقليم دولة أخرى بموافقة الدولة المضيفة، على وجه يتعارض مع الشروط التي ينص عليها الاتفاق. أو أي تمديد لوجودها في الإقليم المذكور إلى ما بعد نهاية الاتفاق.

و- وضع دولة لإقليمها تحت تصرف دولة أخرى ليستخدم من قبل هذه الأخيرة لارتكاب عمل عدواني ضد دولة ثالثة.

ز- إرسال عصابات أو جماعات مسلحة، أو قوات غير نظامية أو مرتزقة من قبل دولة أو باسمها والتي تقوم بأعمال القوة المسلحة ضد دولة أخرى من الخطورة بحيث تعادل الأعمال المعددة أعلاه. أو اشتراك الدولة بدور ملموس في ذلك".

الفرع الثاني: مدى انطباق وصف العدوان على الحرب الفيروسية المعلوماتية

للبحث في مدى تطابق وصف العدوان على الحرب الفيروسية المعلوماتية، يجب إسقاط كل خاصية من خصائص العدوان على العمليات الهجومية بواسطة الفيروسات المعلوماتية، كالآتي:

أولا: أطراف العدوان

وفقا لما جاء به القرار RC/Res 6 فإن العدوان لا يقوم إلا بين دولتين أو أكثر، وهو ما ينطبق مثلا على حالة إيران حينما قامت الولايات المتحدة الأمريكية واسرائيل بضرب المنشآت النووية الإيرانية، وذلك بتسريب فيروس "فلايم".

ثانيا: مبدأ المبادءة[30]

إن الدولة التي تبدأ قبل غيرها من الدول في ارتكاب أحد الأفعال المحددة في المادة 8 مكرر من النظام الأساسي للمحكمة الجنائية الدولية بعد إدراجها بموجب مؤتمر كامبالا 2010، أو بتوصيف من مجلس الأمن الدولي وفقا لاختصاصه المنصوص عليه في المادة 39 من ميثاق الأمم المتحدة– فعلى الرغم من التعديلات المدخلة على النظام الأساسي للمحكمة الجنائية الدولية فإن مجلس الأمن مازال يستأثر بسلطة تحديد الأعمال التي تشكل جريمة عدوان– ،فإنها تعتبر دولة بادئة بالعدوان سواء أعلنت الحرب أم لا، وهو ما تحقق فعلا من خلال العدوان الفيروسي المعلوماتي على دولة إيران من طرف الولايات المتحدة الامريكية وإسرائيل كما أسلفنا الذكر.

ثالثا: القصد العدائي

يعتبر القصد العدائي الركن المعنوي لجريمة العدوان، حيث أكد الوزير الإسرائيلي على أن: "أي شخص يظن أن التجارب النووية تشكل خطرا على أمن بلاده له الحق في محاربة هذا البرنامج بشتى الوسائل وإذا كانت هذه الوسائل تعبرعن حرب الكترونية من خلال فيروسات تهدد بياناتهم التي جمعوها من العمل على المفاعل سيكون شيأً إيجابياً"[31].

وهو ما يحقق النتائج من المبادءة أي المبادرة بالعدوان كخلق الفوضى أو التدخل في الشؤون الداخلية لدولة أخرى وإنزال الأذى للحصول على امتياز من أي نوع كالتدخل في البرنامج النووي الإيراني لتحطيمه.

المطلب الثاني: الحرب الفيروسية كمفهوم جديد للعدوان والنتائج المترتبة عن ذلك

في ظل التطور التكنولوجي السريع للأسلحة، أصبح من الاستحالة اليوم تطبيق المفهوم القديم للعدوان، مما ينتج عنه بالضرورة إدراج الحرب الفيروسية المعلوماتية التي تتم في الفضاء السيبراني ضمن مفهوم العدوان.

الفرع الأول: الحرب الفيروسية كمفهوم جديد للعدوان

حين وضعت الدول مجتمعة على مستوى الجمعية العامة للأمم المتحدة تعريفاً للعدوان وفقا لقرارها الصادر سنة 1974 والذي تم الإبقاء عليه وإدراجه في المادة 8 مكرر من النظام الأساسي للمحكمة الجنائية الدولية بموجب المؤتمر الاستعراضي بكامبالا 2010 لم يكن يخطر في ذهن هؤلاء بأنه سيحدث تطور فيما بعد في وسائل وأساليب الحرب، وتعدد الأدوات التي لا يمكن بأي حال من الأحوال تعريفها بأنها أسلحة بالمفهوم التقليدي للسلاح، ولكن في حقيقة الأمر تعتبر سلاحا من نوع جديد كما قال البعض من المتخصصين.

فليس صعبا على الولايات المتحدة ضرب المنشآت النووية الإيرانية بهذه الطريقة، المكلفة ماديا وغير مكلفة بشريا، بالإضافة إلى عدم إثارتها لأي احتجاجات علنية بوصفها حرباً خفية على من تحسبهم من أعدائها فلا هي محتاجة إلى استصدار قرارات من مجلس الأمن كما كانت تفعل دائما ولا هي محتاجة إلى تأييد المجتمع الدولي في ذلك[32]. فبالقياس إلى استخدام أسلحة الفضاء الالكتروني نجد أنها تمثل نوعا من استخدام القوة ذات الطابع المرن أو الإلكتروني التي ينتج عنها نفس نتائج استخدام القوة بمفهومها التقليدي[33].

ومنه لا شك اليوم في إدراج الحرب الفيروسية المعلوماتية التي تتم في الفضاء السيبراني ضمن مفهوم العدوان، لاعتبارات عديدة أهمها أن التطور الحاصل اليوم في التكنولوجيا العسكرية، أدى إلى تجاوز المفهوم التقليدي والجامد للعدوان الموضح أعلاه.

الفرع الثاني: النتائج المترتبة على اعتبار الحرب الفيروسية عدوانا

ينتج عن اعتبار الحرب الفيروسية المعلوماتية التي تتم عبر الفضاء السيبراني عدوانا من نوع جديد، وأن للدول المتضررة من هذا الهجوم حق الدفاع الشرعي المنصوص عليه في المادة 51[34] من ميثاق الأمم المتحدة والتي تقرر بأن حق الدفاع الشرعي لا يواجه سوى الهجمات المسلحة دون تحديد لنوع السلاح المستعمل في العدوان على الدولة.

إضافة إلى أن السلاح اليوم لم يعد هو ذلك النوع من الأسلحة التقليدية المعروفة بل انسحب عليها تطور تكنولوجي هائل يصعب معه تحديدها أو تصنيفها.

ألا يصح لنا كما يقول الدكتور محمد سعادي أن نوصف الهجومات بالفيروسات المعلوماتية على مصالح الدول الأخرى باعتباره سلاح العصر الرقمي، بأنه عدوان مسلح ولا ينقص استعمال الفيروسات المعلوماتية من صفة العدوانية قياسا بالفيروسات الجرثومية المستعملة كسلاح بيولوجي ضد الدول؟ فما الفرق بين ضرب الدول بالفيروسات الجرثومية واعتبارها حربا بيولوجية وضرب الدول بالفيروسات الالكترونية واعتبارها حربا فيروسية تمس مصالح الدول في الصميم إذا علمنا بأن الدول ومصالحها الكلية اليوم لا تسير إلا بالحواسيب والإعلام الآلي في أدق الأمور وأوسعها[35]. وبذلك عد الفيروس الالكتروني كالفيروس البيولوجي سلاحا جديدا يستخدم في معركة مفتوحة وميدان معركة غير معروفة المعالم، وتكون أثاره عشوائية[36].

ولأهمية الفضاء السيبراني في تسيير الشؤون المدنية والعسكرية، أسست هيئة الأركان العامة في الجيش الإسرائيلي في مارس 2003 شعبة تحمل اسم "شعبة المعالجة عن بعد"، بهدف توفير استجابة فورية لحالات التعرض لهجمات سيبرانية معادية، وبهدف الربط بين نظم الحواسيب العسكرية بالجيش الاسرائيلي، وعمل شبكات معلومات مشتركة لجميع هيئات الطوارئ في الدولة العبرية[37].

حيث وصف رئيس هيئة الأركان العامة السابق "جابي أشكنازي" عام 2009 الفضاء السيبراني كمجال قتال استراتيجي تقني، كما أعلن الجيش الإسرائيلي أنه أصبح من بين أول الجيوش التي تؤسس غرفة حرب رقمية (digital war room) لإدارة العمليات المتقدمة في مجال حرب الفضاء السيبراني، بهدف تمكين الجيش من العمل بشكل سلس في الفضاء السيبراني وإعطائه صورة لحظية واضحة للتطورات المحيطة، ويعتبر الجيش غرفة الحرب الرقمية مركز أعصاب الدولة في عمليات الحماية، حيث سيكون بمقدورها القيام بعمليات اعتراض وتوجيه وتشغيل في الفضاء السيبراني بالتنسيق مع جميع وحدات الجيش[38].

كما أنشأت في سلاح الاتصالات الالكترونية (هتيكشوف)، دائرة الدفاع السايبيري. وتمكن هذه الدائرة قوات الجيش من تنفيذ عمليات برية، وبحرية، وجوية، في عصر يعتمد فيه الجيش أكثر من أي وقت مضى، على تكنولوجيا الحواسيب. وتعمل الدائرة بالتعاون مع معظم وحدات النخبة في الجيش الإسرائيلي، مستخدمة تشكيلة من الوسائل التكنولوجية المتطورة في سبيل تعطيل هجمات العدو السيبرانية[39].

كما أنشأت الولايات المتحدة الأمريكية قيادة حرب الفضاء الالكتروني، وتحولت هذه القيادة الالكترونية التابعة لسلاح الجو إلى القوة الرابعة والعشرين، ويقع مقرها في قاعدة لاكلاند الجوية في تكساس. ويلاحظ أن هذه القوة لن يكون لديها أي طائرات، حيث إن مهمتها هو توفير قوات مدربة ومجهزة مستعدة للقتال بإجراء عمليات الكترونية مستمرة ومتناغمة بصورة تامة مع العمليات الجوية والفضائية[40].

وقد قامت وزارة الدفاع الأمريكية عام 1999 باختراق شبكات الكمبيوتر الصربية لإفساد العمليات العسكرية وإحداث الخلل في البنية المدنية الأساسية، وذلك في محاولة لدعم قوات التحالف، فظهور حرب المعلومات يدفع المخططين الحربيين وغيرهم إلى تنمية قدراتهم في استخدامها ومنه فأسلحة الفضاء الالكتروني لها دور في تغيير طبيعة الحرب حيث بدلا من المخاطرة عن طريق القيام بقصف شبكات الطاقة والسكك الحديدية وخطوط الهاتف من قبل الطيران الحربي، أصبح بالإمكان استخدام شبكات الكمبيوتر والفضاء الالكتروني لإحداث الأثر نفسه[41].

ويدرك الجميع الآن أن الحرب الالكترونية أحدثت متغيرات ثورية في العمليات الحربية الحديثة، فقد حولت الصواريخ الموجهة الكترونيا والتي تحملها الغواصات والطائرات وقوارب الدورية من قوة هجومية إلى قوة دفاعية تحتاج إلى إجراءات ووسائط خاصة للدفاع ضد احتمالات الهجوم[42].

المبحث الثالث: حكم استخدام الأسلحة السيبرانية في القانون الدولي الإنساني

يثير تطبيق قواعد قانونية موجودة من قبل على تكنولوجيا جديدة مسألة ما إذا كانت هذه القواعد تتسم بما يكفي من الوضوح في ظل خصائص هذه التكنولوجيا، وقد شهدت السنوات الماضية إدخال مجموعة واسعة من التكنولوجيات الجديدة إلى ساحة المعركة الحديثة والتي تتم كلها ضمن وعبر الفضاء السيبراني. فهل تشمل أحكام وقواعد القانون الدولي الإنساني هذا النوع الجديد من الأسلحة؟

المطلب الأول: تعدد الآراء بشأن خضوع الأسلحة السيبرانية للقانون الدولي الإنساني

لقد انقسمت الآراء بشأن هذه المسألة فمنهم من رأى أن القانون الدولي الإنساني لا يحتوي أحكاما تتناول بشكل مباشر الهجوم على شبكات الحاسوب أو تدور حول الحرب السيبرانية، لأن تطوير واستخدام الهجمات على شبكات الحاسوب يرجع تاريخها إلى ما بعد اعتماد المعاهدات المتعلقة بالقانون الدولي الإنساني. كما أن هناك رأيًا آخرَ يقول بأن عدم انطباق المعاهدات الإنسانية على هذه الأسلحة، هو أن القانون الدولي مصمم للتعامل مع الأساليب والوسائل الحركية بطبيعتها kinetic، وحيث أن الهجوم على شبكات الحاسوب لا يتضمن إلا القليل مما هو مادي، فإن الهجمات عن طريق الحاسوب تقع خارج نطاق القانون الدولي الإنساني، أي أن هذا الأخير ينطبق على النزاعات المسلحة ولكن الهجوم على شبكات الحاسوب ليس له الطابع "المسلح"[43].

غير أننا لا نحذو حذو هذا الرأي بدليل أن الحرب البيولوجية والكيميائية تخضع للقانون الدولي الإنساني على الرغم من أنها لا تتضمن أسلحة حركية.

وهناك رأي آخر يستبعد الاحتمالات السابقة، مفاده أنه لا يمكن التسليم بأن الاتفاقيات القائمة سكتت بشأن الهجوم على شبكات الحاسوب ومنه يجب إخراج هذه الأسلحة من نطاق قواعد القانون الدولي الإنساني، مستدلا بشرط مانتز[44] وينص هذا المبدأ على أنه " يظل المدنيون والمقاتلون في الحالات التي لا ينص عليها في الاتفاقيات تحت حماية وسلطان مبادئ قانون الشعوب كما استقر بها العرف ومبادئ الإنسانية وما يمليه الضمير العام"[45].

كما أكد أصحاب هذا الرأي بأن الحجة التي تركز على حقيقة أن الهجوم على شبكات الحاسوب يرجع تاريخه إلى ما بعد اعتماد المواثيق الحالية تنطوي على مغالطة أيضا، ذلك أن هذا التبرير كان قد قدم إلى محكمة العدل الدولية لترى مدى مشروعية التهديد بالأسلحة النووية أو استخدامها، ورفضت المحكمة في رأيها الاستشاري القول بأنه نظرا لأن المبادئ والقواعد الإنسانية قد وضعت قبل اختراع الأسلحة النووية، فإن القانون الإنساني يكون غير منطبق عليها – ومن أهم المبادئ التي تحكم استخدام الأسلحة: التمييز، والتناسب، والألآم التي لا مبرر لها،

والضرورة العسكرية... والتي لا يسعنا التطرق إليها بالتحليل في هذا البحث نظرا لتشعبها –. ولأنه ليس هناك ما يدعو للتمييز بين الأسلحة النووية وأسلحة الحاسوب على الأقل من حيث التوقيت الذي استحدثت فيه بالنسبة لدخول المعايير الإنسانية ذات الصلة حيز التنفيذ فإن نفس النتيجة تنطبق على الهجوم على شبكات الحاسوب أي التي تتم عبر الفضاء السيبراني(46).

المطلب الثاني: الإشكاليات والتساؤلات التي يثيرها استعمال الأسلحة السيبرانية

يثير استعمال الأسلحة السيبرانية العديد من الإشكاليات القانونية لعل من بينها مسألة تحديد المسؤول عن الأفعال، ففي معظم الحالات يكون من الصعب، أو من المستحيل، تحديد هوية الفاعل المنفذ للهجوم. وتنجم مصاعب كبيرة عن هذا الأمر نظرا لاعتماد القانون الدولي الإنساني على نسب المسؤولية إلى أطراف النزاع، فعندما يستحيل تحديد هوية منفذ عملية معينة، يستحيل بالتالي تحديد الصلة التي تربط هذه العملية بنزاع مسلح، ومنه يكون من الصعب الوقوف عند تطبيق القانون الدولي الإنساني على مثل هذه العمليات من عدمه. فهل يمكن وصف العمليات المنفذة عن طريق الفضاء السيبراني بأنها تشكل نزاعا مسلحا بالمعنى المنصوص عليه في اتفاقيات جنيف وغيرها من معاهدات القانون الدولي الإنساني وبالتالي إسناد المسؤولية الدولية للطرف المنتهك لقواعد هذا الأخير؟

الفرع الأول: مدى انطباق وصف النزاع المسلح على الهجوم السيبراني

في الشرح الذي نشرته اللجنة الدولية للصليب الأحمر لاتفاقيات جنيف لعام 1949 والبروتوكولين الإضافيين لعام 1977 نجد نهجا موسعا بشأن النزاع المسلح. فشرح الاتفاقيات يعرف النزاع المسلح بأنه " أي خلاف ينشأ بين دولتين ويؤدي إلى تدخل القوات المسلحة حتى إذا أنكر أحد الأطراف وجود حالة الحرب"، وبالمثل فإن شرح البروتوكول الإضافي الأول يحدد أن "القانون الإنساني يغطي أي نزاع بين دولتين يشتمل على استخدام قواتها المسلحة. بغض النظر عن فترة استمرار النزاع أو كثافته"، كما يصف شرح البروتوكول الإضافي الثاني النزاع المسلح بأنه "وجود أعمال عدائية صريحة بين القوات المسلحة تكون منظمة بدرجة أو بأخرى. ومنه فالشرط الضروري في الحالات الثلاث هو مشاركة القوات المسلحة"(47).

لكن لا يمكن الاعتماد فقط على معيار القوات المسلحة، لأن هذه الأخيرة تستخدم بشكل منتظم ضد الأعداء دون أن تنتج بالضرورة حالة نزاع مسلح كحالات الاستطلاع الجوي أو عمليات المراقبة على سبيل المثال(48). ومنه ونظرا للتقدم الهائل في وسائل وأساليب الحرب، ولا سيما حرب المعلومات، لا يكفي لتطبيق القانون الدولي الإنساني الاعتماد على الفاعل – أي القوات المسلحة – وإنما يجب الاعتماد بدرجة أكبر على أثار العمل أي الأضرار.

كما أن فئة لا يستهان بها من فقهاء القانون الدولي والممارسين له عالجوا هذه المسألة وغيرها من التحديات المتعلقة بالقانون الدولي الإنساني خلال مشروع دام مدة ثلاث سنوات ممول من قبل حلف الناتو، نجم عنه دليل "تالين" للقانون الدولي المطبق في الحرب السيبرانية "Tallinn Manuel" مكون من 292 صفحة، حيث يبين هذا الدليل القوانين المنظمة لقواعد الاشتباك عن طريق الانترنت. إذ اتفقوا على أنه متى أحدثت العمليات السيبرانية "Cyber Operations" من قبل دولة ما، دمارا أو أذى، لدولة أخرى فإن ثمة نزاع مسلح دولي. بل إن البعض من هؤلاء الفقهاء والممارسين يرى بأن حدوث أي ضرر ولو بالدرجة الأدنى للضرر يمكن أن يشكل نزاعا مسلحا دوليا(49).

الفرع الثاني: خضوع الأسلحة السيبرانية للقانون الدولي الإنساني بناءً على آثارها

إن عدم وجود ضوابط خاصة بنشاط عسكري معين لا يعني أنه يمكن ممارسة هذا النشاط بدون قيود. فوسائل وأساليب الحرب المستندة إلى التكنولوجيا السيبرانية تخضع لأحكام القانون الدولي الإنساني تماما كما يخضع لها أي سلاح جديد عندما يستخدم في نزاع مسلح[50] اعتمادا على معيار النتائج غير الإنسانية التي تحدثها هذه الأسلحة.

فإذا استخدمت العمليات السيبرانية ضد عدو معين في نزاع مسلح لإلحاق الضرر به عن طريق التلاعب، على سبيل المثال، بنظام المراقبة الجوية بطريقة تؤدي إلى سقوط طائرة مدنية، أو بنظم أنابيب نقل النفط أو منشآت نووية عن طريق العبث بالنظم الحاسوبية المستخدمة بها. فمن الصعب في هذه الحالة نفي كون هذا الهجوم في واقع الأمر وسيلة من وسائل الحرب المحظورة بموجب القانون الدولي الإنساني.

كما أنه عندما تتعرض الحواسيب أو الشبكات التابعة لدولة ما لهجوم أو اختراق أو إعاقة، قد يجعل المدنيين عرضة لخطر الحرمان من الاحتياجات الأساسية مثل مياه الشرب والرعاية الطبية والكهرباء. وإذا تعطلت أنظمة تحديد المواقع GPS عن العمل، قد تحدث إصابات في صفوف المدنيين من خلال تعطيل عمليات إقلاع مروحيات الإنقاذ على سبيل المثال. ويمكن أن تتعرض السدود والمحطات النووية وأنظمة التحكم في الطائرات لهجمات سيبرانية نظرا لاعتمادها على الحواسيب. وتكون الشبكات مترابطة إلى حد يجعل من الصعب الحد من آثار هجوم سيبراني ضد جزء من المنظومة دون الإضرار بأجزاء أخرى أو تعطيل المنظومة بأكملها[51]. فمن خلال السلاح الالكتروني يستطيع العدو أن يخرب شبكة الاتصالات العسكرية، وأن يشل الدورة الاقتصادية والمالية والتجارية والصناعية ... الخ، كل ذلك دون أن يطلق رصاصة واحدة[52]. فالحروب لها قواعد وحدود تنطبق على اللجوء إلى الحرب السيبرانية بنفس القدر الذي تنطبق به على استخدام البنادق والمدفعية والصواريخ وباقي الأسلحة الأخرى[53].

ومن الإحصائيات التي يمكن أن تدل على فعالية الهجمات السيبرانية أو الإلكترونية تلك الهجمات التي تم شنها على العراق خلال حرب الخليج الثانية، حيث تشير مصادر كلية الحرب الأمريكية إلى أن ضرب مولدات الطاقة الكهربائية العراقية أدى بشكل غير مباشر إلى موت ما بين 70 إلى 90 ألف مواطن عراقي كنتيجة مباشرة لعدم توفر الطاقة الكهربائية[54]. كما ظهر الفضاء الالكتروني على الساحة الدولية في الحرب بين جورجيا وروسيا في أغسطس 2008 وفي التوتر ما بين استونيا وروسيا في ماي 2007 على نحو مباشر وعلني، فقد كشفت الهجمات التي تعرضت لها استونيا وجورجيا بأنها كانت غير تمييزية – أي لم تحترم مبدأ التمييز المنصوص عليه في اتفاقيات جنيف – حيث إنها وجهت الخطوط الاتصالات عن طريق توجيه المئات من قنابل " الميجابايت "، وهذا الهجوم لم يتعرض له فقط السكان بل أثر على توقف أرقام الطوارئ التي تستخدم في استدعاء الإسعاف وخدمات المطافئ لما يزيد على ساعة والتي تقع ضمن المنشآت المحمية وفقا للقانون الدولي[55].

ونرى أن المجتمع الدولي لم يكن لديه أية مشكلة في اعتبار استخدام الأسلحة البيولوجية أو الكيميائية يقع تماما ضمن تعريف الهجوم المسلح، على الرغم من كون هذه الأسلحة غير قابلة للكشف عنها بواسطة الحواس البشرية المجردة كما أنها لا تعتبر من الأسلحة الحركية. ومنه فإن نوع الأسلحة المستخدمة في أي نزاع مسلح ليس له أهمية تذكر، وعليه وجب اعتبار الهجوم بالأسلحة المعلوماتية هجوما مسلحا تبعا لنتائجه المحتملة[56].

فخضوع أو عدم خضوع الهجمات السيبرانية للقانون الدولي الإنساني إنما يعتمد على طبيعتها وعلى النتائج المتوقعة منها، حيث تقارب الهجمات الالكترونية الهجمات التقليدية في النتائج ولكنها تختلف في الوسائل واستراتيجيات التنفيذ، فالوسائل التي تستخدم لإحداث الأذى أو الموت أو إحداث التلف أو الدمار هي أعمال غير إنسانية بغض النظر عن الوسيلة أو الطريقة التي استخدمت. فالتجويع والخنق والرمي بالرصاص وإلقاء القنابل وحتى الهجوم الالكتروني كلها خاضعة للقانون الدولي الإنساني بسبب واقع حدوث نتائج إنسانية معينة.

بل والأكثر من ذلك أن الأسلحة التي توصف بأنها أسلحة عشوائية كالنووية والبيولوجية تصبح أكثر تمييزا[57] من الأسلحة التي يتم التحكم فيها الكترونيا – الأسلحة العالية الدقة –، حيث يجبر القائم بالعمليات العدائية في تطبيقه لمبدأ الحيطة أن يعزف عن شن الهجمات لأن إصابة المدنيين تصبح محققة فعلا. والدليل على ذلك أن استعمال القنابل الذكية المجهزة بنظام لتحديد الهدف يشكل أحسن مثال عن ذلك، إذ استعملت هذه التكنولوجيا المتطورة من الأسلحة خلال حرب الخليج الأولى ويوغسلافيا 1999 وحرب أفغانستان 2001، ومع ذلك فإن عدد الضحايا المدنيين سجل ارتفاعا في كل مرة مقارنة مع المرات السابقة[58].

الفرع الثالث: تغيير مفهوم المقاتل وتشتت المسؤولية الدولية في إطار الحرب السيبرانية

تمكن الحرب السيبرانية للمقاتلين الغياب جسديا عن منطقة العمليات الحربية، مما يطرح العديد من الإشكاليات القانونية لعل من بينها مسألة تحديد المسؤول عن الأضرار الناتجة عن استخدام الأسلحة السيبرانية.

أولا: تغيير مفهوم المقاتل

لقد أسفر التطور في مجال الأسلحة وظهور تكنولوجيات جديدة التي يتم التحكم فيها عبر الفضاء السيبراني عن تغيير شامل في مضمون القوّات النظامية، أي الجيوش بمختلف أشكالها وتشكيلاتها، والقوات المتطوعة التي تتكون من أفراد يعملون بدافع وطنيتهم مع الجيوش النظامية.

ففي الماضي كان نقص عديد القوات العسكرية يحدث خللا أمنيا ويهدد أمن الدولة بالتفكك. أما اليوم فلم يعد لعديد القوات العسكرية أي قيمة استراتيجية تذكر، لأن الأسلحة السيبرانية أَوْهَت مفعول الترابط بين قدرة الجيش وكثرته وعززت قدرة الدولة الواحدة، المالكة لهذا السلاح، على ضمان أمنها والدفاع عن نفسها بمفردها[59]. كما أن المقاتل لم يعد يواجه عدوه في ساحة معركة وجها لوجه وإنما المقاتل اليوم هو الذي يجلس خلف شاشات الحواسيب متحكما في العمليات الحربية بمجرد ضغطة زر.

ثانيا: تشتت المسؤولية الدولية في إطار الحرب السيبرانية

كما سلف القول فإن من أهم المسائل التي يثيرها استعمال الأسلحة السيبرانية هو مسألة صعوبة تحديد الفاعل أو منفذ عمليات الهجوم السيبراني، وبالتالي استحالة قيام المسؤولية الدولية في حالة انتهاك قواعد القانون الدولي الإنساني.

حيث توجد العديد من الصعوبات لإيجاد الجهة منفذة الهجمات السيبرانية من بينها غياب الدليل المرئي، وافتقار الآثار التقليدية وصعوبة الوصول إلى الدليل لإحاطته بوسائل الحماية الفنية كاستخدام الجاني لكلمات السر بشكل يمنع الوصول إلى الأدلة الالكترونية أو تشفير المعلومات[60].

كذلك سهولة محو الدليل أو تدميره في وقت قصير جدا، وضخامة كم البيانات والمعلومات وإمكانية وجودها خارج إقليم الدولة[61].

وفي عصر الطائرات بلا طيار وما أفرزته من أضرار جسيمة تجاوزت حدود الدولة التي تستخدمها، تضاعفت أهمية تلك المسؤولية، فراح رجال القانون يطالبون بتطوير قواعدها حتى لا تقف القواعد التقليدية عقبة في سبيل حصول من تصيبهم هذه الأضرار على التعويض العادل. فالمفهوم التقليدي للمسؤولية لم يعد قادرا على التلاؤم مع الآثار والأضرار التي تسببها الثورة العلمية الحديثة، لأن الأضرار أصبحت خطيرة وشاملة، وإثبات الضرر بات صعبا[62].

إن أضرار الطائرات بلا طيار قد تحدث من دون أن يكون بالإمكان نسب أي خطأ إلى الدولة المسؤولة عن الطائرة، فمن الصعب بمكان أن يكون للطائرات بلا طيار مظهر خارجي يدل على صفاتها وجنسيتها مما يعقد عملية الإثبات (خاصة تلك التي تكون الدولة قد اشترتها من الشركات المصنعة). فهل تتحمل كل دولة طرف تطلق أو تسمح بإطلاق أي طائرة بلا طيار في الجو، أو يستخدم إقليمها أو منشآتها لعملية إطلاق من هذا النوع، مسؤولية دولية عن الأضرار التي تسببها هذه الطائرة أو أي من شظاياها، لأي دولة طرف أو لأي شخص من أشخاصها الطبيعيين أو المعنويين؟ وهل تحتفظ الدولة الطرف، التي أطلقت الطائرة بلا طيار في الجو، بالولاية والرقابة عليها خارج حدود الولاية الوطنية للدولة؟ وبعبارة أوضح: هل تتحمل الدولة الطرف، التي أطلقت أو سمحت بإطلاق الطائرة بلا طيار من أرضها أو سمحت بعبور أجوائها، المسؤولية الدولية عن جميع الأضرار التي تصيب الغير؟ فمن يتحمل المسؤولية في هذه الحالة؟ وما هو أساس هذه المسؤولية؟[63].

ربما سنجد الإجابة عن كل هذه التساؤلات في المستقبل، لكن ما يمكن تأكيده هو أن القانون الدولي الإنساني واسع بشكل كبير ليشمل التكنولوجيات الجديدة من الأسلحة، حيث إنه كما حظر أو قيد بعض الأنواع من الأسلحة (الأسلحة الكيميائية، البيولوجية، الألغام المضادة للأفراد...)، فإنه وضع مبادئ وقواعد عامة تسري على كل وسائل وأساليب الحرب مهما بلغت درجة تطورها، ناهيك عن نص المادة 36 من البروتوكول الإضافي الأول لعام 1977 المتعلق بحماية ضحايا النزاعات المسلحة الدولية والتي تلزم الدول بالمراجعة القانونية لأي سلاح جديد يتم إنتاجه[64]. ورغم ما تطرحه الأسلحة السيبرانية من تحديات للقانون الدولي الإنساني على جميع المستويات وخاصة فيما يخص المسؤولية الدولية كما وُضِّح أعلاه. فإن إقرار المسؤولية الدولية في جانب الدولة المتسببة في الضرر أمر لا مفر منه إذا ما ترتب عن استخدام هذه الأسلحة أضرار للمدنيين أو البيئة أو الأعيان المدنية...

إضافة إلى أن الحاسوب حتما لم يتمكن بعد من اتخاذ قرارات المهاجمة بمفرده، ويبقى الإنسان (العقل البشري) هو المتحكم الفعلي في اتخاذ هذه القرارات مهما بلغت تقنيات الحاسوب من تطور[65].

خاتمـــة

يعد الاستخدام العسكري للفضاء السيبيري حقيقة واقعية بالفعل، ومن المرجح أن تنمو أهميته في العقود المقبلة، وفي المقابل فإن احتمالات تحقيق تقدم في مجال الاتفاقيات الدولية لمراقبة استخدام أسلحة الفضاء الالكترونية وتنظيمها تبدو ضئيلة جدا، حتى وإن تم ذلك فإنه لن يتم التوصل إلى حل شامل، لأن نظم الرقابة في الأسلحة التقليدية تعتمد على التحقيق من خلال التفتيش، فإنه وفي ظل الأسلحة الالكترونية يمكن أن تشكل سهولة إخفاء تطوير هذه الأسلحة عقبة أمام نظام التفتيش والتحقيق. ولكن التحالفات الإقليمية قد تحرز تقدما في تنفيذ تدابير تعاونية مثل منظمة حلف شمال الأطلسي من خلال دليل تالين، حيث تضمن هذا الدليل كيفية تطبيق القانون الدولي – القانون الدولي الإنساني خاصة– على الحرب السيبرانية.

وعلى ضوء ما تقدم يمكن الخروج بالنتائج والملاحظات الآتية:

– إن عدم وجود ضوابط خاصة بنشاط عسكري معين لا يعني أنه يمكن ممارسة هذا النشاط بدون قيود، فوسائل وأساليب الحرب المستندة إلى التكنولوجيا السيبرانية تخضع لأحكام القانون الدولي الإنساني تماما كما يخضع لها أي سلاح جديد عندما يستخدم في نزاع مسلح اعتمادا على معيار النتائج غير الإنسانية التي تحدثها هذه الأسلحة. ومنه فمشروعية الأسلحة السيبرانية تتوقف على مدى تقيدها بقواعد ومبادئ القانون الدولي.

– تتمثل إحدى السمات الرئيسية لمنظومات الأسلحة السيبرانية في أنها تتيح للمقاتلين الغياب جسديا عن منطقة العمليات الحربية.

– يمكن لهذه التكنولوجيا الجديدة أن تساعد المقاتلين على توجيه هجماتهم إلى الأهداف العسكرية توجيها أكثر دقة، كما يمكن لهذه التكنولوجيا أن تعرض السكان المدنيين والممتلكات المدنية لقدر أكبر من الأضرار العرضية الناجمة عن ذلك. حيث تتوقف دقة هذا السلاح على مدى قدرة المشغل على التحكم في كم كبير من البيانات والإشراف عليها في وقت واحد، فإذا ما تحكم فيها المشغل بطريقة جيدة أصابت هذه الأسلحة الأهداف العسكرية بدقة محترمة بذلك قواعد القانون الدولي الإنساني (أهمها قاعدة التمييز)، أما إذا لم يتمكن المشغل من التحكم الدقيق فيها فعندها ستسفر عن نتائج كارثية تجاه المدنيين وذلك لعدم إمكانية المشغل من التحكم في العديد من البيانات في آن واحد (فيض المعلومات).

– ضرورة إدراج الحرب الفيروسية المعلوماتية التي تتم في الفضاء السيبراني ضمن مفهوم العدوان. وأن للدول المتضررة من هذا العدوان حق الدفاع الشرعي المنصوص عليه في المادة 51 من ميثاق الأمم المتحدة.

– إن من أهم المسائل التي يثيرها استعمال الأسلحة السيبرانية هو مسألة صعوبة تحديد الفاعل أو منفذ عمليات الهجوم السيبراني، وبالتالي استحالة قيام المسؤولية الدولية في حالة انتهاك قواعد القانون الدولي الإنساني.

الهوامش:

1- د. أحمد أنور زهران، الحرب المحدودة والحرب الشاملة، مكتبة غريب، دون بلد نشر، دون سنة نشر، ص 75.

2- يعد ويليام جيبسون أول من استخدم كلمة cyber مقترنة بكلمة space في مصطلح الفضاء الالكتروني .cyberspace انظر: بيتر سنجر، "دروس الحروب الماضية والاتجاهات التكنولوجية المستقبلية"، في الحروب المستقبلية في القرن الحادي والعشرين، مركز الإمارات للدراسات والبحوث الاستراتيجية، أبو ظبي، 2014، الطبعة الأولى، ص 83.

3- حسن مظفر الرزو، الفضاء المعلوماتي، الطبعة الأولى، مركز دراسات الوحدة العربية، بيروت، 2008، ص 213– 323.

4- جون باسيت، " حرب الفضاء الالكتروني: التسلح وأساليب الدفاع الجديدة "، في الحروب المستقبلية في القرن الحادي والعشرين، الطبعة الأولى، مركز الإمارات للدراسات والبحوث الإستراتيجية، 2014، ص 55.

5- Fred Schreier, on cyber warfare, working paper n° 7, DCAF horizon, 2015, p 16.

6- مايكل ن. شميث، الحرب بواسطة شبكات الاتصال: الهجوم على شبكات الكمبيوتر (الحاسوب) والقانون في الحرب، المجلة الدولية للصليب الأحمر، 2002، ص 87– 88.

7- المرجع نفسه، ص 88.

8- اللجنة الدولية للصليب الأحمر، تقرير عن القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة، المؤتمر الدولي الحادي والثلاثون للصليب الأحمر والهلال الحمر، جنيف، 2011، ص 42 – 43.

9- جمال محمد غيطاس، الحرب وتكنولوجيا المعلومات، نهضة مصر للطباعة والنشر والتوزيع، القاهرة، 2006، الطبعة الأولى، ص 21. وايضا:

Martin C. Libicki, conquest in cyberspace: national Security and information warfare, First published, Cambridge university press, New York, 2007, p 16.

10- عادل عبد الصادق، القوة الالكترونية: أسلحة الانتشار الشامل في عصر الفضاء الالكتروني، السياسة الدولية، العدد 188، المجلد 47، ابريل 2012، القاهرة، ص 32.

11- نديم عبده، حروب المستقبل: دور الكمبيوتر والأسلحة غير الفتاكة في النزاعات المستقبلية، منريخ للطباعة والنشر والتوزيع، بيروت، 1999، ص 35.

12- د. محمد سعادي، أثر التكنولوجيا المستحدثة على القانون الدولي العام، دار الجامعة الجديدة، الإسكندرية، 2014، ص 188 – 190.

13- ان فيروس فلايم لا يمكن أن تستعمله سوى الدولة بسبب تكلفته الباهظة، حيث كلف هذا الفيروس الذي استهدف حواسيب في الشرق الأوسط وإيران 100 مليون دولار. انظر: د. محمد سعادي، المرجع السابق، ص 190 وما بعدها.

14- ربيع محمد يحي، إسرائيل وخطوات الهيمنة على ساحة الفضاء السيبراني في الشرق الأوسط: دراسة حول استعدادات ومحاور عمل الدولة العبرية في عصر الانترنت (2002– 2013)، مجلة رؤى إستراتيجية، مركز الإمارات للدراسات والبحوث الإستراتيجية، أبو ظبي، دون سنة نشر، ص 77.

15- عادل عبد الصادق محمد الجخة، أثر الإرهاب الالكتروني على مبدأ استخدام القوة في العلاقات الدولية، رسالة ماجستير، كلية الاقتصاد والعلوم السياسية، جامعة القاهرة، 2009، ص 152– 153.

16- المرجع نفسه، ص 153.

17- اللجنة الدولية للصليب الأحمر، تقرير عن القانون الدولي الإنساني ...، المرجع السابق، ص 44.

18- زكي محمود، الروبوت المقاتل الأمريكي والحرب العراقية، الطبعة الأولى، دار الروضة للنشر والتوزيع، دون بلد نشر، 2003، ص 43– 44.

19- المرجع نفسه، ص 44.

20- تعتبر الحرب الأمريكية في فيتنام أول استخدام فعلي للطائرات الموجهة بدون طيار ونفذت حوالي 3000 عملية فوق فيتنام. انظر: زكي محمود، المرجع السابق، ص 46.

21- صفات أمين سلامة، أسلحة حروب المستقبل بين الخيال والواقع، مركز الإمارات للدراسات والبحوث الاستراتيجية، العدد 112، ابو ظبي، 2005، الطبعة الأولى، ص 24.

22- بيتر سينجر، الحرب عن بعد: دور التكنولوجيا في الحرب، الطبعة الأولى، مركز الإمارات للدراسات والبحوث الاستراتيجية، أبو ظبي، 2010، ص 60.

23- أ.ي. بالي و ن.ب. مارين، ترجمة يوسف ابراهيم الجهماني، موسوعة الحرب الالكترونية، دار الحوار، سوريا، 1992، الطبعة الأولى، ص 402– 403.

24- بيتر سينجر،" دروس الحروب الماضية والاتجاهات التكنولوجية المستقبلية" ...، المرجع السابق، ص 79.

25- عادل عبد الصادق محمد الجخة، أثر الإرهاب الالكتروني...، المرجع السابق، ص 151– 152.

26- عبد الكريم محمود برم، التقنية في الحرب: البعد الالكتروني، مركز الإمارات للدراسات والبحوث الإستراتيجية، أبو ظبي، 2010، الطبعة الأولى، ص 252.

27- المرجع نفسه، ص 255.

28- Philip Spoerri, «le droit international humanitaire et les nouvelles technologies de l'armement: table ronde sur les sujets actuels du droit international humanitaire: San Remo 8-10 septembre 2011», in guerre et nouvelles technologies, revue internationale de la croix rouge, volume 94, n° 886, 2012, p 583.

29- اعتمدت المادة 8 مكرر من النظام الأساسي للمحكمة الجنائية الدولية بموجب القرار RC/Res 6 المعتمد بتوافق الآراء في الجلسة العامة الثالثة عشر بتاريخ 11 حزيران 2010 من خلال المؤتمر الاستعراضي بكامبالا.

30- د. محمد سعادي، المرجع السابق، ص 193– 194.

31- المرجع نفسه، ص 196– 197.

32- المرجع نفسه، ص 198.

33- عادل عبد الصادق محمد الجخة، أثر الإرهاب الالكتروني...، المرجع السابق، ص 223.

34- راجع المادة 51 من ميثاق الأمم المتحدة.

35- د. محمد سعادي، المرجع السابق، ص 200.

36- عادل عبد الصادق محمد الجخة، حروب المستقبل: الهجوم الالكتروني على برنامج إيران النووي، السياسة الدولية، العدد 184، أبريل 2011، ص 102.

37- ربيع محمد يحي، المرجع السابق، ص 70.

38- المرجع نفسه، ص 70.

39- جيل برعام، تأثير تطور تكنولوجيا الحرب السيبرانية على بناء القوة في إسرائيل، ترجمة يولا البطل، مؤسسة الدراسات الفلسطينية، 2013، ص 14.

40- ريتشارد كلارك و روبرت نيك، حرب الفضاء الالكتروني: التهديد التالي للأمن القومي وكيفية التعامل معه، مركز الإمارات للدراسات والبحوث الاستراتيجية، أبو ظبي، 2012، الطبعة الأولى، ص 59.

41- عادل عبد الصادق محمد الجخة، أثر الإرهاب الالكتروني...، المرجع السابق، ص 177.

42- عبده مباشر، الحرب الالكترونية، دار المعارف، القاهرة، دون سنة نشر، ص 52.

43- مايكل ن. شميث، المرجع السابق، ص 89 – 90.

44- يشكل شرط مارتنز مبدأ أساسياً من مبادئ الحرب يحمل اسم القانوني الروسي "مارتنز".

45- Ahmed Abou-el- Wafa, «current value of customory international humanitarianlaw», revue egyptienne de droit international, vol 63, 2007, p 14.

46- مايكل ن. شميث، المرجع السابق، ص 91.

47- المرجع نفسه، ص 92.

48- المرجع نفسه، ص 93.

49- للتفصيل في مضمون "دليل تالين" انظر:

Michael N. S chmitt, tallinn manual on the international Law applicable to cyber warfare, first published, Cambridge university press, 2013.

50- اللجنة الدولية للصليب الأحمر، تقرير عن القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة ...، المرجع السابق، ص 42.

51- اللجنة الدولية للصليب الأحمر، ما هي القيود التي يفرضها قانون الحرب على الهجمات السيبرانية؟، أسئلة وإجابات، 2013، ص 1.

52- مصطفى نعوس، حق الدولة في استخدام القوة في الفضاء الالكتروني للدفاع عن النفس، مجلة الحقوق، العدد الأول، جامعة الكويت، 2014، ص 575.

53- اللجنة الدولية للصليب الأحمر، ما هي القيود التي يفرضها قانون الحرب على الهجمات السيبرانية... المرجع السابق، ص 1.

54- عادل عبد الصادق محمد الجخة، أثر الإرهاب الالكتروني على مبدأ استخدام القوة في العلاقات الدولية...، المرجع السابق، ص 180– 181.

55- المرجع نفسه، ص 205.

56- مصطفى نعوس، المرجع السابق، ص 578. وأيضا:

– Michael N. Schmitt, « international Law in cyberspace: the koh speech and tallinn manual juxtaposed », harvard international Law journal, volume 54, december 2012, p 18- 24.

57- يعد مبدأ التمييز أهم المبادئ الأساسية للقانون الدولي الإنساني ويقصد به" التزام الأطراف المتحاربة بالتمييز بين المدنيين والعسكرين، وبين الأعيان المدنية والأعيان العسكرية، وكذا التمييز في استخدام الأسلحة بما يضمن حدوث أقل الأضرار". للتفصيل في هذا المبدأ انظر: د. عمر سعد الله، القانون الدولي الإنساني: الممتلكات المحمية، ديوان المطبوعات الجامعية، الجزائر، 2008، ص 54– 56.

58- محمد عبد الحق شربال، الأسلحة الحديثة والقانون الدولي الإنساني، مذكرة ماجستير، كلية الحقوق، جامعة بن يوسف بن خدة، الجزائر، 2011، ص 74 – 75.

59- د. طارق المجذوب، الطائرات بلا طيار كوسيلة حرب: ملاحظات أولية عسكرية– قانونية، مجلة الجيش، العدد 332، لبنان، 23 مارس 2013، ص 11.

60- د. أسامة بن غانم العبيدي، التفتيش عن الدليل في الجرائم المعلوماتية، المجلة العربية للدراسات الأمنية والتدريب، المجلد 29، العدد 58، جامعة نايف العربية للعلوم الأمنية، الرياض، 2013، ص 122.

61- المرجع نفسه، ص 122.

62- د. طارق المجذوب، المرجع السابق، ص 12.

63- المرجع نفسه، ص 13.

64- Cordula Droege, «sortez de mon «cloud»: la cyberguerre: le droit international humanitaire et la protection des civils », in guerre et nouvelles technologies, revue internationale de la croix rouge, volume 94, n° 886, 2012, p 409.

65- Laura Baudin, le droit aujourd'hui: les cyber- attaques dans les conflits armés, l'harmattan, paris, 2014, p 162.