البعد الجديد ـ الخامس ـ في النزاعات المسلحة
ـ الفضاء الإلكتروني ـ

د. حسام عبد الأمير خلف
كلية القانون/جامعة بغداد

ملخص

يتحرك العالم الآن على إيقاع الفضاء الإلكتروني، من التجارة الى التنمية مرورا بالعمليات الحربية، فالفضاء الإلكتروني هو العنصر المميز للعصر الحالي. أن الزيادة الهائلة في استخدام التقنيات الإلكترونية في المجالات المدنية والعسكرية والتجارية منذ عام ٢٠٠٠ كشف لنا بيئة جديدة فيما يتعلق بالامن، حيث أصبح الفضاء الإلكتروني مجال جديد للحكوميين وغير الحكوميين الإسقاط السلطة، والتدخل في الشؤون الداخلية بأعتباره بديلا عن الحروب التقليدية. أن الهجمات الإلكترونية، التي شنت ضد استونيا عام ٢٠٠٧ وجورجيا في عام ٢٠٠٨ ومهاجمة المنشآت النووية الإيرانية بواسطة فيروس ستكسنت في عام ٢٠١٠، اظهرت اليوم أن الفضاء الإلكتروني هو أحد المجالات التي تعبر عن المصالح الجوهرية للدول كما هم الحال في المجالات البحرية والجوية وفي الفضاء الخارجي، في عالم اليوم، لم تعد الحدود البرية هي نفسها، كما أظهرت بوضوح خطر الحرب الإلكترونية باعتبارها بعدا جديدا في ميدان الحروب والتي اصبحت جزءا لا مفر منه في أي مناقشة حول الأمن الدولي.

La dimension nouvelle - Cinquième - dans les conflits armés
-Cyberespace-

Résumé

Aujourd'hui, le monde vit au rythme du cyberespace, du commerce au développement, en passant par les opérations de guerre, le cyberespace est un élément caractéristique de l'ère actuelle. La progression spectaculaire de l'utilisation des cybertechnologies dans les secteurs civils, militaires et commerciaux depuis 2000 a fait apparaître un nouvel environnement en matière de sécurité, où le cyberespace est devenu un nouveau domaine de projection de puissance gouvernementale et non gouvernementale et d'intervention aux affaires intérieures comme un substitut pour les guerres conventionnelles. Les cyber-attaques qui touchèrent l'Estonie en 2007 et la Géorgie en 2008 et à l'attaque des installations nucléaires iraniennes par le virus Stuxnet en 2010, a fait apparaître pour nous que le cyberespace est l'un des domaines qui reflètent les intérêts fondamentaux des Etats, comme ce est le cas dans les domaines maritimes et aériens, et dans l'espace extra-atmosphérique. Dans le monde d'aujourd'hui, les frontières terrestres ne représentent plus la même chose. Il nous montré aussi que les risques de cyberguerre sont clairement devenus un élément inévitable de toute discussion portant sur la sécurité internationale.

مقدمة

ألمذهب الاستراتيجي الكلاسيكية يميز بين أربعة أبعاد، كل منها يشير الى منطقة جغرافية، مادية، خاصة والتي من المرجح أن يندلع في نطاقها النزاع المسلح. كل من هذه الابعاد تثير عدد من المعوقات التي تشكل الخصائص المادية الخاصة بها، كما هو الحال في الحرب البرية، الحرب البحرية، الحرب الجوية واخيرا الحرب في الفضاء، فكل نوع من هذه الحروب يقابل ايضا، من وجهة النظر الاستراتيجية، بعدا خاصا ومحددا: الأرض؛البحر؛ الجو والمساحات الخارجة عن الغلاف الجوي. هذه الابعاد الكلاسيكية في العلوم العسكرية تشير الى مجموعة من النصوص الخاصة في القانون الدولي والتي، تدريجيا، اطرت سير الاعمال العدائية في كل من هذه الابعاد.

فيما يتعلق بقانون النزاعات المسلحة، نجد أن هناك قواعد منظمة لكل بعد من هذه الأبعاد الأربعة كما هو الحال بالنسبة الى الاعلان الذي ينظم النقاط المختلفة للقانون البحري في ١٦ نيسان عام ١٨٥٦، الأنظمة المتعلقة بقوانين وأعراف الحرب البرية، اتفاقية لاهاي ١٨ تشرين الأول ١٩٠٧، أو ايضا، القواعد المتعلقة بمراقبة التلغراف اللاسلكي في وقت الحرب، والحرب الجوية التي وضعتها لجنة الحقوقيين في لاهاي (كانون الأول ١٩٢٢ شباط ١٩٢٣)، تشكل بعض الأمثلة من النصوص المحددة لأبعاد التقليدية والبحر والأرض والهواء[١]. أما بالنسبة الى المساحات الخارجة عن الغلاف الجوي، باعتبارها بعد خاص عسكري، لا يقابل ضرورة أعتماد نص يهدف إلى تنظيم شروط حرب الفضاء، وانما يتم تنظيم الموضوع من قبل هيئة المعاهدات التي إنشئت مبدأ، السماح لبعض الاستثناءات في الاستخدام السلمي للمساحات الخارجة عن الغلاف الجوي، كما هو الحال بالنسبة الى أحكام المواد ٤ من معاهدة المبادئ المنظمة لأنشطة الدول في ميدان استكشاف واستخدام الفضاء الخارجي، بما في ذلك القمر والأجرام السماوية الأخرى في ٢٧ كانون الثاني ١٩٦٧ [٢] والمادة ٣ من اتفاق عام

---

[1] HAMZA CHERIEF, Le cyberespace, « cinquième dimension » du droit des conflits armés ?

http://www.espritcorsaire.com/?ID=268/Hamza_Cherief/Le_cyberespace,_%C2%AB_cinqui%C3%A8me_dimension_%C2%BB_du_droit_des_conflits_arm%C3%A9s_?

[٢] تنص المادة ٤ من هذه المعاهدة على أن (تتعهد الدول الأطراف في المعاهدة بعدم وضع أية أجسام تحمل أية أسلحة نووية أو أي نوع آخر من أسلحة التدمير الشامل في أي مدار حول الأرض، أو وضع مثل هذه الأسلحة على أية أجرام سماوية أو في الفضاء الخارجي بأية طريقة أخرى. وتراعي جميع الدول الأطراف في المعاهدة قصر استخدامها للقمر والأجرام السماوية الأخرى على الأغراض السلمية. ويحظر إنشاء أية قواعد أو منشآت أو تحصينات عسكرية وتجريب أي نوع من الأسلحة وإجراء أية مناورات عسكرية في الأجرام السماوية...الخ). انظر في هذا الخصوص :

١٩٧٩ المنظمة لأنشطة الدول على سطح القمر والأجرام السماوية الأخرى يمكن الاستشهاد بها[١].

اضافة الى هذه الأبعاد الأربعة، هناك حاليا مجال أو بعد خامس، في التطبيق العملي، يتجسد في الفضاء الإلكتروني أو ما يعرف بأسم الفضاء السيبراني أو الأفتراضي. كما هو معروف، شهدت بلدان عديدة زيادة هائلة في الموصولية العالمية[٢] في وقت يتَّسم بتحولات اقتصادية وديمغرافية وبتزايد التفاوت في الدخل وتقييد الإنفاق في القطاع الخاص وانخفاض السيولة المالية، وقد لاحظ موظفو إنفاذ القانون ارتفاع مستويات الجرائم الإلكترونية ، حيث يستغل الأفراد والجماعات الإجرامية المنظمة الفرص الجديدة المتاحة لارتكاب الجرائم بغية تحقيق الأرباح والمكاسب الشخصية[٣]. فعلى الصعيد العالمي، تشمل الجرائم الإلكترونية طائفة

معاهدة المبادئ المنظمة لأنشطة الدول في ميدان استكشاف واستخدام الفضاء الخارجي، بما في ذلك القمر والأجرام السماوية الأخرى ، تم اعتمادها من قبل الجمعية العامة في قرارها ٢٢٢٢ (د-٢١) المؤرخ ١٩ كانون الأول/ديسمبر ١٩٦٦.

[١] تنص المادة ٣ فقرة ٢ من هذه الاتفاقية على ما يلي (يحظر أي تهديد بالقوة أو استخدامها أو الاتيان بأي عمل عدائي أو التهديد به على سطح القمر. ويحظر بالمثل استخدام القمر لارتكاب مثل هذا العمل أو توجيه أي تهديد من هذا النوع فيما يتعلق بالارض،والقمر، والسفن الفضائية...الخ)؛ اما الفقرة ٣ من نفس المادة فنصت (لا يجوز للدول الاطراف في هذا الاتفاق أن تضع في مدار حول القمر، أو مسار اخر متجه الى القمر أو دائرة حوله ، أجساما تحمل اسلحة نووية أو أي أنواع اخرى من أسلحة التدمير الشامل، أو أن تضع مثل هذه الاسلحة أو أن تستخدمها على القمر أو فيه) واخيرا منعت الفقرة ٤ (أنشاء قواعد ومنشات وتحصينات عسكرية، وتجريب أي نوع من الاسلحة واجراء مناورات عسكريةعلى القمر...الخ). أنظر الاتفاق المنظم لانشطة الدول على سطح القمر والاجرام السماوية الاخرى وقد اعتمد الاتفاق بموجب قرار ٦٨١/٣٤ للجمعية العامة للأمم المتحدة في ٥ كانون الأول ١٩٧٩. وافتتح للتوقيع ١٨ ديسمبر ١٩٧٩.

[٢] في عام ٢٠١١ ، يقدر عدد الموصولين بالإنترنت بما لا يقل عن ٢،٣ بليون نسمة، أي ما يعادل أكثر من ثلث مجموع سكان العالم، ويعيش أكثر من ٦٠ في المائة من جميع مستخدمي الإنترنت في البلدان النامية، و لا يتجاوز عمر ٤٥ في المائة من مجموع مستخدمي الإنترنت ال ٢٥ عاما. وبحلول عام ٢٠١٧ ، من المتوقع أن تناهز نسبة المشتركين في خدمة الإنترنت النقالة ذات النطاق العريض ٧٠ في المائة من مجموع سكان العالم. وبحلول عام٢٠٢٠ ، سيفوق عدد الأجهزة المتصلة بالشبكة ("الأشياء المتصلة بالإنترنت") عدد الناس بنسبة ستة إلى واحد، مما سيؤدي إلى تغيير المفاهيم الحالية للإنترنت . ففي عالم الغد المتسم بالموصولية البالغة، سيصعب تصوُّر وقوع "جريمة حاسوبية" وربما أيِّ جريمة أخرى لا تنطوي على أدلة إلكترونية تتعلق بالموصولية بواسطة بروتوكول الإنترنت. تقرير الجمعية العامة ، الوثيقة (UNODC/CCPCJ/EG.4/2013/2) في ٢٣ كانون الثاني ٢٠١٣، فقرة ٣ ، ص ٢.

[٣] تشير التقديرات إلى أنَّ مصدر أكثر من ٨٠% من الجرائم السيبرانية هو شكل من أشكال النشاط المنظم، حيث تقوم الأسواق السوداء للجرائم السيبرانية على دورة تتسم بإعداد البرامجيات الخبيثة والفيروسات الحاسوبية والتحكُّم بشبكات حاسوبية ("اعتداءات البوت نت") وتلقُّف البيانات الشخصية والمالية وبيع البيانات والمتاجرة بالمعلومات المالية . ولم

واسعة من الجرائم المرتكبة بدافع مالي والجرائم المتصلة بالمحتوى الحاسوبي، فضلا عن الأعمال التي تمس بسرية النظم الحاسوبية وسلامتها وقابلية النفاذ إليها[١].

أما في مجال الحروب، نجد أن التكنولوجيا قد تم تسخيرها باستمرار من اجل تقديم اختراعات تهدف الى تطوير وتعزيز استخدام القوة بين الدول. اليوم، هذه التطورات بلغت طفرة في التكنولوجيا المتقدمة مما أدى الى تغير طبيعة الحرب بوتيرة متسارعة، فالتكنولوجيا العسكرية التي أظهرتها قوات التحالف خلال حرب الخليج في عام ١٩٩١، وخاصة استخدام الأسلحة الحركية "الذكية" أو الموجهة بدقة، يشكل المظهر الأكثر المعترف بها علنا من "الثورة في الشؤون العسكرية" الناشئة وصولا الى الحرب الإلكترونية[٢] ، حيث أن فكرة الفضاء الإلكتروني اخذت تلعب دورا في الأمن الدولي والتي ظهرت اهميتها في هذه الحرب التي كانت فيها "أجهزة الكمبيوتر الشخصية تعم جميع طبقات القيادة وجميع وظائف العمليات القتالية" – مما أدى إلى "نقطة تحول في التفكير العسكري عن الحرب الإلكترونية"[٣].

أن الهجمات الإلكترونية اخذت تثير العديد من المسائل القانونية التي هي في غاية الاهمية، في ظل غياب وجود قواعد محددة لتنظيم هذا البعد الجديد في الحرب: هل هي استعمال غير مشروع للقوة؟ هل الهجمات الإلكترونية تنتهك حظرا عاما على استخدام القوة؟ هل يصل هذا النوع الهجمات الى عتبة "الهجوم المسلح" الذي يقوم بتشغيل الحق في الدفاع عن النفس بموجب المادة ٥١ من ميثاق الأمم المتحدة؟ مدى التمييز بين الأهداف المدنية والعسكرية ام انها تجري بشكل عشوائي؟

يعد مرتكبو الجرائم السيبرانية بحاجة إلى مهارات أو تقنيات معقدة. ففي البلدان النامية بصورة خاصة، ظهرت شبكات فرعية تضم شبانًا يرتكبون أعمال احتيال مالي بالحواسيب، بدأ كثيرون منهم بالتورط في الجرائم السيبرانية في أواخر سنوات المراهقة. دراسة شاملة عن مشكلة الجريمة السيبرانية والتدابير التي تتَّخذها الدول الأعضاء والمجتمع الدولي والقطاع الخاص للتصدِّي لها، تقرير الجمعية العامة، الوثيقة (UNODC/CCPCJ/EG.4/2013/2) في ٢٣ كانون الثاني ٢٠١٣، فقرة ٥ ، ص ٣.

[١] المصدر السابق.

[2] Brian T. O'Donnell and James C. Kraska, HUMANITARIAN LAW: DEVELOPING INTERNATIONAL RULES FOR THE DIGITAL BATTLEFIELD, Journal of Conflict and Security Law, Vol. 8, Issue 1 (April 2003),p.135.

[3] Liannej.M. Boer, 'Restating the Law "As It Is": On the Tallinn Manual and the Use of Force in Cyberspace, Amsterdam Law Forum VOL 5:3, 2013,p.4

هدف هذا ألبحث هو الأجابة على الأسئلة ألمطروحة مع بيان لهذا الوجه الجديد من الحروب، حيث تم تخصيص المبحث الأول لتوضيح مفاهيم الفضاء الإلكتروني والحروب التي تجري في هذا النطاق. بعد ذلك، كرس المبحث الثاني الى الموضوع الأساسي المتعلق بمدى مشروعية القوة الإلكترونية أو الحاسوبية، مع بيان مدى امكانية تطبيق قواعد القانون الدولي الانساني في هذا الخصوص.

المبحث الأول
تحديد مفاهيم

أن أي تحقيق في معنى الحرب الإلكترونية يجب أن يبدأ النظر اولا في الفضاء الإلكتروني، بأعتباره البعد الجديد في حروب أليوم، ومن ثم سوف نتطرق الى مضمون هذا النوع من الحروب.

أولا: مفهوم الفضاء الإلكتروني

١. لمحة تاريخية عن الفضاء الإلكتروني

أن الإنترنت هو نتيجة ثانوية للعلوم والتكنولوجيا في سباق الحرب الباردة، فبعد الحرب العالمية الثانية، تصاعد التوتر بسرعة بين الولايات المتحدة والاتحاد السوفياتي، وشكل إطلاق الاتحاد السوفييتي للقمر الصناعي سبوتنيك عام ١٩٥٧[١] إنذار خاصا في الولايات المتحدة، حيث غير هذا إلاطلاق من تصور العالم من الولايات المتحدة كقوة تكنولوجية عظمى، وخلق شعور الضعف بين الشعب الأمريكي، ورفع المكانة الدولية للاتحاد السوفيتي. أن هذا الأمر، أضافة الى تهديد الحرب النووية التي كانت تخيم على البلاد، قد دفع الحكومة الأمريكية إلى تغيير في الإستراتيجية التي أكدت على التكنولوجيا والعلوم، من اجل تقليص الفجوة الملحوظة، حيث صرفت الأموال في العلوم والهندسة والرياضيات والتعليم والبحث على جميع المستويات. من بين المبادرات العديدة، انشأت الولايات المتحدة ومولت وكالة مشاريع البحوث المتقدمة Advanced Research Projects Agency (ARPA) التابعة لوزارة الدفاع بعد بضعة أشهر من إطلاق سبوتنيك، وكانت مهمتها المحافظة على التفوق التقني العسكري للولايات المتحدة ومنع "المفاجأة التكنولوجية"، ولقد ارادت إثبات قدرتها من خلال انشاء شبكة الإنترنت[٢].

كان أبرز مايقلق ألجيش الأمريكي، هي القدرة النظرية لتوجيه ضربة نووية من قبل الاتحاد السوفيتي لتعطيل أنظمة الاتصالات الأمريكية تماما، لا سيما أن هيكل القيادة والسيطرة في الحكومة الأمريكية والجيش لا يمكن أن يصمد أمام مثل هذا الهجوم، وبالتالي، رأى محللون

---

[١] سبوتنك-١ (بالروسية спутник1)هو أول قمر صناعي يسبح في الفضاء، أطلقه الاتحاد السوفييتي السابق في يوم ٤ تشرين الأول عام ١٩٥٧ ضمن سلسلة الأقمار الصناعية السوفياتية ، اعتبر هذا القمر الصناعي سبقًا حققه الاتحاد السوفييتي ضد الولايات المتحدة الأمريكية في إطار الحرب الباردة التي لم تكن تشمل إظهار القدرة العسكرية فقط، بل تعددت ذلك إلي إظهار القدرة التقنية والبحثية لكلا الدولتين، وكان إطلاق هذا القمر الصناعي بداية لسباق الفضاء بين القوتين العظميين.

[2] Michael Gervais, Cyber Attacks and the Laws of War, berkeley journal of international law, Vol. 30:2, 2012،p.527

عسكريون ضرورة أنشاء شبكة اتصالات قوية من شأنها ألصمود في أي مواجهة نووية، إذ كان العنصر الحاسم، الذي يشكل مصدر البقاء، هو تقنية ما تسمى "ألاتصالات الموزعة"، وهي موجودة تحت أنظمة ألأتصالات التقليدية، مثل شبكات الهاتف، أي عملية تحويل البيانات من مدخلات الانتاج.[١]

ردا على هذا التهديد، ألباحث في مركز أبحاث سلاح الجو، ومؤسسة راند[٢]، پول باران Paul Baran ، تصور نظام توزيع يتكون من العقد ذات تبديل متعددة مع العديد من الروابط المرفقة. فبموجب نظام باران، إذا فشلت عقدة واحدة، فهذه المعلومات ليس لها سوى اتخاذ طريق بديل، هذا التكرار جعل قطع الخدمة للمستخدمين أكثر صعوبة، علاوة على ذلك، اقترح باران تحديد مكان وجود العقد بعيدة عن المراكز السكانية لجعل النظام أكثر أمنا[٣]. ألأمر المهم في ذلك، وذات العلاقة بموضوعنا، هو خلق باران لتقنية التبديل بهدف نقل البيانات عبر الشبكة، والذي شكل الأساس الذي تقوم عليه فكرة الإنترنيت أليوم، الذي يمثل مسرح الصراعات الحالية. لكن، مع الاندماج المتزايد بين أجهزة الكمبيوتر في حياة الأفراد جعل نقاط الضعف في الفضاء الإلكتروني واضحا على نحو متزايد أيضا[٤]، خصوصا اذا ما علمنا، أن شبكة الإنترنت يتم تقاسمها بالكامل بين الاستخدامات المدنية والعسكرية في آن واحد، حيث تصاعد استغلال نقاط الضعف من خلال استخدام البرمجيات الخبيثة لارتكاب الجرائم الإلكترونية، الذي ترافق مع نمو الحوسبة الشخصية والإنترنت مما ادى الى ازدياد عدد وتأثير الجهات الفاعلة السيئة بشكل كبير.

٢. تعريف الفضاء الإلكتروني

---

[1] Michael Gervais, Cyber Attacks and the Laws of War …*op.cit.*،p.527.

[٢] مؤسسة راند RAND Corporation هي أكبر مركز فكري في العالم، ومقرها الرئيس في ولاية كاليفورنيا الأمريكية. وتقوم مؤسسة راند، الذي اشتق اسمها من اختصار كلمتي (البحث والتطوير Research and Development) ، بجمع أكبر قدر ممكن من المعلومات، ومن ثم تحليلها وإعداد التقارير والأبحاث التي تركز على قضايا الأمن القومي الأمريكي في الداخل والخارج. يعمل في المؤسسة ما يقارب من ١٦٠٠ باحث وموظف يحمل غالبيتهم شهادات أكاديمية عالية.

[3] Michael Gervais, Cyber Attacks and the Laws of War …*op.cit.*،p.528.

[٤] لقد شاع الإنترنت للاستهلاك الجماهيري من خلال التطبيقات المتعددة التي يوفرها، مثال البريد الإلكتروني، الشبكة العالمية، ملف نقل، ومجموعة كبيرة من البرامج الأخرى التي تربط المستخدمين إلى ما يعرف ب "الفضاء الإلكتروني". وعلاوة على ذلك، مع ظهور الحواسيب الشخصية ومقدمي خدمة الإنترنت (ISP)، الذي ربط المستخدمين بالإنترنت من خلال المجال العام، بدأت الشبكات الأخرى للاتصال مع بعضها البعض.

أن مصطلح الفضاء الإلكتروني(cyberspace) أستخدم لأول مرة من قبل ويليام جيبسون William Gibson في رواية Neuromancer عام ١٩٨٤ التي تتناول قراصنة الكمبيوتر، في هذا السياق، تم استخدم هذا المصطلح للإشارة إلى بيئة افتراضية مشتركة التي تشمل السكان، الأشياء والأماكن التي تتضمن البيانات المرئية التي بالإمكان سمعها ولمسها. من الواضح، هذا التعريف الأدبي تغيير على مر الوقت ليقابل مفهوم الفضاء الإلكتروني الذي يتجسد في المودم اليوم[١].

يرتكز مفهوم الفضاء الإلكتروني على مصطلح علم التحكم الآلي، وقد وصل في لغتنا في منتصف ١٩٩٠، ويعرف بانه جميع البيانات الرقمية التي تشكل الكون من المعلومات التي تكون على اتصال ومترابطة مع كافة أجهزة الكمبيوتر في العالم وذلك بفضل تقنيات الإنترنت[٢]. أما بالنسبة إلى قاموس الكمبيوتر، فيحدد الفضاء الإلكتروني بأنه (الفضاء الافتراضي المتكون من قبل أجهزة الكمبيوتر، أو بينهما في حالة وجود الشبكية)[٣]، أما Greg Rattray ، في مؤلفة الحرب الإستراتيجية في الفضاء الافتراضي، فقد عرف الفضاء الإلكتروني باعتباره (النطاق المادي الناتج عن إنشاء نظم وشبكات المعلومات التي تسمح بالتفاعلات الإلكترونية، فالفضاء الإلكتروني هو البيئة التي تم إنشاؤها من قبل الإنسان، لإنشاء، نقل واستخدام المعلومات في مجموعة متنوعة من الأشكال)[٤]. كما هناك من يعرفه، بأنه المجال المجازي لأنظمة الحاسوب والشبكات الإلكترونية؛ حيثُ تخزن المعلومات إلكترونيًا وتتم الاتصالات المباشرة على الشبكة. لذا فهو عالم غير مادي يشمل مواضيع مثل المعلومات الشخصية، المعاملات الإلكترونية، الملكية الفكرية وغيرها من المواضيع ذات الصلة[٥]. أما في

---

[1]Bradley Raboin , Corresponding Evolution: International Law and the Emergence of Cyber Warfare, Journal of the National Association of Administrative Law Judiciary -31-2, Fall 2011,p.٦٠٧. And, Keith Nicholson, INTERNATIONAL COMPUTER CRIME: A GLOBAL VILLAGE UNDER SIEGE, NEW ENGLAND SCHOOL OF LAW, 1997, p.39.

[2]François Silva, Être e-DRH : postmodernité, nouvelles technologies et fonctions RH, Editions Liaisons, France ,٢٠٠٨ p.٤٨

[3]Daniel Ventre, Cyberespace et acteurs du cyber conflit, Lavoisier, Paris, 2011, p.14.

[4]Daniel Ventre...*op.cit.*, p.63.

[5]لجنة الإسكوا للتشريعات السيبرانية، انظر الموقع الالكتروني:

http://isper.escwa.un.org/FocusAreas/CyberLegislation/tabid/157/language/ar-LB/Default.aspx.

داخل الولايات المتحدة، فأن تعاريف الفضاء الإلكتروني تختلف من دائرة حكومية إلى أخرى، فقد وصفت وزارة الدفاع الفضاء الإلكتروني بأنه "مجال عالمي ضمن بيئة المعلومات التي تتكون من شبكة مترابطة من البنى التحتية لتكنولوجيا المعلومات، بما في ذلك الإنترنت وشبكات الاتصالات السلكية واللاسلكية، وأنظمة الكمبيوتر، والمتضمنة المعالجات وأجهزة التحكم." في هذه الأثناء، صدر عام ٢٠٠١ من قبل خدمة أبحاث الكونغرس Congressional Research Service (CRS) تقرير تم بموجبه إعادة تعريف الفضاء الإلكتروني بكونه (الترابط الكلي للبشر من خلال أجهزة الكمبيوتر والاتصالات السلكية واللاسلكية دون النظر إلى الجغرافية المادية). أخيرا، الإستراتيجية العسكرية القومية لعمليات الفضاء الافتراضي اقترحت التعريف التالي: (مجال يتميز باستخدام [أجهزة الكمبيوتر والأجهزة الإلكترونية الأخرى] لتخزين وتعديل وتبادل البيانات عن طريق أنظمة الشبكات والبنى التحتية المادية المرتبطة بها).[١]

ثانيا: مفهوم الحرب الإلكترونية

أن مصطلح الحرب الإلكترونية كثيرا ما يختلط بمصطلحات اخرى، تكون بعيده عن مجال النزاع المسلح، الأمر الذي يقتضي تمييزه عن المفاهيم الاخرى، اضافة الى تحديد العنصر الاساسي في هذه الحرب.

١. تعريف الحرب الإلكترونية

أن مفاهيم "الحرب الإلكترونية "، "الاعتداء الإلكتروني" و "النزاع الإلكتروني " لم يتم تعريفها بشكل محدد في القانون الدولي، إذ ليس هناك سوى تعريف تقليدي واحد فقط الذي وضعته منظمة شانغهاي للتعاون [٢]، وهو يتعلق بمفهوم أوسع يتعلق ب (حرب المعلومات)، الذي يعرف بأنه (اشتباك بين دولتين أو أكثر من الدول، تهدف إلى الإضرار بالأنظمة ومصادر التكنولوجيا بهدف نقل الضرر الى الانظمة السياسية، الاقتصادية، الاجتماعية، ودفع

---

[1] Bradley Raboin, Corresponding Evolution: International Law and the Emergence of Cyber Warfare, Journal of the National Association of Administrative Law Judiciary -31-2,Fall 2011,p.٦٠٨.٦٠٧ .

[٢] منظمة شانغهاي للتعاون هي منظمة غير حكومية اقليمية تضم كل من روسيا، الصين، كازاخستان، قرغيزستان، طاجيكستان ، أوزبكستان و تركيا منذ سنة ٢٠١٤ ، تأسست في عام ٢٠٠١ في شنغهاي.

الحشود إلى زعزعة الاستقرار في المجتمع والدولة، وأيضا لإجبار الدولة على اتخاذ قرارات في مصلحة طرف معاد)[1].

كما يلاحظ مايكل شميت Michael Schmitt، أن مصطلح "حرب المعلومات"، غالبا ما يساء استخدامه، فحرب المعلومات تتعلق فقط بعمليات تكنولوجيا المعلومات في أوقات النزاع المسلح وتستبعد كل تلك التي أجريت في وقت السلم.

تطبيقا لهذا المبدأ في مجال العمليات الإلكترونية، فأن مصطلح "الحرب الإلكترونية"، "الاعتداء الإلكتروني" و "الإنترنت" يجب أن تكون محفوظة للنزاعات المسلحة في إطار القانون الدولي الإنساني. أما التهديدات التي يشكلها الفضاء الإلكتروني للأمن والتي لا يمكن اعتبارها نزاع مسلح، فيمكن أن تعتبر ضمن نطاق "الجرائم الإلكترونية"؛ "العمليات الإلكترونية"؛ "التجسس الإلكتروني " أو، عند الاقتضاء، "الإرهاب الإلكتروني" أو "القرصنة الإلكترونية"، ولكن ينبغي في أي حال من الأحوال، أن لا تناقش مع الشروط التي يمكن أن تثيرها تساؤلات أو استفسارات حول انطباق قانون النزاعات المسلحة[2].

أما على المستوى الوطني، فهناك بعض التعريفات المختلفة، على سبيل المثال، داخل الولايات المتحدة، عرفت وزارة الدفاع الهجوم في دليل الجيش الامريكي DCSINT رقم ١,٠٢ الهجوم لإلكتروني بأنه :(الاستخدام المتعمد للأنشطة التخريبية، أو التهديد بها، ضد أجهزة الكمبيوتر و / أو الشبكات، بقصد إلحاق الأذى بأهداف اجتماعية ؛ أيديولوجية ؛ دينية ؛ سياسية أو ما شابه ذلك. أو لترويع أي شخص لتنفيذ مثل هذه الأهداف)[3]، أما في تقرير خدمة أبحاث الكونغرسCRS لعام ٢٠٠١، فقد تم تقديم تعريفا أكثر عمومية: (الحرب الإلكترونية يمكن استخدامها لوصف مختلف جوانب الدفاع والهجوم المعلومات وشبكات الكمبيوتر في الفضاء الإلكتروني، وكذلك حرمان قدرة الخصم على أن تحذو حذوها)[4].

---

[1]Nils Melzer, *Les cyber-opérations et le jus in bello*, dans, Faire face aux cyberconflits, le Forum du désarmement, Institut des Nations Unies pour la recherche sur le désarmement (UNIDIR) United Nations, Geneva, 2012, p.3.

[2] Nils Melzer…,*op.cit.*p.3-4.

[3]Michael Gervais, Cyber Attacks and the Laws of War…*op.cit.*p.533.

[4]Bradley Raboin…,*op.cit.*p.٦٠٩ .

في نهاية المطاف، الحرب الإلكترونية، بغض النظر عن تعريف محدد مستخدم، أصبحت رمزا لاستخدام الدولة الأسلحة تعمل ضمن مجال الفضاء الإلكتروني والتي ترمي الى إحداث مشاكل واثار مدمرة في العالم الحقيقي.

٢. أسلحة الحروب الإلكترونية

أن الأسلحة الإلكترونية أصبحت تستخدم بشكل متزايد ضد أهداف عسكرية ومدنية، ومن المهم معرفة أن الأسلحة الإلكترونية تأتي في الواقع في شكلين مختلفين: الأول هو طريقة التسليم الفعلي الأسلحة، وهو جهاز قياسي مستخدم فعليا بمثابة بوابة الإلكترونية التي يتم من خلالها تنسيق الهجمات لإلكترونية والأسلحة لإلكترونية التي تم تأسيسها[١]. أما النوع الثاني من الأسلحة الإلكترونية هو عنصر الفضاء الإلكتروني. هذه الأسلحة غير الملموسة يحتمل أن تكون مؤلفة من برامج الكمبيوتر، شبكة الفيروسات، وقيادة عمليات رقمية. على الرغم من التطور المستمر، فأن الأنواع الأكثر شيوعا من ألأسلحة لإلكترونية، بما في ذلك وظائفها الأساسية، والقدرات، والاستخدامات، ترد في أدناه[٢].

(١)الحرمان من الخدمة

هجوم الحرمان من الخدمة Denial-of-Service (DoS) يعرف بأنه (اعتداء على الشبكة من خلال إغراقها بسيل من البيانات غير اللازمة او طلبات إضافية ما يسبب بطء الخدمات أو توقفها تماما) .عموما، هجمات DOS تعمل من خلال شل موارد الموقع الإلكتروني على شبكة الانترنت أو شبكة الكمبيوتر، وجعلها غير صالحة للاستعمال من قبل الأكثرية المستعملة لهذا المورد مع كمية هائلة من طلبات الحصول على المعلومات، مما يؤدى إلى عدم القدرة على الاستجابة للمعلومات المشروعة وطلبات الحصول على البيانات.

أن نشر هجوم –الحرمان من الخدمة(DOS) يعمل على نحو مماثل لهجوم حجب الخدمة القياسية، ولكنه ينطوي على التنسيق واستخدام العديد من أجهزة الكمبيوتر المصابة قبل العمل في انسجام تام لتعطيل شبكة الكمبيوتر المستهدفة أو الخدمة. على وجه التحديد، المعتدي

---

[١]يقصد بذلك أنه يأخذ الأجهزة الموجودة داخل العالم المادي من واقع الحياة اليومية، مثل أجهزة الكمبيوتر، وأجهزة المودم، وكابلات التوصيل لبناء ونشر هجوم عبر الانترنت. وثمة طريقة لمنع مثل هذه الهجمات سيكون تدمير هذه الأجهزة المادية التي هي في مجال الفضاء الإلكتروني

[2]Bradley Raboin…*op.cit.* p.610-611.

يستخدم الآلاف من أجهزة الكمبيوتر المصابة ألمعروفه باسم زومبي (zombies)[1] لمهاجمة نظام واحد في وقت واحد [2]. هجمات DDoS تبقى جذابة وسلاح فعال في الحرب الإلكترونية لأنها تزيد أضعافا مضاعفة عن قوة هجمات حجب الخدمة القياسية، وهي متوفرة بتكلفة منخفضة نسبيا.

بالأضافة الى ذلك، هناك هجوم حرمان دائم من الخدمة Permanent Denial-of-Service (PDoS)، هذا الهجوم يسبب أضرار جسيمة في النظام الأمر الذي يتطلب استبدال أو إعادة تثبيت الأجهزة. خلافا لهجوم دوس الذي يستخدم لتخريب خدمة أو موقع، أو كغطاء للتسليم البرامج الضارة، فأن هجوم PDoS يهدف بشكل محض الى تخريب الأجهزة[3].

(٢)البرامج الخبيثة[4]

البرامج الخبيثة، أو البرمجيات الخبيثة، تعمل عادة عن طريق (تعطيل وظائف الكمبيوتر العادية، أو عن طريق فتح باب خلفي لمهاجم بعيد من أجل ألسيطرة على جهاز الكمبيوتر)[5]. الفيروسات، هي الشكل الأكثر شيوعا من البرامج الخبيثة، قد تعمل لحذف ملفات معينة في الكمبيوتر أو جعل مثل هذه الملفات غير صالحة للأستعمال. على وجه التحديد، الفيروس يعلق نفسه على برنامج كمبيوتر أو ملف وينتشر من جهاز كمبيوتر إلى آخر، والانتقال عبر شبكات الكمبيوتر عن طريق التكرار الذاتي. بالإضافة إلى ذلك، أن الفيروس عادة يحمل (حمولة) التي تمثل أحد الآثار الجانبية للفيروس، وعادة يعمل على أفساد أو تدمير بيانات

---

[1] الحواسيب المصابة بفيروس zombie عادة ما يتم استخدامها لترسل أو تستضيف بريداً يحوي مواداً ممنوعة كاستغلال القاصرين، أو لتنظيم هجمات حجب الخدمة الموزعة distributed denial-of-service attacks كطريقة للابتزاز.

[2] Bradley Raboin…*op.cit.*,p.612.

[3] SCHAAP, ARIE J, CYBER WARFARE OPERATIONS: DEVELOPMENT AND USE UNDER INTERNATIONAL LAW, Air Force Law Review , Volume 64, 2009, p.135.

[4] تعود فكرة انشاء البرامج الخبيثة الى عالم رياضيات والمهندس المبكرلانظمة الحوسبة جون فون نيومان، حيث قام في عام ١٩٤٩، بتقديم سلسلة من المحاضرات النظرية في جامعة الينوي ، دعا فيها الى انشاء منظمة معقدة للتشغيل الذاتي، حيث تستكشف إمكانية تطوير الآلات ذاتية التكرار. فون نيومان تصور الآلات التي يمكن أن تبني نسخ ذاتية ، وهي تعتبر مقدمة لنظرية فيروس الكمبيوتر مودم اليوم. أن تكرار الذات هو السمة المميزة لفيروسات الكمبيوتر والديدان، فمن خلال تكرار الذات، يتم الانتشار في أجهزة الكمبيوتر أضعافا مضاعفة. أنظر المصدر :

Michael Gervais, Cyber Attacks and the Laws of War…,*op.cit.*, p.525.

[5] SCHAAP, ARIE J…*op.cit.*,p.135.

الكمبيوتر على جهاز الكمبيوتر المصاب. الفيروسات عادة لديها القدرة على البقاء بسرية موجودة في جهاز الكمبيوتر المصاب، ليصبح مدمرا فقط عند تشغيل المستخدم أو يفتح البرنامج الذي قد تم إدراج البرنامج الخبيث فيه[١]. النموذج المشترك ألأخر من البرامج الخبيثة هي الدودة Computer worm ، التي تؤدي وظائف مماثلة عن طريق الانتشار من كمبيوتر إلى آخر، وإصابة، في نهاية المطاف، شبكة الكمبيوتر بأكملها. مع ذلك، الدودة تختلف عن الفيروس بكونها اسرع منها كما انها قادرة على حد سواء الانتقال عبر نظام الحاسوب دون مساعدة من مستخدمي الكمبيوتر وأنها قادرة على تكرار نفسها مباشرة آلاف المرات داخل جهاز كمبيوتر واحد. الديدان تميل إلى تستهلك كميات هائلة من الذاكرة، ونتيجة لذلك، أجهزة الكمبيوتر المصابة، والشبكات، غالبا ما تصبح لا تستجيب. مع التطورات الأخيرة في مجال الانترنت، الديدان قد تمنح الآن الأفراد نفق في أنظمة الحاسوب والسيطرة من بعيد على الكمبيوتر المصاب[٢].

(٣)القنابل المنطقية

القنابل المنطقية، هي نوع أكثر تقدما من البرامج الخبيثة، وهي عبارة عن تعليمات برمجية ضارة مصممة بحيث تعمل عند حدوث أحداث معينة أو تحت ظروف معينة أو لدى تنفيذ أمر معين، وتؤدي إلى تخريب أو مسح بيانات أو تعطيل النظام[٣]. القنبلة المنطقية يمكن أن تبقى نائمة لفترات طويلة من الزمن لم تكن متصورة ومن ثم يتم تفعيلها، مما يجعل آثارها أكثر بكثير من أن تكون واسعة الانتشار. بمجرد تفعيلها، القنبلة المنطقية قد تسبب أضرارا بالغة لجهاز الكمبيوتر المصاب، مما يجعله غير صالح للاستعمال تماما، وحذف بيانات محددة، أو حتى تعمل لتنشيط أكثر تعقيدا لهجوم DOS[٤].

(٤) برامج الخداع

تعرف أيضا باسم أنتحال العنوان آبي Spoofing IP Adress وهو نوع من الاختطاف التقني الذي يسمح للمخترق المستخدم تشغيل الكمبيوتر في حين يظهر كمضيف موثوق به. أي أنه يؤدي إلى تضليل مستقبل المعلومات حيث يبدو انها مرسلة من جهة معينة في حين أنها في الواقع مرسلة من جهة أخرى؛ الأمر الذي يسمح بدخول المعلومة إلى الشبكة ويجعل

---

[1] Bradley Raboin…*op.cit.*p.613. And , SCHAAP, ARIE J…*op.cit.*,p.135-136.

[2] SCHAAP, ARIE J…*op.cit.*,p.136.

[3] SCHAAP, ARIE J…*op.cit.*, p.١٣٧.

[4]Bradley Raboin…*op.cit.*p.614.

مستقبلها يتعامل معها دون معرفة هوية مرسلها الحقيقي[١]، فمن خلال إخفاء الهويه الحقيقية، يمكن القراصنة الوصول إلى شبكات الكمبيوتر وموارد الشبكة. ففي اللحظة التي يتفاعل بها المستخدم مع أي من محتويات صفحة الويب الاحتيالية، يكسب المخترق اختطاف القدرة على الوصول إلى شبكة المعلومات الحساسة أو ميزات البرامج الأساسية للكمبيوتر[٢].

(٥)أحصنة طروادة

أحصنة طروادة، كما يوحي الأسم، تعمل كنوع من البرامج الضارة بناء على خداع أجهزة الكمبيوتر المستهدفة ودفعها إلى الاعتقاد أن برنامج خبيث سوف يؤدي، في الواقع، وظيفة مفيدة أو المطلوب منها. بدلا من ذلك، حصان طروادة يتمكن من الوصول الغير مصرح به إلى جهاز الكمبيوتر المصاب. في وقت لاحق، برامج حصان طروادة يسمح للمستخدم عن بعد ألوصول إلى الكمبيوتر المصاب ويمكن أن يسخر أيضا جهاز الكمبيوتر المصاب ليكون بمثابة مورد في وقت لاحق من هجمات DOS [٣]. يمكن لأحصنة طروادة أن تسبب أضرارا خطيرة عن طريق حذف الملفات وتدمير المعلومات على النظام، كما يمكنها أيضا إنشاء باب خلفي على أجهزة الكمبيوتر التي تتيح لمستخدمين البرنامج الخبيث الوصول إلى النظام، وربما السماح للتسوية المعلومات السرية أو الشخصية. على عكس الفيروسات والديدان، أحصنة طروادة لا تتكاثر عن طريق إصابة الملفات الأخرى كما أنها لا تكرر بالذات[٤].

(٦)التلاعب الرقمي

التلاعب بالصور الرقمية هو تغيير صورة باستخدام أدوات برنامج الحاسوب والبرمجيات لإنتاج صورة متفق عليها، الأمر الذي يعكس في كثير من الأحيان معنى جديدا. هذه التقنية تنطوي على الصور الموجودة بالفعل، مثل الصور الفوتوغرافية أو أشرطة الفيديو. في الاستخبارات والمجتمعات الأمنية تكمن مقاصد تغيير الصورة في التضليل أو الخداع. أن برمجيات التلاعب بالصور الرقمية قد ازدادت مع التطور التقني حيث أصبح الناس أكثر مهارة في استخدام البرنامج، وقد أصبحت مهمة الكشف عن التلاعب بالصور صعبة للغاية

---

[١] د. فاتن سعيد بامفلح ، حماية أمن المعلومات في شبكة المكتبات بجامعة أم القرى، دراسة حالة ص١٦. أنظر الموقع الالكتروني:

http://www.kau.edu.sa/Files/0012433/Researches/56927_27244.pdf.

[2] SCHAAP, ARIE J...*op.cit.*, p.13٧. And. Bradley Raboin...*op.cit.*p.61٥.

[3] Bradley Raboin...*op.cit,*.p615.

[4] SCHAAP, ARIE J...*op.cit.*, p.136.

والتلاعب الرقمي للصور الفوتوغرافية الآن متطورة بحيث يستحيل أحيانا تمييز ما إذا كان الناس أو الأشياء في صورة كانت هناك فعلا عندما تم التقاط الصورة[١].

من الامثلة على التلاعب الرقمي التي تعكس الحروب الالكترونية، في عام ٢٠٠٦، تم الكشف أن وسائل الإعلام تشارك في التلاعب بالصورة خلال الصراع بين اسرائيل وجماعة حزب الله اللبنانية. ومن المتصور تماما أن الدولة تشارك بسهولة في التلاعب بالصورة، وربما حتى تغيير الصور المعروضة على الانترنت من قبل الدول الأخرى[٢].

يبدو مما تقدم، أن الاسلحة الإلكترونية تتميز بمجموعة من الخصائص[٣]:

١. أنها لا تتطلب أي موقع محدد للأنطلاق (كمبيوتر ثابت أو محمول، الهواتف، ومواقع ألأنترنيت ...الخ)؛
٢. أنها يمكن إنشاؤها أو استخدامها في أي مكان، من قبل أي شخص، مع أو بدون دوافع محددة؛
٣. أنها تترك القليل من الوقت للتوقع، الوقاية ، الكشف أو الاستجابة نظرا لسرعة العمل الإلكتروني الهائلة ؛
٤. أنها عموما تستخدم العديد من أجهزة الكمبيوتر في العديد من البلدان لزيادة الكفاءة التشغيلية وتعقيد مهمة خبراء تقنية المعلومات.

أن هذه الأسلحة الرئيسية في الحرب الإلكترونية قد أصبحت، وعلى نحو متزايد، ممكن الوصول إليها من قبل عدد متزايد من الدول، حيث حددت ألدراسات الحديثة أن هناك، ونظرا للتكاليف المتواضعة للمشاركة في إجراء عمليات الحرب الإلكترونية الأساسية، ما يقرب من ١٤٠ دولة لديها برامج الحرب الإلكترونية التشغيلية[٤]. أن مدى توافر هذه الأسلحة، وآثارها ذات القدرة التدميريه الكبيرة التي من الممكن أن تسببها هذه الأسلحة على البنى التحتية الحساسة للعدو ، انما يدل على الأهمية القصوى لفهم الآثار القانونية المترتبة على الحرب الإلكترونية.

---

[1] SCHAAP, ARIE J...*op.cit.*, p.137.

[2] SCHAAP, ARIE J...*op.cit.*, p.138.

[3] Laurn Baudin , Les cyber – attaques dans les conflits armé: qualification juridique, imputabilité et moyens de réponse envisagés, L'Harmattan,Paris, 2014,p. ٤٥.

[4]Bradley Raboin...*op.cit.*p.616.

ثالثا: العمليات الإلكترونية في الصراعات الحالية

١. استونيا

خلال الحرب العالمية الثانية، وضع الاتحاد الأتحاد السوفيتي تمثال تذكاري من البرونز في عاصمة تالين لدولة استونيا، وقد وجد الاستونيين أن عرض هذا التمثال يمثل رمزا للاحتلال من قبل الاتحاد السوفيتي والقمع السياسي المرتكب في أعقاب الحرب العالمية الثانية، في حين أن روسيا تعتبر رؤية التمثال في استونيا بمثابة تحية للجنود السوفيت الذين سقطوا في الحرب . في نيسان من عام ٢٠٠٧، قررت السلطات في استونيا إزالة هذا التمثال المثير للجدل، وقد كانت نتيجة هذا القرار ليلتين من الاحتجاجات وأعمال الشغب الجماهيري في إستونيا المعروفة باسم (ليلة البرونزي)[١]. في الأسابيع التي تلت ليلة البرونزي، شهدت البنية التحتية الرقمية في استونيا هجوم الكتروني واسع النطاق منشؤها في الغالب روسيا، علما أن إستونيا تعتبر واحدة من أكثر الدول التي تعتمد على الإنترنت في العالم، ولقد استخدم "hacktivists"[٢] هجمات DDoS ضخمة لاستهداف خوادم الويب في استونيا وجعل حركة المرور في توقف تام، كما تضمنت الأهداف المحددة ايضا الأخبار والمواقع الحكومية[٣]. الهجوم ترك في نهاية المطاف الدولة في حالة من الفوضى، فبعد ساعات فقط من الهجوم، المواقع على شبكة الإنترنت من البنوك الرائدة في استونيا، والصحف، والوكالات الحكومية الرئيسية تحطمت، مما دفع البلاد الى العزلة في مجال الفضاء الإلكتروني. إستونيا تعتبر أول دولة تتعرض لهجوم منسق على نطاق واسع ضد أنظمة الكمبيوتر التي تديرها الدولة.

مما تجدر الاشار اليه، أن هذه الهجمات قد نشأت من عدة دول أخرى، بهدف التمويه، الامر الذي جعل تتبع المصدر النهائي مستحيلا[٤]. في نهاية المطاف، الهجوم على استونيا

---

[1] Bradley Raboin…*op.cit*.p.٦١٦.

[٢] كل شخص يكسب الوصول غير المصرح به إلى ملفات الكمبيوتر أو الشبكات من أجل تحقيق مزيد من الغايات الاجتماعية أو السياسية. أنظر الموقع الالكتروني المتعلق بقاموس اكسفورد:

http://www.oxforddictionaries.com/definition/english/hacktivist.

[3] Michael Gervais ,Cyber Attacks and the Laws of War, p.540. And, Marco Benatar , The Use of Cyber Force: Need for Legal Justification? Goettingen Journal of International Law 1.2009. p.376.

[٤] تجدر الاشارة هنا الى أن 30% من الهجمات كان مصدرها جامعات في كاليفورنيا في الولايات المتحدة الأمريكية بهدف التمويه عن المصدر الحقيقي لهذه الهجمات. أنظر :

اظهر عدة حقائق مثيرة للقلق، لا سيما فيما يتعلق بمسألة الإسناد في الهجمات الإلكترونية، وسهولة الهجمات الإلكترونية وتدمير العالم الحقيقي سببها هجمات نفذت فقط في مجال الفضاء الإلكتروني .

٢. جورجيا

بدأت الحرب الروسية الجورجية في ليلة ٧ آب ٢٠٠٨، بعد أشهر من التوتر المتصاعد، ولقد تميزت بداية الأعمال العدائية المفتوحة بأجراء قصف على بلدة أوسيتيا الجنوبية تسخينفالي من قبل الجيش الجورجي ردا على الإجراءات الانفصالية، حيث شنت هجمات جوية وبرية مفاجئة ضد القوات الثورية التي تقع في محافظات أوسيتيا الجنوبية وأبخازيا ، ولقد ردت روسيا بسرعة على حملة القصف بهجمة مرتدة ضخمة[١]. خلال هذه الحرب القصيرة، تم استخدام الهجمات الكترونية الى جانب الثالوث الحركي الذي تضمن هجمات جوية، أرضية وبحرية، الهدف الرئيسي من الحملة الإلكترونية كان لدعم الغزو الروسي لجورجيا من خلال استهداف البنية التحتية الحيوية. لقد كان حجم الهجمات الكترونية على مستوى عال من الاهمية، حيث تم مهاجمة ما يقارب أربعة وخمسين من المواقع الجورجية بصورة اجمالية[٢]، ولقد كانت جميعها تقريبا من شأنها أن تنتج فوائد للجيش الروسي. أن الهجمات الإلكترونية استهدفت مباشرة العناصر الإعلامية والاقتصادية للسلطة الوطنية، المواقع الحكومية، المؤسسات المالية الجورجية، جمعيات رجال الأعمال، بالاضافة الى موقع وزارة الخارجية الجورجية وغيرها من المواقع الحكومية الرئيسية بما في ذلك الرئاسة والوزارات والمحاكم والبرلمان، وقد شملت ايضا استهداف وسائل الإعلام ومرافق الاتصالات، والتي عادة ما قد تعرضت للهجوم من قبل صواريخ أو قنابل خلال المرحلة الأولى من الغزو، بهدف منع الوصول إلى الأخبار والمواقع الحكومية، بالإضافة إلى جعل الأمر أكثر صعوبة لإجراء تقييم الأضرار ساحة المعركة وتنسيق الاستجابات الفعالة. بالاضافة الى ذلك، كان للهجمات الكترونية آثار نفسية هامة من خلال خلق حالة من الذعر والارتباك في السكان المحليين. لقد كانت شدة الهجمات الإلكترونية

Laurn Baudin , Les cyber – attaques dans les conflits armé: qualification juridique, imputabilité et moyens de réponse envisagés, L'Harmattan,Paris, 2014,p. ٣٧.

[1] Bradley Raboin…*op.cit*.p.٦١٩-620.

[2] Handler, Stephenie Gosnell, New Cyber Face of Battle: Developing a Legal Approach to Accommodate Emerging Trends in Warfare, Stanford Journal of International Law, 48 Stan. J. Int'l L. 209 (2012) , p.224.

كافية لتدفع الحكومة الجورجية الى نقل خوادم لمواقع الحكومة على الانترنت الى كل من أستونيا والولايات المتحدة في محاولة لإحباط استمرار هجمات DDoS [1].

في الحقيقة ان القدرة على تحقيق التزامن بين كل من الهجمات الإلكترونية والهجمات العسكرية التقليدية يجعل من فعالية التدمير مزدوجة .

٣ . إيران

ستكسنت Stuxnet من البرامج الخبيثة التي تم استخدمها لمهاجمة منشأة لتخصيب اليورانيوم الإيراني في ناتانز، لقد تم الكشف عنه لأول مرة في حزيران ٢٠٠٩ من قبل الباحثين في أمن الحاسوب، وقد اكتشف العديد من إصدارات حتى منتصف عام ٢٠١٠. على الرغم من أن تعريف الأسلحة الالكترونية أمر دقيق، فان الخبراء في مجال الأمن الإلكتروني نظروا في هجوم ستكسنت باعتباره أول برهان ملموس على قدرة الأسلحة الالكترونية[2].

أن أجهزة الطرد المركزي المستخدمة في محطة ناتانز لتخصيب اليورانيوم كانت المستهدف الحقيقي من قبل ستكسنت، ومن أجل الوصول إلى هذه الاجهزة كان على ستكسنت أن يصيب أجهزة الكمبيوتر ذات العلاقة بالتحكم الصناعي المستخدمة في برمجة وسيطرة البرامج الآلية التي تسيطر على محولات تردد أجهزة الطرد المركزي. لقد قام ستكسنت باستغلال نقاط الضعف في نظام التشغيل مايكروسوفت ويندوز قبل إصابة الجهاز بأكمله، من خلال استغلال الثغرات في تطبيق البرمجيات المتعلقة بوحدات ألبرمجة الآلية، لكي تأمر محولات التردد بالإضرار بأجهزة الطرد المركزي.

مما تجدر الاشارة اليه، أن أجهزة كمبيوتر التحكم الصناعي التي كان يجب على ستكسنت إصابتها لم تكن متصلا مباشرة إلى شبكة الإنترنت، حيث أن بروتوكولها الأمني يسمح فقط باستخدام الوسائل المادية والكهربائية أو الكهرومغناطيسية لعزل الأنظمة الأخرى، ولا سيما الإنترنت، ولقد كان من الضروري، مع ذلك، السماح للمشغلين أو الشركات بتحديث البرمجيات لاجهزة الكمبيوتر وإرسال أو استرداد البيانات، وللقيام بذلك، كانوا يستخدمون، كما هو الحال في كثير من الأحيان، مفاتيح USB. لذلك، قد تم تصميم ستكسنت للاستفادة من

---

[1] Handler, Stephenie Gosnell…*op.cit*.p.224.

[2] Brian Weeden, *Incompatibilité entre les priorités offensives et défensives des États pour les cyber-activités, dans ,Faire face aux cyberconflits*, le Forum du désarmement , Institut des Nations Unies pour la recherche sur le désarmement (UNIDIR)United Nations, Geneva, 2012, p.21.

هذه العادة، حيث انه أصاب مفاتيح USB، مما ادى الى انتشار دودة بين أجهزة الكمبيوتر على ألشبكة ألمحلية. ستكسنت تم بثه من ثلاث موجات من الهجمات ضد خمس منظمات موجودة في إيران، ثم انتشر إلى العديد من الشبكات حتى وصل إلى أجهزة الكمبيوتر التحكم الصناعي المسئولة عن التنفيذ[١].

مطوري ستكسنت اتخذوا العديد من التدابير للحد من انتشاره، فعلى عكس غيره من البرامج الضارة، ستكسنت لم يكن دودة، فهو لم يكن مصمم للانتشار في أسرع وقت ممكن في الإنترنت، بل كان أنتشاره من خلال مفاتيح USB وضمن شبكة محلية وكل العنصر المصاب لا يمكن أن يصيب سوى ثلاثة أخرى من العناصر[٢]. ستكسنت كان يحتوي على التعليمات البرمجية التي تشير إلى أن (تدميره) يكون في ٢٤ حزيران ٢٠١٢[٣].

في الحقيقة، أن العوامل التي تفسر انتشار ستكسنت تكمن في نقطتين أساسيتين: الأولى، غياب تصحيح أو معالجة نقاط الضعف في ويندوز والأخرى تتعلق بطريقة استخدام مفتاح USB التي كانت غير آمنة وعلى نطاق واسع.

توخيا للدقة، إن كان ستكسنت أصاب جميع هذه الأنظمة، ليس هناك دليل على أنه أتلف أنظمة في أماكن أخرى غير إيران. أن تحليلات التعليمات البرمجية لستكسنت من قبل

---

[١]أن جميع أجهزة الكمبيوتر المصابة بستكسنت تستخدم مايكروسوفت ويندوز؛ البرنامج الخبيث استفاد من أربعة مآثر أو مجالات للاستغلال للوصول إلى "يوم الصفر" في نظام التشغيل Windows بالتسلل إلى الأهداف. النسخة الأولى من ستكسنت الذي اكتشف في حزيران ٢٠٠٩، استغل نقطة ضعف بتنفيذ التعليمات البرمجية عن بعد في التخزين المؤقت للطباعة ويندوز. مايكروسوفت لم ينشر التصحيح إلا في أيلول ٢٠١٠ لهذا الخلل الذي أكتشف في نيسان ٢٠٠٩ من قبل مجلة أمن المعلومات Hakin9 . ألنسخة ألجديدة من ستكسنت الذي اكتشف في آذار ٢٠١٠، استغلت نقطة ضعف تنفيذ التعليمات البرمجية عن بعد في طريقة Windows بمعالج ملفات الاختصار أو ألروابط. مايكروسوفت قامت بنشر إشعار أمني بخصوص هذه الثغرة في تمّوز ٢٠١٠ والتصحيح في الشهر التالي له. بعد تحليل ستكسنت، شركة أمن تكنولوجيا المعلومات سيمانتيك Symantec كشفت في جلسة خاصة لمايكروسوفت لاثنين من نقاط الضعف التي يمكن أن تؤدي إلى رفع الامتياز.

Brian Weeden, *Incompatibilité entre les priorités offensives et défensives des États pour les cyber-activités…op.cit.*p.21-22.

[٢]على الرغم من هذه القيود، في أيلول ٢٠١٠، ستكسنت قد أصاب أكثر من ١٠٠،٠٠٠ ضيف أو متلقي الطعم في ١٥٥ بلدا.

[٣]في تشرين الأول ٢٠١٠، شركة سيمنز أكدت أن ١٥ من عملائها الصناعيين في جميع أنحاء العالم – بما فيها المصانع الكيماوية، ومحطات الطاقة ومرافق الإنتاج – كانت قد "تأثرت" بواسطة ستكسنت. مع ذلك، نحن نجهل انه ما إذا كان هؤلاء العملاء، الذين استخدموا البرمجة الآلية في شركة سيمنز للسيطرة على أنظمة مختلفة، قد عانوا من الأضرار بسبب ستكسنت.

مجتمع أمن المعلومات خلصت إلى أن ستكسنت كان مبرمجا فقط للتشغيل ضد أجهزة الكمبيوتر التحكم الصناعية المستخدمة في أجهزة الطرد المركزي الإيراني في ناتانز.

إذا وكما رأينا، أن هذه الهجمات المتعلقة بالفضاء الإلكتروني لها عواقب هائلة على الدول المستهدفة، الأمر الذي يثير العديد من التساؤلات حول حق الدول المتضررة في استخدام القوة العسكرية؟ كذلك ، القانون الواجب التطبيق في هذه النزاعات الحديثة؟ لاسيما أنه لحد ألان لا يوجد نص محدد للتعامل مع هذه الأسلحة الجديدة.

المبحث الثاني
قوانين الحرب في الفضاء الإلكتروني أو الافتراضي

عندما كان مقبولا اللجوء إلى استخدام القوة ، فأن قوانين الحرب تحكم، في حدود المقبول في زمن الحرب، سلوك أطراف النزاع في حالة حدوث هجوم داخل إحدى الأبعاد الأربعة المتعارف عليها في مسرح الصراع. لكن السؤال الذي يطرح نفسه هو حالة حدوث هجوم خارج المسرح المحدد للصراع ، أي ضمن حدود الفضاء الافتراضي، فما هو حكم هذا الهجوم؟ وكيف تنطبق قوانين الحرب؟

في هذا المبحث سوف نحاول الوصول الى بعض الأجوبة، حيث تم تخصيص الجزء الأول منه إلى تحليل طبيعة الهجوم الإلكتروني، حول ما إذا كانت هذه الهجمات تنتهك الحظر العام على (استخدام القوة) بموجب المادة ٢ (٤) من ميثاق الأمم المتحدة، وهل تصل مثل هذه الهجمات إلى عتبة (الهجوم المسلح) الذي يقوم بدوره بتشغيل الحق في الدفاع عن النفس بموجب المادة ٥١ من الميثاق. أما الجزء الثاني من هذا المبحث، فسوف نتناول فيه كيفية تطبيق قانون النزاع المسلح على هذا البعد الجديد في النزاعات المسلحة.

أولا: طبيعة الهجمات الإلكترونية

أن الهجوم الإلكتروني برز كواحد من خيارات الأمن الوطني الواعدة والأكثر إتاحة لإنجاز المهمة والدفاع عن النفس، وهو يشمل أنشطة تهدف إلى (تعطيل ، منع، إضعاف أو تدمير المعلومات الموجودة في أجهزة الكمبيوتر وشبكات الكمبيوتر أو أجهزة الكمبيوتر والشبكات أنفسهم)[1]. أن بعض الباحثين يؤكدون أن استخدام شبكة الكمبيوتر في الهجوم يشكل استخدام القوة، في حين أن البعض الاخر يذهب إلى أن الهجوم له تأثير غير قسري. هذا النقاش أمر مهم ويعمل على صياغة القانون الدولي ، وهو يدفع إلى طرح الأسئلة التالية : هل الهجمات الإلكترونية تنتهك حظرا عاما على استخدام القوة؟ وهل يصل الهجوم الإلكتروني الى عتبة (الهجوم المسلح) الذي يقوم بتشغيل الحق في الدفاع عن النفس بموجب المادة ٥١ من ميثاق الأمم المتحدة؟

---

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

١. **هل الهجمات الإلكترونية تنتهك حظرا عاما على استخدام القوة؟**

ألمادة ٢ (٤) من ميثاق الأمم المتحدة تعلن أنه :

(يمتنع أعضاء الهيئة جميعا 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).

مع ذلك، يسمح الميثاق لاثنان من استثناءات على هذا الحظر، وهما: الحق في الدفاع عن النفس في حالة الهجوم المسلح فضلا عن استخدام القوة بتفويض من مجلس الأمن الدولي.

أن تحديد ما إذا كانت الهجمات الإلكترونية تنتهك هذا الحظر العام على استخدام القوة يتطلب أولا بيان ما هي القوة في الفضاء الالكتروني، وثانيا ما إذا كانت الهجمات الإلكترونية يمكن أن تصل إلى المستوى المناسب التبرير الدفاع عن النفس في ظل هذه المعايير.

أن نقطة الانطلاق في بدء هذا التحليل تكمن اتفاقية فيينا لقانون المعاهدات، التي تنص على قواعد لتفسير المعاهدات، فعلى الرغم من اعتمادها بعد الميثاق، يتفق خبراء القانون الدولي بصفة عامة على أن قواعد الاتفاقية تعكس القانون الدولي العرفي.

اتفاقية فيينا تنص على أنه :

(يجب أن تفسر المعاهدة بحسن نية ووفقا للمعنى العادي الذي يعطى لشروط المعاهدة في سياقها وفي ضوء موضوعها والغرض منها)[١].

المعنى العادي من (القوة) واسع ويشمل المفاهيم التقليدية للهجمات الحركية، فضلا عن غيرها من التدابير القسرية، على سبيل المثال: الأدوات المالية، أي منح أو حجب التسامح أو المهل للمطالبة بالديون للمنتفعين ؛ ألأدوات الدبلوماسية، أي التفاوض والدعوة بين ممثلي الدولة؛ ألأدوات ألإيديولوجية أو الدعائية، إي نشر علامات ورموز مختارة بعناية لقطاعات المجتمع ذات الصلة مع تخصيصها للتأثير على النخبة الحاكمة[٢]. بموجب قراءة واسعة لمفهوم (القوة)، فأن كل هذه الأدوات العسكرية، الاقتصادية، الدبلوماسية والأيديولوجية، قد تكون خاضعة للتنظيم بموجب الميثاق.

---

[١] المادة ٣١ من اتفاقية فيينا لقانون المعاهدات لسنة ١٩٦٩.

[2] Michael Gervais, Cyber Attacks and the Laws of War,p.٥٣٦.

مع ذلك، في ضوء (الهدف والغرض) من الميثاق، فأن (القوة) يجب أن تقرأ بصورة أكثر ضيقا، إذ أن الهدف الصريح من الأمم المتحدة هو الحفاظ على السلم والأمن الدوليين، فضلا عن (أن ننقذ الأجيال المقبلة من ويلات الحرب)، ويوحي مفهوم القوة في عام ١٩٤٥ اقتصاره على الصك العسكري فقط. أن تاريخ صياغة الميثاق يعزز هذا الاستنتاج، فخلال الأعمال التحضيرية قدم اقتراحا لتوسيع نطاق المادة ٢ (٤) إلى الصكوك الإستراتيجية الأخرى، تحديدا، الإكراه الاقتصادي، إلا أن الأمم المتحدة رفضت مثل هذا الاقتراح[1]. فمن خلال استبعاد، صراحة، الإكراه الاقتصادي من تعريف القوة في صياغة المادة ٢ (٤)، هناك إقرار ضمني برفض الأدوات الإيديولوجية والدبلوماسية كذلك.

أن الأسلحة الإلكترونية هي متعددة ويمكن أن تكون إما ممثل مساعد في مسرح الصراع أو الحدث الرئيسي، فهي ليست أسلحة متجانسة يمكن أن تؤدي إلى إجابات واضحة حول ما إذا كانت تنتهك الحظر المفروض على استخدام القوة. إضافة إلى ذلك، أن الآثار الضارة الناجمة عن الهجمات الإلكترونية لا تعد ولا تحصى الأمر الذي يجعل تصنيفها على حد سواء أكثر تعقيدا وأكثر ضرورة. في الحقيقة، أن آثار الهجمات الإلكترونية يمكن أن تتراوح من إزعاج بسيط (مثل هجوم دوس DDoS الذي يعطل حركة المرور على الشبكة مؤقتا)، إلى التدمير المادي (مثل تغيير الأوامر لمولد الطاقة الكهربائية الأمر الذي يؤدى إلى انفجارها)، وحتى الموت (مثل تعطيل خطوط الطوارئ لأول للمستجيبين بحيث لا يمكن إجراء مكالمات للشرطة أو خدمات الإسعاف). أن التعامل مع مختلف أشكال الهجمات الإلكترونية بمثابة استخدام القوة يتطلب قراءة واسعة للمادة ٢ (٤) يتضمن الضرر غير المادي.

في الحقيقة، توجد عدة نماذج ممكنة لتحديد ما إذا كان الهجوم الإلكتروني يرتفع إلى مستوى استخدام القوة.

النهج الأول في تحليل القوة هو فحص طريقة التسليم أو الألقاء. فبموجب هذا النموذج، يتم تصنيف ألاسلحة الإلكترونية من خلال طريقة محددة لتقديم هجوم على العدو، سواء كان هو فيروس، دودة، اقتحام الشبكة، أو بعض الهجمات الإلكترونية الأخرى، فحظر هذا النموذج للهجمات الإلكترونية يكون على أساس كيفية تنفيذها. فالأضرار الجسيمة التي يمكن ان تسببها أنواع معينة من الهجمات الإلكترونية في جميع أنحاء العالم بالمقارنة مع آثار محدودة

[1] Michael Gervais, Cyber Attacks and the Laws of War,p.٥٣٧.

لهجمات اخرى يوفر الأساس لهذا النهج. اذ هناك اسلحة الكترونية معينة هي بطبيعتها أكثر تدميرا وخطورة من غيرها[1].

النهج الثاني لتحليل القوة ينظر الى الأسلحة الإلكترونية بموجب نموذج صارم للمسؤولية، بموجب هذا النهج فأن أي استخدام للهجمات الإلكترونية ضد البنى التحتية الحرجة يكون أو يمثل استخدام القوة، حيث يؤذن بالدفاع عن النفس ضد الهجمات الإلكترونية التي تستهدف البنية التحتية الحيوية. ويجادل أنصار المسؤولية الصارمة بأنه النموذج المناسب بسبب الطبيعة المدمرة الآنية للهجمات الإلكترونية، والتي تخلق مستوى كاف من ضرر تبرر الدفاع عن النفس الاستباقي. أما الانتقادات التي وجهت الى هذا النموذج، أن آثار الهجمات الإلكترونية قد تكون عشوائية وغير منضبطة، كما أنها لا يستهدف دائما وعمدا البنية التحتية الحيوية التي قد تتعطل في نهاية المطاف، باعتباره نتيجة ثانوية[2].

المنهج الثالث لتحليل القوة يتناول الهجمات الإلكترونية كأدوات تعادل أسلحة الحركية التقليدية وذلك من خلال النظر إلى النتائج المباشرة للهجوم. فأذا كانت النتيجة تؤدي الى حظر استخدام القوة التي تسببها اسلحة حركية معينة، فيجب أن ينظر الى الاسلحة الإلكترونية بطريقة مماثلة. لذلك، فأن فالهجوم الإلكتروني هو استخدام للقوة إذا كان المهاجم يسعى إلى إحداث دمار مادي مباشر أو الإصابة أو الوفاة[3].

الخلل في هذا المنهج هي أن معظم الهجمات الإلكترونية لا تسبب أضرارا مادية مباشرة أو الموت، على سبيل المثال، لهجوم الذي يؤدي الى اغلاق مؤقت لخطوط الاتصال للشرطة الطوارئ وخدمات الإسعاف قد لا يسبب ضرر مادي أو حالة وفاة مباشرة، ولكن يمكن بسهولة أن تسبب ذلك بشكل غير مباشر على حد سواء، لذلك أن رسم خط بين الآثار المباشرة وغير المباشرة لهجوم الإلكتروني هو صعب للغاية.

مايكل شميت Michaël N. SCHMITT.N يفترض النموذج الذي حقق عنصر جذب من قبل فقهاء القانون، شميت ينادي بالنهج القائم على النتيجة. هذا الإطار يتطلب فحص ما إذا كانت النتائج المتوقعة إلى حد معقول من الهجوم الإلكتروني تشبه عواقب شن الهجوم التقليدي. يوفر شميت ستة معايير لتقييم عواقب الهجمات الإلكترونية على الدولة المستهدفة: الشدة، الفورية، المباشرة، الغزو، القابلية للقياس، والشرعية المفترضة. ذا أسهم

---

[1] Michael Gervais, Cyber Attacks and the Laws of War,p.٥٣٨.

[2] Michael Gervais, Cyber Attacks and the Laws of War,p.٥٣٨.

[3] Michael Gervais, Cyber Attacks and the Laws of War,p.٥٣٩.

الهجوم الإلكتروني بقواسم مشتركة كافية بين العوامل الستة، له ما يبرره من تمديد الحظر المفروض على القوة[1].

فبموجب معايير شميت، أن شدة هذا الهجوم الإلكتروني لا يرقى الى استخدام القوة، بينما كانت الهجمات الإلكترونية الفورية، وكانت النتائج ضئيلة، لا سيما اذا لم يكن هناك أي ضرر مادي أو معاناة للقياس، وانما تسبب هذه الاضطرابات في الغالب إزعاج مؤقت. على سبيل المثال، تعطل حركة المرور التي سببها هجوم ذي صلة غير مباشرة لتأثير قسري نتيجة قرار الحكومة الاستونية لإزالة التمثال، فعلى الرغم من أن هذا الهجوم يعتبر تدخلا غير شرعي، إلا أن النتائج الصافية لا تشبه فيه الكفاية لاستخدام القوة.

٢. هل يصل الهجوم الإلكتروني الى عتبة (الهجوم المسلح) الذي يقوم بتشغيل الحق في الدفاع عن النفس بموجب المادة ٥١ من ميثاق الأمم المتحدة؟

عندما يكون هناك صراع بين الدول، يطالب ميثاق الامم المتحدة من اعضائه (تسوية منازعاتهم الدولية بالوسائل السلمية على وجه لا يجعل السلم والأمن والعدل الدولي عرضة للخطر)[2]. وبالتالي، فإن سلطة الدولة بأستخدام القوة تتبع سواء من مجلس الأمن أو من خلال حق الدولة في التصرف دفاعا عن النفس الفردي أو الجماعي. السؤال العالق هو ما إذا كانت الهجمات الإلكترونية يمكن أن تصل إلى عتبة (الهجوم المسلح) الذي يقوم بتشغيل الحق في الدفاع عن النفس بموجب المادة ٥١ من الميثاق، وهو الاستثناء على تحريم اللجوء إلى التهديد أو استخدام القوة والتي تنص على ما يلي:

(ليس في هذا الميثاق ما يضعف أو ينتقص الحق الطبيعي للدول، فرادى أو جماعات، في الدفاع عن أنفسهم إذا اعتدت قوة مسلحة على أحد أعضاء "الأمم المتحدة" وذلك إلى أن يتخذ مجلس الأمن التدابير اللازمة لحفظ السلم والأمن الدولي)٣.

هل هناك فرق بين (هجوم مسلح) بموجب المادة ٥١ و (استخدام القوة) بموجب المادة ٢ (٤)؟

يرى بعض العلماء أن أي استخدام للقوة من جانب القوات المسلحة النظامية يشكل هجوم مسلح في حد ذاته. بموجب هذا الرأي، أي عمل هجومي من قبل وحدة ألانترنت

---

[1] *Ibid.*

[2] المادة ٢ (٣) من ميثاق الامم المتحدة.

[3] نجد أيضا هذا المفهوم في معاهدة لشبونة في ١٣ كانون الأول عام ٢٠٠٧ هو نص الاتحاد الأوروبي في المادة ٤٢§٧، كذلك الحال بالنسبة الى حلف شمال الأطلسي في ٤ نيسان ١٩٤٩ في المادة (٥) ، ايضا في دليل تالين القاعدة ١٦.

العسكرية هو هجوم مسلح لأنها تنبع من القوات المسلحة للدولة. مما تجدر الاشارة اليه في هذا الخصوص، أنه في الولايات المتحدة، الصين، إيران، إسرائيل والدول الأخرى في جميع أنحاء العالم، قد تم أنشاء بالفعل وحدة الانترنت العسكرية، لذلك، ينظر الى الأعمال الهجومية من قبل تلك الوحدات على الانترنت في حد ذاته بمثابة هجوم مسلح الذي يطلق الحق في ممارسة الدفاع عن النفس الفردي أو الجماعي[١].

بينما يرفض آخرون هذا النهج في حد ذاته، مستندين الى اختبار محكمة العدل الدولية الذي يقوم على (النطاق والآثار) بأعتباره المعيار الأنسب لتحديد متى يتم تشغيل المادة ٥١، حيث ترى بأن هناك تمييز جوهري بين (استخدام القوة) و (هجوم مسلح). ففي القضية المعنونة (الأنشطة العسكرية وشبه العسكرية في نيكاراغوا وضدها) بين نيكاراغوا والولايات المتحدة في ٢٧ حزيران عام ١٩٨٦ حددت محكمة العدل الدولية الفرق في المقام الأول على اساس (النطاق والآثار)، هكذا، قررت أنه ليس كل استخدام للقوة يبرر ممارسة حق الدفاع عن النفس من جانب واحد[٢].

بغض النظر عن حجم أو تأثير الهجوم، سواء كان حركي أو الكتروني، فأن نوع السلاح المستخدم هنا في الهجوم المسلح هو سلاح غير مادي، فعندما تستخدم الهجمات الإلكترونية لدعم القوات التقليدية تعتبر اسلحة وبالتالي يجب أن ينظم استخدامها. ويدعم هذه التصريحات رأي محكمة العدل الدولية في ٨ تمّوز ١٩٩٦ بعنوان مشروعية التهديد أو استخدام الأسلحة النووية، حيث توضح الفقرة ٣٩ أن الحظر العام لاستخدام القوة التي يسنها ميثاق الأمم المتحدة لا يخل بأستخدام الأسلحة الخاصة وينطبق على أي استخدام للقوة، بغض النظر عن الأسلحة المستخدمة[٣]. هكذا، يمكننا أن نقدر أن الهجمات الإلكترونية قد تأتي ضمن استخدام القوة بالمعنى المقصود في المادة ٢ (٤) من ميثاق الامم المتحدة، شريطة أن آثار هذه الهجمات قابلة للمقارنة من حيث الفتك والدمار مع تلك الناجمة من هجوم تقليدي أو نووي أو بيولوجي أو كيميائي[٤].

---

[1]Michael Gervais, Cyber Attacks and the Laws of War, p.542.

[2]Michael Gervais, Cyber Attacks and the Laws of War, p.542.

[٣]أكد مجلس الأمن هذا الرأي عندما أذن الولايات المتحدة للرد بقوة في الدفاع عن النفس لهجمات ٩/١١، حيث كانت "أسلحة" الطائرات المختطفة .

[3] Michael Gervais, Cyber Attacks and the Laws of War,p.543

[4]Laurn Baudin , Les cyber – attaques dans les conflits armé: qualification juridique, imputabilité et moyens de réponse envisagés, L'Harmattan,Paris, 2014,p.١٠٣.

أما دليل تالين[1]، فينص على أن العمليات الإلكترونية تشكل استخدام القوة حينما يكون مستواها (الدرجة /عتبة الشدة) وآثارها ، مقارنة مع العملية التقليدية (ليست الإلكترونية)، قد وصلت إلى مستوى من توظيف القوة، ويركز التحليل على العوامل الكمية والنوعية. اما المؤشرات التي تسمح بوصف العملية الإلكترونية باعتبارها استخدام للقوة فهي: شدة الضرر، الفورية، السبب والنتيجة، درجة الغزو ـ التغلغل في النظام، تقييم الآثار، الطابع العسكري، مشاركة الدولة بالاضافة الى قرينة الشرعية[2].

كما تنص القاعدة رقم ١٣ من دليل تالين:

(الدولة التي تكون هدف في عملية الكترونية بمستوى مماثل لتلك التي تندرج تحت هجوم مسلح لديها القدرة على ممارسة حقها الأصيل في الدفاع عن النفس. الحقيقة أن العملية الإلكترونية يمكن أن تصنف على أنها هجوم مسلح لا يتوقف فقط على حجمها ولكن أيضا الآثار التي تنتجها)٣.

ولقد اكدت الولايات المتحدة الامريكية هذا المنظور عام ٢٠٠٣، حيث اعترفت بضرورة وقاية وحماية أنظمة الكمبيوتر من تهديدات وشيكة، واصفة أجزاء رئيسية من الفضاء الإلكتروني بأعتبارها تمثل بنية تحتية وطنية حساسة[4]، فأذا كان هدف الهجوم الإلكتروني هو أحداث ضرر للبنية التحتية الحرجة (هدف حيوي)، فهذا يبرر اتخاذ تدابير للدفاع عن النفس.

---

[1] نشر حلف شمال الأطلسي (الناتو) في عام ٢٠١٣ دليلاً بإسم (تالين) متكون من ٢٨٢ صفحة، للقوانين الدولية المطبقة في حالة نشوب حروب الكترونية وتنظيم قواعد الإشتباك عبر الإنترنت.

[2] هذه النقاط التي اقترحها Michaël N. SCHMITT سابقا في تحليله للعمليات الالكترونية ، أضافة الى معيارين أخرين تم اضافتهم من قبل الخبراء في الدليل .أنظر كتاب :

Laurn Baudin , Les cyber – attaques dans les conflits armé: qualification juridique, imputabilité et moyens de réponse envisagés, L'Harmattan,Paris, 2014,p. ١٠٣.

[3] Laurn Baudin , Les cyber – attaques dans les conflits armé: qualification juridique, imputabilité et moyens de réponse envisagés…op.cit.p.121-122.

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

Laurn Baudin… *op.cit.* p.117.

Marco Benatar, The Use of Cyber Force: Need for Legal Justification?, Goettingen Journal of International Law 1.2009. p.394.

هكذا، يبدو لنا ان الهجات الإلكترونية قد تؤدي بشكل قانوني الى الحق في الدفاع عن النفس بموجب المادة ٥١ متى كان من شأنها أن تلحق دمارا كبير في العناصر الهامة في الدولة المستهدفة أي (البنية التحتية الوطنية الهامة).

ثانيا: مدى أمكانية تطبيق قواعد القانون الدولي الانساني على الهجمات الإلكترونية

أن سلوك المحاربين اثناء النزاعات المسلحة، الدولية وغير الدولية، يخضع الى العديد من القيود التي تهدف الى التخفيف قدر الإمكان من ويلات الحرب، وبما أن الهجمات الإلكترونية، تمثل بعدا جديدا خامسا يضاف الى الابعاد الاربعة الموجودة حاليا، باعتباره سلاحا جديدا في الحرب، فيجب أن يكون استخدامها في حدود مبادئ القانون الدولي الإنساني.

١. الضرورة العسكرية

يقيد القانون الإنساني الدولي استخدام القوة لأهداف من شأنها تحقيق أهداف عسكرية مشروعة، وهي التي تعرف بأنها (تلك التي تسهم مساهمة فعالة في العمل العسكري سواء كان ذلك بطبيعتها أم بموقعها أم بغايتها أم باستخدامها، والتي يحقق تدميرها التام أو الجزئي أو الاستيلاء عليها أو تعطيلها في الظروف السائدة حينذاك ميزة عسكرية أكيدة)[١]. والجدير بالذكر كذلك، أن اتفاقية لاهاي الرابعة تحظر تدمير ممتلكات العدو أو حجزها، إلا إذا كانت ضرورات الحرب تقتضي حتماً هذا التدمير أو الحجز[٢]. بالاضافة الى ذلك، يعتبر انتهاك مبدأ الضرورة العسكرية (جريمة حرب) في نظام روما الأساسي للمحكمة الجنائية الدولية[٣].

اذا ألاهداف العسكرية أو المجاز مهاجتمها تقتصر على تلك الكائنات التي تسهم في العمل العسكري أو تلك التي يحقق أتلافها أو تدميرها ميزة عسكرية أكيدة، وبالتالي، فأن الهجوم الإلكتروني الذي يستهدف أنظمة الكمبيوتر العسكرية للعدو يلبي شرط الضرورة العسكرية بحكم الرابطة العسكرية الخالصة.

لكن تحديد ما إذا كان الهدف خلق (ميزة عسكرية أكيدة) يعتبر امر معقد نوعا ما، فتعقيد أنظمة الكمبيوتر يجعل حساب الميزة العسكرية تحديا، أذ أن قيمة السلاح الإلكتروني

---

[١] المادة ٥٢ فقرة ٢ من الملحق (البروتوكول) الأول الإضافي إلى اتفاقيات جنيف لسنة ١٩٧٧.

[٢] المادة ٢٣ فقرة ز من اتفاقية لاهاي الخاصة باحترام قوانين وأعراف الحرب البرية في ١٨ أكتوبر/ تشرين الأول ١٩٠٧.

[٣] المادة ٨ من نظام روما الأساسي للمحكمة الجنائية الدولية المعتمد في روما في ١٧تموز/ يوليه ١٩٩٨.

غالبا ما تكمن في الأثر التعاقبي على الأنظمة التي تعتمد على الهدف الأولي. كما أن معظم المهاجمين في الحرب الإلكترونية لا يملكون معلومات كافية للتنبؤ بالآثار غير المباشرة للهجوم. فالمهاجم الإلكتروني الذي يخترق أنظمة الكمبيوتر لمحطة التوليد الكهربائي قد يحقق ميزة عسكرية، ولكن هذا النظام قد يكون له طبقات غير متوقعة التي تمنع الحصول على مثل هذه الميزة، في هذه الظروف، الميزة العسكرية ليست واضحة بما يكفي لتلبية شرط الضرورة العسكرية[١]. مع ذلك، من مزايا الهجوم الإلكتروني، المهاجم يستطيع أن يدافع عن التحديات التي تواجه باستخدام القوة من خلال إنشاء سجل معلومات التي تمثل ادرك المهاجم عن النظام المستهدف وقت الهجوم، في حين أن قوانين الحرب لا تتطلب مثل هذه السجلات، أن سجل المعلومات يعتبر طريقة بسيطة نسبيا لحماية قرار المهاجم لاستدعاء الضرورة العسكرية لاستهداف كائن.

في نهاية المطاف، أن تقييم ما إذا كان الهجوم الإلكتروني نشأ عن ضرورة عسكرية يعتمد على تحديد كل حالة على حدة، وهذا هو مماثل لتقييم الضرورة العسكرية في الهجمات التقليدية.

٢. التميز

من المبادئ الاساسية في القانون الدولي الانساني هو مبدأ التمييز، حيث جاء (تعمل أطراف النزاع على التمييز بين السكان المدنيين والمقاتلين وبين الأعيان المدنية والأهداف العسكرية، ومن ثم توجه عملياتها ضد الأهداف العسكرية دون غيرها، وذلك من أجل تأمين احترام وحماية السكان المدنيين والأعيان المدنية)[٢]. كما يتطلب من المهاجمين ضمان أن يتمتع السكان المدنيون والأشخاص المدنيون بحماية عامة ضد الأخطار الناجمة عن العمليات العسكرية، ولا يجوز أن يكون السكان المدنيون بوصفهم هذا وكذلك الأشخاص المدنيون محلاً للهجوم، وبالتالي، يحظر "الهجمات العشوائية".[٣] والجدير بالذكر أن نظام روما الأساسي يعتبر الفشل في التمييز بين المدنيين والمقاتلين بأنه (جريمة حرب)[٤]. الغرض من التمييز هو

---

[1] Michael Gervais, Cyber Attacks and the Laws of War,p.٥٦٤

[٢] المادة ٤٨ من لملحق (البروتوكول) الأول الإضافي إلى اتفاقيات جنيف المعقودة في ١٢ آب / أغسطس ١٩٤٩ والمتعلق بحماية ضحايا المنازعات الدولية المسلحة ١٩٧٧.

[٣] المادة ٥١ فقرة ١ . ٢ من لملحق (البروتوكول) الأول الإضافي إلى اتفاقيات جنيف المعقودة في ١٢ آب / أغسطس ١٩٤٩ والمتعلق بحماية ضحايا المنازعات الدولية المسلحة ١٩٧٧.

[٤] المادة ٨ من نظام روما الأساسي للمحكمة الجنائية الدولية المعتمد في روما في ١٧تموز/ يوليه ١٩٩٨.

أقتصار الهجمات على المقاتلين والأهداف العسكرية فقط. أما بالنسبة الى المدنيين الذين يشاركون مباشرة في الأعمال العدائية، فهم ليسوا محميين، بحكم المشاركة، اذ أنهم يفقدون الوضع المحمي لهم.

فيما يخص الهجمات الإلكترونية، ضمن محيط الفضاء الإلكتروني، نجد أن هناك صعوبة في تحقيق مثل هذا التمييز، فغالبا ما يكون هناك خط غير معروف وغامض بين الأهداف العسكرية والمدنية، الأمر الذي يطرح التساؤلات التالية:

(١)هل الهجمات الإلكترونية تمييز بين الأهداف المدنية والعسكرية؟

أن قوانين الحرب المعمول بها تلزم أطراف النزاع بأستهداف المقاتلين وليس المدنيين، وإذا كان يتم استهداف المدنيين، فيجب ألتأكد من أن هؤلاء الأفراد قد تم مصادرة وضعهم المحمي نتيجة مشاركتهم في الاعمال القتالية. ومن أجل تحديد ما إذا كانت الهجمات الإلكترونية تميز بشكل صحيح بين الأهداف المدنية والعسكرية، لا بد من فهم التمييز بين المقاتلين والمدنيين. فالقوات المسلحة لطرف النزاع تتكون من كافة القوات المسلحة والمجموعات والوحدات النظامية التي تكون تحت قيادة مسئولة عن سلوك مرؤسيها...الخ[١]، كما يتطلب من المقاتلين أن يميزوا أنفسهم عن السكان المدنيين أثناء اشتباكهم في هجوم أو في عملية عسكرية تجهز للهجوم[٢]. أما بالنسبة الى المدني، فهو أي شخص لا ينتمي إلى فئة من فئات الأشخاص المشار إليها في البنود الأول والثاني والثالث والسادس من الفقرة (أ) من المادة الرابعة من الاتفاقية الثالثة[٣]، والمادة ٤٣ من هذا البروتوكول الأول الاضافي لاتفاقيات

---

[١] المادة ٤٣ من لملحق (البروتوكول) الأول الإضافي إلى اتفاقيات جنيف المعقودة في ١٢ آب / أغسطس ١٩٤٩ والمتعلق بحماية ضحايا المنازعات الدولية المسلحة ١٩٧٧.

[٢] المادة ٤٤ فقرة٣ من لملحق (البروتوكول) الأول الإضافي إلى اتفاقيات جنيف المعقودة في ١٢ آب / أغسطس ١٩٤٩ والمتعلق بحماية ضحايا المنازعات الدولية المسلحة ١٩٧٧.

[٣] تنص المادة ٤ فقرة أ من اتفاقية حنيف الثالثة بشأن معاملة أسرى الحرب والمؤرخة في ١٢ آب/أغسطس ١٩٤٩:

١. أفراد القوات المسلحة لأحد أطراف النزاع، والمليشيات أو الوحدات المتطوعة التي تشكل جزءا من هذه القوات المسلحة.

٢. أفراد المليشيات الأخرى والوحدات المتطوعة الأخرى، بمن فيهم أعضاء حركات المقاومة المنظمة، الذين ينتمون إلي أحد أطراف النزاع ويعملون داخل أو خارج إقليمهم، حتى لو كان هذا الإقليم محتلا ...الخ.

٣. أفراد القوات المسلحة النظامية الذين يعلنون ولاءهم لحكومة أو سلطة لا تعترف بها الدولة الحاجزة.

٦. سكان الأراضي غير المحتلة الذين يحملون السلاح من تلقاء أنفسهم عند اقتراب العدو لمقاومة القوات الغازية دون أن يتوفر لهم الوقت لتشكيل وحدات مسلحة نظامية، شريطة أن يحملوا السلاح جهرا وأن يراعوا قوانين الحرب وعاداتها.

جنيف لسنة١٩٧٧. وإذا ثار الشك حول ما إذا كان الشخص مدنياً أم غير مدني فإن ذلك الشخص يعد مدنياً.

اذا تعريف ألمقاتل، بموجب القانون الدولي الإنساني، يتطلب مستوى من التنظيم أو مسؤولية القيادة، وهذه الصفات موجودة داخل الدول بالنسبة الى القوات المسلحة التي لديها قدرات الإنترنت.

أن تعريف القانون الدولي الإنساني للمقاتل قد يكون غير ملائم فيما يتعلق بالفضاء الإلكتروني، حيث يمكن للأفراد الغير منظمين المشاركة بسهولة في الهجمات الإلكترونية ضد العدو، وهذا الامر ينطبق على ما يسمى hacktivists التي تؤدي هجمات DDoS لأسباب وطنية أو أيديولوجية. في تلك الحالات، هل يجب أن يسمح للدولة المستهدفة ألرد بمستوى مناسب من ألقوة؟ هذا هو سؤال مهم عندما تصبح ألأسلحة الإلكترونية متاحة على نحو متزايد للجماهير.

في مجال الحرب الإلكترونية، فأن hacktivists لا يندرج ضمن تعريف المقاتلين الشرعيين وكما أنهم لا يعاملون على أنهم مدنيين محميين بموجب البروتوكول الأول (ما لم يقوموا بدور مباشر في الأعمال العدائية وعلى مدى الوقت الذي يقومون خلاله بهذا الدور)[١]. لذا، خلال الفترة التي يشارك فيها hacktivists في الصراع، فهم أهداف صالحة. ومع ذلك، أي استخدام القوة ضدهم يجب أن يكون محددا بمبدأ التناسب.

من جانب أخر، هناك قلق في إطار مبدأ التمييز عندما يجبر المهاجم الإلكتروني المدني للمشاركة في الصراع، فكما هو معلوم، أن أجهزة الكمبيوتر المدنية لا يمكن أن تصنف بأعتبارها أهداف عسكرية ما لم تشارك مباشرة في الأنشطة العسكرية، وهنا يمكن للمهاجمين، في مجال الفضاء الالكتروني، اختطاف أو سرقة الحواسيب المدنية لإدراجها في هجوم الروبوتات ضد العدو، وبالتالي إشراك هذه الحواسيب في أنشطة عسكرية. ان مثل هذا الاكراه أو القسر يشمل اثنين من الانتهاكات[٢]: أولا، المهاجم الإلكتروني يهاجم بشكل غير قانوني أجهزة الكمبيوتر المدنية ببرامج خبيثة الأمر الذي يجبر الكمبيوتر على الاستجابة الى أوامر وتعليمات المهاجم. هنا يمكن للدولة المستهدفة الرد بصورة متناسبة بهجمات مرتدة ضد هذه

---

[١] المادة ٥١ فقرة ٣ من البروتوكول الأول الإضافي لاتفاقية جنيف ينص على (يتمتع الأشخاص المدنيون بالحماية التي يوفرها هذا القسم ما لم يقوموا بدور مباشر في الأعمال العدائية وعلى مدى الوقت الذي يقومون خلاله بهذا الدور. كذلك، أنظر المادة ٤٧ من نفس البروتوكول.

[2] Michael Gervais, Cyber Attacks and the Laws of War, p. ٥٦٦ .

الحواسيب المختطفة، مسببة أضرار جانبية على البنية التحتية المدنية. في هذه الحالة، المهاجم الإلكتروني الأصلي هو المسؤول عن الضرر اللاحق لممتلكات المدنيين التي سببتها الدولة المستهدفة.

ثانيا، المهاجم الإلكتروني يجبر المدنيين، بشكل غير قانوني، على المشاركة في الأعمال العدائية، وبموجب اتفاقية جنيف الرابعة، لا يجوز إرغام الأشخاص المحميين على القيام بعمل (لها علاقة مباشرة بسير العمليات الحربية)[١]. فالمهاجم الإلكتروني يجبر المدنيين بشكل غير قانوني على المشاركة في العمليات العسكرية بصورة مباشرة، وهذه الحالة تقابل ما يعرف(الدروع البشرية). فهجمات DDoS وتكتيكات الهندسة الاجتماعية[٢] التي تنطوي على المدنيين هي تكتيكات مشكوك فيها التي تستحق التدقيق الصارم لتحديد ما إذا كانت تنتهك مبادئ القانون الدولي.

في الحقيقة، أن التمييز بين الأهداف المدنية والعسكرية أمر معقد في حرب الفضاء الإلكتروني، مع ذلك، فأن استهداف أهداف عسكرية بحتة لن ينتهك مبدأ التمييز[٣]، أما اذا كانت هناك هجمات الكترونية تستهدف عمدا قتل المدنيين أو تدمير الأعيان المدنية، فمثل هذه الهجمات غير قانونية بشكل واضح بموجب قانون الدولي الانساني.

(٢)الهجمات الإلكترونية هل تجري بشكل عشوائي؟

---

[١] المادة ٤٠ من أتفاقية جنيف الرابعة بشأن حماية الأشخاص المدنيين في وقت الحرب المؤرخة في ١٢آب/أغسطس ١٩٤٩.

[٢] الهندسة الاجتماعية أو ما يعرف بفن اختراق العقول هي عبارة عن مجموعة من التقنيات المستخدمة لجعل الناس يقومون بعمل ما أو يفضون بمعلومات سرية. تستخدم الهندسة الاجتماعية أحياناً ضمن احتيال الإنترنت لتحقيق الغرض المنشود من الضحية، حيث أن الهدف الأساسي للهندسة الاجتماعية هو طرح أسئلة بسيطة أو تافهة (عن طريق الهاتف أو البريد الإلكتروني مع انتحال شخصية ذي سلطة أو ذات عمل يسمح له بطرح هكذا أسئلة دون إثارة الشبهات). أنظر الموقع الالكتروني:
http://www.isecur1ty.org/%D9%83%D8%AA%D8%A7%D8%A8-social-engineering-the-art-of-human-hacking/ .

[٣] أنظر المادة ٥٢ من الملحق (البروتوكول) الأول الإضافي إلى اتفاقيات جنيف المعقودة في ١٢ آب / أغسطس ١٩٤٩ والمتعلق بحماية ضحايا المنازعات الدولية المسلحة.

حتى لو كان الهجوم الإلكتروني يميز بشكل صحيح بين المدنيين والمقاتلين، فيجب على المهاجمين تجنب الهجمات العشوائية امتثالا للتمييز بين المقاتلين المدنيين. ويقصد بالهجمات العشوائية هي تلك التي تكون غير دقيقة وتتسبب بأضرار جانبية[1]، أو هو ذلك الهجوم الذي لا يتخذ فيه المهاجم التدابير اللازمة لتجنب ضرب أهداف غير عسكرية[2]، علما أن قسم من الأضرار الجانبية تكون مقبولة في زمن الحرب. أن شرط التناسب هو محاولة لحد الدول من الانخراط في مستوى مفرط من القوة عن طريق الزام الدول بأستخدام أساليب أقل قوة التي من شأنها أن تقلل من الأضرار الجانبية وغير الضرورية متى كان ذلك ممكنا، وهو ما اكده البروتوكول الإضافي الأول بقوله:

(ينبغي أن يكون الهدف الواجب اختياره حين يكون الخيار ممكناً بين عدة أهداف عسكرية للحصول على ميزة عسكرية مماثلة، هو ذلك الهدف الذي يتوقع أن يسفر الهجوم عليه عن إحداث أقل قدر من الأخطار على أرواح المدنيين والأعيان المدنية)٣.

ايضا، يتطلب القانون العرفي، على النحو المبين في المادة ٥٧ من البروتوكول الإضافي، من المهاجمين اتخاذ "الرعاية المستمرة" و "جميع الاحتياطات المعقولة" لتجنب السكان المدنيين والأعيان المدنية.

في كثير من الحالات، تعتبر الهجمات ألإلكترونية هي الأفضل مقارنة مع ألهجوم الحركي، فالهجوم ألإلكتروني الذي يستهدف محطة توليد كهربائية يرتب اضرار اقل، مادية او بشرية، مقارنة مع هجوم مماثل حركي ناتجة عن قنابل جوية على سبيل المثال. أن قدرة الهجوم ألإلكتروني لتعطيل أنظمة العدو دون انفجار هي بطبيعتها أكثر تمييزا من الهجوم الحركي الذي يدمر نفس النظام ولكن أيضا يقتل الفنيين الذين يقومون بتشغيل النظام.

---

[1] المادة ٥٢ فقرة ٤ – تحظر الهجمات العشوائية، وتعتبر هجمات عشوائية :

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،

ج) أو تلك التي تستخدم طريقة أو وسيلة للقتال لا يمكن حصر آثارها على النحو الذي يتطلبه هذا اللحق "البروتوكول"، ومن ثم فإن من شأنها أن تصيب، في كل حالة كهذه، الأهداف العسكرية والأشخاص المدنيين أو الأعيان المدنية دون تمييز.

[2] سلوان جابر هاشم، حالة الضرورة في القانون الدولي الانساني، المؤسسة الحديثة للكتاب، لبنان، ط ١،٢٠١٣ ، ص ١٣٤.

[3] المادة ٥٧ من الملحق (البروتوكول) الأول الإضافي إلى اتفاقيات جنيف المعقودة في ١٢ آب / أغسطس ١٩٤٩ والمتعلق بحماية ضحايا المنازعات الدولية المسلحة.

لكن عدم القدرة النسبية للهجوم ألإلكتروني على التمييز يثير بعض الاشكالات القانونية، فالأنظمة العسكرية عادة ما تكون أكثر أمانا من ألانظمة المدنية، لذا، فمن السهل أطلاق هجوم ألكتروني يستهدف نظام مدني الذي يعتمد عليه الجيش بدلا من مهاجمة النظام العسكري مباشرة. علاوة على ذلك، فأن توقع وفهم نتائج الهجوم ألإلكتروني يتطلب قدرا كبيرا من المعلومات الاستخباراتية حول النظم المستهدفة، وحتى مع هذه المعلومات، يمكن لعدد من العوامل، خارجة عن سيطرة المهاجم، أن تقود الهجوم ألإلكتروني، عن غير قصد، الى تجاوز الهدف المقصود منه. فالهجمات الإلكترونية التي تستخدم فيروس أو دودة، على سبيل المثال، يمكن أن تتحول بسرعة الى خارج نطاق السيطرة، وتؤدي الى اختراق أنظمة مدنية وإلحاق أضرار بالممتلكات والتي تفوق قصد المهاجم نفسه[1]. على أن هذا لا يمنع من امكانية تصميم اسلحة الإلكترونية قادرة على التمييز، ومن بين أحد الأمثلة على الهجمات الإلكترونية المصممة للتمييز بين الاهداف المدنية والعسكرية بقصد مهاجمة مع التمييز هي دودة ستكسنت Stuxnet worm التي استهدفت المنشآت النووية في إيران، والتي اشرنا اليها سابقا.

من الأشكاليات الأخرى التي تواجه المهاجمين في الفضاء الإلكتروني، ما يتعلق بالأهداف ذات الاستخدام المزدوج، أي التي تخدم أغراض مدنية وعسكرية على حد سواء، فالمهاجمون، في الفضاء الالكتروني، قد يصنفون مجموعة متنوعة من الكائنات ذات الأستخدام المزدوج كأهداف عسكرية مشروعة، مثل البنية التحتية المدنية، طالما تستعمل لأغراض عسكرية، وتشمل هذه الفئة محطات توليد الطاقة، الاتصالات، الجسور، والبنية التحتية المدنية الأخرى التي يستخدمها الجيش في زمن الحرب.

مع ذلك، إذا كان القصد من الهجوم الإلكتروني هو تحقيق ميزة عسكرية من خلال استهداف أنظمة الكمبيوتر المستخدمة لأهداف عسكرية، وإذا كان المهاجمون قد نفذوا مثل هذه الهجمات مع أخذ الاحتياطات المعقولة للآثار الجانبية المحتملة، فأن لأسلحة الإلكترونية تعتبر هنا الوسيلة ألأكثر دقة والقدرة على التكيف مقارنة مع ألهجوم بالأسلحة التقليدية الأخرى.

٣. مبدأ التناسب

[1] Michael Gervais, Cyber Attacks and the Laws of War, p. ٥٧٠ .

مبدأ التناسب مشابه للتمييز في أنه يعكس القلق من عواقب الهجوم على المدنيين والأهداف المدنية، فهو يحكم درجة ونوع القوة المستخدمة لتحقيق هدف عسكري من خلال مقارنة الفائدة العسكرية المتوقعة المكتسبة بالأضرار العرضية المتوقعة التي قد تتسبب للمدنيين والأعيان المدنية. مبدأ التناسب نابع من المادة ٥١ من البروتوكول الإضافي الأول لاتفاقيات جنيف، الذي ينص على حظر الهجوم متى كان:

(يمكن أن يتوقع منه أن يسبب خسارة في أرواح المدنيين أو إصابة بهم أو أضراراً بالأعيان المدنية، أو أن يحدث خلطاً من هذه الخسائر والأضرار، يفرط في تجاوز ما ينتظر أن يسفر عنه ذلك الهجوم من ميزة عسكرية ملموسة ومباشرة)[١].

كذلك، المادة ٥٧ تتطلب بالمثل من المهاجمين أن يمتنعوا عن :

(اتخاذ قرار بشن أي هجوم قد يتوقع منه، بصفة عرضية، أن يحدث خسائر في أرواح المدنيين أو إلحاق الإصابة بهم، أو الأضرار بالأعيان المدنية، أو أن يحدث خلطاً من هذه الخسائر والأضرار، مما يفرط في تجاوز ما ينتظر أن يسفر عنه ذلك الهجوم من ميزة عسكرية ملموسة ومباشرة)[٢].

ايضا، نجد ان نظام روما الأساسي قد تضمن اشارة الى مبدأ التناسب عند سرده لجرائم معينة[٣].

أن الهجوم الذي يسفر عن وفيات في صفوف المدنيين أو تدمير الممتلكات المدنية ليس انتهاكا في حد ذاته، بل ما هو محظور، بموجب مبدأ التناسب، هو الهجوم المتهور، أو الهجوم الذي يأخذ عمدا أرواح المدنيين أو تدمير الممتلكات المدنية التي تتجاوز ما هو ضروري لتحقيق هدف عسكري.

التناسب ينطبق أيضا على الآثار غير المباشرة للهجوم، فعلى سبيل المثال، الهجوم الإلكتروني هو المسؤول عن الآثار غير المباشرة التي تصيب السكان المدنيين نتيجة هجوم

---

[١] المادة ٥١ فقرة ٥ من الملحق (البروتوكول) الأول الإضافي إلى اتفاقيات جنيف، ١٩٧٧ .

[٢] المادة ٥٧ فقرة ٣ من الملحق (البروتوكول) الأول الإضافي إلى اتفاقيات جنيف، ١٩٧٧ .

[٣] أنظر المادة ٨ فقره (أ) ٤ (إلحاق تدمير واسع النطاق بالممتلكات والاستيلاء عليها دون أن تكون هناك ضرورة عسكرية تبرر ذلك وبالمخالفة للقانون وبطريقة عابثة)؛ كذلك الفقرة (ب) ٤ (عمد شن هجوم مع العلم بأن هذا الهجوم سيسفر عن خسائر تبعية في الأرواح أو عن إصابات بين المدنيين أو عن إلحاق أضرار مدنية أو إحداث ضرر واسع النطاق وطويل الأجل وشديد للبيئة الطبيعية يكون إفراطه واضحاً بالقياس إلى مجمل المكاسب العسكرية المتوقعة الملموسة المباشرة).

على نظام السيطرة على محطة كهربائية، فبعض هذه الهجمات لها مثل هذه الآثار غير المباشرة الخطيرة والتي هي محظورة كما جاء في المادة ٥٦ من البروتوكول الإضافي الأول: (لا تكون الأشغال الهندسية أو المنشآت التي تحوي قوى خطرة ألا وهي السدود والجسور والمحطات النووية لتوليد الطاقة الكهربية محلاً للهجوم، حتى ولو كانت أهدافاً عسكرية، إذا كان من شأن مثل هذا الهجوم أن يتسبب في انطلاق قوى خطرة ترتب خسائر فادحة بين السكان المدنيين...الخ)[١]

مع ذلك، أن مبدأ التناسب يجب أن يجعل المهاجمين يفضلون الهجوم الإلكتروني على الهجوم الحركي، فمن بين مزايا الهجوم الإلكتروني هو أنه يسمح للدولة ألتقليل من الأضرار الجانبية، فكما ذكر سابقا، الهجوم الإلكتروني عادة ما يكون أقل فتكا من الهجوم الحركي، بالإضافة إلى ذلك، الهجوم الإلكتروني من المحتمل عكسه أي قابل للأنعكاس. أن هذه الخصائص تكون مرغوبة للدولة التي تريد تطبيق مستوى مناسب من القوة دون التسبب بخسائر غير متناسبة في صفوف المدنيين.

مع ذلك، هناك تحديات ترافق الهجوم الإلكتروني، فعلى سبيل المثال، دون آلية عكس الهجوم، الهجمات الإلكترونية لا تسمح للهدف بالاستسلام، على خلاف الهجوم الذي يستخدم المشغل البشري الذي يستطيع بدوره تقييم الأوضاع المتغيرة. فالهجوم الإلكتروني الذي يتم أطلاقه في البيئة الفضائية دون القدرة على الغائه أو استرجاعه لا يمكن أن يأخذ بعين الاعتبار رغبة الدولة المستهدفة على الاستسلام، وهو حق بموجب القانون الدولي العرفي[٢].

أن تحليل التناسب فيما يتعلق بالهجوم الكتروني يجب دائما النظر على أساس كل حالة على حدة، كما أن المقارنة بين عدد المدنيين الضحايا مع عدد المقاتلين الذين قتلوا غير كافي، وانما يجب النظر الى قيمة الهدف وعما إذا كان الهجوم قد حقق ميزة عسكرية أكيدة وأظهار الحذر المناسب اتجاه حياة المدنيين وممتلكاتهم.

٤. الغدر

---

[١] المادة ٥٦ فقرة ١ من الملحق (البروتوكول) الأول الإضافي إلى اتفاقيات جنيف، ١٩٧٧ .

[٢] المادة ٤١ من الملحق (البروتوكول) الأول الإضافي إلى اتفاقيات جنيف المعقودة في ١٢ آب / أغسطس ١٩٤٩ والمتعلق بحماية ضحايا المنازعات الدولية المسلحة.

الغدر هو شكل من أشكال الخداع، التي يصر فيها جانب واحد أنه يتصرف بحسن نية في إجراء الأعمال العدائية، ولكن بمجرد تقدم الفرصة نفسها، يقوم بشكل متعمد بتصرفات تنم عن سوء النية، والسلوك الغادر محظور بموجب قانون الصراع المسلح لأنه يقوض القدرة على استعادة السلام، وهو ما نص عليه البروتوكول الإضافي الأول بقوله:

(يحظر قتل الخصم أو إصابته أو أسره باللجوء إلى الغدر. وتعتبر من قبيل الغدر تلك الأفعال التي تستثير ثقة الخصم مع تعمد خيانة هذه الثقة وتدفع الخصم إلى الاعتقاد بأن له الحق في أو أن عليه التزاماً بمنح الحماية طبقاً لقواعد القانون الدولي التي تطبق في المنازعات المسلحة)[1].

أن الحرب الإلكترونية مغرية لأولئك الذين يرغبون في الانخراط في السلوك الغادر، حيث يجد المهاجمون فرص وافرة للتأثير أو تضليل الخصوم لأن معظم الهجمات الإلكترونية المتطورة تنطوي على بعض مستوى من الإخفاء. مع ذلك، أن الإخفاء أو التمويه وحده لا يمثل دائما انتهاكا للشرعية، فالحيل الحربية هي تكتيك شائع في الحرب التقليدية، مثل الهجمات المباغتة، الهجمات الدعائية أو التراجع، والتكتيكات النفسية...الخ، فهي مشروعة للتأثير أو لتضليل العدو. من الامثلة الحديثة في هذا الخصوص، نذكر حالة العراق اثناء حرب ٢٠٠٣، فحسب ريتشارد كلارك، المستشار الخاص للرئيس بشأن الأمن الإلكتروني في عهد إدارة بوش، كتب في الحرب الإلكترونية (الهجوم الإلكتروني الأمريكي في العراق)، يوضح بأنه قبل الغزو الأمريكي للعراق عام ٢٠٠٣، اخترقت الولايات المتحدة نظام البريد الإلكتروني في وزارة الدفاع العراقية، حيث تم مراسلة ضباط الجيش العراقي على البريد الإلكتروني، وقد ذكرت القيادة المركزية الأمريكية في البريد الإلكتروني أن هدف الولايات المتحدة كان فقط أزاحة صدام حسين وأبنائه من السلطة وليس لديهم أي مصلحة في الإضرار بقواتهم، وكانت النتيجة أن العديد من المسؤولين العسكريين العراقيين اتبعوا مشورة القيادة المركزية الأمريكية، واختار أن يمضوا بعيدا عن المعركة حتى قبل أن تبدأ[2]. أن حيلة القيادة المركزية الأمريكية هي مثال على شرعية حيل الحرب الإلكترونية.

---

[1] المادة ٣٧ فقرة ١ من الملحق (البروتوكول) الأول الإضافي إلى اتفاقيات جنيف، ١٩٧٧ . كذلك تنص المادة ٢٣ فقرة ب من اتفاقية لاهاي الرابعة لسنة١٩٠٧والخاصة باحترام قوانين وأعراف الحرب البرية على حظر (قتل أو جرح أفراد من الدولة المعادية أو الجيش المعادي باللجوء إلى الغدر).

[2] Michael Gervais, Cyber Attacks and the Laws of War, p.٥٧٤ .

مع ذلك، ليس كل الهجمات الإلكترونية يتم وصفها على هذا النحو، على سبيل المثال، فإن الهجوم الإلكتروني ينتهك قانون النزاعات المسلحة لو كان لغرض أرسال معلومات كاذبة، وبالتالي خداع قوات العدو في الاعتقاد أن الأعمال العدائية قد انتهت وحثها على إلقاء أسلحتهم قبل هجوم بري. كذلك، الحرب الإلكترونية تقدم تعقيدات إضافية بالنسبة الى الهجمات الإلكترونية التي تخدع الدول المستهدفة بالاعتقاد أن هذا الهجوم نشأ من مصدر آخر، سواء كان المصدر هو غير المقاتلين أو طرف ثالث. فبموجب المادة ٣٧ (١) (ج) من البروتوكول الإضافي (التظاهر بوضع المدني غير المقاتل)، هو مثال للسلوك الغادر. فيما يتعلق بالحرب الالكترونية أن خداع الخصوم في الاعتقاد بأن الهجوم نشأ من شخص غير مقاتل او مدني يمثل انتهاك لقوانين الحرب.

٥. الآلام لا داعي لها

حظرالآلام أو المعاناة غير الضرورية يقيد ترسانة الدولة من خلال حظر أنواع معينة من الأسلحة التي من شأنها أن تضاعف دون جدوى عذاب الأشخاص العاجزين عن القتال أو التي تجعل من موتهم أمرا محتوما، ويقصد بالآلام التي لا مبرر لها وفق ما عرفته محكمة العدل الدولية (ضرر أكبر من الضرر الذي لا محيد عن احداثه من أجل تحقيق الأهداف العسكرية المشروعة)[١]، ويعترف القانون الدولي الإنساني على أنه:

(ليس للمتحاربين حق مطلق في اختيار وسائل إلحاق الضرر بالعدو)٢.

كما ورد في فتوى محكمة العدل الدولية بشأن الأسلحة النووية، (الدول لا تملك حرية غير محدودة لاختيار الوسائل في الأسلحة التي يستخدمونها)[٣]. أن هذا الحظر يشجع الدول على استخدام مستوى مناسب من القوة لتحقيق الغايات العسكرية. الفكرة الأساسية هي أن الضرر يجب أن يكون في مستوى لا يزيد مما هو ضروري لتحقيق الأهداف العسكرية المشروعة، فبموجب هذا المبدأ، الأسلحة العشوائية، مثل الأسلحة البيولوجية أو الكيميائية، هي غير قانونية. أن حظر الآلام غير الضرورية يتقاطع في كلا الاتجاهين في مجال الحرب الإلكترونية، فمن جهة، الهجمات الإلكترونية غالبا ما يصعب السيطرة عليها، وبالتالي، فهي

---

[١] سلوان جابر هاشم، حالة الضرورة في القانون الدولي الانساني، مصدر سابق، ص ١٥٣.

[٢] المادة ٢٢ من اتفاقية لاهاي الرابعة لسنة١٩٠٧ الخاصة باحترام قوانين وأعراف الحرب البرية.

[٣] نفس المضمون ورد في ديباجة اتفاقية حظر أو تقييد استعمال أسلحة تقليدية معينة مفرطة الضرر، أو عشوائية الاثر لعام ١٩٨٠، وكذلك اتفاقية اوتاوا لحظر استعمال وتخزين وانتاج ونقل الالغام المضادة للافراد . أنظر : سلوان جابر هاشم، حالة الضرورة في القانون الدولي الانساني، مصدر سابق، ص ١٥٤. ١٥٥.

عشوائية في آثارها ، فالسلاح الإلكتروني الذي يوظف استخدام دودة يمكن ان تصيب عن غير قصد الملايين من أجهزة الكمبيوتر في جهودها للعمل على شبكة واحدة مستهدفة. مع ذلك، حتى الآن الأسلحة الإلكترونية في كثير من الأحيان تقدم أدنى مستوى من القوة التي يمكن استخدامها بالمقارنة مع الهجمات الحركية التقليدية. فالهجوم الحركي بأستخدام القنابل ضد مبنى من أجل إيقاف محطة توليد كهربائي يؤدي إلى المزيد من الضرر والدمار مقارنة مع الهجمات الإلكترونية التي تستهدف نفس الهدف. وبالتالي، فإن القادة العسكريين غالبا ما يجدون أنه من الأفضل أستخدام الهجوم الكتروني لأنه يؤدي الى تجنيب الأرواح والبنية التحتية المادية.

اذا الهجمات الإلكترونية يجب أن تكون السلاح المفضل في ترسانة الدولة، مقارنة مع الاسلحة الحركية، ويكون الهجوم الإلكتروني غير قانوني متى ما كانت نتائجه مشابهة للهجوم الحركي التقليدي التي تنتهك الحظر المفروض على الآلام غير ضرورية.

الـخـاتـمـة

أن بيان الهجمات الإلكترونية الغير الحركية بأعتبارها احدى الركائز الأساسية في القتال يسلط الضوء على ظهور بعدا جديدا خامسا في الحرب يتمثل في الفضاء الإلكتروني. فالتكتيكات والاستراتيجيات الجديدة المستخدمة خلال الحرب الروسية–الجورجية وكذلك في كل من استونيا وايران تنذر بعهد جديد من الهجمات الإلكترونية التي سوف تستخدم كجزء من حملة متعددة الأبعاد، لا سيما وان هذه الهجمات الإلكترونية تتميز بكونها منخفضة التكلفة، تنفذ عن بعد، فورية أو آنية ، ذات تكتيك قوي من حيث الإكراه أو الدمار، وغالبا ما ترتكب دون إثارة المساءلة بسبب صعوبة الاسناد. أن هذه الصفات تضمن أن الدول والجهات الفاعلة من غير الدول سوف تستمر في تطوير وإطلاق الهجمات الالكترونية في المستقبل المنظور. نتيجة لذلك، فإنه من الأهمية بمكان بالنسبة للنظام القانوني الدولي التكيف ومعالجة هذا الاستخدام المتطور للعمليات في الفضاء الإلكتروني والذي لايزال يعتبر ساحة معركة خارجة على القانون نسبيا بسبب أنعدام القواعد القانونية الكافية لتنظيم مثل هذا البعد الجديد.

أن كيفية عمل الهجمات الإلكترونية ، وكيف يتم استخدامها في الممارسة العملية يثير، في الحقيقة، العديد من الأسئلة الصعبة عند محاولة احتواء الفضاء الإلكتروني ضمن نظام الحرب الذي تم تشيده قبل فترة طويلة، لكن المشاكل الناتجة عن الهجمات الإلكترونية غالبا ما تكون مشابهة لمشاكل الهجمات التقليدية، الاختلافات بين الحرب التقليدية والإلكترونية تكمن في الدرجة، وليس النوع. بالتالي، فإن النظام القانون الإنساني الدولي الذي يحكم الحرب التقليدية يمكن نقله على نحو فعال فيما يتعلق بالهجمات الإلكترونية، مع الحاجة الى تطوير قواعد جديدة اضافية تعالج مستجدات هذا البعد الجديد في النزاعات المسلحة.

التوصيات

(١) تنسيق الجهود الدولية من اجل التوصل الى ابرام معاهدة خاصة بالهجوم إلكتروني أو الحرب الإلكترونية[١].

(٢)ضرورة اعتماد الرقابة الشاملة من قبل الدول على الهجمات الإلكترونية التي يمكن ان تشن من قبل اطراف ثالثة، افراد او شركات أو جهات غير حكومية .

(٣) تحديد المحفل المناسب لمحاكمة الدول الراعية للهجمات الإلكترونية، من المرشحين بدءا من محكمة العدل الدولية إلى المحاكم الوطنية والمحاكم المتخصصة.

(٤)تقييد خوادم بروكسي لأن ذلك من شأنه أن يجعل الأمر أكثر صعوبة بكثير بالنسبة للمهاجمين للسيطرة على جهاز كمبيوتر آخر[٢].

(٥)تطوير النظام الجنائي لدولي ليشمل تحديدا الجرائم الناتجة عن الهجوم إلكتروني أو الحرب الإلكترونية.

(٦)تشكيل لجان تحقيق دولية مختصة بالهجمات الإلكترونية بهدف التحقيق واعداد التقارير اللازمة.

(٧)أستخدام حق الدفاع الشرعي، في حالة التيقن من مصدر الهجوم، يجب أن يكون مرتبطا بالهجمات التي تستهدف البنية التحتية للدولة المستهدفة، ويكون ضمن نطاق الفضاء لإلكتروني الغير حركي.

---

[١]لقد دافع عن فكرة وجود معاهدة هجوم إلكتروني أو الحرب الإلكترونية من قبل عدد من الأطراف، وأبرزها روسيا، حيث اقترحت روسيا صياغة معاهدة للحد من تطوير الأسلحة السيبرانية واستخدام هجمات الكترونية. الأمم المتحدة أيضا مؤي قوي للمعاهدة دولية بشأن الحرب الإلكترونية، حيث وضح حمدون توريه الأمين العام للاتحاد الدولي للاتصالات أن (الحرب الإلكترونية ستكون أسوأ من تسونامي).

Handler, Stephenie Gosnell…*op.cit.*p.٢٣٦.

[٢]في شبكات الكمبيوتر، تعتبر وحدة الخدمة النائبة أو البروكسي بمثابة خادم (قد يكون عبارة عن أحد نظم الكمبيوتر أو أحد البرامج التطبيقية) يعمل كحلقة وصل بين الطلبات الواردة من أجهزة الزبائن التي تبحث عن المصادر المطلوبة من وحدات الخدمة الأخرى. ويمكن الإشارة إلى وحدة الخدمة البديلة باسم وحدة خدمة بروكسي أو يمكن الاكتفاء بكلمة بروكسي.

المصادر

أولا: المصادر العربية

١. اتفاقية لاهاي الخاصة باحترام قوانين وأعراف الحرب البرية في ١٨ أكتوبر/ تشرين الأول ١٩٠٧.

٢. اتفاقية جنيف الثالثة بشأن معاملة أسرى الحرب والمؤرخة في ١٢ آب/أغسطس ١٩٤٩.

٣. اتفاقية لاهاي الرابعة في ١٨ أكتوبر/ تشرين الأول ١٩٠٧ الخاصة باحترام قوانين وأعراف الحرب البرية.

٤. ميثاق الأمم المتحدة في ٢٦ حزيران/يونيه ١٩٤٥.

٥. معاهدة المبادئ المنظمة لأنشطة الدول في ميدان استكشاف واستخدام الفضاء الخارجي، بما في ذلك القمر والأجرام السماوية الأخرى في ٢٧ كانون الثاني لسنة ١٩٦٧.

٦. اتفاقية فيينا لقانون المعاهدات لسنة ١٩٦٩.

٧. البروتوكول الأول الإضافي إلى اتفاقيات جنيف المعقودة في ١٢ آب / أغسطس ١٩٤٩ والمتعلق بحماية ضحايا المنازعات الدولية المسلحة لسنة ١٩٧٧.

٨. الاتفاق المنظم لانشطة الدول على سطح القمر والاجرام السماوية في ٥ كانون الأول ١٩٧٩.

٩. نظام روما الأساسي للمحكمة الجنائية الدولية المعتمد في روما في ١٧تموز/ يوليه ١٩٩٨.

١٠. تقرير الجمعية العامة ، الوثيقة (UNODC/CCPCJ/EG.4/2013/2) في ٢٣ كانون الثاني ٢٠١٣.

المراجع

أولا: المراجع العربية

١. سلوان جابر هاشم، حالة الضرورة في القانون الدولي الانساني، المؤسسة الحديثة للكتاب، لبنان، ط١ ، ٢٠١٣ .

ثانيا: المراجع الاجنبية

1) Bradley Raboin , Corresponding Evolution: International Law and the Emergence of Cyber Warfare, Journal of the National Association of Administrative Law Judiciary -31-2, Fall 2011,p.٦٠٧.

2) Brian T. O'Donnell and James C. Kraska, Humanitarian Law: Developing International Rules for the Digital Battlefield, Journal of Conflict and Security Law, Vol. 8, Issue 1 (April 2003).
3) Brian Weeden, *Incompatibilité entre les priorités offensives et défensives des États pour les cyber-activités, dans, Faire face aux cyberconflits*, le Forum du désarmement, Institut des Nations Unies pour la recherche sur le désarmement (UNIDIR)United Nations, Geneva, 2012.
4) Daniel Ventre, Cyberespace et acteurs du cyber conflit, Lavoisier, Paris, 2011.
5) François Silva, Être e-DRH : postmodernité, nouvelles technologies et fonctions RH, Editions Liaisons, France , ٢٠٠٨.
6) Handler, Stephenie Gosnell, New Cyber Face of Battle: Developing a Legal Approach to Accommodate Emerging Trends in Warfare, Stanford Journal of International Law, 48 Stan. J. Int'l L. 209 (2012).
7) Keith Nicholson, INTERNATIONAL COMPUTER CRIME: A GLOBAL VILLAGE UNDER SIEGE, NEW ENGLAND SCHOOL OF LAW, 1997.
8) Laurn Baudin , Les cyber - attaques dans les conflits armé: qualification juridique, imputabilité et moyens de réponse envisagés, L'Harmattan,Paris, 2014.
9) Lianne j.M. Boer, Restating the Law "As It Is": On the Tallinn Manual and the Use of Force in Cyberspace, Amsterdam Law Forum VOL 5:3, 2013.
10) Marco Benatar, The Use of Cyber Force: Need for Legal Justification? Goettingen Journal of International Law 1.2009.

11) Michael Gervais, Cyber Attacks and the Laws of War, berkeley journal of international law, Vol. 30:2, 2012.

12) Nils Melzer, *Les cyber-opérations et le jus in bello*, dans, Faire face aux cyberconflits, le Forum du désarmement, Institut des Nations Unies pour la recherche sur le désarmement (UNIDIR) United Nations, Geneva, 2012.

13) SCHAAP, ARIE J, CYBER WARFARE OPERATIONS: DEVELOPMENT AND USE UNDER INTERNATIONAL LAW, Air Force Law Review , Volume 64, 2009.

ثالثا: المواقع الالكترونية

لجنة الإسكوا للتشريعات السيبرانية، انظر الموقع الالكتروني:

http://isper.escwa.un.org/FocusAreas/CyberLegislation/tabid/157/language/ar-LB/Default.aspx.

HAMZA CHERIEF, Le cyberespace, « cinquième dimension » du droit des conflits armés ?

http://www.espritcorsaire.com/?ID=268/Hamza_Cherief/Le_cyberespace,_%C2%AB_cinqui%C3%A8me_dimension_%C2%BB_du_droit_des_conflits_arm%C3%A9s_?

د. فاتن سعيد بامفلح ، حماية أمن المعلومات في شبكة المكتبات بجامعة أم القرى، دراسة حالة ص١٦. أنظر الموقع الالكتروني:

http://www.kau.edu.sa/Files/0012433/Researches/56927_27244.pdf.

http://www.oxforddictionaries.com/definition/english/hacktivist.

http://www.isecur1ty.org/%D9%83%D8%AA%D8%A7%D8%A8-social-engineering-the-art-of-human-hacking/ .