فاعلية القانون الدولي الإنساني في تنظيم الحرب السيبرانية

م.م. رفيف طلال خالد

م.م. ايمان عبد الواحد مجيد

جامعة كركوك – قسم شؤون الأقسام الداخلي

rafeeftalal752@uokirkuk.edu.iq

Eman abdul wahid maged

المقدمة

تتسبب الهجمات السيبرانية التي نشهدها اليوم في تكاليف اقتصادية كبيرة، وغالبًا ما تحدث خارج إطار النزاع المسلح. ولحسن الحظ، لم تؤدي إلى أضرار كبيرة للبشر حتى الآن. ومع ذلك، فإن هجمات سيبرانية أكثر تعقيدًا نجحت في تعطيل إمدادات خدمات أساسية للسكان المدنيين. يبدو أن قطاع الرعاية الصحية خصوصًا أكثر عرضة لهذه الهجمات ويتأثر بها بشكل كبير، إضافة إلى تأثر قطاعات أخرى من البنية التحتية المدنية، مثل أنظمة الكهرباء والمياه والصرف الصحي. تزداد هذه الهجمات تواترًا وتشتد حدتها بسرعة تفوق التوقعات. يوفر القانون الدولي الإنساني طبقة إضافية من الحماية ضد آثار الأعمال العدائية، حيث يتعين على المتحاربين احترام وحماية المرافق الطبية والعاملين فيها في جميع الأوقات. وبالتالي، تُعتبر الهجمات السيبرانية ضد قطاع الرعاية الصحية أثناء النزاع المسلح غالبًا انتهاكًا للقانون الدولي الإنساني. وبالمثل، يتمتع المدنيون والأعيان المدنية والأشياء الضرورية لبقاء السكان المدنيين بحماية خاصة بموجب مبادئ القانون الدولي الإنساني الخاصة بالتمييز، والتناسب، والاحتياط، مما يضمن حماية قوية للبنية التحتية المدنية الحيوية ضد آثار الهجمات السيبرانية خلال النزاعات المسلحة.

أهمية البحث:

ان الفضاء السيبراني بما يحمله من فوائد للبشرية هو يحمل في ذات الوقت مخاطر جمة. ولعل الحرب السيبرانية أحدها، حيث تثير الحرب السيبرانية العديد من القضايا المتعلقة بمدى انطباق قواعد ومبادئ القانون الدولي الإنساني عليها. حيث

الهجمات السيبرانية التي تصل إلى مستوى الهجمات فقط –كما هو محدد في القانون الدولي الإنساني– تخضع للحظر الذي يفرضه القانون الدولي الانساني على الهجمات المباشرة ضد الأعيان المدنية، والهجمات العشوائية وغير المتناسبة. ومما يعقد الامر هنا هو انه لم يتم الى الان تحديد تعريف نهائي للهجمات السيبرانية في إطار القانون الدولي الإنساني ما يجعل حياة الكثير من المدنيين موضع تهديد كذلك الكثير من الاعيان المدنية يمكن ان تكون في خطر، ولن تتحقق الحماية القانونية الكاملة بموجب قواعد القانون الدولي الأساسية إلا عندما تعترف الدول بأن الهجمات السيبرانية التي تعطل عمل الكثير من المؤسسات الحيوية في الدول تخضع لقواعد القانون الدولي الإنساني.

مشكلة البحث:

تثير الخصائص الفريدة للفضاء السيبراني أسئلة حول تفسير قواعد القانون الدولي الإنساني، ويتعين على الدول معالجتها على وجه السرعة. إن التأكيد على أن القانون الدولي الإنساني ينطبق على الفضاء السيبراني ومناقشة تأويلاته لا يعني أن وضع قواعد جديدة قد لا يكون مفيدًا أو حتى مطلوبًا. ولكن في حالة وضع قواعد جديدة ينبغي أن تُبنى على القانون الحالي وتعززه.

منهجية البحث:

سنعتمد في دراستنا لبحثنا (فاعلية القانون الدولي الإنساني في تنظيم الحرب السيبرانية) المنهج التحليلي الوصفي، وذلك من خلال تحليل نصوص اتفاقيات لاهاي وجنيف وبروتوكولاتها الملحقة والتي تعتبر مصدر لقواعد مبادئ القانون الدولي الإنساني وبحث مدى انطباقها على الحرب السيبرانية لتعرف على مدى فاعلية قواعد ومبادئ القانون الدولي الإنساني في مواجهة هذا النوع الجديد من الحروب.

هيكلية البحث:

سنقسم بحثنا هذا الى مبحثين نتناول في المبحث الأول الإطار المفاهيمي للحرب السيبرانية وفيه مطلبين نركز في المطلب الأول على التعريف بالحرب السيبرانية بينما نفرد المطلب الثاني لبحث خصائص الحرب السيبرانية، اما المبحث الثاني وضع الحرب السيبرانية في إطار القانون الدولي الإنساني وبعض تطبيقاتها، ففيه مطلبين افردنا المطلب الأول لبحث انطباق القواعد والمبادئ الإنسانية على الحرب السيبرانية، اما المطلب الثاني فخصناه لبحث تطبيقات الهجمات السيبرانية.

المبحث الأول

الإطار المفاهيمي للحرب السيبرانية

ان انتقال النشاطات الإنسانية إلى الفضاء السيبراني، حمل معه مشاكل وتعقيدات هذه النشاطات، وإذا ما أردنا وصف العصر الحالي، فإننا سنختصره في ثلاث كلمات (عصر الفضاء الإلكتروني)، بحيث أصبح الإنترنت هو العمود

الفقري لكل الأنشطة في الحياة اليومية تقريبا، سواء على مستوى الأفراد، أو الجماعات، أو حتى الحكومات والدول1. تشكل الحرب السيبرانية تحديًا معاصرًا يعيد تعريف مفاهيم النزاع والأمن في العصر الرقمي. يتضمن الإطار المفاهيمي للحرب السيبرانية دراسة الجوانب التقنية والقانونية والأخلاقية المرتبطة باستخدام الفضاء السيبراني كبيئة للصراع. تُعتبر الحرب السيبرانية استخدامًا متعمدًا للهجمات الرقمية لتعطيل أو تدمير البنية التحتية الحيوية، مثل شبكات الكهرباء والاتصالات والمؤسسات المالية، مما يعكس مدى تطور التهديدات في العالم الحديث. تعتمد هذه الحروب على أدوات متقدمة مثل الفيروسات والبرامج الضارة وهجمات الحرمان من الخدمات. سوف نتناول في هذا المبحث التعريف بالحرب السيبرانية من خلال المطلب الأول، وخصائص الحرب السيبرانية من خلال المطلب الثاني.

المطلب الأول

التعريف بالحرب السيبرانية

إن الغموض في تعريف الحرب السيبرانية لم يمنع الأوساط الأكاديمية أو العسكرية أو الحكومات من محاولة وضع تعريف. ولعل المقالة البحثية المبتكرة والمعنونة بشكل استفزازي لعام 1993 Cyberwar is Coming بواسطة أركيلا ورونفيلدت، أنشأ فئة من التعريفات (المثيرة للقلق) التي زعمت أن الحرب السيبرانية كانت تهديدًا وشيكًا2. يشير نيلز ميلزر إلى أن الحرب الإلكترونية أو السيبرانية هي تلك التي "تحدث في الفضاء السيبراني باستخدام الوسائل والأساليب الرقمية". ويعتقد ميلزر أنه بينما يشير مصطلح "الحرب" عمومًا إلى الأعمال العدائية العسكرية خلال النزاعات المسلحة، فإن الفضاء السيبراني يمثل بُعدًا مختلفًا. هذا الفضاء يتضمن "شبكة مترابطة عالميًا من المعلومات الرقمية والبُنى التحتية للاتصالات، بما في ذلك الإنترنت، وشبكات الاتصالات، وأنظمة الكمبيوتر والمعلومات الموجودة

[1] – د. راجي يوسف محمود البياتي: الإرهاب السيبراني نماذج من الجهود الدولية للحد منه، مجلة تكريت للعلوم السياسية، ع28، 2022، ص88.

[2] – عمران طه عبدالرحمن عمران: الحروب السيبرانية دراسة تأصيلية للمفهوم، دراسة بحثية منشورة على موقع المركز الديمقراطي العربي، القاهرة، متاح على الرابط التالي: https://democraticac.de/?p=96510 .(2024/7/15)

بها". بناءً على ذلك، يعتبر ميلزر أن إصابة شبكة كمبيوتر تابعة لأحد الخصوم ببرمجيات خبيثة تُعدّ "عملًا من أعمال الحرب الإلكترونية"، في حين أن "القصف الجوي بناءً على أمر عسكري إلكتروني" لا يُصنّف كعمل من أعمال الحرب السيبرانية[3]. هناك تعريف آخر للحرب السيبرانية يصفها بأنها "أعمال هجومية ودفاعية، متكافئة أو غير متكافئة، تتم في الشبكات الرقمية بواسطة الدول أو كيانات تشبه الدول (أو ما دون الدول). وتشتمل هذه الأعمال على مخاطر تهدد البنية التحتية الوطنية الحيوية والأنظمة العسكرية"4. عرف كل من ريتشارد أ. كلارك وروبرت كناك الحرب الإلكترونية بأنها (أعمال تقوم بها دولة تهدف إلى اختراق أجهزة الكمبيوتر والشبكات التابعة لدولة أخرى بهدف التسبب في أضرار جسيمة أو تعطيلها)5. يتطلب هذا النوع من الحروب (درجة عالية من الترابط بين الشبكات الرقمية والبنية التحتية من جانب المدافع، بالإضافة إلى تقدم تكنولوجي من جانب المهاجم)6. وينقص هذه التعاريف في الغالب الإشارة الى القواعد الأساسية للقانون الدولي الإنساني.

تعرف الحرب الإلكترونية أو السيبرانية بأنها (مجموعة من الإجراءات التي تُنفذ بهدف الاستطلاع الإلكتروني للأنظمة والوسائل الإلكترونية المعادية، وتعطيل عمل هذه الأنظمة والوسائل، ومقاومة الاستطلاع الإلكتروني من قِبل العدو، والحفاظ على استقرار عمل الأنظمة الإلكترونية الصديقة في ظل استخدام العدو لأساليب الاستطلاع والاعتراض الإلكتروني)7. ويمكن فهم هذه الحروب على أنها (تهديد مستقبلي وليس تهديدًا حاليًّا، وتتناسب تمامًا مع نموذج حرب

[3] – **Nils Melzer: Cyberwarfare and international law, Cambridge University Press,** 2011, p.4.

[4] – Shane M, Coughlan: "Is there a common understanding of what constitutes cyber warfare?", master theses, University of Birmingham School of Politics and International Studies, 30 September 2003, p. 2.

[5] – انصر سفاح كريم: الحروب الإلكترونية وأثرها على الامن القومي، مقال منشور على موقع مركز النهرين للدراسات الاستراتيجية–رئاسة الوزراء–مستشارية الامن القومي، متاح على الرابط التالي: https://www.alnahrain.iq/post/1031 .(2024/7/15)

[6] – Shane M, Coughlan, op.cit. p.2.

[7] – انصر سفاح كريم، مصدر سابق.

المعلومات)8. وهذا التعريف الأخير غير دقيق لان الحرب السيبرانية أصبحت تهديداً حقيقيا وحالياً لا يمكن تجاهله.

ايضاً، يُستخدم مصطلح "الحرب السيبرانية" للإشارة إلى (مجموعة متنوعة من الأنشطة، ويُقصد به هنا العمليات القتالية التي تحدث في الفضاء الإلكتروني وترقى إلى مستوى النزاع المسلح أو تُجرى في سياقه، وفقًا لمفهوم القانون الدولي الإنساني. عندما تتعرض الحواسيب أو الشبكات التابعة لدولة معينة لهجوم أو اختراق أو تعطيل، فإن ذلك قد يعرض المدنيين لخطر فقدان الاحتياجات الأساسية مثل المياه النظيفة والرعاية الطبية والكهرباء). على سبيل المثال، إذا تعطلت أنظمة تحديد المواقع، قد يتعرض المدنيون للإصابات نتيجة لتعطيل عمليات إنقاذ مثل إقلاع المروحيات. تتعرض السدود، والمحطات النووية، وأنظمة التحكم في الطائرات للهجمات السيبرانية نظرًا لاعتمادها على الحواسيب والشبكات المترابطة، مما يجعل من الصعب تقليل آثار الهجوم على جزء من النظام دون التأثير على أجزاء أخرى أو تعطيل النظام بأسره. قد يؤدي ذلك إلى تضرر مئات الآلاف من الناس، وتهديد صحتهم وحياتهم. لذلك، يجب على أطراف النزاع توخي الحذر بشكل مستمر لحماية المدنيين أثناء الحروب السيبرانية، وهو أحد أهم الأدوار التي يجب القيام بها، حيث أن الحرب لها قواعد وحدود تنطبق على الحرب السيبرانية بنفس القدر الذي تنطبق به على استخدام الأسلحة التقليدية مثل البنادق والمدفعية والصواريخ9.

يمكن للباحث هنا ان يدلو بدلوه محاولنا التعريف بالحرب السيبرانية على انها (أنشطة هجومية ودفاعية تحدث في الفضاء الرقمي باستخدام الوسائل الإلكترونية، تستهدف اختراق وتعطيل الشبكات والأجهزة التابعة لدول أو كيانات أخرى). ويمكن ان تشمل هذه الأنشطة الاستطلاع، وتعطيل الأنظمة، ومقاومة الاستطلاع المعادي، وحماية الأنظمة الصديقة. يمكن أن تؤدي الهجمات السيبرانية إلى أضرار كبيرة تشمل تهديد الخدمات الأساسية مثل المياه والرعاية الطبية. اذاً يمكن الباحث هنا القول ان الحرب السيبرانية تمثل تهديد حقيقي ومقلق لكثير من الدول خصوصاً وانها لم يتم تناولها بشكل مباشر في اتفاقيات القانون الدولي الإنساني بسبب حداثة هذا النوع من الحروب مما خلق فجوة في الحماية للمدنيين والاعيان المدنية.

[8] – Shane M, Coughlan, op.cit. p.2.

[9] – د. بن تغري موسى: الحرب السيبرانية والقانون الدولي الإنساني، مجلة الاجتهاد القضائي، مج12، عدد خاص (العدد التسلسلي 22)، جامعة محمد خيضر بسكرة، الجزائر، 2020، ص202.

المطلب الثاني

خصائص الحرب السيبرانية

تعد الحروب والنزاعات المسلحة أحد مظاهر الحياة، لقد عانت البشـــرية من ويلاتها على مر العصور، حيث تجعل هذه النزاعات السكان المدنيين في حالة من الاستضعاف وتعرض حقوقهم للانتهاك والاســـتغلال10. ولعل من نتائج التطور التقني وظهور الفضاء السيبراني ان أصبح لدينا ما يعرف بالحروب السيبرانية. تتميز الحروب السيبرانية بعدد من الخصـــائص التي تجعلها جذابة للفاعلين الدوليين، سواء كانوا دولًا أو جهات غير حكومية.

اولاً: تعتبر الحرب الرقمية حربًا تقنية متطورة: – حيث تركز على شـــبكة الإنترنت التي تتميز بالتطور المســـتمر والتنوع والابتكار في تقنياتها. ترتبط هذه الحرب بالمصالح الحيوية للدول، وتتميز بسرعة التنفيذ وإمكانية المراوغة، مما يمنح المهاجم ميزة واضـــحة على المدافع. كما أن أهداف الحرب الســـيبرانية وتأثيراتها غير محددة، وقد تتجاوز مخاطرها ميادين القتال التقليدية لتطال أكثر المواقع الســـيادية والحســـاســـة، بعيدًا عن دائرة المعارك المباشرة11.

ثانياً: انخفاض تكلفتها مقارنة بأدوات الحرب التقليدية: – إذ لا يتطلب انخراط طرف غير دولتي في هذا النوع من الصراعات تصنيع أسلحة مكلفة مثل حاملات الطائرات أو المقاتلات المتطورة لتهديد الأطراف الأخرى بشـــكل جدي. يكفي بدلاً من ذلك تطوير البرمجيات اللازمة وامتلاك الأجهزة الحاسوبية المناسبة لتحقيق هذا الهدف12.

ثالثاً: قدرت الحرب الســـيبرانية على تحقيق نتائج ملموسة ضمن الصراعات والنزاعات المسلحة: – كما تختلف العقيدة العسكرية وقواعد الاشتباك في الحروب السيبرانية بشكل كبير عن تلك المطبقة في الحروب التقليدية. وقد أثرت حروب الفضـــاء الســـيبراني بشـــكل كبير على طبيعة المواجهات، إذ أصبح بإمكان أطراف غير دولية أن تشارك، حيث أن الأسلحة المستخدمة في هذه الحروب ليست

[10] – نهى عبد الخالق احمد و د. سلوى احمد ميدان: المسؤولية الدولية عن استغلال الأطفال في القانون الدولي الإنساني، مجلة كلية القانون للعلوم القانونية والسياسية، مج11، 2022، ص208.

[11] – د. شويرب جيلالي وفائزة دمراد: مفهوم الحروب السيبرانية والامن السيبراني، مج11، ع1، مجلة الحقوق والحريات، جامعة محمد خيدر بسكرة، الجزائر، 2023، ص163.

[12] – وفاء بوكابوس: تحول القوة في العلاقات الدولية "دراسة في انتقال القوة من التقليدية الى الحديثة"، ط1، المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية، المانيا، 2019، ص69.

حكرًا على الدول. وهذا يجعل وصف حروب الفضاء السيبراني بأنها حروب غير متكافئة دقيقًا[13].

رابعاً: تتسم الحرب السيبرانية بميزة بارزة وهي فشـــل مفهوم الردع التقليدي: – يرجع ذلك إلى أن الهجمـات الإلكترونيـة غـالبًـا مـا تترك آثـارًا غير واضـحـة أو أدلة على وقوعها، كما أن الدمار الناتج عنها قد يشـمل التجسـس والتسـلل والتدمير بدون الحاجة إلى دماء أو أنقاض. بالإضـــافة إلى ذلك، فإن أطراف الحرب السيبرانية قد تكون غير واضحة، وتـداعيـاتهـا خطيرة من خلال تـدمير المواقع الإلكترونية وملئها بالفيروســات. كما أن اتســاع الفضـاء السـيبراني قد يسـمح بزيادة عدد المهاجمين وامتداد الصـراع في الزمان والمكان14. في الحرب السيبرانية، يكون هذا المفهوم غير فعّال بسبب عدة عوامل، أبرزها صـعوبة تحديد الدولة أو الجهة التي نفذت الهجوم. إذ يمكن للقوة المهاجمة شـــن هجوم على دولة لصالح دولة أخرى انطلاقًا من دولة ثالثة عبر اســتخدام خوادم موجودة هناك، مما يجعل تحديد مصـدر الهجمات الإلكترونية شـبه مسـتحيل في كثير من الأحيان.

خامسـاً: تتميز الحروب السـيبرانية بعدم وجود حدود جغرافية واضـــحة: – حيث لا يوجد مفهوم السـيادة بمعناه التقليدي في العالم الواقعي، حيث لا يمكن منـع الأطراف الأخرى من الـدخول إلـى المناطق الخاضعة لسيادة دولة معينة. يمكن وصف الحدود في الفضـاء الإلكتروني بأنها حدود مائعة أو غير موجودة، إذ تتداخل الشبكات بين الدول بشكل كبير، حيث تشترك الدول الصغيرة والكبيرة في نفس الشـــبكات التي قد تكون موجودة في بلدان أخرى. علاوة على ذلك، تشمل الحروب السيبرانية عمليات تدعم العمل العسكري مثل التجسس على الإشارات، أو التشـــويش على نظـام تحـديـد المواقع العـالمي وإعاقته لدى العدو، وعرقلة عمليات توجيه الأسـلحة العسكرية المعادية. تتنوع البرمجيات المستخدمة في عمليات التســـلل والاختراق، ومن أبرزها القنابل المنطقيـة، وهي قطع من التعليمـات البرمجيـة المضـــافة عمدًا إلى نظام برمجي، تقوم بإطلاق وظيفة ضـارة عند توافر شـروط محددة. كما تشـمل البرمجيات الديدان الحاســوبية التي تعتبر أدوات جديدة تتطور بســرعة مســتمرة وتحتاج إلى فك شـــفرتهـا. جوهر العقيدة العســكريـة في الحرب السـيبرانية يعتمد على السـعي لكسـب الحروب من

[13] – نورة شلوش: القرصنة الالكترونية في الفضاء السيبراني "التهديد المتصاعد من الدول"، مجلة مركز بابل للدراسات الإنسانية، مج8، ع2، جامعة بابل، 2018، ص57.

[14] – د. شويرب جيلالي وفائزة دمراد، مصدر سابق، ص163.

خلال استهداف البنية التحتية الاستراتيجية للهياكل الإلكترونية للخصم. بالتوازي مع ذلك، يستمر تطوير استراتيجيات وقدرات للحماية عبر أنظمة الدفاع السيبراني لضمان التفوق والحماية في هذا المجال المتطور15. تعتمد القوة السيبرانية في الحروب على استخدام الأجهزة والبرامج. تشمل الأجهزة أنظمة الحاسوب مثل وحدة المعالجة المركزية، ومحرك الأقراص الضوئية، ولوحة المفاتيح، بالإضافة إلى الأقمار الصناعية. أما البرامج، فتتضمن الصياغات البرمجية التي توجه عمليات الحاسوب، بما في ذلك البرمجيات الضارة والفيروسات. على سبيل المثال، تشمل لغة الاستعلام الهيكلية مجموعة من التعليمات للتفاعل مع قواعد البيانات، وعمليات الحقن الإلكتروني التي تتضمن إدخال برمجيات ضارة في الأنظمة الحاسوبية المستهدفة. كما تشمل البرمجة النصية للمواقع، التي تُستخدم لتشويه وإتلاف صفحات الويب الخاصة بالعدو، كما حدث في الهجوم الإلكتروني الروسي على إستونيا، حيث هاجم القراصنة الروس مواقع تابعة للحكومة الإستونية16. مما سبق يستنتج الباحث ان تتميز الحروب السيبرانية بعدد من الخصائص التي تجعلها جذابة للفاعلين الدوليين، بما في ذلك انخفاض تكلفتها مقارنة بالحروب التقليدية. لا تتطلب هذه الحروب استثمارات ضخمة في الأسلحة، بل يمكن أن تتم باستخدام البرمجيات والأجهزة الحاسوبية. كما أنها قادرة على تحقيق نتائج ملموسة في الصراعات المسلحة، تستهدف البنية التحتية الاستراتيجية للخصم، وتفتقر إلى الحدود الجغرافية الواضحة، مما يجعل مفهوم الردع التقليدي غير فعال. تعتمد الحروب السيبرانية على أدوات متطورة مثل الفيروسات والقنابل المنطقية، وتتميز بصعوبة تتبع مصدر الهجمات وعدم وضوح الأطراف المشاركة.

المبحث الثاني

وضع الحرب السيبرانية في إطار القانون الدولي الإنساني وبعض تطبيقاتها

الغالبية العظمى من الوسائل المتطورة للصراع المسلح التي تستخدم تكنولوجيا المعلومات والاتصالات هي ذات استخدامات متعددة، أي أنها ليست مصممة فحسب لتدمير البنى التحتية

[15] – د. انعام عبد الرضا سلطان العكابي: توظيف الحروب السيبرانية في تطوير مفهوم القوة للدول الكبرى، ع73، مجلة قضايا سياسية، جامعة النهرين، 2023، ص431-432.

[16] – احمد عيسى الفتلاوي: الهجمات السيبرانية "دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر، ط1، منشورات زين الحقوقية، بيروت، 2018، ص68.

المعلوماتية بل لمهام قتالية أخرى أيضـــا17. إن وضـــع "الحرب الســـيبرانية" يرتبط بالقانون الذي يحكمها، وهو القانون الدولي الإنساني. إذا ما دارت هذه الحرب في ســياق نزاع بين الدول قد يوصــف بأنه حرب، فإن هذا القانون هو الذي يحكم ســلوك أطراف النزاع. وعليــه، لا ينطبق القــانون الــدولي الإنســـــاني إلا إذا نُفذت العمليات الإلكترونية في ســياق نزاع مســلح وكانت مرتبطة به18. مع ذلك، فـإن العـديـد من العمليـات التي تُصـــنَّف كحرب ســيبرانية قد لا تحدث في ســياق نزاع مســلح على الإطلاق. قد تُســتَخدم مصــطلحات مثل الهجمات الإلكترونية أو الإرهاب الإلكتروني، مما يســتدعي فكرة أســاليب الحرب، ولكن العمليات التي تشــير إليها هذه المصــطلحات لا تُنفَّذ بالضــرورة في نزاع مسلح. يمكن للعمليات الإلكترونية أن تُستخدم، وهي تُســتخدم بالفعل، في جرائم تُرتكب في حالات يومية لا تتعلق بـالحرب على الإطلاق. قبل الانتقال إلى القواعد التي تحكم سير العمليات العدائية، من المهم معالجة مســألة كانت موضــوعًا للنقاش لفترة من الزمن، وهي نوع الســلوك، ولا ســيما نوع العملية الإلكترونيــة، الــذي يؤدي إلى تطبيق القواعــد التي تحكم ســير العمليات العدائية19. ســنقســم هذا المبحـث الى مطلبين، نتنـاول في المطلـب الأول مدى انطباق قواعد ومبادئ القانون الدولي الإنساني على الحرب الســيبرانية كذلك ســنعرج على بعض التطبيقات المهمة في هذا الشأن في المطلب الثاني.

المطلب الأول

انطباق القواعد والمبادئ الإنسانية على الحرب السيبرانية

ينطبق القانون الدولي الإنســـاني بمبادئه وقواعده بشــكل عام على أي نزاع مســلح، بما في ذلك الحروب السيبرانية. على الرغم من أن اتفاقيات القانون الدولي الإنساني لم تذكر الهجمات السيبرانية بشكل خاص، إلا أن هذا لا يقلل من أهميتها. يشير شرط مارتينز، وهو من المبادئ الراسخة في القانون الدولي الإنساني، إلى أن "المدنيين والمقاتلين يظلون تحت حماية وسلطة مبادئ القانون الدولي المستمدة من التقاليد الراســخة ومبادئ الإنســانية وما يمليه الضــمير العام، حتى في الحالات التي لا تغطيها

[17] – د. بن تغري موسى، مصدر سابق، ص206.

[18] – كوردولا درويغ: لا تقترب من حدود فضائي الإلكتروني، الحرب الإلكترونية والقانون الدولي الإنساني وحماية المدنيين، مجلة اللجنة الدولية للصليب الأحمر، مج94، ع886، 2012، ص542.

[19] – أمير فرج يوسف: جريمة مكافحة الإرهاب الالكتروني – الإرهاب الرقمي– في ظل اتفاقية دول مجلس التعاون لمكافحة الارهاب، ط1، دار الكتب والدراسات العربية، الإسكندرية، 2016، ص 253.

اتفاقية دولية". بناءً على ذلك، يخضع كل ما يحدث أثناء النزاع المسلح لمبادئ القانون الدولي الإنساني، ولا يوجد فراغ قانوني بالنسبة للهجمات السيبرانية. بالإضافة إلى ذلك، فإن قبول العرف الدولي كمصدر للقانون الدولي، كما هو منصوص عليه في المادة 38 من النظام الأساسي لمحكمة العدل الدولية، يؤكد خطأ أولئك الذين يرفضون انطباق القانون الدولي الإنساني على الهجمات السيبرانية بسبب غياب نص قانوني محدد20. على الرغم من شمولية مبادئ وقواعد القانون الدولي الإنساني، لا يمكن إنكار التغيرات التي طرأت على طبيعة الحروب منذ اعتماد اتفاقية جنيف الأصلية قبل نحو مائة وخمسين عامًا. فقد تطورت وسائل وأساليب الحروب إلى درجة لم يكن يتصورها واضعو تلك الاتفاقية. ويُعد الاستخدام المتزايد للفضاء السيبراني للأغراض العسكرية أحد أهم الأسباب التي تدعو إلى إعادة النظر في القواعد التي تنظم سير النزاعات المسلحة وصياغتها بشكل يتلاءم مع طبيعة هذه الاستخدامات الحديثة21. من الواضح أن هناك حاجة ملحة لتكييف الحرب السيبرانية مع القانون الدولي الإنساني. نظرًا لأن الأعمال السيبرانية قد تنتهك العديد من أحكام القوانين المسلحة الحالية أو تكون خارج نطاق هذه القوانين تمامًا، ينبغي احترام الأطر والاتفاقيات الرئيسية في هذا القانون.

فيما يتعلق بتطبيق مبدأ الإنسانية، الذي يشمل عدم التسبب في آلام غير مبررة، يمكن القول إن تطبيق هذا المبدأ على الهجمات السيبرانية لا يختلف عن جميع أشكال وأساليب الحرب الأخرى، من حيث ضرورة تجنب التسبب في أضرار أو آلام غير مبررة22. وفي إطار تطبيق مبدأ التمييز على الهجمات السيبرانية، لا يجوز لأطراف أية حرب أن يخوضوها دون أن يلتزموا بتطبيق مبدأ التمييز أثناء تنفيذ هجماتهم على العدو، والحرب السيبرانية واحدة من هذه الحروب، وهي تستلزم تطبيق هذا المبدأ بشكل صارم، لأن تأثيرها واسع المدى يصيب المدنيين كما المقاتلين، ويُصيب الأعيان المدنية

[20] – مايكل ن. شميت: الحرب بواسطة شبكات الاتصال الهجوم على شبكات الكمبيوتر (الحاسوب) والقانون في الحرب، المجلة الدولية للصليب الأحمر، مختارات من أعداد 2002، ص90.

[21] – Jeffrey T. G Kelsey, Hacking in to international humanitarian law: The principles of distinction and neutrality in the age of cyber warfare, Michigan law review, 2008, Vol. 106, Issue7, P 1437.

[22] – مايكل ن. شميت، مصدر سابق، ص135.

كما الأهداف العسكرية23. وهذا يعني أنه عند تخطيط وتنفيذ العمليات الإلكترونية، يجب أن تقتصر الأهداف المسموح بها على الأهداف العسكرية، مثل أجهزة الكمبيوتر أو النظم الحاسوبية التي تسهم بفعالية في العمليات العسكرية. لا يجوز توجيه الهجمات عبر الفضاء الإلكتروني نحو النظم الحاسوبية المستخدمة في المنشآت المدنية البحتة.

ولقد أشار دليل تالين، على الرغم من عدم إلزامية قواعده، إلى أنه لا يجوز استهداف الأعيان المدنية بالهجمات السيبرانية. فعلى سبيل المثال، يُحظر توجيه الهجمات السيبرانية التي قد تدمر الأنظمة المدنية والبنية التحتية، إلا إذا كانت هذه الأنظمة تُعتبر أهدافًا عسكرية يُسمح باستهدافها وفقًا للظروف السائدة24.

اما مبدأ التناسب، فإن البنى التحتية المدنية محمية وتشمل هذه الحماية البنى التي تدعم المستشفيات والمرافق الطبية، مراكز رعاية المسنين، النظم المالية، نظم دعم الحياة، الأجهزة الطبية الهامة، سلاسل الإمداد، وسائل النقل، مرافق الأخبار، دور العبادة والمراكز الدينية، المرافق التعليمية، المسعفين، وأجهزة إنفاذ القانون. تجدر الإشارة إلى أن هذه القائمة ليست شاملة25. يواجه تطبيق مبدأ التناسب على الهجمات السيبرانية بعض الصعوبات، نظرًا لأن الأضرار العرضية أمر لا مفر منه بسبب عدم وجود فاصل واضح في كثير من الأحيان بين الفضاء السيبراني المستخدم من قبل المدنيين وذلك المستخدم من قبل القوات والجماعات المسلحة والمدنيين المشاركين في الأعمال العدائية26. وبالرغم من الصعوبة العملية المشار إليها إلا أن دليل تالين بشأن القانون المطبق على الحروب السيبرانية، تضمن وجوب الالتزام بمبدأ التناسب، من حيث حظر الهجمات السيبرانية التي من شأنها أن تسبب الخسارة في ارواح المدنيين أو أصابتهم أو الأضرار بالأعيان المدنية أو مزيجاً منهما، والتي تكون مفرطة مقارنة بالميزة العسكرية الملموسة والمباشرة التي يتوقع من الهجوم

[23] – علاء الدين بو مرعي: دراسات وتقارير: مبدأ التمييز، والأساليب والوسائل الحربية الحديثة دراسة على ضوء مبادئ القانون الدولي الإنسان–آذار2023، المركز الاستشاري للدراسات والوثائق، لبنان، ص15.

[24] – مايكل ن. شميت، مصدر سابق، ص105.

[25] – جودي ر. وستبي: دعوة إلى الاستقرار الجيوسيبراني، مقال منشور ضمن العمل الجماعي لدكتور حمدون إ. توريه: البحث عن السلام السيبراني، الاتحاد الدولي للاتصالات، يناير 2011، ص 65.

[26] – د. احمد عبيس نعمة الفتلاوي، الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية والسياسية جامعة بابل – كلية القانون، العدد الرابع، السنة الثامنة، 2016، ص638.

الحصول عليها27. يجب على الأطراف المتصارعة اتخاذ الاحتياطات اللازمة لتقليل آثار الهجمات، مما يتطلب أن تكون نظم الحواسيب العسكرية منفصلة بشكل كافٍ عن النظم المدنية لحماية السكان المدنيين من الهجمات العشوائية والعرضية. يمكن أن يكون استخدام نظم الحواسيب العسكرية التي يديرها متعاقدون مدنيون لأغراض مدنية مثيراً للقلق. بالإضافة إلى ذلك، يمكن لتكنولوجيا المعلومات أن تساهم في تقليل الأضرار العرضية للمدنيين أو البنية التحتية المدنية. على سبيل المثال، قد يكون تعطيل خدمات معينة تُستخدم لأغراض عسكرية ومدنية أقل ضرراً من تدمير البنية التحتية بالكامل. في هذه الحالات، يفرض مبدأ الاحتياطية على الدول اختيار الوسائل الأقل تأثيراً لتحقيق أهدافها العسكرية28. فيما يخص مبدأ الضرورة العسكرية، يُعترف بوجود حالة ضرورة خلال النزاعات المسلحة التي قد تُجبر المقاتل على اتخاذ إجراءات تتجاوز السلوكيات المعتادة المسموح بها. ومع ذلك، يجب ألا تُجرد هذه الحالة من الشروط الضرورية والضوابط اللازمة لتقييدها، خاصة فيما يتعلق بمبادئ "التناسب" و"التمييز". لا يمكن السماح بانتهاك هذه الضوابط، بغض النظر عن التطورات والتغيرات في العلاقات بين الدول29، أشار دليل تالين إلى أنه عندما تتوفر خيارات متعددة لأهداف عسكرية تحقق نفس الميزة العسكرية، يجب اختيار الهدف الذي يشكل أقل خطر على المدنيين والأعيان المدنية في الهجوم السيبراني. يتطلب تطبيق مبدأ الضرورة العسكرية اختيار الهجوم الذي يسبب أقل قدر من الأضرار والإصابات، خاصة عندما تكون هناك عدة أهداف يمكن استهداف أحدها لتحقيق ميزة عسكرية أكبر. في هذه الحالات، يحق للمهاجم توجيه الهجمات السيبرانية مباشرة نحو الهدف العسكري الذي يحقق أكبر ميزة عسكرية في إطار النزاع المسلح. وينبغي

[27] – مايكل ن. شميت، مصدر سابق، ص121.

[28] – كورديولا درويغ: الحرب السيبرانية والقانون الدولي الإنساني: كيف نحمي المدنيين من الآثار العرضية لهجوم إلكتروني؟ مجلة الإنساني، ع52، مارس 2011، متاح على الرابط التالي: https://blogs.icrc.org/alinsani/2011/03/20/50/43 (2024/7/19).

[29] – اياد محمد أبو مصطفى: مبدأ الضرورة العسكرية وانتهاكات قواعد القانون الدولي الإنساني "دراسة تطبيقية على مخالفة إسرائيل لمبدأ الضرورة العسكرية خلال حرب مايو 2012"، مجلة جامعة الازهر–غزة، سلسلة العلوم الإنسانية، مج23، ع2، 2021، ص335.

النظر في الأضرار التي قد تلحق بالمنشآت والبنية التحتية الحيوية للمدنيين، بالإضافة إلى الحرمان الناتج عن تعطيل وظائف وخدمات هذه المنشآت، وفقاً لمبدأ الضرورة[30]. ووفقاً لما تقدم فأن هناك امكانية لتطبيق مبادئ وقواعد القانون الدولي الإنساني، حيث يظهر أهمية ذلك على الرغم من عدم ذكر الهجمات السيبرانية بشكل محدد في الاتفاقيات القائمة. كما يبرز فيما سبق الحاجة الملحة لتكييف القوانين الدولية لمواجهة تحديات الفضاء السيبراني وضمان حماية فعالة للمدنيين والبنية التحتية المدنية من الأضرار غير المبررة.

المطلب الثاني

تطبيقات الهجمات السيبرانية

سوف نتطرق في هذا المطلب الى بعض النماذج للهجمات السيبرانية على الصعيد الدولي لنبين مدى قوة وتأثير تلك الهجمات على امن البلدان المستهدفة وانها لا تقل ضرراً عما يقع في سياق الحروب التقليدية.

اولاً: الهجمات السيبرانية الروسية على أوكرانيا: –

في الفترة التي سبقت الغزو الروسي لأوكرانيا في العام 2022، أثار الخبراء مخاوف بشأن الهجمات الإلكترونية الروسية على أوكرانيا واحتمال انتشارها إلى دول أخرى. هناك سابقة لكلا الأمرين. ففي عامي 2015 و2016، أطلقت روسيا عمليات إلكترونية أدت إلى انقطاع التيار الكهربائي في أوكرانيا، وفي عام 2017، استخدمت روسيا برنامج محاسبة أوكراني لإطلاق برامج ضارة مدمرة تُعرف باسم NotPetya والتي على الرغم من أنها كانت متنكرة في هيئة برامج فدية، إلا أنها في الواقع "شفرت الملفات بشكل لا رجعة فيه"، مما جعل دفع الفدية "غير مجدٍ". انتشر NotPetya في جميع أنحاء العالم، مما تسبب في أضرار بلغت 10 مليارات دولار. نظرًا لهذا التاريخ وسنوات من التكهنات حول شكل الحرب التي تشنها قوة إلكترونية، كانت التوقعات عالية بأن العمليات الإلكترونية ستلعب دورًا رئيسيًا في الغزو الأولي. بدلاً من ذلك، يبدو أن دورها كان محدودًا نسبيًا، مما أثار الدهشة بين العديد من المتابعين للعمليات الإلكترونية الروسية. على سبيل المثال، أعلن رئيس لجنة الاستخبارات في مجلس الشيوخ مارك وارنر أنه "مندهش من أن [الروس] لم يطلقوا حقًا مستوى الخبث الذي تتضمنه ترسانتهم الإلكترونية". كانت حوادث الأمن السيبراني المعروفة في الفترة التي سبقت الغزو والأسابيع التي أعقبته مباشرة متواضعة نسبيًا في التأثير. على سبيل المثال، في منتصف

[30] – مايكل ن. شميت، مصدر سابق، ص130.

فبراير، أدى هجوم رفض الخدمة الموزع الذي شنته المؤسسة العسكرية الروسية إلى تعطيل الوصول إلى مواقع الويب الخاصة بالعديد من الإدارات الحكومية وأكبر بنكين في أوكرانيا لفترة وجيزة، كما أدت العمليات الإلكترونية إلى تعطيل بعض خدمات الإنترنت بشكل متقطع. كما اكتشف الباحثون عدة أنواع من برامج مسح البيانات الضارة، التي تدمر أو تفسد البيانات، على الأنظمة الأوكرانية قبل الغزو وبعده، على الرغم من أن البرامج الضارة يبدو أنها تسببت في أضرار محدودة حتى الآن31.

ثانياً: الهجمات السيبرانية على استونيا: –

إن الإرهاب الإلكتروني الذي ضرب إستونيا في عام 2007 لم يكن مجرد إزعاج مؤقت؛ بل كان في واقع الأمر نسخة خفيفة من شكل جديد من أشكال العنف الرقمي الذي قد يوقف الخدمات العامة والتجارة وعمليات الحكومة. وقد لاحظ وزير الدفاع الإستوني جاك آفيكسو أن الهجمات الإلكترونية الناجحة "يمكن مقارنتها بشكل فعال بإغلاق الموانئ أمام البحر"32.

والحصار هو تشبيه مناسب، لأن الهجمات الإرهابية الإلكترونية في المستقبل قد تؤدي إلى تعطيل إمدادات المياه والكهرباء في البلاد، والاتصالات السلكية واللاسلكية (قطع اتصالاتها بالعالم)، والدفاعات الوطنية. لقد أثارت خطورة الهجمات على إستونيا استجابة دولية سريعة. ولم يكن لدى إستونيا سوى القليل من الاستعدادات الرسمية للدفاع السيبراني خارج إطارها لمكافحة الأعمال الإرهابية التقليدية33، أصبحت إستونيا واحدة من أوائل الدول في العالم التي طورت استراتيجية وطنية شاملة للأمن السيبراني34. وطلب

31 – Kristen E. Eichensehr: SYMPOSIUM ON UKRAINE AND THE INTERNATIONAL ORDER UKRAINE, CYBERATTACKS, AND THE LESSONS FOR INTERNATIONAL LAW, AJIL UNBOUND, Vol. 116, 2022, p.145-146.

32 – Stephen Herzog: Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses, Journal of Strategic Security 4, no. 2 , 2011, p.53.

33 – Ulrich Sieber and Phillip W. Brunst, Cyberterrorism—the use of the Internet for terrorist purposes (Strasbourg: Council of Europe Publishing, 2007), 161-166.

34 – استراتيجية الأمن السيبراني، وزارة الدفاع الإستونية، 2008، متوفرة على: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/cyber-security-

فريق الاستجابة لحالات الطوارئ الحاسوبية الحكومي المساعدة من فنلندا وألمانيا وإسرائيل وسلوفينيا لاستعادة عمليات الشبكة الطبيعية. قدمت فرق الاستجابة لحالات الطوارئ الحاسوبية التابعة لحلف شمال الأطلسي مساعدة إضافية، في حين قدمت وكالة الأمن السيبراني الأوروبية التابعة للاتحاد الأوروبي تقييمات فنية متخصصة للوضع المتطور. وعلاوة على ذلك، حدث مستوى عال من تبادل المعلومات الاستخباراتية بين الدول الغربية أثناء الأزمة. وبينما استخدم المتسللون الناطقون بالروسية الإنترنت كسلاح وأداة للتعبئة، استخدمت إستونيا وحلفاؤها الشبكات الرقمية لمواجهة الهجمات بنجاح35.

ثالثاً: الهجمات السيبرانية المتبادلة بين إيران وإسرائيل: –

تعرضت إسرائيل لهجمات سيبرانية نفذتها مجموعة "أنونيموس"، مما كبدها خسائر مادية ومعنوية كبيرة. هذا يشير إلى تحول في وسائل الصراع مع إسرائيل نحو الاعتماد على التكنولوجيا والفضاء السيبراني في الحروب القادمة. في أبريل 2013، تعرضت المواقع الإسرائيلية لأكبر الهجمات السيبرانية، حيث نجحت المجموعة في اختراق مواقع الحكومة والجيش والصناعات العسكرية، بما في ذلك موقع رئيس الوزراء، ووزارة الدفاع، والاستخبارات، ومجلس الوزراء، وسوق الأوراق المالية، والمحاكم الإسرائيلية، وشرطة تل أبيب، ووزارة التعليم، وبنك القدس. بالإضافة إلى ذلك، نشرت المجموعة بيانات شخصية لأكثر من 5000 مسؤول إسرائيلي، تضمنت أسماؤهم وأرقامهم والعناوين الشخصية لبريدهم الإلكتروني. وفي السياق ذاته، نفذت إيران عمليات سيبرانية رداً على نزاعات أو توترات أو تحركات اعتبرتها هجومية. صُممت هذه العمليات لإلحاق تكاليف ملموسة وإظهار القدرة على استهداف استراتيجي، مع الحفاظ على إمكانية الإنكار المعقول وتجنب التصعيد. كما تعرضت إيران لهجمات سيبرانية متعددة شنتها الولايات المتحدة الأمريكية، باعتبارها حليفًا استراتيجيًا لإسرائيل. استخدمت الولايات المتحدة فايروس "Stuxnet"، الذي تم تطويره لاستهداف المنشآت الصناعية الإيرانية، وخاصة النووية منها، مما أدى إلى تدمير أكثر من 1000 جهاز طرد

strategy/@@download_version/993354831bf

c4d689c20492459f8a086/file_en

.(2024/7/19)

[35] – Stephen Herzog, op.cit. p.53.

مركزي، فضـــلاً عن الهجمات التي تعرضـــت لها محطات النفط الإيرانية36.

من خلال دراســتنا للتطبيقات الســابقة للحرب الســـيبرانية يظهر جلياً للباحث مدى الدمار الذي تخلفه الهجمات السيبرانية والتي في الغالب لا تميز بين المدنيين والعســـكريين ولا بين الاعيان المدنية والعســـكرية، كل هذا يتطلب تحرك جاد لتنظيم هذه الحرب بما يتلائم مع روح الإنســـانية التي حملتها قواعد ومبادئ القانون الدولي الإنســـاني منذ اتفاقية جنيف الام التي ابرمت في النصف الثاني من القرن التاسع عشر.

الخاتمة

يمكن ان نلخص أهم الاستنتاجات والمقترحات التي توصــلنا اليها من البحث في موضــوع "فاعلية القانون الدولي الإنساني في تنظيم الحرب السيبرانية" وهي كالتالي:

أولاً: الاستنتاجات: -

1 - تُمثل الهجمات الســـيبرانية تهديداً متزايداً للبنية التحتية المدنية والحيوية، مثل قطاع الرعاية الصـــحية، وأنظمة الكهرباء والمياه. هذه الهجمات تتسـبب في أضـرار قد تصـل إلى تعطيل الخدمات الأساسية للمجتمعات المدنية.

2- رغم أن القانون الدولي الإنســاني لم يذكر الهجمات الســـيبرانية بشـــكل محدد، إلا أنه يمكن تطبيق مبادئه على النزاعات السيبرانية، بما في ذلك مبادئ التمييز والتناسب والاحتياط.

3 - تتميز الحرب السيبرانية بعدم وجود حدود جغرافية واضـحة وصـعوبة تحديد مصـدر الهجمات، مما يعقد عملية الردع التقليدي ويجعل من الصـعب تطبيق قواعد الحرب التقليدية بشكل مباشر.

ثانياً: المقترحات: -

1 - يجــب على المجتمع الــدولي تكييف وتحديث قواعد القانون الدولي الإنســـاني لتشـــمل الهجمات السيبرانية بشكل أكثر وضـوحاً، مع الأخذ في الاعتبار الخصائص الفريدة للفضاء السيبراني.

4 - توضح الهجمات السيبرانية مثل تلك التي شـنتها روسـيا على أوكرانيا أن هذه الهجمات يمكن أن تكون فعـالـة ومـدمرة بقـدر مـا يمكن أن تكون الهجمات التقليدية، مما يؤكد على الحاجة لتطبيق قوانين واضحة ومناسبة.

---

[36] - د. شيماء معروف فرحان: التحول في مفهوم القوة والصراع "دراسة في الحروب السيبرانية"، مجلة قضايا سياسية، ع75، 2023، ص509-510.

2 – تعزيز التعاون الدولي وتبادل المعلومات بين الدول لمواجهة التهديدات السـيبرانية. يجب أن يشمل هذا التعاون تحسين القدرة على الكشف عن الهجمات وتطوير استراتيجيات دفاعية متكاملة.

3 – وضع استراتيجيات وقائية لتقليل الأضرار المحتملة للهجمات السـيبرانية، بما في ذلك تحسـين البنية التحتية الأمنية وتعزيز الوعي السـيبراني بين الأفراد والمؤسسات.

4 – يجب أن تعمل الدول والمنظمات الدولية على توضـيح وتعريف مفهوم الهجمات السـيبرانية بشـكل دقيق ضـمن إطار القانون الدولي، لضـمان توافق أفضل بين القوانين والتطبيقات العملية.

5 – دعم البحـث والتطوير في مجـال الأمن السـيبراني والقانون الدولي لتأمين الفضـاء السـيبراني وضمان حماية فعالة للمدنيين والبنية التحتية الحيوية من الهجمات السيبرانية.

الملخص

إن الحرب السيبرانية هي نتيجة طبيعية للثورة التكنولوجية في القرن الحادي والعشرين، والتي كانت ثورة بلا حدود. وتمثل الحرب السيبرانية تهديدًا متزايدًا للبنية التحتية المدنية للدول قبل العسكرية، مثل قطاع الرعاية الصحية وأنظمة الكهرباء. وتسبب هذه الهجمات أضرارًا قد تصل إلى حد تعطيل الخدمات الأساسية. ورغم أن القانون الدولي الإنساني لا يذكر الهجمات السيبرانية على وجه التحديد، إلا أن مبادئه يمكن تطبيقها على الحرب السيبرانية. وتتميز الحرب السيبرانية بعدم وجود حدود جغرافية واضحة وصعوبة تحديد مصدر الهجمات، مما يعقد عملية الردع التقليدي ويجعل من الصعب تطبيق قواعد الحرب التقليدية بشكل مباشر. وهنا يتعين على المجتمع الدولي تكييف وتحديث قواعد القانون الدولي الإنساني لتشمل الهجمات السيبرانية بشكل أكثر وضوحًا، مع مراعاة الخصائص الفريدة للفضاء السيبراني. كما ينبغي تعزيز التعاون الدولي وتبادل المعلومات بين الدول لمواجهة التهديدات السيبرانية. وينبغي أن يشمل هذا التعاون تحسين القدرة على اكتشاف الهجمات وتطوير استراتيجيات دفاعية متكاملة.

الكلمات المفتاحية: القانون الدولي الإنساني، الحرب السيبرانية، الهجمات السيبرانية، التعاون الدولي، البنية التحتية الحيوية.

Abstract

Cyber warfare is a natural consequence of the technological revolution of the 21st century, which has been a revolution without borders. Cyber warfare poses an increasing threat to the civilian infrastructure of states before their military ones, such as the health care sector and electricity systems. These attacks cause damage that may even disrupt essential services. Although international humanitarian law does not specifically mention cyber-attacks, its principles can be applied to cyber warfare. Cyber warfare is characterized by the lack of clear geographical boundaries and the difficulty of identifying the source of attacks, which complicates the process of conventional deterrence and makes it difficult to apply the rules of conventional warfare directly. Here, the international community must adapt and update the rules of international humanitarian law to include cyber-attacks more clearly, taking into account the unique characteristics of cyberspace. International cooperation and information exchange between states should also be strengthened to confront cyber threats. This cooperation should include improving the ability to detect attacks and developing integrated defense strategies.

Keywords: International Humanitarian Law, Cyber Warfare, Cyber Attacks, International Cooperation, Critical Infrastructure.