تحديات تطبيق مبدأ التمييز في ساحة المعركة السيبرانية

دكتوره

حنان أحمد الفولى أبوزيد

أستاذ مشارك في القانون الدولي العام – كلية الحقوق

جامعة طيبة

المقدمة:

إن مبدأ التمييز هو أحد المفاهيم الأساسية في القانون الدولي الإنساني؛ حيث يتمتع بعض الأشخاص والأشياء بالحماية ضد الهجمات بسبب وضعهم المدني، ومع التحول الرقمي الذي أدى الى بزوغ عصر جديد من الصراع مع أساليب جديدة تمامًا لتنفيذ العمليات العسكرية. تطور مسرح الحرب منتقلاً للفضاء السيبراني، ومن هنا برزت تحديات جديدة تهدد تطبيق مبدأ التمييز الذي يعد حجر الزاوية في حماية المدنيين أثناء النزاعات المسلحة، حيث يواجه اليوم اختبارًا غير مسبوق. ففي حين كانت الخطوط الفاصلة بين المقاتلين والمدنيين واضحة نسبيًا في النزاعات التقليدية الحركية، أصبح هذا التمييز أكثر صعوبة وتعقيدًا في العصر الرقمي. إن تداخل الأنشطة المدنية والعسكرية في الفضاء السيبراني، وصعوبة تحديد هوية المشاركين في العمليات الإلكترونية، وتمييز الأفراد والأشياء التي تشارك في القتال، وتلك التي لا تشارك فيه، قد أدى إلى إرباك في تطبيق هذا المبدأ مهددا بتقويضه.

مشكلة البحث :

تتمحور مشكلة البحث في الإجابة على سؤال رئيسي وهو: **ما هي التحديات التي تواجه تطبيق مبدأ التمييز في ظل التحول الرقمي للحروب، وتهدد حياة هذا المبدأ؟ وهل يمكن تطبيق هذا المبدأ في سياق النزاعات السيبرانية؟**

ويتفرع عن هذا السؤال الرئيسي عدة أسئلة فرعية تتمثل في:

1. هل يشكل الهجوم السيبراني نزاع مسلح في مفهوم القانون الدولي الإنساني؟
2. متى تعد مساهمة المدنيين في العمليات السيبرانية مشاركة في الاعمال العدائية؟
3. هل المفاهيم التقليدية للمدني والمقاتل في القانون الدولي الإنساني، والتي وُضعت في سياق الحروب التقليدية، قابلة للتطبيق على الفاعلين في الفضاء

السيبراني؟ وإذا لم تكن كذلك، كيف يمكن تكييفها لتلائم طبيعة الحرب السيبرانية؟

أهمية البحث:

- **الأهمية العلمية :**

1. يساهم في تطوير الفهم النظري لمبدأ التمييز في سياق الحرب السيبرانية، وهو مجال ناشئ في القانون الدولي الإنساني.

2. يسلط الضوء على التحديات القانونية والعملية، غير المسبوقة، التي فرضتها ساحة المعركة السيبرانية على تطبيق مبدأ التمييز.

3. يقدم تحليلاً قانونيا ونقديا معمقًا لتحديد متى ترقى مساهمات المدنيين في الأنشطة السيبرانية إلى مستوى المشاركة المباشرة في الأعمال العدائية، وذلك في ضوء دليل تالين[1] والدليل التفسيري للجنة الدولية للصليب الأحمر[2]، كما يستعرض العواقب القانونية لهذه المشاركة وفقًا لقواعد القانون الدولي الإنساني.

4. يجري مقاربة قانونية لتقييم مدى ملاءمة وصلاحية مفهومي "المدني" و"المقاتل" - كما هما معرفان في القانون الدولي الإنساني - للتطبيق في سياق الفضاء السيبراني.

---

[1] دليل تالين هو دراسة أكاديمية غير ملزمة تهدف إلى توضيح كيفية تطبيق القانون الدولي على الحرب السيبرانية، تم إعداده من قبل مجموعة دولية من الخبراء القانونيين بدعوة من مركز التميز للدفاع السيبراني التعاوني التابع لحلف الناتو في تالين (عاصمة استونيا)، تضمن الدليل قواعد وتعليقات حول تطبيق القانون الدولي على العمليات السيبرانية، بما في ذلك مبدأ السيادة، المسؤولية الدولية، وقواعد القانون الدولي الإنساني، وبالرغم أنه غير ملزم قانوناً، إلا أنه يحظى باحترام واسع في الأوساط القانونية والدبلوماسية، هناك نسخة باللغة الإنجليزية ونسخة مترجمة باللغة العربية، وقد اتخذنا من كلا النسختين مرجع، ولكن الرجوع الرئيسي للنسخة باللغة الانجليزية حيث أن النسخة المترجمة لا تحتوى على التعليقات، واقتصرت على القواعد .

[2] الدليل التفسيري هو دليل صادر عن اللجنة الدولية للصليب الأحمر بشأن مفهوم المشاركة المباشرة في الأعمال العدائية.

تهدف هذه المقاربة إلى تحديد التحديات والثغرات في تطبيق هذه المفاهيم على النزاعات السيبرانية.

ـ الأهمية العملية:

1. يساعد في تطوير استراتيجيات أفضل لحماية البنية التحتية المدنية الحيوية من الهجمات السيبرانية خلال النزاعات المسلحة.

2. يقدم أساساً لصياغة سياسات وقوانين جديدة تتعلق بالحرب السيبرانية، مما قد يساهم في تعزيز الأمن السيبراني الدولي.

3. يساعد القادة العسكريين وصانعي القرار في فهم التبعات القانونية والأخلاقية للعمليات السيبرانية.

مصطلحات البحث:

1. مبدأ التمييز: تتعدد صياغاته في الفقه القانوني، فيعرف بـ" **مبدأ التمييز بين المقاتلين والمدنيين"** أو**" مبدأ التمييز بين المقاتلين وغير المقاتلين "** ويفضل البعض المصطلح الثاني لشموله المقاتلين الذين كفوا عن المشاركة في الاعمال العدائية،[1] وتستخدم اللجنة الدولية للصليب الأحمر بشكل أساسي المصطلح الاول في وثائقها ومنشوراتها الرسمية، كما تستخدم الأمم المتحدة ووكالاتها المتخصصة، مثل مكتب الأمم المتحدة لتنسيق الشؤون الإنسانية **(OCHA)**، ذات المصطلح في

[1] انظر هذا الرأي: العقون ساعد، مبدأ التمييز بين المقاتلين وغير المقاتلين وتحديات النزاعات المسلحة المعاصرة، رسالة ماجستير، كلية الحقوق، جامعة الحاج لخضر، باتنة، الجزائر، 2009. ولمزيد من التفصيل حول المصطلح انظر:

Sabin Guțan, The Meaning of the Term Noncombatant in International Humanitarian Law – Interpretation of the Provision of Article 37/1/c of the Additional Protocol I of Geneva of 1977. International conference Knowledge-Based Organization, Vol.28, 2022, PP. 51-56.

تقاريرها ووثائقها المتعلقة بالقانون الدولي الإنساني، في حين تستخدم بعض المنظمات غير الحكومية، مثل منظمة العفو الدولية ومنظمة Human Rights Watch، كلا المصطلحين في تقاريرها وبياناتها الصحفية، وفي الأوساط الأكاديمية والبحثية، يُستخدم كلا المصطلحين بشكل متبادل، مع ميل نحو استخدام المصطلح الأول، وسوف يستخدم البحث المصطلح الأول لأنه الأكثر شيوعاً واستخداماً من قبل المنظمات الدولية الرئيسية، مثل اللجنة الدولية للصليب الأحمر والأمم المتحدة، ولاتساقه مع اتفاقيات جنيف الأربع لعام 1949 وبروتوكولاتها الإضافية التي تستخدم، بشكل أساسي، مصطلح "المدنيين" كما ان هذه الآليات اعتبرت ان المدني هو كل شخص لا ينطبق عليه وصف المقاتل .

2. الحرب السيبرانية: أدت رقمنة النزاعات المسلحة الى استخدام عدد من المصطلحات التي تطلق على النزاعات والحروب الحديثة التي تستخدم فيها التكنولوجيا والتقنيات المتقدمة، والتي تكون فيها التكنولوجيا والفضاء الرقمي ساحات رئيسية للنزاع، إلى جانب الساحات التقليدية مثل الأرض والبحر والجو، وهذه المصطلحات هي:

- الحرب السيبرانية **(Cyber Warfare):** تشمل الهجمات على أنظمة الحاسوب والشبكات والبنية التحتية الرقمية، وتركز على استهداف الأنظمة المعلوماتية والبيانات.

- الحرب الإلكترونية **(Electronic Warfare):** وتتعلق بالتشويش على الاتصالات الإلكترونية والرادارات، وتركز على الطيف الكهرومغناطيسي، وهي المصطلح الاقدم في الاستخدام وأكثر ارتباطاً بالعمليات العسكرية التقليدية.

- الحرب الرقمية **(Digital Warfare):** مصطلح أوسع يشمل جميع أشكال الصراع في البيئة الرقمية، قد يتضمن عناصر من الحرب السيبرانية والإلكترونية.

نظرًا لأن مصطلح "الحرب السيبرانية" هو الأكثر شيوعًا واستخدامًا في الوقت الحالي، لا سيما في الأوساط الأكاديمية والقانونية والعسكرية على الصعيد الدولي، فسيعتمد البحث هذا المصطلح بمفهوم شامل، يغطي كافة أشكال العمليات العدائية في الفضاء الرقمي. بمعنى أنه سيشمل ضمنيًا المفاهيم المرتبطة بالحرب الرقمية والإلكترونية، مع التركيز على الجوانب المتعلقة بالهجمات على أنظمة المعلومات والبنية التحتية الرقمية.

منهج البحث:

تم توظيف المنهج الوصفي لبناء إطار مفاهيمي شامل لموضوع البحث، مما يوفر أساسًا نظريًا متينًا للدراسة. كما تم استخدام المنهج الاستقرائي لاستكشاف وتحديد الإشكاليات القانونية والعملية التي تواجه تطبيق مبدأ التمييز في النزاعات السيبرانية، كما تم توظيفه في استقراء أمثلة عملية تدعم وجهات نظر الباحث وتعزز اراءه. وتم تطبيق المنهج الاستنباطي لتحليل هذه الإشكاليات المحددة بعمق، بهدف استخلاص رؤية استشرافية لمستقبل تطبيق مبدأ التمييز في سياق النزاعات السيبرانية. في سبيل صياغة حلول مقترحة لمواجهة التحديات التي تعترض تطبيق المبدأ في الفضاء السيبراني.

خطة البحث:

المبحث الأول: الإطار المفاهيمي لمبدأ التمييز والحرب السيبرانية

المطلب الأول: ماهية مبدأ التمييز في القانون الدولي الإنساني

المطلب الثاني: مفهوم الحرب السيبرانية وخصائصها

المبحث الثاني: تحديات النطاق الشخصي لمبدأ التمييز في الفضاء السيبراني

المطلب الأول: وضع المقاتل في الحرب السيبرانية

المطلب الثاني: المشاركة المدنية في ساحة المعركة السيبرانية

المبحث الثالث: تحديات النطاق العيني لمبدأ التمييز في الفضاء السيبراني

المطلب الأول: غموض مفهوم الهجوم في الفضاء السيبراني

المطلب الثاني: تداخل البنية التحتية المدنية والعسكرية في الفضاء السيبراني

المبحث الأول: الإطار المفاهيمي لمبدأ التمييز والحرب السيبرانية

يشهد عالمنا المعاصر تحولات جذرية في طبيعة النزاعات وأساليب الحرب، مما يستدعي إعادة النظر في المفاهيم والمبادئ القانونية التقليدية. وفي هذا السياق، يبرز مبدأ التمييز كأحد الركائز الأساسية في تنظيم سير العمليات العدائية، بينما تظهر الحروب السيبرانية كنمط جديد من أنماط الصراع يتحدى الأطر القانونية القائمة، وتعد دراسة الإطار المفاهيمي لكل من مبدأ التمييز والحروب السيبرانية خطوة أولية وضرورية لفهم طبيعة التحديات الراهنة التي تواجه هذا المبدأ في ساحة المعركة السيبرانية.

المطلب الأول: ماهية مبدأ التمييز في القانون الدولي الإنساني

يقوم القانون الدولي الانساني على نوعين من المبادئ الخاصة به، والتي تسري وتنطبق فقط في حالة النزاعات المسلحة، النوع الاول هي المبادئ الخاصة بسير العمليات العدائية والتي تنظم سبل ووسائل القتال، وكذلك الاسلحة التي من شأنها أن تسبب الآماً لا تتناسب مع الهدف المشروع للحرب، ومن أمثلتها مبدأ حظر الالام التي لا مبرر لها. اما النوع الثاني فهي المبادئ التي تحمي الاشخاص الذين لا يشاركون او كفوا عن المشاركة في الاعمال العدائية، ومن امثلتها مبدأ التناسب.[1]

ومبدأ التمييز من المبادئ القانونية الخاصة التي يقوم عليها القانون الدولي الإنساني، والتي استقرت وثبتت في الاتفاقيات الدولية، والأعراف الدولية، الا انه يمتاز عن غيره من مبادئ القانون الدولي الانساني بأنه يندرج ضمن النوعين فهو من جهة يقيد سبل ووسائل القتال غير التمييزية (العمياء وعشوائية الأثر) ومن جهة اخرى يحمى الفئات غير المشاركة في العمليات العدائية.

[1] انظر: هشام بشير، إبراهيم عبد ربه إبراهيم، المدخل لدراسة القانون الدولي الإنساني، المركز القومي للإصدارات القانونية ، القاهرة ، ط1 ، 2012م ، ص 50 – 51، أ.د/ بدر الدين عبد الله حسن حمد، القانون الدولى الإنساني، مكتبة المتنبي، 1444ه، ص71.

أولا: تعريف مبدأ التمييز:

ينطلق مبدأ التمييز من مسلمة مفادها أنه إذا كان افراد القوات المسلحة – بما فيهم المتطوعون وأفراد الميليشيات غير النظامية – لهم وحدهم حق مهاجمة العدو ومقاومته، في العمليات العدائية، فإن العمليات القتالية يجب أن توجه لهم وحدهم، فالأفراد العاديون – سواء المواطنين المتمتعين بجنسية الدولة أو الأجانب المقيمين على أراضيها- لا يشتركون، من حيث الأصل، في العمليات القتالية، ومن ثم يجب الا تمتد العمليات القتالية إليهم، ويحظر توجيه الهجمات لهم.[1]

فطالما ان المدنيين ليسوا مقاتلين فهم محميّون من كلّ هجوم، وعليه فإن الهجمات التي لا تميز بين المقاتلين والمدنيين، وبين الأهداف العسكرية والأعيان المدنية محظورة، ومن ثم يجب على الدول أن تراعي عند شن العمليات الحربية التمييز بين المقاتلين وغير المقاتلين وبين الاهداف العسكرية والاعيان المدنية بحيث تقتصر هجماتها على المقاتلين دون المدنيين وعلى الاهداف العسكرية دون الاعيان المدنية.[2]

ويتضح من ذلك أن مبدأ التمييز يعمل على نطاقين: أحدهما شخصي، يقوم على التمييز بين المدنيين والمقاتلين على مستوى الأشخاص، والآخر مكاني، يقوم على التمييز بين الاهداف والأعيان على مستوى المنشآت والمباني، مدنية كانت أم عسكرية.[3]

---

[1] حسين على الدرديري ، القانون الدولي الإنساني(ولادته- نطاقه- مصادره)، دار وائل للنشر، ط1 ، 2012م ، ص 428

[2] محمد أحمد سليمان عيسى، المبادئ الأساسية التي تحكم النزاعات المسلحة في الشريعة الإسلامية والقانون الدولي الإنساني، أعمال المؤتمر العلمي الدولي: القانون الدولي الإنساني في ضوء الشريعة الإسلامية، ضمانات التطبيق والتحديات المعاصرة، غزة: الجامعة الإسلامية - كلية الشريعة والقانون واللجنة الدولية للصليب الأحمر، 2015، ص 405.

[3] حيدر كاظم علي، مبدأ التمييز بين المدنيين والمقاتلين (دراسة في ضوء أحكام القانون الدولي الإنساني)، مجلة الكلية الاسلامية الجامعة، مج 1، ع22، 2013، ص 383.

نشأة مبدأ التمييز نشأة عرفية، ولأهميته حاز اهتمام اللجنة الدولية للصليب الأحمر، وتم تطويره وتدوينه في العديد من الاتفاقيات الدولية الإنسانية.[1]

ويشير مبدأ التمييز في القانون الدولي الإنساني إلى وجوب التفرقة بين الأهداف العسكرية المشروعة من جهة، والمدنيين والأعيان المدنية من جهة أخرى، وذلك أثناء النزاعات المسلحة، حيث يهدف إلى حماية المدنيين والأعيان المدنية من آثار الأعمال العدائية، ويُلزم أطراف النزاع باتخاذ كافة الاحتياطات الممكنة لتجنيب السكان المدنيين هذه الأثار، ويقصر الهجمات على الأهداف العسكرية فقط، ويوجب على اطراف النزاع ألا تستهدف عملياتها الحربية المدنيين وأولئك الأشخاص الذين أصبحوا غير قادرين على القتال - أي الجرحى والمرضى والغرقى وأسرى الحرب - أو أفراد الخدمات الطبية والدينية سواء كانوا مدنيين أم عسكريين، وأفراد الدفاع المدني وأفراد منظمات الإغاثة الإنسانية الدوليين والمحليين المرخص لهم بأعمال الإغاثة. وفيما يتعلق بالأعيان يوجب مبدأ التمييز على الأطراف المتحاربة، والامتناع عن استهداف كل مبني لا يشكل هدفا عسكريا، وبصفة خاصة السدود والمحطات النووية لتوليد الطاقة الكهربائية، والممتلكات التي لا غنى عنها لبقاء السكان المدنيين على قيد الحياة، وتوفير الحماية للمناطق الآمنة والمحايدة ومنزوعة السلام، والمحلات غير المحمية عسكريا والأعيان الثقافية.[2]

---

[1] العقون ساعد، مبدأ التمييز بين المقاتلين وغير المقاتلين وتحديات النزاعات المسلحة المعاصرة، مرجع سابق، ص 24 -حسين على الدرديرى، القانون الدولي الإنساني (ولادته- نطاقه- مصادره) مرجع سابق ، ص 427.

[2] محمد أحمد سليمان عيسى، المبادئ الأساسية التي تحكم النزاعات المسلحة في الشريعة الإسلامية والقانون الدولي الإنساني، أعمال المؤتمر العلمي الدولي: القانون الدولي الإنساني في ضوء الشريعة الإسلامية، ضمانات التطبيق والتحديات المعاصرة، غزة: الجامعة الإسلامية - كلية الشريعة والقانون واللجنة الدولية للصليب الأحمر، 2015، ص 405.

ويمكن تلخيص المقصود بهذا المبدأ في النقاط التالية[1]:

1. يجب على أطراف النزاع التمييز في جميع الأوقات بين المقاتلين والمدنيين. فالمدنيون لا يجوز أن يكونوا هدفًا للهجوم، ويجب اتخاذ كافة الاحتياطات الممكنة لتجنيبهم آثار الأعمال العدائية.

2. يجب التمييز بين الأعيان المدنية (كالمنازل والمدارس والمستشفيات) والأهداف العسكرية. فالأعيان المدنية محمية من الهجوم، إلا إذا تحولت إلى أهداف عسكرية.

3. تُعرَّف الأهداف العسكرية بأنها تلك الأهداف التي تسهم إسهامًا فعالًا في العمل العسكري، سواء بطبيعتها، أم بموقعها، أم بغايتها أم باستخدامها، والتي يحقق تدميرها كليًا أو جزئيًا أو الاستيلاء عليها أو تعطيلها ميزة عسكرية أكيدة.

4. تحظر الهجمات العشوائية التي لا تميز بين الأهداف العسكرية والمدنيين أو الأعيان المدنية. كما يحظر استخدام أسلحة أو أساليب قتال لا يمكن حصر آثارها بما يتفق مع هذا المبدأ.

5. في حالة الشك، يجب اعتبار الأشخاص مدنيين والأعيان مدنية ومن ثم لا يجوز مهاجمتها.

ثانيا: أهمية مبدأ التمييز في حماية المدنيين:

لما كانت الغاية من القانون الدولي الانساني هي حماية الفئات غير المساهمة في العمليات القتالية؛ لذا يعد مبدأ التمييز هو أساس القانون الدولي الإنساني، ويمكن اختصار وظيفة هذا المبدأ في لفظ واحد وهو الحماية.[2] حيث يشكل حصانة عامة

[1] المواد 48، 51، 52 من البروتوكول الإضافي الأول لعام 1977م بشأن حماية ضحايا النزاعات المسلحة الدولية.

[2] عامر الزمالي، التفرقة بين المقاتلين وغير المقاتلين وصلتها بالنظام الأساسي للمحكمة الجنائية الدولية، منشور في كتاب المحكمة الجنائية الدولية وتوسيع نطاق القانون الدولي الإنساني، جامعة دمشق واللجنة الدولية للصليب الاحمر، 2004، ص20.

للعناصر المدنية غير المساهمة في العمليات العدائية، وبالتالي يمثل حجر الأساس في تحقيق الهدف المنشود للقانون الدولي الإنساني.

وقد صنف القاضي البيجاوي هذا المبدأ ضمن " القواعد الآمرة في القانون الدولي الإنساني " حيث أنه قانون" معنى اساساً بالتمييز في استخدام الاسلحة "[1]، كما قضت غرفة الاستئناف بالمحكمة الجنائية الدولية ليوغوسلافيا السابقة في قرار تاديتش أن مبدأ "التمييز" الذي يشكل جوهر قانون الاستهداف ينطبق على النزاع المسلح سواء كان دولي او غير دولي.[2]

يلعب مبدأ التمييز دوراً محورياً في تقييد وسائل وأساليب الحرب، إذ يحظر استخدام الأسلحة التي لا تميز بطبيعتها بين المقاتلين والأهداف العسكرية من جهة، والمدنيين والأعيان المدنية من جهة أخرى. كما يسهم في حظر الاستخدام العشوائي للأسلحة، حتى وإن كان السلاح تمييزياً في حد ذاته، لكنه يُستخدم بطريقة غير تمييزية لا توجه نحو هدف عسكري محدد.

باختصار، يمكن القول إن مبدأ التمييز يشكل درعاً واقياً للمدنيين في خضم النزاعات المسلحة، ويسهم في الحد من الآثار المدمرة للنزاعات المسلحة عليهم، من خلال حظر استهدافهم، وتقييد استخدام الأسلحة غير التمييزية، وحظر الاستخدام العشوائي للأسلحة التي تؤثر على المدنيين والأعيان المدنية.

---

[1] مشار اليه في: شوقي سمير، محكمة العدل الدولية والقانون الدولي الإنساني، رسالة ماجستير، جامعة الجزائر، كلية الحقوق، 2007/2006، ص 88.

[2] Prosecutor v. Tadic, case no. IT-94-1. Decision on defence motion for interlocutory appeal on jurisdiction. 127 (Oct 2, 1995).

ثالثا: الأساس القانوني لمبدأ التمييز:

مبدأ التمييز هو النتيجة الحتمية والضرورية لتحقيق الهدف المشروع من الحرب، كما أوضحه إعلان سان بطرسبرج لعام 1868م بأنه "إضعاف القوى العسكرية للعدو"[1].

وعلى الرغم عدم النص عليه صراحة في اتفاقيات لاهاي 1907، إلا أنها عبرت عن روحه. وقد تم ترسيخ هذا المبدأ بشكل أكبر في اتفاقيات جنيف 1949 والبروتوكول الإضافي الأول 1977، حيث تم تحديد فئات المقاتلين وغير المقاتلين بوضوح، وحظر الهجمات المباشرة ضد المدنيين والأهداف المدنية.

ويجد مبدأ التمييز أساسه الاتفاقي في المواد 48 و51 و52 من البروتوكول الإضافي الأول لاتفاقيات جنيف 1977م[2]، حيث نصت المادة 48 صراحة على المبدأ بقولها "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" وحظرت المادة 51 الهجوم ضد المدنيين والهجمات العشوائية التي لا توجه الى هدف عسكري محدد، أما المادة 52 فقد قصرت الهجمات على الأهداف العسكرية فقط. ووضعت المقصود بالأهداف العسكرية.

ويلاحظ ان المواد التي تناولت مبدأ التمييز في البروتوكول الاول لم تكن محل أي تحفظ من قبل الدول الاطراف فيه،[3] وهو ما يبين شعور الدول بالقيمة الجوهرية

---

[1] ديباجة اعلان سان بطرسبرج الموقع في التاسع والعشرين من نوفمبر 1868 في شأن حظر استعمال قذائف معينة في وقت الحرب.

[3] البروتوكول الإضافي الأول لاتفاقيات جنيف المؤرخة في 12 أغسطس 1949م ، والمتعلق بحماية ضحايا النزاعات المسلحة الدولية ، والمؤرخ 8 يونيو 1977م ، وسوف نشير اليه لاحقا، على سبيل الاختصار بالبروتوكول الإضافي الأول .

[3] المادة 48 تم اعتمادها بالإجماع، أما المادة 2/51 تم اعتمادها بصالح 77 صوتا ومعارضة صوت واحد و16 ممتنعا

لهذا المبدأ. وقد رسخت العديد من الدول لهذه القيمة في مرافعاتها الشفوية أمام محكمة العدل الدولية اثناء نظر الرأي الاستشاري بشأن الاسلحة النووية حيث ابدت ان مبدأ التمييز " أول المبادئ الأساسية للقانون الدولي الإنساني"[1] وهو ما اكدته المحكمة نفسها حيث قالت " أول المبادئ الأساسية التي تشكل نسيج القانون الدولي الانساني باعتباره يستهدف حماية المدنيين والاعيان المدنية، ويقدم تمييزاً بين المقاتلين وغير المقاتلين"[2]

وقد أكد النظام الأساسي للمحكمة الجنائية الدولية لعام 1998 على وجوب التمييز بين المقاتلين وغير المقاتلين، واعتبر الهجمات المباشرة ضد المدنيين أو الأهداف المدنية على أنها جرائم حرب.[3]

أما عن الأساس العرفي لمبدأ التمييز فهو يعد قاعدة من قواعد القانون الدولي العرفي تواتر الالتزام بها من قبل الدول في ممارساتها أثناء النزاعات المسلحة الدولية وغير الدولية، وقد ورد هذا المبدأ كأول قاعدة في دراسة اللجنة الدولية للصليب الأحمر لتقنين قواعد" القانون الدولي الإنساني العرفي"[4]، بالصيغة الاتية " يميز

عن التصويت، أما المادة 2/52 فقد تم اعتمادها لصالح 70 صوتاً دون معارضة وامتناع 7 عن التصويت.

[1] د. شوقي سمير، محكمة العدل الدولية والقانون الدولي الانساني، مرجع سابق، ص 85.

[2] Legality of the threat or use of nuclear weapons, ICJ Reports 1996, p.257, para.78.

[3] م2/8 من النظام الأساسي للمحكمة الجنائية الدولية 1998 م.

[4] قامت اللجنة الدولية للصليب الأحمر بتكليف فريق من الخبراء القانونيين بإجراء دراسة مستفيضة حول الممارسات الدولية في النزاعات المسلحة، شملت الدراسة تحليل ممارسات أكثر من 50 دولة، وتم فحص الوثائق الرسمية، والأدلة العسكرية، والتشريعات الوطنية، وغيرها من المصادر ذات الصلة، واستغرقت الدراسة حوالي 10 سنوات من البحث والتحليل، وشارك فيها أكثر من 150 خبيراً وباحثاً من مختلف أنحاء العالم، وبعد الانتهاء من الدراسة، قامت اللجنة بصياغة مجموعة من القواعد العرفية للقانون الدولي الإنساني، والتي تعكس الممارسات الدولية السائدة في هذا المجال، وتم نشر هذه القواعد في كتاب بعنوان "القانون الدولي الإنساني العرفي" عام 2005، والذي يتضمن 161 قاعدة عرفية، مصنفة في ستة أقسام رئيسية تغطي مختلف جوانب القانون الدولي الإنساني، وقد حظيت هذه القواعد باعتراف واسع من قبل المجتمع الدولي، وأصبحت مرجعاً هاماً للدول والمنظمات الدولية والمحاكم في تطبيق القانون الدولي

أطراف النزاع في جميع الأوقات بين المدنيين والمقاتلين- وتوجه الهجمات الى المقاتلين فحسب، ولا يجوز أن توجه إلى المدنيين"[1]وتكرس ممارسة الدول هذا المبدأ كأحد قواعد القانون الدولي العرفي المنطبقة في النزاعات المسلحة الدولية وغير الدولية.[2]حيث أخذت بهذا المبدأ الكثير من الكتيبات العسكرية للدول بما فيها الكتيبات الخاصة بدول ليست، أو لم تكن في حينه، اطرافًا في البروتوكول الإضافي الأول،[3] كما أعلنت المملكة المتحدة في المؤتمر الدبلوماسي الذى أدى إلى اعتماد البروتوكولين الاضافيين[4] أن الفقرة الثانية من المادة 51 هي إعادة تأكيد قيمة "لقاعدة موجودة في القانون الدولي العرفي" كما أشارت الكثير من الدول إلى مبدأ التمييز في مرافعاتها أمام محكمة العدل الدولية في قضية الأسلحة النووية[5]، كما أكدت الطبيعة العرفية لهذا المبدأ المحكمة ذاتها في هذه القضية بقولها إن مبدأ التمييز هو أحد " مبادئ القانون الدولي العرفي التي لا يجوز انتهاكها" .

كما استشهدت بهذا المبدأ العديد من الدول في بياناتها الرسمية، منها بيانات لدول ليست، أو لم تكن في حينه، أطرافا في البروتوكول الإضافي الأول، كما استشهدت

الإنساني.

[1] جون مارى هنكرتس ، لويز دوزوالد- -بك ، القانون الدولي الإنساني العرفي، اللجنة الدولية للصليب الأحمر، المجلد الأول: القواعد ، القاهرة ، 2007، الفصل الأول ، القاعدة 1، ص 3 .

[2] المرجع السابق ، ص 3 .

[3] من أمثلة ذلك كتيبات الدليل العسكري لكل من السويد وفرنسا واندونسيا وكينيا .

[4] المؤتمر الدبلوماسي بشأن إعادة تأكيد القانون الدولي الإنساني المنطبق على المنازعات المسلحة وتطويره والمنعقد في الفترة (1974-1977) .

[5] فتوى محكمة العدل الدولية بشأن مشروعية استخدام الأسلحة النووية أو التهديد باستخدامها لعام 1996م، منشورات الأمم المتحدة.

به دول أطراف ضد دول ليست أطراف.[1] ويترتب على الطبيعة العرفية لمبدأ التمييز إلزامه لكافة الدول دون استثناء.

المطلب الثاني: مفهوم الحرب السيبرانية وخصائصها

أولا: تعريف الحرب السيبرانية

تعد العمليات السيبرانية واحدة من بين أبرز تكتيكات الحروب الحديثة، وهو ما برز بجلاء في الحرب الروسية الأوكرانية التي اشتعلت في فبراير 2022، وهى من أشد المخاطر في وقتنا المعاصر، فهي حروب أكثر فتكا من الحروب العادية، تستخدم فيها تقنيات المعلومات والاتصالات كأدوات رئيسية للهجوم والدفاع، وأطرافها قد تكون الدول، أو المنظمات، أو الجماعات، أو حتى الأفراد، وتهدف الى تعطيل أو تدمير البنية التحتية الحيوية، وسرقة المعلومات الحساسة، والتجسس، ونشر الدعاية، أو إحداث اضطرابات اقتصادية وسياسية، وتتمثل أسلحتها في استخدم برامج ضارة، فيروسات، هجمات حجب الخدمة، اختراق الأنظمة، والهندسة الاجتماعية،[2]وتتمثل ساحة المعركة الرقمية في الفضاء السيبراني، بما في ذلك شبكات الكمبيوتر، الإنترنت، وأنظمة التحكم الصناعية، ويتمثل اثرها فيما تحدثه من اضطرابات في الخدمات الأساسية، والخسائر اقتصادية، وتهديدات الأمن القومي والسلامة العامة.[3]

---

[1] جون مارى هنكرتس ، لويز دوزوالد- بك ، القانون الدولي الإنساني العرفي، مرجع سابق، ص5 .

[2] الهندسة الاجتماعية (Social Engineering) هي أسلوب يستخدمه المهاجمون السيبرانيون للتلاعب بالأشخاص و خداعهم من أجل الحصول على معلومات حساسة أو حثهم على اتخاذ إجراءات تضر بأمن المعلومات. وتعتمد على استغلال العوامل النفسية والاجتماعية للتأثير على الضحايا. فهي تكتيك يستغل الثغرات البشرية بدلاً من الثغرات التقنية للتسلل إلى الأنظمة والحصول على معلومات حساسة. وتعد من أكبر التهديدات الأمنية في العصر الرقمي، مما يتطلب الجمع بين التدابير التقنية والتوعية البشرية للحماية منها.

[3] ياسين محمد أحمد بونة، الهجمات السيبرانية: الحرب الرقمية التي تجاوزت الحدود الجغرافية، مجلة شمال افريقيا للنشر العلمي، الاكاديمية الافريقية للدراسات المتقدمة، مج1، ع 4، ديسمبر 2023، ص 162 .

لا يوجد تعريف متفق عليه دوليًا ومعلن رسميًا للحرب السيبرانية، وفي المصطلح العام كما ورد في قاموس أكسفورد، تعني "الحرب السيبرانية" "استخدام تكنولوجيا الكمبيوتر لتعطيل أنشطة دولة أو منظمة، وخاصة الهجوم المتعمد على أنظمة المعلومات لأغراض استراتيجية أو عسكرية"[1] وتبعا لقاموس كامبريدج تعرف الحرب السيبرانية على أنها " نشاط استخدام الإنترنت لمهاجمة أجهزة الكمبيوتر في بلد ما من أجل إتلاف أشياء مثل أنظمة الاتصالات والنقل أو إمدادات المياه والكهرباء، ويمكن أن يؤدي استخدام الحرب الإلكترونية إلى زعزعة استقرار الأنظمة المالية أو نظام الهاتف أو شبكة الطاقة"[2]

ووفقا للجنة الدولية للصليب الأحمر (ICRC) الحرب السيبرانية هي " تدابير عدائية ضد عدو تهدف إلى اكتشاف، أو تغيير، أو تدمير، أو تعطيل، أو نقل البيانات المخزنة في جهاز حاسوب أو التلاعب بها أو إرسالها عبر جهاز حاسوب"[3]، كما عرفتها وزارة الدفاع الامريكية بأنها " استخدام القدرات السيبرانية التي يتمثل هدفها الأساسي في تحقيق اهداف أو آثار عسكرية في الفضاء السيبراني أو من خلاله " [4]

وقد عرف مايكل شميت الحرب السيبرانية بأنها " الإجراءات التي تتخذها الدولة من أجل الهجوم على نظم المعلومات للعدو، بهدف التأثير عليها والإضرار بها، والدفاع عن نظم المعلومات الخاصة بالدول المهاجمة"[5]، وعرفها دليل تالين بأنها"

---

[1] Oxford Dictionary, Available from ; https://en.oxforddictionaries.com/definition/cyberwarfare. [accessed Sep 06 2024].

[2] Meaning of cyber warfare in English, available at: https://cutt.us/ZNs5q

[3] International Committee of the Red Cross, 'Cyber Warfare' , Available at; https://www.icrc.org/en/document/cyber-warfare [accessed Sep 06 2024].

[4] US Department of Defense, 'Dictionary of Military and Associated Terms'(8 November 2010 as amended through 15 February 2012) Joint Publication 1-02,66.

[5] مايكل شميت، الحرب بواسطة شبكات الاتصال: الهجوم على شبكات الحاسوب والقانون في الحرب، المجلة الدولية

عمليات سيبرانية، سواء كانت هجومية أو دفاعية، والتي يهدف من خلالها بصورة معقولة التسبب بالإصابة، أو وفاة الأشخاص، أو الإضرار، أو تدمير الاعيان"[1] ويري البعض ان هذا التعريف لا يحدد الحرب السيبرانية، ولكنه يستخدم المصطلح "بمعنى وصفي بحت وغير معياري". وأنه ينبغي على المجتمع الدولي صياغة تعريف قانوني للحرب السيبرانية يحظى بقبول جميع الدول، وذلك كخطوة أولى نحو وضع مجموعة من القواعد الملزمة التي تنظم هذا النوع من النزاعات المسلحة.[2]

أما "الهجمات السيبرانية " فقد عرفها دليل العمليات السيبرانية والإرهاب السيبراني للجيش الأمريكي بأنها "التهديد أو الاستخدام المتعمد للأنشطة التخريبية ضد شبكات الحاسوب بقصد التسبب في ضرر، أو تعزيز الأهداف الاجتماعية، أو الإيديولوجية، أو الدينية، أو السياسية التي قد تلحق الضرر بشبكات الكمبيوتر والمرافق المادية والأشخاص"[3]، وعرفها دليل تالين بأنها "عمليات سيبرانية، سواء

للصليب الأحمر، 2002، ص 130 .

[1] دليل تالين بشأن القانون الدولي المطبق على الحروب السيبرانية (النسخة المترجمة للعربية)، بالتعاون مع حلف شمال الأطلسي، وبدعمٍ من فريق مؤلف من خبراء السيبرانية، واللجنة الدولية للصليب الأحمر والقيادة السيبرانية الأميركية تحرير مايكل شيمت، ترجمة على محمد كاظم الموسوي، 2017، القاعدة 30، ص 7. وسنشير له فيما بعد اختصاراً بـ " دليل تالين".

[2] Sharona Mann, legal challenges in the realm of cyber warfare, J. INT'L L. & POL. ONLINE FORUM ,March , 2020, p13, Available at; https://www.nyujilp.org/wp-content/uploads/2020/03/Mann-Note_Final-Draft_EIC-Approved.pdf [accessed Sep 07 2024].

[3] US Army Training & Doctrine Command, DCSINT Handbook no. 1.02, Critical infrastructure threats and terrorism at VI1-2,15 August 2005.cited in; Leanne Christine Van Breda, The effectiveness of the principle of distinction in the context of cyber warfare, A dissertation submitted in partial fulfilment for the Degree of LL M in International law, University of Johannesburg , 2014 ,p17.

كانت هجومية أو دفاعية، والتي يهدف من خلالها بصورة معقولة التسبب بالإصابة، أو وفاة الأشخاص، أو الاضرار، أو تدمير الأعيان"[1]

ومن الجدير بالذكر هنا أن "الجرائم السيبرانية" تختلف عن "الهجمات السيبرانية" لأنها تنطوي على جرائم ينظمها القانون الوطني، مثل الاحتيال الالكتروني، فهذه الأفعال مجرمة بموجب القوانين الوطنية، ولكنها غير محظورة بموجب القانون الدولي.[2]

ثانيا: سمات وخصائص الحرب السيبرانية:

يمكن مهاجمة الفضاء السيبراني بثلاثة أشكال رئيسية:

1. الهجوم السيبراني: يهدف إلى إحداث ضرر وتعطيل فوري. وهو عبارة عن أي نوع من المناورات الهجومية التي تستهدف أنظمة المعلومات والبنى التحتية والشبكات وأجهزة الحاسوب الشخصية. وتتم هذه الهجمات عادة من مصادر مجهولة بهدف سرقة أو تغيير أو تدمير أهداف محددة عن طريق اختراق الأنظمة الضعيفة.[3]

2. التجسس السيبراني: هو الحصول على معلومات غير مصرح بها. في حالة الحرب السيبرانية، يقوم أحد الأطراف بسرقة معلومات تكتيكية واستراتيجية مثل تحركات القوات ونقاط القوة والضعف في أنظمة الأسلحة وأي معلومات حساسة أخرى ضرورية لشن الحرب.[4]

---

[1] دليل تالين، القاعدة 30، ص 7 .

[2] Leanne Christine Van Breda, The effectiveness of the principle of distinction in the context of cyber warfare, op .cit, p17.

[3] Andy Manoske, 'How Does Cyber Warfare Work', (Forbes, 18 July, 2013), Available at; https://www.forbes.com/sites/quora/2013/07/18/how-does-cyber-warfare-ork/#3166548a44ce [accessed Sep 11 2024].

[4] Ibid, p1

3. التخريب: هو عملاً مباشراً، حيث يتخذ أحد الأطراف دوراً نشطاً للقيام بعمل ما. وفي الحرب السيبرانية، قد يتراوح التخريب بين إسقاط موقع حكومي إلى التسبب في انصهار نووي في محطة للطاقة النووية. على عكس التجسس الذي يهدف إلى العلم، يركز التخريب على القيام بعمل فعلي.[1]

وقد اكتسبت الهجمات السيبرانية المزيد من الدعاية في السنوات الأخيرة، حيث شكلت نوعًا جديدًا من التهديدات الهجينة. وتشبه التهديدات السيبرانية التهديدات في البعد الخامس للحرب، وتشير إلى حملة مستمرة ضد البنية التحتية لتكنولوجيا المعلومات في الدولة المستهدفة، مما يؤدي إلى تدمير شامل لشبكة الإنترنت، والبريد العشوائي، وإصابة البرامج الضارة.[2]

يمكن أن تتم هجمات الشبكات الحاسوبية من قبل الجهات الفاعلة الحكومية وغير الحكومية على حد سواء، وأيضًا من قبل مجموعات من الأفراد ذوي الخبرة العالية أو الشركات المتعددة الجنسيات .تتراوح العمليات السيبرانية الفعلية في السنوات الماضية من اختراق الشبكات الحكومية أو العسكرية، مثل هجمات تيتان رين Titan Rain attacks في عام 2003 عندما تم اختراق منشآت وزارة الدفاع الأمريكية ومختبرات ناسا وشركة لوكهيد مارتن وأنظمة أخرى وفقدت العديد من التيرابايت من المعلومات.[3]

---

[1] Andy Manoske, 'How Does Cyber Warfare Work', op.cit , p2

[2] لمزيد من التفصيل حول أنواع الهجمات السيبرانية انظر:

Saman Iftikhar, Cyberterrorism as a global threat: a review on repercussions and countermeasures, PeerJ Computer Science, January 15, 2024. 10:e1772 https://doi.org/10.7717/peerj-cs.1772 [accessed Oct 01 2024].

[3] تميزت هجمات "تيتان رين" بنهجها المنهجي والمنظم. وعلى عكس محاولات الاختراق النموذجية التي قد تستهدف منظمة أو شبكة واحدة، فقد استهدفت هذه الهجمات، التي يُعتقد أنها من تدبير قراصنة صينيين، البنية التحتية الحيوية والشبكات الحساسة داخل الولايات المتحدة، لم تثبت هذه الحادثة القدرات المتزايدة للمهاجمين السيبرانيين فحسب، بل

وتتسم الهجمات السيبرانية بطبيعة سرية تجعل من الصعب تحديد هوية مرتكبيها، على الرغم من أن ذلك ليس مستحيلاً. فالأسلحة السيبرانية مصممة لاستغلال ثغرات غير معروفة في الأهداف، مما يؤدي إلى عدم إدراك المسؤولين أنهم يتعرضون للهجوم إلا بعد فوات الأوان. وحتى بعد تحديد مصدر الهجوم، سواء كان مجموعة أو فرداً، يصعب تحديد ما إذا كان الجاني يعمل بالتنسيق مع حكومة دولة ما. وفي كثير من الأحيان، تستطيع الحكومات بسهولة إنكار أي صلة لها بهذه الهجمات وتجنب نسبتها إليها. ومثال على ذلك ما حدث مع فيروس الفدية "واناكراي" (WannaCry)،[1] حيث نسبت الولايات المتحدة الفيروس إلى عضو في حكومة

أكدت أيضًا على ضعف أنظمة الأمن القومي في مواجهة التهديدات الرقمية. واستخدم المهاجمون مجموعة من التقنيات للتسلل إلى هذه الشبكات. إحدى الطرق الشائعة كانت "التصيد الاحتيالي الموجه"، حيث تم استهداف أفراد معينين برسائل بريد إلكتروني تحتوي على مرفقات أو روابط ضارة. عند فتحها، كانت هذه المرفقات تقوم بتثبيت برامج ضارة على جهاز المستخدم، مما يمنح المهاجمين إمكانية الوصول إلى الشبكة. كما استغل القراصنة نقاط الضعف في البرامج وأنظمة التشغيل للحصول على وصول غير مصرح به إلى الأنظمة، لمزيد من التفصيل حول هذه الهجمات أنظر:

Negrea Petru-Cristian, Cyber Conflict and International Relations: A Comprehensive Analysis of Cyber Deterrence Strategies in Contemporary Geopolitics, PhD thesis, February 2024, p25. Available from: https://www.researchgate.net/publication/378334428_Cyber_Conflict_and_International_Relations_A_Comprehensive_Analysis_of_Cyber_Deterrence_Strategies_in_Contemporary_Geopolitics [accessed Oct 04 2024].

[1] كان هجوم برمجيات الفدية "واناكراي" في مايو 2017 حدثًا بارزًا في مجال الأمن السيبراني العالمي، حيث أثر على نطاق غير مسبوق شمل أكثر من 150 دولة وعطل مجموعة واسعة من المنظمات والأفراد. تسعى هذه المراجعة الشاملة للأدبيات إلى تعزيز النظرة العامة الأولية، مع نسج نسيج من الرؤى الأكاديمية الأوسع والتحليلات المفصلة بدقة.

استغل "واناكراي" ثغرة معروفة في نظام التشغيل ويندوز، تُعرف باسم "إيترنال بلو". قامت هذه البرمجيات الخبيثة بتشفير الملفات على الأنظمة المصابة بطريقة مبتكرة، ثم طالبت بفدية بعملة البيتكوين المشفرة لتحرير البيانات المشفرة. وقد كشف هذا الحادث عن الضعف الشديد لقطاع الرعاية الصحية أمام التهديدات السيبرانية، وكانت هيئة الخدمات الصحية الوطنية في المملكة المتحدة (NHS) من أكثر الكيانات تأثرًا بالهجوم. فقد تأثرت أكثر من 600 منظمة داخل

كوريا الشمالية، لكن وزارة خارجية كوريا الشمالية ردت على الفور بنفي أي علاقة لها بالحادثة.[1]

تُعتبر العمليات السيبرانية في جوهرها شكلاً من أشكال القتال، حيث تتطلب تخطيطًا دقيقًا وتحديدًا واضحًا للأهداف، وتوافر معلومات استخباراتية شاملة على المستويات التكتيكية والعملياتية والاستراتيجية، بالإضافة إلى ضرورة وجود قواعد اشتباك خاصة بها في الفضاء الإلكتروني.[2]

في سيناريو كارثي للحرب السيبرانية، تم وصف تسلسل مروع من الأحداث يمكن أن يؤدي إلى انهيار شامل للمجتمع في غضون 15 دقيقة فقط. يبدأ هذا السيناريو بتعطل أنظمة البريد الإلكتروني العسكرية، ثم يتصاعد بسرعة ليشمل انفجار مصافي النفط وخطوط الأنابيب، وانهيار أنظمة التحكم في حركة الطيران، وخروج قطارات الشحن ومترو الأنفاق عن مسارهم. كما تختلط البيانات المالية وتصبح غير موثوقة، وتنقطع الشبكة الكهربائية في شرق الولايات المتحدة، وتخرج الأقمار الصناعية

شبكة NHS، بما في ذلك مؤسسات المستشفيات، بشكل كبير. أدى الهجوم إلى اضطرابات واسعة النطاق في الخدمات الطبية الحيوية، مما تجلى في إلغاء مواعيد العيادات الخارجية، وتأخير حالات الدخول الاختيارية، وتحويل خدمات الطوارئ بشكل غير مسبوق. لمزيد من التفصيل انظر:

Negrea Petru-Cristian, Cyber Conflict and International Relations: A Comprehensive Analysis of Cyber Deterrence Strategies in Contemporary Geopolitics,op.cit,p32.

[1] Luzzatto, Cadet Andrew. “Regulating Cyber Warfare Through the United Nations.” *The Cyber Defense Review*, Vol. 7, No. 4, 2022, p. 263. Available from; https://www.jstor.org/stable/48703304. [accessed Sep 20 2024].

[2] Guyonneau, Rudy, and Arnaud Le Dez. “Artificial Intelligence in Digital Warfare: Introducing the Concept of the Cyberteammate.” *The Cyber Defense Review*, Vol. 4, No. 2, 2019, p105.

المدارية عن السيطرة. نتيجة لهذه الأحداث المتتالية، ينهار المجتمع بسرعة مع نقص الغذاء ونفاد الأموال. والأسوأ من ذلك كله، قد تظل هوية المهاجم لغزًا.[1]

وتهدد الحرب السيبرانية المجتمع بشكل شامل. فالحرب السيبرانية الاستراتيجية لا تميز بين المدنيين والعسكريين. وتماماً مثل الأسلحة النووية في الحرب الباردة، فإن الأسلحة السيبرانية من المرجح أن تستهدف الموارد المدنية بقدر ما تستهدف الموارد العسكرية. وبينما من الواضح أن القنبلة النووية أكثر تدميراً من قطعة برمجيات خبيثة بمفردها، إلا أن الهجوم السيبراني يمكن أن يتسبب في خسائر وإصابات بين المدنيين. علاوة على ذلك، من الصعب للغاية تحديد الجهة التي شنت الهجوم.[2]

المبحث الثاني: تحديات النطاق الشخصي لمبدأ التمييز في الفضاء السيبراني

يتطلب النطاق الشخصي لمبدأ التمييز حماية المدنيين من الهجمات، مع السماح فقط بمهاجمة القوات المسلحة لطرف النزاع. لكن في الحروب السيبرانية، أصبح التمييز بين المشاركين وغير المشاركين في القتال أكثر صعوبة، مما أدى إلى غموض في تطبيق هذا المبدأ. إن تصنيف الشخص كـ"عسكري" أو "مدني" له أهمية كبيرة، حيث يمكن مهاجمة العسكريين أو المشاركين مباشرة في الأعمال العدائية بشكل قانوني، بينما يتمتع المدنيون بالحماية من الهجوم المباشر. ولا يجوز استهداف

[1] War in the Fifth Domain – Are the Mouse and Keyboard the New Weapons of Conflict?' The Economist (1 July 2010); cited on; David Turns, Cyber Warfare and the Notion of Direct

Participation in Hostilities, Journal of Conflict & Security Law, Journal of Conflict and Security Law, 2012, Vol. 17 No. 2 p283

[2] Andy Manoske, 'How Does Cyber Warfare Work', op.cit, P2 .

المدنيين إلا عند مشاركتهم المباشرة في الأعمال العدائية، وفقط خلال فترة مشاركتهم في أعمال محددة ضمن سير العمليات العدائية بين أطراف النزاع المسلح.[1]

لذا سوف نتناول وضع المقاتل في الحروب السيبرانية كأحد تحديات النطاق الشخصي لمبدأ التمييز، ثم الوضع القانوني للمدنيين في ضوء مشاركتهم الواسعة في الأنشطة السيبرانية.

المطلب الأول: وضع المقاتل في الحرب السيبرانية

عرفت المادة 1/50 من البروتوكول الإضافي الأول المدني تعريفاً سلبياً بأنه شخص لا ينتمي إلى فئات محددة مذكورة فيه وفي اتفاقية جنيف الثالثة، وفي الدليل التفسيري، عرفت اللجنة الدولية للصليب الأحمر مصطلح "المدني" في حالات النزاع المسلح الدولي بشكل مختلف عنه في النزاع المسلح غير الدولي. ويُعرَّف مفهوم المدني لأغراض مبدأ التمييز في النزاعات المسلحة الدولية بأنه "جميع الأشخاص الذين ليسوا أعضاء في القوات المسلحة لطرف في النزاع ولا مشاركين في أي عمل من أعمال النزاع"[2]، وهكذا تحاكي اللجنة الدولية للصليب الأحمر صياغة المادة 50 والمادة 51(3) من البروتوكول الإضافي الاول وتعرف المدنيين بشكل سلبي بأنهم ليسوا جزءاً من مجموعات معينة.[3] وعلى نفس المنوال عرف القاموس العملي للقانون

[1] Kubo Macak, Mauro Vignati, Civilianization of Digital Operations: A Risky Trend, Lawfare, Wednesday, April 5, 2023, Available at; https://www.lawfaremedia.org/article/civilianization-digital-operations-risky-trend [accessed Sep 10, 2024].

[2] المادة 3/51 من البروتوكول الإضافي الأول، والمادة 3/13 من البروتوكول الإضافي الثاني، الدليل التفسيري، الفقرة جيم، سابعا، ص 70.

[3] Dan-Iulian Voitasec, Cyber Hostilities: Civilian Direct Participation, Challenges of the Knowledge Society (2016): 550-4. [accessed Sep 19 2024].

الإنساني[1] المدني تعريف سلبي بأنه "الشخص الذي لا يتبع أيًّا من المجموعات التالية:....."، وبصفة عامة يمكن القول انه وفقا لقواعد القانون الدولي الإنساني يمكن تعريف المدنيين في النزاعات المسلحة الدولية بأنهم الأشخاص من غير الأعضاء في القوات المسلحة لأحد أطراف النزاع، أو الأشخاص المشاركين في هبة جماعية ضد غزو محتمل، أما المدنيين في النزاعات المسلحة. أما المدنيين في النزاعات المسلحة غير الدولية بأنهم جميع الأشخاص من غير الأعضاء في القوات المسلحة الحكومية أو في الجماعات المسلحة المنظمة التابعة لطرف من أطراف النزاع.[2]

أما دليل تالين فلم يتعرض لتعريف المدني في القاعدة التي تحمل اسم " المدنيون"، الا ان التعليقات على المادة اشارت الى ان المدنيين في النزاع المسلح غير الدولي هم أولئك الأشخاص الذين ليسوا أعضاء في القوات المسلحة لدولة أو القوات المسلحة المنشقة أو غيرها من الجماعات المسلحة المنظمة.[3]

أما المقاتلين فقد ورد تعريفهم في قواعد القانون الدولي الإنساني العرفي بأنهم "جميع أفراد القوات المسلحة لطرف في النزاع (عدا الأفراد الطبيين والدينيين)"[4]،

---

[1] القاموس العملي للقانون الانساني، تأليف: فرانسواز بوشيه- سولنييه، ترجمة: محمد مسعود، مراجعة: د.عامر الزمالي ومديحة مسعود، الناشر: دار العلم للملايين، 2006، متاح على الرابط : Médecins Sans Frontières | القاموس العملي للقانون الإنساني (guide-humanitarian-law.org) (تاريخ الاطلاع: 15-9-2024) .

[2] روابحى عمر، إشكالية تحديد مفهوم المقاتل الشرعي في النزاعات المسلحة غير المتكافئة، مجلة معارف: قسم العلوم القانونية، السنة الحادية عشر- العدد 21- ديسمبر 2016، ص 178، 180 .

[3] Tallinn Manual on the International Law Applicable to Cyber Warfare – prepared by the International Group of Experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence, Cambridge University Press, 2013, Rule 29, Commentary para 4, p105.

[4] جون مارى هنكرتس ، لويز دوزوالد- بك ، القانون الدولي الإنساني العرفي ، مرجع سابق ، المجلد الثاني، الفصل الأول، القاعدة .3 .

وحددت فئاتهم على سبيل الحصر اتفاقية جنيف الثالثة[1]، والبروتوكول الإضافي الاول[2] اللتين وضعا اربعة شروط يتعين توافرها في المليشيات من غير القوات المسلحة لكي يكتسبوا صفة المقاتل، والتي تعد بمثابة معايير لوضع المقاتل، وهي: القيادة، الشارة المميزة، حمل السلاح علنا، الالتزام بقوانين واعراف الحرب.[3] وفي ضوء ذلك يثور التساؤل من هو المقاتل في الفضاء السيبراني؟ وبصيغة اخري هل تصلح معايير وضع المقاتل الاربعة لتحديد المقاتل في ساحة المعركة السيبرانية؟

في سياق الحرب السيبرانية، قد يصبح معيار القيادة متطلباً شكلياً وغير ذي معنى فعلي. فبينما يستبعد هذا المعيار الجهات الفاعلة الفردية، محافظاً بذلك على الطابع الجماعي للحرب، إلا أن مفهوم القيادة في الفضاء السيبراني يحتاج إلى تفسير أكثر مرونة وشمولية. فالقيادة في العمليات السيبرانية قد لا تتطلب الهيكل التقليدي الهرمي المعروف في الحروب التقليدية. بل قد تتخذ أشكالاً أكثر تعقيداً وتنوعاً، مثل التنسيق عبر شبكات لامركزية أو توجيهات عامة يتم تنفيذها بشكل مستقل. وبالتالي، فإن تطبيق مفهوم القيادة في الحرب السيبرانية يحتاج إلى إعادة تعريف وتكييف ليتناسب مع طبيعة هذا المجال الجديد من الصراع، فمعظم المجموعات السيبرانية وان كان لديهم نفس الهدف، الا أنهم يفتقرون إلى الانضباط المشترك، فإمكانية أن تكون المجموعة المسلحة التي توجد على الإنترنت منظمة بشكل كافٍ ضئيلة.[4]

---

[1] المادة الرابعة من اتفاقية جنيف الثالثة لعام 1949 بشأن أسرى الحرب.

[2] المادة 43 من البروتوكول الإضافي الأول 1977.

[3] م2/4 من اتفاقية جنيف الثالثة، م 43 والفقرات 2،3 من المادة 44 من البروتوكول الإضافي الأول. انظر أيضا: إسحاق صلاح أبو طه، المقاتل الشرعي وغير الشرعي وفقاً لقواعد القانون الدولي الإنساني، مجلة الدراسات القانونية والسياسية، مج 4، ع 202018، ص 20.

[4] Marco Roscini, Cyber Operations and the Use of Force in International Law, Oxford University Press, Oxford, 2014, p. 195.

والواقع انه في سياق الحرب السيبرانية، لا يبدو اشتراط وجود قيادة عسكرية صارمة أو رسمية ضرورياً بشكل خاص للحفاظ على المساءلة أو السيطرة على الأفراد المنخرطين في الأنشطة القتالية. وإذا تم الإبقاء على شرط التبعية للقيادة العسكرية كأساس لمنح صفة المقاتل في الفضاء السيبراني، فقد يتحول هذا الشرط إلى مجرد إجراء شكلي - عملية ورقية تمنح الوضع العسكري أو تدمج بيروقراطياً منظمة مدنية في قوة مسلحة تابعة للدولة.

مثل هذه التدابير الشكلية والفارغة من المضمون لن تحقق سوى القليل من الناحية العملية- إن وجدت- بل قد تؤدي إلى تقويض احترام القانون الذي يُفهم أنه يتطلب مثل هذه الإجراءات. وبالتالي، فإن إعادة النظر في مفهوم القيادة والتبعية العسكرية في سياق الحرب السيبرانية أمر ضروري لضمان فعالية وملاءمة القوانين التي تنظم هذا المجال الجديد من الصراع.[1]

كما تقوض طبيعة الحرب السيبرانية التطبيق التقليدي للمعيارين الثاني والثالث من معايير وضع المقاتل، وهما حمل الشارات المميزة والأسلحة علنًا، وقد اقترح بعض العلماء أنه نظرًا لاستحالة تمييز مستخدمي الحاسوب بعلامات مميزة، فيجب تطبيق شرط عرض العلامات على أجهزة الحاسوب أو الأنظمة، تمامًا كما يجب تمييز السيارات والطائرات والسفن العسكرية بعلامات مميزة. إلا أن البعض يري أن هذا الاقتراح غير مقبول لأن وضع علامة على حاسوب عسكري سيؤدى إلى جعل أي نظام متصل به هدفًا مشروعًا.[2]

---

[1] See; Mačák, Kubo, "Unblurring the Lines: Military Cyber Operations and International Law." *Journal of Cyber Policy* 6 (3), 2021, p420. Available at; https://doi.org/10.1080/23738871.2021.2014919 [accessed Sep 19. 2024].

[2] See, Zhixiong Huang and Yaohui Ying, The application of the principle of distinction in the cyber context: A Chinese perspective, International Review of the Red Cross (IRRC), 2020, 102 (913), p349.

في الفضاء السيبراني، نادرًا ما يتواجه المحاربون وجهًا لوجه. وعلى عكس الهجمات التقليدية التي تعتمد على المظهر الخارجي، يتم اختيار أهداف الهجمات السيبرانية بناءً على وظيفتها أو قيمتها المعلوماتية. لذا، فإن التمييز في الهجمات السيبرانية يتطلب التركيز على سلوك الهجوم نفسه - كاختيار الهدف، وطرق الاختراق، والوسائل المستخدمة لإحداث الضرر - بدلاً من المظهر الخارجي للمهاجمين، ولذلك فإن هذين المعيارين- وجود علامة مميزة ثابتة يمكن التعرف عليها عن بعد، وحمل الأسلحة علانية- غير مناسبين للسياق السيبراني وبالتالي ربما لا يلزم أخذهما في الاعتبار في الحرب السيبرانية.

أما المعيار الرابع، وهو الامتثال للقانون الدولي الإنساني، فلا غنى عنه ولم يتغير بشكل ملحوظ مع ظهور تكنولوجيا الشبكات الحاسوبية[1]، الا انه ورغم أهميته من الناحية الإنسانية والقانونية، فإن متطلب وجود نظام تأديبي داخلي، والذي نجده في التعبيرات اللاحقة للمعيار الرابع،[2] يبدو غير ملائم لطبيعة هجمات الشبكات الحاسوبية؛ فبينما كانت أنظمة العدالة العسكرية ضرورية في الحروب التقليدية لفرض الانضباط ومتابعة القوات المتنقلة، فإن هجمات الشبكات الحاسوبية لا تتطلب ذلك. فالمشاركون في هذه الهجمات لا يحتاجون للابتعاد جغرافيًا.[3]

تكشف النزاعات المسلحة المعاصرة عن وجود المدنيين ونشاطهم بشكل كبير في ساحة المعركة السيبرانية، ويمكن تلخيص ذلك في دورين على وجه الخصوص:

---

[1] Harrison Dinniss, Cyber Warfare, and the Laws of War, Cambridge University Press, Cambridge, 2012, p. 149

[2] الفقرة الأولى من المادة 43 من البروتوكول الإضافي الأول لعام 1977م.

[3] Sean Watts, The Notion of Combatancy in Cyber Warfare, 2012 4th International Conference on Cyber Conflict (CYCON 2012), 05-08 June 2012, p248 [accessed Sep 21. 2024].

أولاً، كمرتزقة أو أعضاء في شركات أمنية وعسكرية خاصة لتنفيذ عمليات إلكترونية عدائية هجومية ودفاعية، وثانياً، كقراصنة (مدنيين) يقدمون مساهمات مماثلة.[1]

فعلى الرغم من أن بعض الدول لديها وحدات حرب معلومات ترتدي الزي العسكري، إلا أن المدنيين هم المسؤولون في معظم الحالات عن إجراء عمليات المعلومات، وخاصة الهجمات الإلكترونية. وهناك سببان لتمثيل المدنيين بكثافة في العمليات السيبرانية. أولاً، تتطلب مثل هذه العمليات، وخاصة الهجمات الإلكترونية، معرفة متخصصة للغاية. ثانيًا، طبيعة التكنولوجيا تجعلها غير ضرورية لأفراد القوات المسلحة. وعلى الرغم من الأسباب العملية للغاية التي تدعو إلى اللجوء للمدنيين والمقاولين لتنفيذ الهجمات السيبرانية، فإن العديد من الانشطة السيبرانية التي من المرجح أن يشاركوا فيها سوف تشكل بلا شك مشاركة مباشرة.[2]

والادوار التي يمارسها المشاركين في الهجمات السيبرانية تتمثل في ثلاث فئات:[3]

1. تصميم البرامج المستخدمة في عمليات الحرب الإلكترونية الهجومية أو الدفاعية.
2. تثبيت هذه البرامج على أنظمة الحاسوب، ويعملون كمسؤولين عن الخدمة ويقدمون الصيانة الفنية لها.
3. تشغيل برامج الحاسوب فعليًا وفق سيناريو الحرب السيبرانية.

من الممكن أن يكون أي من هؤلاء الأفراد من العسكريين الفعليين أو المدنيين.

---

[1] Ahmed Aubais Al fatlawi, Beyond the Battlefield: Navigating the Legal Challenges of Civilian Cyber Participation in Modern Warfare, ATSK Journal of Law, August 2024, Vol 1, Issue 1, Article 5, p5.

[2] Vasileios Karatzias, *Direct Participation of Civilians in Cyber, p6* , Available at; https://www.academia.edu/21147788/Direct_Participation_of_Civilians_in_Cyber_Hostilities_in_times_of_Armed_Conflict [accessed Sep 19. 2024].

[3] David Turns, Cyber Warfare and the Notion of Direct Participation in Hostilities, Journal of Conflict & Security Law, Vol. 17 No. 2 , 2012 , p289.

إن المدنيين أصبحوا يشكلون أهمية متزايدة كمكملات مباشرة للقوات المسلحة. والواقع أن المدنيين أصبحوا الآن في كثير من الأحيان يؤدون وظائف دعم بالغة الأهمية في العديد من المواجهات العسكرية التي تتطلب تكنولوجيا عالية. وسواء أكانوا يديرون أنظمة قيادة المعارك في الجيش، أو يديرون أنظمة الاتصالات، أو يساعدون في استخدام الأسلحة المتطورة، فإن المدنيين يشكلون بوضوح عنصراً أساسياً في القوات المسلحة الحديثة.[1]

لم يعد دور المدنيين الذين تستخدمهم الدول مقتصرًا على المهام الثانوية في الحرب السيبرانية، بل أصبحوا، مع تزايد التعقيد التقني للأسلحة الحديثة، يكتسبون أهمية متزايدة كداعمين مباشرين للقوات المسلحة. في الواقع، غالبًا ما يقوم المدنيون الآن بوظائف دعم حاسمة في العديد من المهام العسكرية عالية التقنية. يشكل الموظفون المدنيون مكونًا أساسيًا للقوات المسلحة الحديثة، سواء في إدارة أنظمة قيادة المعركة للجيش، أو إدارة أنظمة الاتصالات، أو المساعدة في استخدام الأسلحة المتطورة.

من جهة اخري، هناك غموض كبير يحيط بهوية الأفراد المشاركين في الحرب السيبرانية مما ينعكس على وضعهم القانوني، فتحقيق متطلبات مبدأ التمييز في الحروب السيبرانية هو أمر في غاية التعقيد، إذ إن المهاجم في الأغلب يكون بعيدًا عن مكان الهجوم ولمسافةٍ تتجاوز المئات من الكيلومترات، مما يجعل التأكد من الالتزام به أمرًا غاية في الصعوبة، فالهجمات السيبرانيّة على أوكرانيا في 2022، استهدفت مواقع الحكومة الأوكرانية، فقد نسَبَت المخابرات الأمريكية الهجمات إلى مهاجمين روس، إلاَ أنَّ الحكومة الروسية نفَت تورّطها.[2]

[1] [2] David Turns, Cyber Warfare and the Notion of Direct Participation in Hostilities, op.cit , p279.

[2] في عام 2022، تعرضت أوكرانيا لعدة هجمات سيبرانية كبيرة في سياق الحرب الروسية الأوكرانية، ففي يناير

فالحرب السيبرانية تمثل "حربًا رخيصة" لمحارب يفتقر إلى التكنولوجيا، حيث تقتصر التكلفة على شراء أجهزة الحاسوب، وبرامج استغلال، والوصول إلى الشبكة المستهدفة، والخبرة في التعامل مع الحاسوب.

من ذلك يمكن القول أن تحول الأعمال العدائية من العالم المادي (الحرب الحركية) إلى الفضاء الإلكتروني يؤثر على تعريف المقاتلين أو التعريف السلبي للمدنيين. كما ان الطبيعة المتغيرة للأعمال العدائية إلى الهجمات الإلكترونية قد تجعل التمييز بين ساحات القتال والطابع المدني أقل وضوحًا، حيث يمكن لعدد متزايد من المدنيين المشاركة في صفوف القوات المسلحة.[1]

المطلب الثاني: المشاركة المدنية في ساحة المعركة السيبرانية

يتميز الفضاء السيبراني بطبيعة فريدة وسهولة وصول، مما يتيح للمدنيين المشاركة بشكل واسع في الأنشطة السيبرانية المرتبطة بالنزاعات المسلحة. ويعد استخدام المدنيين في هذا السياق أمرًا جذابًا نظرًا لصعوبة تحديد مصدر الهجمات ولخبراتهم التقنية، ومع تزايد مشاركة المدنيين في الحروب السيبرانية، أصبح تحديد

2022، تعرضت العديد من المواقع الحكومية الأوكرانية لهجوم إلكتروني أدى إلى تعطيلها، وفي فبراير تعرضت لهجوم على شبكة الكهرباء أدى إلى انقطاع التيار الكهربائي في بعض المناطق. وأشارت التقارير إلى أن الهجوم نفذته مجموعة قرصنة مرتبطة بروسيا، كما تعرضت لهجمات إلكترونية متعددة على البنية التحتية الحيوية، بما في ذلك محطات الطاقة والمطارات والسكك الحديدية بهدف تعطيل الخدمات الأساسية، وهجمات برامج الفدية التي تشفر البيانات وتطلب دفع فدية مقابل فك التشفير، والتي استُهدفت العديد من المؤسسات الأوكرانية، بما في ذلك البنوك والمستشفيات.

هذه الهجمات السيبرانية كانت جزءًا لا يتجزأ من الصراع الهجين الذي تواجهه أوكرانيا، والذي يجمع بين الأساليب العسكرية التقليدية والتكتيكات غير التقليدية مثل الحرب الإلكترونية وحملات التضليل الإعلامي. وقد أدت هذه الهجمات إلى إلحاق أضرار كبيرة بالبنية التحتية الأوكرانية وزعزعة استقرار البلاد.

[1] Ahmed Aubais Al fatlawi, Beyond the Battlefield: Navigating the Legal Challenges of Civilian Cyber Participation in Modern Warfare, op.cit, p43.

وضعهم القانوني أكثر تعقيدًا،[1]فقد أثبتت النزاعات الحديثة، أن المدنيين يميلون بشكل متزايد إلى المشاركة في الجوانب السيبرانية للحرب. وتعد مشاركة الاوكرانيين المدنيين في الاعمال العدائية بالنزاع الروسي الاوكراني هي المثال الاحدث والأوضح، حيث يشارك الأوكرانيين المدنيين في الحرب من خلال التطبيقات، فقد قام المبرمجين في اوكرانيا ببناء تطبيقات وبرامج روبوتية وأدوات عبر الإنترنت للقتال في الخطوط الأمامية، يتم من خلالها تنسيق توصيل الإمدادات، والعثور على طرق الإجلاء، والمساهمة في الهجمات الإلكترونية ضد مواقع الويب العسكرية الروسية، كما يستخدم الأوكرانيون تطبيقًا على الهاتف لرصد هجمات الطائرات بدون طيار والصواريخ الروسية، فيقومون بالإبلاغ عنها بضغطة زر باستخدام تطبيق Eppo على هواتفهم المحمولة،[2] فيما وصف بأنه تجنيد الشعب الاوكراني بأكمله،[3] وهذا يوضح كيف أصبح من السهل "تسليح" المدنيين بالقدرات السيبرانية مقارنة بالأسلحة التقليدية.

كما أن نطاق الأنشطة التي تشكل مشاركة مباشرة في الأعمال العدائية واسع في المجال السيبراني[4]، بحيث يمكن اعتبار أفعال بسيطة مثل شن هجمات رفض الخدمة

---

[1] David Wallace, Shane Reeves, and Trent Powell, Direct Participation in Hostilities in the Age of Cyber: Exploring the Fault Lines, Harvard National Security Journal , Vol. 12, 2021, p 176.

[2] Drew Harwell, instead of consumer software, Ukraine's tech workers build apps of war,

The Washington Post, March 24, 2022, Available at: https://www.washingtonpost.com/technology/2022/03/24/ukraine-war-apps-russian-invasion/ [Accessed Aug 10. 2024]

[3] Dan Sabbagh ,Ukrainians use phone app to spot deadly Russian drone attacks, The Guardian, October 29, 2022. https://2u.pw/vov9QQ9g [Accessed Aug 10. 2024] .

[4] يشارك المدنيون بنشاط في الأعمال العدائية بدوافع مختلفة، وينقسمون إلى مجموعتين: 1. المجموعة "غير الضارة":

أو بناء شبكات الروبوتات أو حتى إرسال معلومات استخباراتية عبر الرسائل النصية بمثابة مشاركة مباشرة تبرر استهداف المدنيين المعنيين. وهذا من شأنه توسيع دائرة الأفراد الذين يمكن استهدافهم بشكل كبير في النزاعات المستقبلية.

ومع ذلك، فإن قاعدة المشاركة المباشرة في الأعمال العدائية (DPH) تنص على أنه لا يمكن استهداف المدنيين إلا أثناء فترة مشاركتهم الفعلية في الأعمال العدائية، وهو ما قد يكون من الصعب تحديده في السياق السيبراني بسبب عدم وجود انتشار مادي في معظم الأنشطة السيبرانية.

ويشارك المدنيون بنشاط في الأعمال العدائية بدوافع مختلفة، وينقسمون إلى مجموعتين:[1]

1. المجموعة "غير الضارة": وهؤلاء لا يقصدون إلحاق الضرر بالضحية، وتتراوح دوافعهم بين المزاح وإثبات الذات والشعور بالمتعة والتحدي.

2. المجموعة "الضارة": هؤلاء يقصدون التسبب في خسائر بدوافع سياسية أو معادية للمجتمع أو لتحقيق مكاسب مالية.

والمدني قد يتصرف ضد دولته أو ضد الدولة المعادية، وفي كلتا الحالتين يرتكب جريمة، وقد يكون ذلك بسبب عدم الرضا عن سياسة الحكومة أو للاعتراض عليها.

وهؤلاء لا يقصدون إلحاق الضرر بالضحية، وتتراوح دوافعهم بين المزاح وإثبات الذات والشعور بالمتعة والتحدي.2. المجموعة "الضارة": هؤلاء يقصدون التسبب في خسائر بدوافع سياسية أو معادية للمجتمع أو لتحقيق مكاسب مالية. انظر في ذلك :

Tomasz Andrzej Lewandowski, Can mouse clicking be seen as involvement in armed conflict? Some notes on the direct participation in hostilities in cyberspace, Przegląd Prawniczy Uniwersytetu im. Adama Mickiewicza, June 2013, p198.

[1] Tomasz Andrzej Lewandowski, Can mouse clicking be seen as involvement in armed conflict? Some notes on the direct participation in hostilities in cyberspace, Przegląd Prawniczy Uniwersytetu im. Adama Mickiewicza, June 2013, p198.

يُطلق على هذا النوع من السلوك اسم "الهاكتيفيزم" hacktivism، ويشمل هجمات حجب الخدمة الموزعة على مواقع الحكومة ونشر بيانات عليها، كما أن صناعة ألعاب الكمبيوتر لها تأثير على هذه المسألة، حيث سهلت ظهور ما يسمى بـ "الجنود الافتراضيين" الذين يتخصصون في الحرب الافتراضية من خلال ألعاب الإنترنت. وغالبًا ما يكونون غير مدركين لعواقب أفعالهم ويعتبرونها شكلاً مثيرًا للترفيه.[1]

ويمكن لأي مدني لديه مهارات قرصنة مناسبة، بغض النظر عن دوافعه، أن يتسبب في أضرار جسيمة للبنية التحتية الإلكترونية في أي مكان بالعالم، مما يثير التساؤل حول المقصود بالمشاركة العدائية في ساحة المعركة السيبرانية، وكيفية تحديد بداية ونهاية هذا الوقت نظرا لما يترتب على ذلك من نتائج خطيرة تتمثل في فقدان المدني للحماية التي يكفلها له مبدأ التمييز، وهو ما سنبحث عنه في السطور التالية.

أولا: صعوبة تحديد الأفعال التي تشكل مشاركة مباشرة في الأعمال العدائية

نص البروتوكول الإضافي الأول في المادة 3/51 على فقدان المدنيين صفتهم المدينة إذا قاموا بدور مباشر في الاعمال العدائية، وهو ما أكده دليل تالين بشأن القانون الدولي المطبق على الحروب السيبرانية بنصه على ان " يتمتع الأشخاص المدنيون بالحماية من الهجوم لحين مشاركتهم المباشرة في العمل العدائي ويفقدون هذه الحماية على مدى هذا الوقت"[2] .

ولطالما شكَّلت المشاركة المباشرة في الأعمال العدائية، بوصفها استثناءً من حصانة المدنيين، أحد الجوانب الخلافية لمبدأ التمييز، وظلت إحدى التحديات الجسيمة

[1] Tomasz Andrzej Lewandowski, Can mouse clicking be seen as involvement in armed conflict? Some notes on the direct participation in hostilities in cyberspace , op.cit, p198.

[2] القاعدة 35 من دليل تالين .

التي يواجهها القانون الدولي الإنساني،[1] ومن المتوقع أن تزداد حدة هذه المسألة في ظل الحروب السيبرانية، التي تشهد اتجاهًا متناميًا نحو مشاركة المدنيين فيها بشكل متزايد.

ومن المؤسف أن معاهدات القانون الدولي الإنساني لا تحدد الأفعال التي تشكل مشاركة مباشرة في الأعمال العدائية،[2] وفي ظل هذا الغياب لتعريف المشاركة المباشرة في الاعمال العدائية رغم ما يترتب عليها من نتائج قانونية هامة وخطيرة، فقد أثارت هذه القضية العديد من الأسئلة في سياق الحرب الحركية، ولمعالجة هذا الافتقار إلى الوضوح، دعت اللجنة الدولية للصليب الأحمر خبراء عسكريين وإنسانيين وعلماء القانون الدولي لدراسة مفهوم "المشاركة المباشرة في الأعمال العدائية" بهدف تعزيز تنفيذ مبدأ التمييز، وانتهت الدراسة إلى صياغة دليل تفسيري لمفهوم المشاركة المباشرة في العمليات العدائية[3]، وقد اشتمل هذا الدليل على مجموعة

---

[1] Mohammed Naqib Ishan Jan, Mohammad Hisham Mohammad Kamal, IHL and the challenges of civilian involvement in armed conflict: examining the crux of the notion of direct participation in hostilities, *International Journal of Business, Economics and Law, Vol. 4, Issue 3 (June)*, 2014, p 73.

[2] عند مناقشة المادة 51 من API لم تتفق الاطراف في المؤتمرات الدبلوماسية على تعريف دقيق للمصطلح، كما ذكرت دراسة اللجنة الدولية للصليب الأحمر حول القانون الدولي الإنساني العرفي أنه لا يوجد تعريف دقيق لمصطلح المشاركة في الاعمال العدائية. انظر في ذلك: د. معماش صلاح الدين، مبدأ التمييز في القانون الدولي الإنساني واستعمال الطائرات بدون طيار، دائرة البحوث والدراسات القانونية والسياسية، جامعة أمحمد بوقرة، الجزائر، مج6، ع1، 2022، ص 48.

[3] أجرت اللجنة الدولية للصليب الأحمر ومعهد **T.M.C. Asser** هذا المشروع من عام 2003 إلى عام 2008. وشارك نحو 50 خبيراً، بصفتهم الشخصية ومن خلفيات مختلفة (أكاديمية وعسكرية وحكومية وغير حكومية)، في خمسة اجتماعات غير رسمية، ولم يسع المشروع والدليل التفسيري إلى تغيير القواعد الملزمة للقانون الدولي الإنساني العرفي أو التعاهدي، بل يعكسان الموقف المؤسسي للجنة الدولية للصليب الأحمر بشأن كيفية تفسير القانون الدولي الإنساني الحالي في ضوء الظروف السائدة في النزاعات المسلحة المعاصرة"، وقد صُمم المشروع لمعالجة ثلاثة أسئلة: أولاً، "من يُعتبر مدنياً لأغراض مبدأ التمييز؟"؛ وثانياً، "ما هو السلوك الذي يرقى إلى المشاركة المباشرة في الأعمال العدائية؟"؛ وثالثاً: ما هي الأشكال التي تحكم فقدان الحماية ضد الهجوم المباشر؟ ولم يهدف التوجيه التفسيري

من المعايير التراكمية التي بموجبها يتم اعتبار الفعل المحدد مشاركة مباشرة في الأعمال العدائية.[1] وعلى الرغم من ان الدليل التفسيري لم يأخذ في الاعتبار بصفة خاصة الحرب السيبرانية، حيث يسعي لتوضيح مفهوم المشاركة المباشرة في الأعمال العدائية بشكل عام، إلا أن هناك بعض الفقرات التي لها تأثير مباشر على وضع المدنيين المشاركين بشكل مباشر في الأعمال العدائية السيبرانية، وسوف نتناول في السطور التالية هذه المعايير للتعرف على الأنشطة السيبرانية التي إذا مارسها المدني كانت مشاركة مباشرة في الاعمال العدائية.

الشرط الأول- عتبة الضرر: يشمل "الضرر العسكري" أي تأثير سلبي على العمليات أو القدرات العسكرية لطرف النزاع. وفي حال عدم وجود ضرر عسكري محدد، يجب أن يكون الفعل المعتبر مشاركة مباشرة في الأعمال العدائية قادراً على التسبب بالموت أو الإصابة أو الدمار على الأقل. أما مجرد إحداث إزعاج لا يكفي لاعتباره ضرراً عسكرياً معتبراً في هذا السياق.[2]

إلى تغيير القانون الدولي الإنساني العرفي أو الاتفاقي، بل عكس موقف اللجنة الدولية للصليب الأحمر بشأن تفسير القانون الدولي الإنساني الحالي في ضوء الظروف السائدة في النزاعات المسلحة المعاصرة. وهو وثيقة غير ملزمة للدول، حتى وإن كان من الممكن أن تؤثر على ممارسات الدول. انظر في ذلك :

François Delerue, Civilian Direct Participation in Cyber Hostilities, Journal promoted by the Law and Political Science Department, ssue 19 (October, 2014) , p 5.

[2] نيلس ميلزر، الدليل التفسيرى لمفهوم المشاركة المباشرة في العمليات العدائية بموجب القانون الدولي الإنساني، اللجنة الدولية للصليب الأحمر، الطبعة العربية الاولي، المركز الإقليمي للإعلام، القاهرة، مارس، 2010م ، ص 46 وما بعدها، وسوف نشير الى هذا الدليل فيما بعد، اختصارا، باسم " الدليل التفسيري " .

Nils Melzer, Interpretive Guidance on the Notion of Direct Participation in the Hostilities Under International Humanitarian Law, International Committee of the Red Cross, (2009) .

[2] نيلس ميلزر، الدليل التفسيرى لمفهوم المشاركة المباشرة في العمليات العدائية بموجب القانون الدولي الإنساني، مرجع سابق، ص 46-47 .

ووفقا لهذا الشرط فإن التدخل الإلكتروني في شبكات الحاسوب العسكرية من شأنه التسبب في ضرر عسكري، وكذلك التنصت على القيادة العليا للخصم أو نقل معلومات الاستهداف التكتيكي للهجوم،[1] لكن الهجمات السيبرانية التي تؤدي الى تعطيل أنظمة الكمبيوتر التي تتحكم في شبكة السكك الحديدية الوطنية وإغلاق النظام بأكمله، مما يؤدي إلى إلغاءات عبر الشبكة، وبالتالي ازعاج الجمهور المسافر في الدولة المستهدفة، لن يصل إلى عتبة الضرر المطلوبة، أما إذا تسبب إغلاق النظام في حدوث خلل في الإشارة، مما يؤدي إلى خروج قطار ذخيرة عن مساره، أو تسبب في حدوث خلل في أجهزة الحاسوب على متن القطار مما يؤدي إلى تصادم قطارين للركاب، فإن ذلك سيشكل الموت أو الإصابة أو الدمار اللازم للوصول إلى عتبة الضرر المطلوب.[2]

ويستبعد هذا الشرط الأفعال التي تؤثر على الحياة المدنية كالعمليات السيبرانية التي تؤدى لانقطاع الكهرباء، أو المياه، أو إمدادات الغذاء، أو التلاعب بشبكات الحاسوب حيث لن تصل إلى عتبة الضرر في غياب الآثار العسكرية الضارة، وهو ما يراه البعض غير منطقي، لما يمكن ان تسببه هذه الأعمال من اثار خطيرة على الأمن العام والصحة والاقتصاد.[3]

إذا نظرنا إلى الهجمات السيبرانية التي استهدفت إستونيا عام 2007، وتلك التي وقعت خلال النزاع بين روسيا وجورجيا عام 2008 - على افتراض أن مدنيين، وليس أفراداً من القوات المسلحة الروسية، هم من نفذوها – سنخلص الى أن هذه

[1] Zhixiong Huang and Yaohui Ying , The application of the principle of distinction in the cyber context: A Chinese perspective, op.cit, p 352. Also; Tallinn Manual, p48.

[2] David Turns, Cyber Warfare and the Notion of Direct Participation in Hostilities, op.cit, pp 286–287.

[3] Ahmed Aubais Al fatlawi, Beyond the Battlefield: Navigating the Legal Challenges of Civilian Cyber Participation in Modern Warfare, op.cit, p46.

الهجمات لم ترقَ إلى مستوى المشاركة المباشرة في الأعمال العدائية، وذلك لأنها لم تستوف هذا المعيار.[1] فقد أدت الهجمات على الأنظمة الحاسوبية الإستونية إلى اضطرابات واسعة النطاق في هذه الدولة المتقدمة تكنولوجياً. حيث تعطلت المواقع الحكومية والبنكية والإعلامية، مما أثر سلباً على الاقتصاد والحياة اليومية. ومع ذلك، لم تُسجل أي حالات وفاة أو إصابات، ولم يتم رصد أي أضرار مادية مباشرة للممتلكات نتيجة لهذه الهجمات.[2]

وفي حالة جورجيا، كان تأثير الهجمات السيبرانية أقل حدة مقارنة بإستونيا، ويرجع ذلك إلى اعتماد جورجيا الأقل على التكنولوجيا في إدارتها العامة ونظامها المصرفي. فاقتصرت الآثار بشكل رئيسي على الجانب الدعائي، مثل تشويه الموقع الإلكتروني للرئاسة الجورجية. وعليه، فإن هذه الحالة تُعد أبعد عن اعتبارها مشاركة مباشرة في الأعمال العدائية مقارنة بحالة إستونيا.[3]

أما هجمات ستكسنت "Stuxnet" على إيران بين عامي 2009 و2010،[4] فقد تسببت في تدمير حوالي 1000 جهاز طرد مركزي في منشأة "نطنز" النووية

---

[1] Zhixiong Huang and Yaohui Ying , The application of the principle of distinction in the cyber context: A Chinese perspective, op.cit, p 352.

[2] David Turns, Cyber Warfare and the Notion of Direct Participation in Hostilities, op.cit, P287.

[3] Ibid, p.287.

[4] هي عملية سيبرانية غير مسبوقة ضد محطة الطاقة النووية الإيرانية تمت من خلال نشر برنامج خبيث يسمى "ستكسنت". ويعتبر هذا البرنامج فريدًا من نوعه نظرًا لبنيته وخصائصه المميزة، يتميز "ستكسنت" بأنه لا ينشط إلا في ظروف محددة للغاية، وله هدفان واضحان هما: توجيه أجهزة الطرد المركزي لتخصيب اليورانيوم للعمل بسرعات مختلفة، مما يؤدي إلى إتلاف الأجهزة وعملية التخصيب، إرسال إشارات خاطئة توحي بأن النظام يعمل بشكل طبيعي، مستخدمًا شهادات من شركتين معروفتين، وفيما يتعلق بالجهات المسؤولة عن الهجوم، تشير عدة أدلة إلى تورط الولايات المتحدة وإسرائيل، منها الوقت والموارد اللازمة لإنشاء برنامج خبيث بهذا التعقيد، وتصريحات لمسؤولين حكوميين .

See; Evangelia Linaki, Cyber Warfare and International Humanitarian Law:a Matter of

الإيرانية، مما أدى إلى تأخير برنامج إيران النووي، لكن لم يتم الإبلاغ عن وفيات نتيجة لهذه الهجمات، فإذا افترضنا ان من قام بذلك مدنيين فإن ذلك يعد من قبيل المشاركة في الاعمال العدائية حيث إنه يحقق عتبة الضرر.[1]

وفي سياق النزاع الروسي الاوكراني يري البعض أن تقديم الاوكرانيين المدنيين المعلومات حول تحركات القوات الروسية للجيش من خلال تطبيق الهاتف الذكي، وتبادل المعلومات الاستخباراتية الرقمية، لا يحقق عتبة الضرر إلا إذا كانت المعلومات ضرورية لتنفيذ عملية عسكرية محددة، مثل نقل معلومات الاستهداف التكتيكي لهجوم.[2]

وعلى الرغم من التوافق العام بين دليل تالين والدليل التفسيري فيما يتعلق بمعيار عتبة الضرر، الا ان بينهما اختلاف، فبينما يتطلب الدليل التفسيري وجود ضرر فعلي أو احتمال معقول لتحقيقه، يستخدم دليل تالين مصطلح "التأثير المقصود أو الفعلي"، فيركز دليل تالين على النية وراء الهجوم السيبراني، بغض النظر عن حدوث ضرر مادي فعلي، وبالتالي فالمدني الذي ينوي إحداث ضرر كافٍ وينفذ هجومًا إلكترونيًا عدائيًا سيفقد الحماية كمدني بموجب دليل تالين، مما يقلص الحد الأدنى من الحماية للمدنيين المشاركين في الأعمال العدائية الإلكترونية، ويجعل استهدافهم أسهل.[3]

Applicability, Journal of International Law of Peace and Armed Conflict, Vol 27, April 2014, p174.

[1] Ahmad Khalil & Mohamad bitarn, Navigating legal frontiers in cyber warfare: insights from the russia-ukraine conflict, Vol 14, No2, June 2024 , p 257.

[2] Kubo Macak, Will the centre hold? Countering the erosion of the principle of distinction on the digital battlefield, International Review of the Red Cross, 105 (923), 2023, pp 972-973.

[3] see; Shannon Bosch, the international humanitarian law notion of direct participation in hostilities: a review of the ICRC interpretive guide and subsequent debate , African Journals Online, vol 17, No 3 , Sep 17, 2014,pp 1007-1013

الشرط الثاني- السببية المباشرة: يجب أن تكون هناك علاقة سببية مباشرة بين الفعل والضرر نفسه، ويجب أن يقوم المدني بتنفيذ العمل بنفسه حتى يتم اعتباره مشارك بصفة مباشرة في الأعمال العدائية. ولا يكفي مجرد تسهيل المجهود الحربي العام لتلبية معيار السببية المباشرة، بل يجب أن يتم إلحاق الضرر بطرف النزاع في خطوة سببية واحدة،[1]ولا يكفي مجرد وجود سلسلة أحداث سببية متصلة. ويشير الدليل التفسيري في هذا السياق الى مثال عامل مصنع الأسلحة حيث لا يُعتبر مشاركًا بشكل مباشر في الأعمال العدائية وفق هذا الشرط، وهو ما ينطبق على مطور الأسلحة السيبرانية".[2] ولكن قد تختلف طبيعة الأسلحة السيبرانية في هذا الصدد، فنظرًا للدفاعات السيبرانية النشطة والمتغيرة للخصم، قد تنشأ الحاجة إلى ترقية مستمرة للأسلحة السيبرانية أثناء الهجوم نفسه. وتتطلب هذه الترقيات تعاونًا وثيقًا بين المهاجم ومطور الأسلحة السيبرانية، مما يزيد من حدة مشاركة المطور في الهجوم. وبالتالي، فإن بعض أفعال مطوري البرمجيات يمكن أن تصل إلى عتبة السببية المباشرة، كونها لا تبعد سوى خطوة واحدة عن إحداث الضرر،[3] من جهة اخري، يري البعض ان معظم حالات تصميم الأسلحة السيبرانية تكون موجهة لعملية سيبرانية محددة.

---

http://dx.doi.org/10.4314/pelj.v17i3.05 Accessed 15 Sept. 2024, also; Dan-Julian Voitasec, cyber hostilities: civilian direct participation, *Challenges of the Knowledge Society,2016* , pp 552-553, Available at; https://www.proquest.com/scholarly-journals/cyber-hostilities-civilian-direct-participation/docview/1814061053/se-2 [Accessed Aug 10. 2024].

[1]ICRC Interpretive Guidance, at 53.

[2] ICRC, Fourth Expert Meeting on the Notion of Direct Participation in Hostilities: Summary Report, Geneva,27–28 November 2006, p. 48.

[3] Matheson, Colton. "From Munitions to Malware: A Comparative Analysis of Civilian Targetability in Cyber Conflict." *Journal of Law & Cyber Warfare*, vol. 7, no. 2, 2019, pp. 39. *JSTOR*, https://www.jstor.org/stable/26777971. [Accessed Sep 22. 2024] .

وبالتالي تتوفر الصلة السببية المباشرة بين إنتاج السلاح السيبراني والضرر المتوقع، وبالتالي يمكن اعتبار منتج هذا السلاح مشاركًا مباشرًا في الأعمال العدائية.[1]

والواقع انه على عكس الهجمات التقليدية التي تستهدف عادةً تدمير هدف مادي، فإن التأثيرات المرجوة من الهجمات السيبرانية تكون في الغالب غير مباشرة وتنطوي على سلاسل من الأسباب والنتائج، كما أن العديد من الأحداث المتداخلة بين السبب الأول والتأثير النهائي تكون ردود أفعال بشرية. بالإضافة إلى ذلك، قد لا تكون حلقات السلسلة السببية كلها متشابهة، فقد تشمل إجراءات ونتائج حاسوبية، أو تصورات وقرارات بشرية، تتضافر جميعها لتحقيق نتيجة معينة.[2]

ولا يوجد أي تعليق على معيار السببية المباشرة في دليل تالين، وفي الفضاء السيبراني يمكن زرع برامج ضارة لتنشط لاحقاً. كما أن الحرب الحديثة تشمل أمثلة على البعد الجغرافي، مثل الطائرات بدون طيار والصواريخ بعيدة المدى. ووفقاً للدليل التفسيري، لا يؤدي البعد الزمني أو الجغرافي بين فعل المدني والضرر الناتج إلى قطع الرابط السببي.[3] رغم ذلك، فإن المدني الذي يصمم برامج ضارة ويتيحها علناً على الإنترنت لا يستوفي معيار السببية المباشرة. وعليه، لا يُعتبر مشاركاً مباشراً في الأعمال العدائية، حتى لو استُخدمت تلك البرامج لإلحاق الضرر بالعدو.[4]

---

[1] Ahmed Aubais Al fatlawi, Beyond the Battlefield: Navigating the Legal Challenges of Civilian Cyber Participation in Modern Warfare, op.cit, P47.

[2] David Turns, Cyber Warfare and the Notion of Direct Participation in Hostilities, op.cit, p 288.

[3] David Wallace, Shane Reeves, and Trent Powell, Direct Participation in Hostilities in the Age of Cyber: Exploring the Fault Lines, op.cit, p 180 .

[4] Ibid , p188.Also see; Shannon Bosch, the international humanitarian law notion of direct participation in hostilities: a review of the ICRC interpretive guide and subsequent debate, AJOL African Journals Online, Vol 17,No 3, 2014, pp 1013-1018. http://dx.doi.org/10.4314/pelj.v17i3.05.

الشرط الثالث- شرط العدائية: بالإضافة إلى الشرطين الموضوعيين السابقين، يجب أن تتكون أي مشاركة مباشرة في الأعمال العدائية من عنصر ذاتي ثالث، وهو الصلة بالعمليات العدائية فيجب أن يكون العمل مصممًا خصيصًا لدعم طرف في نزاع مسلح وإلحاق الضرر بالطرف الآخر.[1] لذلك، لا يمكن اعتبار أي سلوك يفتقر إلى ارتباط كافٍ بالأعمال العدائية مشاركة مباشرة فيها. ولا يمكن اعتبار مشاركة المدنيين مشاركة مباشرة في الأعمال العدائية إذا كانوا غير مدركين تمامًا للدور الذي يلعبونه في سير الأعمال العدائية.

في المجال السيبراني، يساعد هذا الشرط في التمييز بين الهاكرز الوطنيين الداعمين لبلدهم، والجماعات مثل Anonymous التي تنفذ أعمالًا مماثلة دون هدف دعم طرف معين في النزاع. ورغم أن استخدام "شبكة الروبوتات" لتنفيذ هجمات رفض الخدمة الموزعة عبر أجهزة الحاسوب المدنية المخترقة يجعل هذه الأجهزة أهدافًا عسكرية، إلا أن أصحابها غير المدركين لهذا الاستخدام يحتفظون بحمايتهم كمدنيين. وذلك لأن الشرط يأخذ في الاعتبار نية المهاجم وليس الضحية.[2]

وغالبا ما يواجه الهدف صعوبة في تمييز نية الهجوم السيبراني، إذ لا تكفي التفاصيل الفنية وحدها لتحديد مصدره، سواء كان دولة أو إرهابيين أو مجرمين. وحتى مع معرفة المصدر، يبقى تقييم الضرر الفعلي والتأثير المقصود أمراً صعباً، خاصة مع إمكانية تشابه الهجمات التجسسية والتخريبية من الناحية الفنية. كما قد تتسم بعض الهجمات الإلكترونية بتأثيرات تتراكم ببطء وتدريجياً، مثل الهجوم على نظام مالي مصمم لإفساد البيانات بشكل تدريجي.

---

[1] Interpretive Guidance, p. 46.

[2] Urban Praprotnik, Principle of Distinction in Cyber Warfare, Contemporary Military Challenges, Vo.26, I.2, June 2024, p 29, https://doi.org/10.2478/cmc-2024-0011 Accessed 2 Sept. 2024.

ولا يأخذ دليل تالين في الاعتبار المتطلبات التي تقضي بأن يكون الفعل دعمًا لطرف في النزاع وعلى حساب طرف آخر، ومن ناحية أخرى، يمكن أن تصبح الصلة بالعمليات العدائية متوفرة في مرحلة مبكرة من عملية الحرب السيبرانية، على سبيل المثال، إذا تم تصميم برنامج وكتابته خصيصًا لتعطيل أنظمة أسلحة معينة في الدولة المستهدفة. وعليه يمكن ان تنطبق الصلة بالعمليات العدائية قبل ارتكاب الفعل العدائي فعليًا أكثر من أثناء ارتكابه أو بعده.[1]

ويري البعض أن الشروط التراكمية قد تصعّب تصنيف بعض الأنشطة العدائية السيبرانية للمدنيين كمشاركة مباشرة في الأعمال العدائية، فأول صراع حدث في الفضاء السيبراني هو الصراع في كوسوفو، حيث استخدم القراصنة الصربيون مجموعة واسعة من الوسائل لوقف قصف الناتو لبلغراد، مثل الدعاية والتواصل وتضليل العدو والهجمات الفيروسية وهجمات حجب الخدمة والقصف بالبريد الإلكتروني. ولكن حتى بافتراض وجود نية عدائية ذاتية لدى القراصنة، لا يمكن تفسير هذه الأمثلة على أنها مشاركة مباشرة في الأعمال العدائية لأنها تفتقر إلى عتبة الضرر اللازمة، كما أن مجرد الدعاية لا يمكن فهمها إلا من حيث الارتباط السببي غير المباشر لأن الضرر المحتمل لم يتم إحداثه في خطوة سببية واحدة ولم يكن جزءًا من استراتيجية صربية عامة.[2]

[1] David Turns, Cyber Warfare and the Notion of Direct Participation in Hostilities, op.cit, P289

[2] Tomasz Andrzej Lewandowski, Can mouse clicking be seen as involvement in armed conflict? Some notes on the direct participation in hostilities in cyberspace, op.cit, p200.

ومن هنا فإن تسارع الهجمات السيبرانية يقدم بعدًا جديدًا لقضية المشاركة المدنية. ففي المجال الرقمي، يصبح التمييز بين أدوار المدنيين والمقاتلين أكثر صعوبة بسبب الطبيعة المجهولة واللامركزية للعمليات السيبرانية.[1]

ثانيا: تحديات تحديد بداية ونهاية المشاركة المباشرة في الأعمال العدائية

لا يتضمن قانون النزاعات المسلحة أي حظر على مشاركة أي فئة في العمليات السيبرانية، الا ان هذه المشاركة لها عواقبها القانونية التي تختلف حسب الفئة التي ينتمي إليها الفرد.[2] فالمدنيون لا يحظر مشاركتهم المباشرة في العمليات السيبرانية التي تصل لمستوى العمليات العدائية، ولكن يفقدون الحماية من الهجمات على مدى الوقت الذي يشاركون فيه في العمليات العدائية.[3]، ثم يستعيدون الحصانة عندما ينسحبون من عمل المشاركة المباشرة، ولا يجوز مهاجمتهم بعد ذلك، وهو ما يطلق عليه مصطلح "الباب الدوار"[4]

ولقد كانت المشاركة المباشرة في الأعمال العدائية قاصرة على حالة المدنيين الذين يقاتلون بالفعل ضد العدو باستخدام أساليب مماثلة للمقاتلين. أما المنظور الجديد

---

[1] Ahmed Aubais Al fatlawi, Beyond the Battlefield: Navigating the Legal Challenges of Civilian Cyber Participation in Modern Warfare, op.cit, p53.

[2] دليل تالين، الفصل الرابع، القسم الأول، القاعدة 25.

[3] دليل تالين، الفصل الرابع، القسم الأول، القاعدة 29.

[4] ظهر مصطلح "الباب الدوار" أو "Revolving Door" لأول مرة في مقال للكولونيل W. W. Hayes بعنوان "الحرب الجوية وقانون الحرب" عام 1990، وما زالت اللجنة الدولية للصليب الأحمر (ICRC) تستخدمه عند الإشارة إلى مشاركة المدنيين في الأعمال العدائية المباشرة. ويشبر المصطلح إلى الفقدان والاستعادة المستمرين للحماية من الهجوم أثناء الأعمال العدائية، ويتحدد أساسًا بفترات مشاركة المدنيين. وتعتمد المدة التي يظل فيها هذا الباب المفاهيمي مفتوحًا على مدة المشاركة المباشرة. بعبارة أخرى، يتمتع المدنيون بالحماية من الهجوم عندما يكون "الباب" مفتوحًا، ويصبحون عرضة للاستهداف عندما يكون مغلقًا، وبهذا المفهوم، فإن حالة الحماية للمدنيين تتغير وفقًا لمشاركتهم في الأعمال العدائية، حيث يفقدون الحماية عند المشاركة المباشرة ويستعيدونها عند التوقف عن المشاركة، مما يشبه حركة الباب الدوار في دخول وخروج الأشخاص.

للأعمال العدائية فقد مكن المدنيين من القيام بأعمال عدائية دون التواجد في ساحة المعركة. فنتيجة لتطور التكنولوجيات الجديدة التي قادها اختراع أجهزة الحاسوب والإنترنت، انتقل مفهوم ساحة المعركة من الواقع إلى الفضاء السيبراني.[1]

وتعد مدة المشاركة المباشرة في الأعمال العدائية من أكثر الأجزاء إثارة للجدل في الدليل التفسيري، ويشير الدليل بشكل محدد إلى مسألة الحرب السيبرانية عندما لا يتطلب تنفيذ عمل عدائي تنقلاً جغرافيًا، كما قد يكون الحال في هجمات شبكات الحاسوب أو أنظمة الأسلحة التي يتم التحكم فيها عن بُعد، فإن مدة المشاركة المباشرة في الأعمال العدائية ستقتصر على التنفيذ الفوري للعمل والتدابير التحضيرية التي تشكل جزءًا لا يتجزأ من ذلك العمل،[2] وبناءً على ذلك، يبدو أن مدة المشاركة السيبرانية المباشرة تقتصر على تنفيذ العمل. ولا يمكن اعتبار الرحلة إلى المكان الذي سيطلق منه المدني هجومًا سيبرانيًا، والعودة منه، بمثابة انتشار وعودة، ولا تعد جزءًا من المشاركة المباشرة في الأعمال العدائية، على عكس إطلاق الهجوم السيبراني، ومع ذلك، يتخذ دليل تالين موقفًا معاكسًا، حيث يتبني موقفًا أوسع[3]، حيث يدرج في مفهوم المشاركة المباشرة الأعمال التي تسبق أو تلي مباشرة العمل المؤهل، بما في ذلك السفر من وإلى موقع تنفيذ الهجوم السيبراني.[4] ويعتبر إنشاء الفيروسات جزءًا من هذه الإجراءات التحضيرية، لكن مجرد إنشائها دون معرفة الهدف لا يستوفي

[1] Tomasz Andrzej Lewandowski, Can mouse clicking be seen as involvement in armed conflict? Some notes on the direct participation in hostilities in cyberspace, op.cit, pp 195-196.

[2] Interpretative Guidance , p68.

[3] ينص دليل تالين على ان «أي فعل من أعمال المشاركة المباشرة في الأعمال العدائية من جانب مدني يجعل هذا الشخص قابلاً للاستهداف طوال الوقت الذي يشارك فيه في الفعل المؤهل للمشاركة المباشرة" واتفق جميع الخبراء على أن هذا سيشمل على الأقل الإجراءات التي تسبق أو تلي قانون التأهيل مباشرة. وعلى سبيل المثال، فإن الانتقال من وإلى الموقع الذي يوجد فيه الحاسوب المستخدم لإجراء عملية سيكون مشمولاً في هذه الفكرة.

[4] Tallinn Manual , p. 103

شرط الضرر، كما تشمل الإجراءات التحضيرية شراء المعدات وجمع المعلومات اللازمة للهجوم.

في الهجمات الإلكترونية، لا يتضمن الانتشار والعودة عادةً تحركًا جغرافيًا، بل يشمل إخفاء الآثار الرقمية ومنع المطاردة المحتملة بعد تنفيذ الهجوم، وبذلك، تبدأ المشاركة المباشرة في الأعمال العدائية مع اتخاذ أول إجراء تحضيري للهجوم، وتنتهي عندما يتوقف المدني عن الهجوم ويفصل نفسه عن العمل.

وقد استخدم القراصنة الباكستانيون هذه الأساليب في صراعهم مع الهند عام 1998، حيث هاجموا مواقع حكومية وسرقوا بيانات حساسة.[1]

ويميز الدليل التفسيري بين المدنيين الذين يشاركون في الأعمال العدائية بشكل متقطع وأولئك الذين هم أعضاء في جماعة مسلحة منظمة. يفقد المدنيون الحماية ضد الهجوم المباشر طوال مدة كل عمل محدد يرقى إلى مستوى المشاركة المباشرة في الأعمال العدائية، بينما يتوقف أعضاء الجماعات المسلحة المنظمة التابعة لطرف غير حكومي في نزاع مسلح عن كونهم مدنيين، ويفقدون الحماية ضد الهجوم المباشر، طالما أنهم يتولون وظيفتهم القتالية المستمرة.[2]

ويري البعض ان تطبيق مفهوم "الباب الدوار" على المدنيين المشاركين من خلال الوسائل السيبرانية غير عملي لسببين. أولاً، السرعة التي يمكن بها شن الهجمات

---

[1] في عام 1998، قام القراصنة الباكستانيون بشن هجمات على مواقع إلكترونية هندية، مستهدفين بشكل رئيسي المواقع المتعلقة بالشؤون النووية مثل مركز بهابها للبحوث الذرية ومركز إنديرا غاندي للبحوث الذرية، بالإضافة إلى مواقع حكومية أخرى. كما قاموا بنشر أدلة إرشادية عبر الإنترنت للهواة، توضح كيفية مهاجمة المواقع الهندية باستخدام هجمات حجب الخدمة الموزعة (DDoS) بشكل أساسي. وتمكنوا حتى من سرقة بعض البيانات المتعلقة بالبرنامج النووي الهندي.

Tomasz Andrzej Lewandowski, Can mouse clicking be seen as involvement in armed conflict? Some notes on the direct participation in hostilities in cyberspace, op.cit, p 200.

[2] Interpretative Guidance, p.70.

السيبرانية تحول دون تحديد هوية المهاجم قبل نهايتها، ثانيًا يتم اكتشاف معظم الهجمات السيبرانية بعد ارتكابها، عندما يستعيد الجاني المدني بالفعل حمايته المدنية.[1]حيث سيكون من الصعب جدًا مهاجمة مدني يشارك مباشرة في الأعمال العدائية في اللحظة التي يقوم بها بالهجوم بسبب وقت التتبع. فحتى لو ثبت أن المدني "أ" مسؤول عن هجوم معين على محطة الطاقة، لا يمكن مهاجمته لأنه توقف بالفعل عن المشاركة.

ويثور التساؤل حول الموقف حينما يطلق الفرد عمليات سيبرانية متكررة على مدى فترة ممتدة، والتي ترقى جميعها إلى أفعال مؤهلة للمشاركة المباشرة. ولقد انقسم فريق الخبراء الحكوميين في تحليله لهذا الموقف. حيث رأى بعضهم أن كل حادثة تقف بمفردها كفعل من أفعال المشاركة المباشرة، وعلى هذا النحو، فإن الفرد لا يمكن استهدافه إلا خلال فترات محددة من المشاركة وليس خلال الفترات بينهما. ويعتقد آخرون أن مثل هذا النهج "لا معنى له من الناحية العملية باعتباره مثالاً على "الباب الدوار"، وأن الفاعل يمكن استهدافه طوال الفترة بأكملها.[2] فيرى شميت أن التفسير المعقول لعبارة "لمثل هذا الوقت" في حالة الصراع السيبراني هو أن يشمل "الفترة الكاملة التي ينخرط خلالها المشارك السيبراني المباشر في عمليات سيبرانية متكررة.[3]

[1]Ahmed Aubais Al fatlawi, Beyond the Battlefield: Navigating the Legal Challenges of Civilian Cyber Participation in Modern Warfare, op.cit, p50. Also; François Delerue ,Civilian Direct Participation in Cyber Hostilities, op.cit, p11 .

[2] Tallinn Manual, p. 104.

[3] Michael N. Schmitt, Cyber Operations and the Jus in Bello: Key Issues, *Naval War College International Law Studies, 2011*, vailable at SSRN: https://ssrn.com/abstract=1801176

وكما يصعب تحديد المدة الزمنية للمشاركة المباشرة في العمليات السيبرانية، والتي تحدد متى يصبح الفرد هدفًا مشروعًا. يصعب كذلك تحديد الجهات الفاعلة السيبرانية بسبب خصائص مثل التخفي والإخفاء، وتأخر العمليات زمنيًا باستخدام تقنيات مثل القنابل المنطقية. كما ان الطبيعة المستمرة للعمليات السيبرانية قد تجعل الفرد هدفًا مشروعًا طوال مدة استمرار هذه العمليات، مما يمثل مبادرة لتجاهل مبدأ التمييز.[1]

يُعدّ التحدي الأبرز الذي يواجه مبدأ التمييز فيما يتعلق بمشاركة المدنيين في الحروب السيبرانية ما يتطلبه المبدأ من ضرورة تعليق أو إلغاء الهجوم المباشر على المدني إذا أصبح خارج نطاق القتال. حيث تكمن الإشكالية في تحديد هذا الوضع، أي ما الذي يُعدّ خروجًا عن نطاق القتال في حالة الأعمال العدائية التي تجري في الفضاء الإلكتروني؟ هل يكفي مجرد إيقاف تشغيل الحاسوب لاعتبار المدني خارج دائرة القتال؟ إضافةً إلى ذلك، فإن وسائل وأساليب مهاجمة المدنيين المشاركين في الحرب الإلكترونية غير محدودة، مما يزيد من تعقيد هذه المسألة. وبالتالي، فإن هذه التحديات تستلزم بحثًا معمقًا وتحليلًا دقيقًا بغية وضع معايير واضحة للتعامل مع مشاركة المدنيين في الحروب السيبرانية بما ينسجم مع مبدأ التمييز المنصوص عليه في القانون الدولي الإنساني.

وفي ظلّ التحديات التي تكتنف تطبيق مبدأ التمييز في ميدان المعركة السيبرانية عند انخراط المدنيين في الهجمات السيبرانية، تجدر الإشارة إلى أن استخدام القوة ضد هؤلاء المدنيين لا يزال محكومًا بالقيود القانونية الأخرى المستمدة من أحكام القانون الدولي الإنساني، ألا وهي مبادئ التناسب والضرورة العسكرية والإنسانية. وتؤدي هذه المبادئ أيضًا دورًا محوريًا في تحديد درجة الهجوم على مدني يشارك

[1] Urban Praprotnik, Principle of Distinction in Cyber Warfare, Contemporary Military Challenges, op.cit, P30 .

بشكل مباشر في الأعمال العدائية من منزله الخاص بينما يقوم برعاية أطفاله في الوقت ذاته. ولا شكّ أن إطلاق صاروخ لتدمير منزله وكلّ من فيه من مدنيين أبرياء سيكون أمرًا متنافيًا مع المبادئ سالفة الذكر. فهذه المبادئ السامية تشكّل صمام أمان يكفل حماية المدنيين من ويلات الحرب، حتى في حال مشاركتهم في الأعمال العدائية، وتضع حدودًا واضحة لا يجوز تجاوزها بأيّ حال من الأحوال، مهما كانت الظروف والمبررات، ولنا ان نستذكر هنا كلمات جان بيكتيه الشهيرة "إذا كان بإمكاننا إخراج المتسلل من العمل عن طريق أسره، فلا ينبغي أن نجرحه؛ وإذا كان بإمكاننا الحصول على نفس النتيجة عن طريق جرحه، فيجب ألا نقتله. إذا كان هناك وسيلتان لتحقيق نفس الميزة العسكرية، وفي حالتنا لوقف مدني عن هجوم على شبكة إلكترونية يجب أن نختار الوسيلة التي تسبب الضرر الأقل.

المبحث الثالث: تحديات النطاق العيني لمبدأ التمييز في الفضاء السيبراني

يرتبط مبدأ التمييز بحظر الهجمات العشوائية، حيث تُعرَّف هذه الهجمات بأنها تلك التي لا تستهدف هدفًا عسكريًا محددًا أو تستخدم وسائل قتال غير قابلة للتوجيه الدقيق.[1] وفي سياق الحرب السيبرانية، يواجه هذا المبدأ تحديات كبيرة نظرًا لصعوبة تطبيق مفهوم النزاع المسلح التقليدي على الهجمات السيبرانية، وكذلك بسبب التداخل الكبير بين البنية التحتية العسكرية والمدنية في الفضاء السيبراني، مما يجعل التمييز بين الأهداف المشروعة وغير المشروعة أمرًا بالغ الصعوبة.

المطلب الأول: غموض مفهوم الهجوم المسلح في الفضاء السيبراني

الفضاء السيبراني هو مجال فريد من نوعه يتحدى المفاهيم التقليدية لاستخدام القوة والهجمات المسلحة والتجسس، ينشأ الفضاء السيبراني من الإنترنت، وهي مجموعة عالمية من شبكات البيانات الحاسوبية المترابطة التي تُستخدم لأغراض

[1] م 4/51 من البروتوكول الإضافي الأول .

مادية وفكرية. إنه جزئيًا مجال مادي، يُستخدم للأنشطة التجارية (مثل الخدمات المصرفية الإلكترونية) وإدارة البنية الأساسية (مثل أنظمة التحكم الصناعية)، وجزئيًا مجال فكري فهو منصة لتبادل المعلومات والاتصالات.[1]

لقد قدم البروتوكول الإضافي الأول تعريفاً للهجوم، إلا أن هذا التعريف يبدو قاصراً عن الإحاطة بجميع جوانب المسألة. فالتركيز على الأعمال العنيفة وحدها قد يغفل أهمية النتائج العنيفة التي قد تنجم عن أعمال غير عنيفة ظاهرياً، ولعل أبرز مثال على ذلك حظر الهجمات الكيميائية والبيولوجية والإشعاعية. فهذه الهجمات، رغم أنها لا تنطوي على استخدام قوة حركية مباشرة، إلا أن عواقبها وخيمة وقد تؤدي إلى الموت.

وبتطبيق هذا المنطق على العمليات السيبرانية، يمكن اعتبار أي عملية تسبب إصابات للأشخاص أو أضراراً للممتلكات بمثابة هجوم، وبالتالي تخضع لكافة قواعد القانون الدولي الإنساني.[2] كما ان هذا التعريف وإن كان كافيًا في عصر كانت فيه الهجمات تُنفّذ بالوسائل التقليدية، لأن هذه الوسائل عنيفة بطبيعتها. فإنه قد لا يشمل بعض العمليات السيبرانية حيث أنها معقّدة بطبيعتها، فقد تفي بالغاية العسكرية المطلوبة من دون التسبب بآثارٍ مدمرة أو ضارة أحيانًا.[3]

ففي ضوء هذا التعريف لا تعتبر جميع الهجمات على الشبكات الحاسوبية "هجمات" بالمعنى المقصود في قانون النزاعات المسلحة. أي ترقي الى مستوى

---

[1] Benjamin Mueller , *THE LAWS OF WAR AND CYBERSPACE: On The Need For A Treaty Concerning Cyber Conflict* . LSE IDEAS, Jun 2014. P.5 *JSTOR,* http://www.jstor.org/stable/resrep45315. [Accessed Sep 20. 2024].

[2] Tallinn Manual, Rule 30, para. 2, p 106 .

[3] حسن فياض، الهجمات السيبرانية من منظور القانون الدولى الإنساني، مجلة الدفاع الوطنى، ع 114، أكتوبر، 2020 متاح على الرابط : الهجمات السيبرانية من منظور القانون الدولي الإنساني | الموقع الرسمي للجيش اللبناني (lebarmy.gov.lb) (تاريخ الاطلاع: 2023/9/1م) .

النزاع المسلح، فالهجمات التي تستخدم فقط لجمع المعلومات الاستخبارية، أو اختراق جدار الحماية، أو إدخال فيروس، أو السيطرة على الشفرات، أو استرجاع بيانات سرية، أو التدخل في الاتصالات، لا تعتبر هجمات وفقًا لمعايير القانون الدولي الإنساني، لأنها تفتقر إلى العنف. ويختلف الوضع تماماً إذا استهدف الهجوم السيطرة على جهاز حاسوب معادٍ - عسكري أو مدني- وتسبب ذلك في إصابات بشرية أو أضرار جسيمة بالممتلكات المادية مثل تعطيل الجهاز المستهدف بشكل دائم أو تعطيل البرمجيات الداعمة للحياة. هنا تعد "هجمات" وفقاً لقانون النزاعات المسلحة، وبالتالي تخضع لنفس القواعد التي تنطبق على الهجمات الحركية. ومنها مبدأ التمييز،[1] وهذا يعني أن الهجمات الإلكترونية التي تستخدم العنف يجب أن تستهدف فقط المقاتلين والأهداف العسكرية، وأن تتجنب إلحاق الضرر بالمدنيين والأهداف المدنية قدر الإمكان.

لذا ثار الجدل حول تفسير مفهوم الهجمات بشكل أوسع، فالعملية السيبرانية التي تستهدف البنية التحتية السيبرانية المدنية "موارد الاتصالات والتخزين والحوسبة التي تعمل عليها أنظمة المعلومات" دون أن يكون لها آثار مادية، يمكن أن تكون أكثر ضرراً بكثير من تلك التي تسبب أضراراً محدودة.[2]

---

[1] اللجنة الدولية للصليب الأحمر، الحرب السيبرانية: القانون الدولي الإنساني يوفر طبقة إضافية من الحماية، سبتمبر 2019، متاح على الرابط: https://2u.pw/yBD7b6t0 (تاريخ الاطلاع: 2024/9/15م) .

Ahmad Khalil, Challenges to the principle of distinction …in cyber warfare: Navigating international humanitarian law compliance, Prawo I Wiez; Law & Social Bonds, June 2024, p112. https://www.researchgate.net/publication/381830929 Accessed 20 Sept. 2024.

[2] Eitan Diamond , "Applying International Humanitarian Law to Cyber Warfare." *Law and National Security: Selected Issues*, edited by Pnina Sharvit Baruch and Anat Kurz, Institute for National Security Studies, 2014, pp76-77.

على سبيل المثال، لنتصور هجوماً إلكترونياً خلال نزاع مسلح على أنظمة الخصم المصرفية، أو الضريبية، أو معاشات الحكومة، أو حجوزات شركات الطيران. يجادل منتقدو التفسير المقيد بأنه يبدو غير منطقي حظر العمليات التي لها آثار مادية فقط، بمعنى آخر، قد تكون الهجمات السيبرانية التي تعطل الخدمات والبنى التحتية المدنية الحيوية، حتى دون تدمير مادي، أشد ضرراً من الهجمات المسلحة المحدودة. لذا يرى البعض ضرورة توسيع مفهوم الهجوم ليشمل مثل هذه العمليات السيبرانية شديدة الأثر رغم افتقارها للعنف المادي[1].

ومن أمثلة العمليات السيبرانية التي قد ترقى إلى مستوى استخدام القوة في النزاعات السيبرانية العمليات التي تؤدي إلى انهيار محطة نووية، والعمليات التي تتسبب في فتح سد فوق منطقة مأهولة مما يؤدي إلى دمار، والعمليات التي تعطل نظام مراقبة الحركة الجوية مما يتسبب في تحطم طائرات، واستخدام هجوم سيبراني لإغلاق محطة دفاع جوي، واختراق شبكة الدفاع المركزية للعدو، وشن هجمات سيبرانية على محطات الإعلام.[2]

لا شك أنه عندما تكون هناك حرب حركية قائمة بالفعل (نزاع مسلح دولي أو غير دولي)، فإن القانون الدولي الإنساني ينطبق على العمليات السيبرانية المرتبطة بهذا النزاع.[3] ومن الأمثلة المعاصرة على الحرب السيبرانية المرتبطة بحرب حركية

---

[1] Michael N. Schmitt ,"THE LAW OF CYBER TARGETING." *Naval War College Review*, vol. 68, no. 2, 2015, pp. 16–17. *JSTOR*, http://www.jstor.org/stable/26397834 Accessed 20 Sept. 2024.

[2] KARATZIAS Vasileios, Direct Participation of Civilians in Cyber Hostilities in times of Armed Conflict, op.cit, p2 .

[3] Tallinn Manual, Commentary on Rule 35, para. 5, p120. Also ; Stephenie Gosnell Handler, The new Cyber Face of Battle: Developing a legal Approach to Accommodate Emerging Trends in Warfare, in: Stanford Journal of International Law, Vol 48, 2012, p. 233.

الحرب السيبرانية الروسية الاوكرانية، الا ان السؤال يثور حول ما إذا كانت العمليات السيبرانية وحدها، في غياب نزاع مسلح حركي، يمكن أن تشكل نزاعاً مسلحاً بحد ذاتها بحيث ينطبق عليها القانون الدولي الإنساني.[1]

وللإجابة على هذا السؤال، من الضروري التمييز بين النزاع المسلح الدولي وغير الدولي، حيث قد تختلف الإجابة بحسب نوع النزاع.

ففيما يتعلق بالنزاع المسلح الدولي يمكن أن يبدأ نزاع مسلح دولي على أساس تبادلات سيبرانية فقط إذا كانت دولتان أو أكثر متورطة وكانت طبيعة العمليات السيبرانية ترقى لمستوى "الهجمات"، ومن امثلة ذلك، لو افترضنا أن دولاً هي من نفذت عملية ستوكسينت ضد إيران عام 2010 والتي تسببت بأضرار مادية، فيمكن القول بأن الدول المعنية كانت في حالة نزاع مسلح دولي خلال فترة تنفيذ تلك العملية المدمرة. أما بالنسبة للنزاع المسلح غير الدولي فمن غير المرجح أن تفي التبادلات السيبرانية وحدها بمعايير النزاع المسلح غير الدولي لسببين:

1. يجب أن تواجه الدولة "جماعة مسلحة منظمة". والتنظيم عبر الإنترنت فقط قد لا يكفي لتلبية شروط التنظيم والقيادة والهيكلية المطلوبة قانوناً.

2. يجب أن يكون العنف المرتبط بالنزاع طويل الأمد وبمستوى عالٍ من الشدة. فالعمليات السيبرانية المعزولة أو قصيرة الأمد، حتى لو سببت أضراراً، لا ترقى لهذا المستوى.

ومن امثلة ذلك الهجمات السيبرانية ضد إستونيا حيث لم تشكل نزاعاً مسلحاً غير دولي لأن المشاركين، رغم تنسيقهم، لم ينظموا في مجموعة مسلحة واحدة. كما أن

[1] Schmitt, Michael N. "THE LAW OF CYBER TARGETING, op.cit, p13.

الهجمات، رغم تعطيلها الواسع للخدمات، لم تتسبب بأضرار جسدية أو إصابات ولم تمتد لفترة زمنية كافية.[1]

فالعمليات السيبرانية المنفذة من قبل جهات غير حكومية لن تعتبر جزءاً من نزاع مسلح وتخضع للقانون الدولي الإنساني إلا إذا كانت مصاحبة لهجمات مسلحة تقليدية. لذا فالسيناريو الأكثر احتمالاً هو أن تصاحب العمليات السيبرانية هجمات حركية، وبالتالي تخضع لقواعد القانون الدولي الإنساني على هذا الأساس، أما إذا جاءت منفصلة، فستخضع للقوانين الوطنية وقوانين حقوق الإنسان فقط دون القانون الدولي الإنساني.

لا يوجد حتى الآن سابقة قانونية واضحة تحدد متى تشكل الهجمات السيبرانية استخداماً للقوة أو هجوماً مسلحاً نظراً لحداثة هذا النوع من الهجمات نسبياً. لكن يبدو أن هناك اتجاهاً نحو تبني "نهج قائم على التأثيرات" لتحديد ذلك. ووفقاً لهذا النهج، لا يتم التركيز كثيراً على طبيعة الهجوم كونه إلكترونياً، بل على التأثيرات الناتجة عنه. فإذا أدى الهجوم السيبراني إلى تأثيرات وأضرار كبيرة تعادل تلك الناجمة عن هجوم مسلح تقليدي، فيمكن اعتباره هجوماً مسلحاً يبرر الرد عليه بالقوة دفاعاً عن النفس، على سبيل المثال، هجوم سيبراني يعطل النظام المالي ويضر بشدة بالاقتصاد والتجارة قد يعتبر بمثابة هجوم مسلح وفقاً لهذا النهج القائم على التأثيرات،

تندرج العمليات السيبرانية التي تؤثر على الوظائف الاقتصادية أيضاً في إطار الغموض المتأصل في القانون الدولي، فهي تتأرجح بين كونها شكلاً من أشكال العقوبات الاقتصادية، وهي ممارسة قانونية، وبين اعتبارها نوعاً من الحصار، الذي يُعد عملاً من أعمال الحرب.[2]

---

[1] Ibid, pp. 14–15.

[2] Hunker, Jeffrey. *Cyber War and Cyber Power: Issues for NATO Doctrine*. NATO

ويقدم دليل تالين وجهات نظر مثيرة للاهتمام في هذه المسألة. فهو يؤيد التقسيم التقليدي بين النزاعات المسلحة الدولية وغير الدولية، ويعترف بأن العمليات السيبرانية وحدها قد تشكل صراعات مسلحة اعتمادًا على الظروف - وخاصة على الآثار المدمرة لمثل هذه العمليات.[1]وفي هذا الصدد، يعرّف الدليل "الهجوم السيبراني" بموجب القانون الدولي الإنساني بأنه "عملية سيبرانية، سواء كانت هجومية أو دفاعية، من المتوقع بشكل معقول أن تتسبب في إصابة أو وفاة أشخاص أو إلحاق الضرر أو تدمير الأشياء"[2].

إن تحديد ما إذا كان الهجوم السيبراني ينشئ حالة نزاع مسلح يعتمد على نتائج ذلك الهجوم. فالهجمات غير الحركية يمكن أن تترتب عليها عواقب مادية، وفي كثير من الحالات قد تكون أشد وطأة من تلك الناجمة عن الهجمات باستخدام الأسلحة التقليدية. على سبيل المثال، الهجمات السيبرانية التي تستهدف أنظمة التحكم في السكك الحديدية عن طريق التلاعب بتعليمات التحويل، أو التلاعب بمعالجة المياه لمنطقة حضرية كبيرة، أو تغيير بيانات مثل فصيلة الدم أو الحساسية في نظام السجلات الطبية المحوسب، أو التجسس السيبراني الذى قد يؤدي إلى إلحاق الضرر بالبلاد على الأقل بنفس شدة الهجوم المادي.[3]

Defense College, 2010.p 8, *JSTOR*, http://www.jstor.org/stable/resrep10354.Accessed 20 Sept. 2024.

[1] يتضح ذلك في تعريف دليل تالين النزاع المسلح الدولي في اطار العمليات السيبرانية بأنه " العمليات العدائية السيبرانية التي تحدث بين دولتين أو عدة دول" [القاعدة 22] ، وتعريف النزاعات المسلحة غير الدولية بأنها " عنف مسلح ممتد، الذى يشمل أو يقتصر على العمليات السيبرانية، ويحدث بين القوات المسلحة الحكومية والقوات التابعة لجماعة أو جماعات مسلحة، أو فيما بين هذه الجماعات. والمواجهة ينبغي أن تصل الى أدنى مستوى من الكثافة والأطراف المشاركة في النزاع ينبغي أن تظهر لديها درجة كافية من التنظيم" [القاعدة 23] .

[2] دليل تالين بشأن القانون الدولي المطبق على الحروب السيبرانية (النسخة المترجمة للعربية)، الفصل الرابع، القسم الثاني، القاعدة 30 ، ص 7 .

[3] Jack Goldsmith, How Cyber Changes the Laws of War, The European Journal of

يجب عدم الخلط بين هذا التحليل والحالات التي يتم فيها شن هجمات على شبكات الحاسوب "لإعداد ساحة المعركة" لهجوم وشيك باستخدام القوات العسكرية التقليدية. ومثال نموذجي على ذلك هو هجوم شبكة الحاسوب ضد شبكة الدفاع الجوي. وبقدر ما ترتبط هذه العمليات بإطلاق وشيك لهجوم حركي، فإنها تشير إلى بدء نزاع مسلح. ولا حاجة لهجوم شبكة الحاسوب أن يتسبب إما في إصابة بشرية أو ضرر مادي لأن الهجوم يعد بالفعل جزءًا لا يتجزأ من هجوم سيفعل ذلك.

مع الوعي بحقيقة أن الهجوم السيبراني قد ينطوي على معايير القانون الإنساني، فكيف يتم تطبيق مفهوم المشاركة المباشرة في نزاع يستخدم هجوم الشبكات الحاسوبية؟ أولاً، بما أن هجوم الشبكات الحاسوبية يمكن أن يتسبب في إصابة، أو وفاة أو ضرر أو دمار للقوات المعادية، فإن أولئك الذين يقومون بعمليات تنتج مثل هذه الآثار يشاركون بلا شك بشكل مباشر في الأعمال العدائية. كما تشمل المشاركة المباشرة بشكل معقول هجمات الشبكات الحاسوبية الموجهة ضد قدرات العدو القتالية الفورية.

وبالتالي، تنطبق قواعد القانون الإنساني كلما كانت الهجمات السيبرانية المنسوبة إلى دولة أكثر من مجرد حوادث متفرقة ومعزولة، وتهدف إما إلى التسبب في إصابات، أو وفيات أو أضرار أو دمار (وما يماثلها من آثار)، أو كانت هذه العواقب متوقعة. ومن الأمثلة على ذلك:

1. قيام دولة بشن هجوم سيبراني يتسبب في تعطيل شبكة الكهرباء في دولة أخرى، مما يؤدي إلى انقطاع الطاقة على نطاق واسع وتعريض حياة المدنيين للخطر.

2. استخدام دولة للهجمات السيبرانية لتعطيل أنظمة الملاحة الجوية في دولة أخرى، مما يهدد سلامة الطائرات المدنية ويعرض الركاب للخطر.

International Law, Vol. 24 no. 1, p133.

3. قيام دولة بتنفيذ هجوم سيبراني على منشآت صناعية في دولة أخرى، مما يتسبب في حدوث انفجارات أو تسرب مواد خطرة، وينتج عنه إصابات وأضرار بيئية جسيمة.

في مثل هذه الحالات، يمكن اعتبار الهجمات السيبرانية بمثابة بدء لنزاع مسلح، وتصبح قواعد القانون الدولي الإنساني واجبة التطبيق لحماية المدنيين والأعيان المدنية من آثار تلك الهجمات. فيجب مراعاة الآثار المترتبة على العواقب غير المباشرة للحرب السيبرانية ومتطلبات إمكانية التوقع المعقول للضرر. فإذا كانت العواقب غير المباشرة هي في الواقع القصد من وراء الهجوم، فإن الضرر الناتج سيكون متوقعًا بشكل موضوعي وسيكون له الصلة المطلوبة بالعمليات العدائية، لكنه سيفشل في اختبار السببية المباشرة. أما إذا لم تكن العواقب غير المباشرة مقصودة أو متوقعة، فقد يظل الضرر محتملاً بشكل موضوعي، لكن ستنقصه الصلة بالعمليات العدائية والسببية المباشرة.

الأفعال الإجرامية أو الخاصة البحتة التي تحدث في وقت متزامن مع النزاع المسلح لا تكفي لتلبية هذا الشرط، وبطبيعة الحال، إذا كانت عائدات جريمة إلكترونية مرتبطة بتمويل عمليات عسكرية معينة، فمن المرجح أن توجد علاقة حربية، ولكن ارتكاب مدني لجريمة إلكترونية ضد ممتلكات أو أفراد عسكريين معاديين لا ينشئ في حد ذاته علاقة حربية لأن هذه الأفعال قد تتم لتحقيق مكاسب شخصية بحتة لا علاقة لها بالنزاع المسلح.[1]

[1] Michael N. Schmitt, Military Necessity and Humanity in International Humanitarian Law: Preserving the Delicate Balance, 50 VA.J. INT'L L. 2010, p 735.

المطلب الثاني: تداخل البنية التحتية المدنية والعسكرية في الفضاء السيبراني

بموجب مبدأ التمييز، تلتزم أطراف النزاع المسلح بالتمييز في جميع الأوقات بين السكان المدنيين والمقاتلين، وبين الأهداف المدنية والأهداف العسكرية، ولا يجوز لها توجيه عملياتها إلا ضد الأهداف العسكرية.[1] وعليه، يجب توجيه العمليات السيبرانية فقط ضد الأهداف العسكرية، أي "تلك الأهداف التي تساهم بطبيعتها، أو موقعها، أو غرضها، أو استخدامها بشكل فعال في العمل العسكري، والتي يوفر تدميرها الكلي أو الجزئي أو الاستيلاء عليها أو تحييدها، في الظروف السائدة في ذلك الوقت، ميزة عسكرية محددة".[2]

ويعتبر أي هدف لا يقع ضمن هذا التعريف هدفًا مدنيًا ولا يجوز أن يكون هدفًا للهجوم.[3] وعلاوة على ذلك، في حالة الشك فيما إذا كان الهدف المخصص عادة لأغراض مدنية يُستخدم لتقديم مساهمة فعالة في العمل العسكري، فيجب افتراض أنه لا يُستخدم على هذا النحو، وبالتالي لا يجوز جعله هدفًا للهجوم.[4]

تعتبر معدات ومرافق القوات المسلحة أهدافاً عسكرية بطبيعتها. فعلى سبيل المثال، تعد منشأة القيادة والتحكم والبنية التحتية السيبرانية المطورة لمهام عسكرية محددة من الأهداف العسكرية على هذا الأساس. كما يمكن أن يكون موقع معين هدفاً عسكرياً، كما هو الحال عند استخدام الوسائل السيبرانية لفتح بوابات سد لإغراق منطقة ومنع العدو من استخدامها.

وبصرف النظر عن المعدات العسكرية، فإن الهدف العسكري الأكثر احتمالاً في السياق السيبراني هو الجسم الذي يستوفي معيار "الاستخدام"، أي الذي كان يستخدم

---

[1] المادة 48 من البروتوكول الإضافي الأول 1977م.

[2] المادة 2/52 من البروتوكول الإضافي الأول 1977م.

[3] المادة 1/52 من البروتوكول الإضافي الأول 1977م.

[4] المادة 3/53 من البروتوكول الإضافي الأول 1977م.

سابقاً أو لا يزال يستخدم لأغراض مدنية، ولكنه الآن يستخدم، ولو جزئياً، لأغراض عسكرية. وتجدر الإشارة إلى ضرورة توخي الحذر عند تطبيق هذا المعيار على الأنشطة السيبرانية. فعلى سبيل المثال، لا يجعل مجرد إرسال العسكريين للبريد الإلكتروني عبر الإنترنت أن يصبح الانترنت بأكمله هدفاً مشروعاً، وأخيراً، يمكن أن يصبح الجسم المدني هدفاً عسكرياً من خلال "الغرض"، والذي يشير إلى الاستخدام المستقبلي المقصود للجسم. فعلى سبيل المثال، إذا كانت هناك معلومات استخباراتية موثوقة بأن مزرعة خوادم مدنية ستبدأ قريباً في تخزين بيانات عسكرية، فإن المزرعة تصبح هدفاً عسكرياً يمكن مهاجمته حتى قبل بدء تخزين البيانات.[1]

أشار دليل تالين الى أنه لا يجوز أن تكون الأعيان المدنية هدفًا للهجمات السيبرانية، فلا يجوز على سبيل المثال توجيه الهجمات السيبرانية التي من شأنها تدمير الأنظمة المدنية والبنية التحتية، ما لم تعد هذه الأنظمة من قبيل الأهداف العسكرية التي يجوز استهدافها وفق الظروف السائدة.

إلا أن الإشكالية الرئيسية فيما يتعلق بالحرب السيبرانية أن معظم البني التحتية السيبرانية ذات استخدام مزدوج، حيث تخدم أغراضًا مدنية وعسكرية. ففي الفضاء السيبراني الشبكات المدنية والعسكرية مترابطة، حيث تعتمد العديد من الشبكات العسكرية على البنية التحتية السيبرانية المدنية مثل كابلات الالياف البصرية البحرية أو الأقمار الصناعية أو أجهزة التوجيه، وفي المقابل تعتمد المركبات ووسائل النقل البحري وأجهزة مراقبة حركة الطيران المدنية بشكل متزايد على أنظمة الملاحة بالأقمار الاصطناعية التي تستخدم أيضا من قبل العسكريين وتستخدم سلاسل الامدادات اللوجستية المدنية والخدمات المدنية الاساسية شبكات الانترنت والاتصالات ذاتها التي تمر من خلالها بعض الاتصالات العسكرية.[2] فواقع النشاط

[1] Schmitt, Michael N. "THE LAW OF CYBER TARGETING, op.cit, p. 18.

[2] القانون الدولى الإنساني والعمليات السيبرانية خلال النزاعات المسلحة، ورقة موقف اللجنة الدولية للصليب

السيبراني العسكري في القرن الحادي والعشرين هو اعتماده الكبير على البنية الأساسية المدنية مما يوسع بشكل كبير نطاق الأهداف العسكرية، بما في ذلك الأنظمة التي تعتمد عليها وظائف مدنية مهمة.[1]

ووفقا لدليل تالين فإن الاعيان ذات الاستخدام المزدوج هي أهداف عسكرية دون قيد أو شرط بسبب الغرض العسكري الذي تخدمه[2]. وبالتالي يمكن تصنيف جميع عناصر البني التحتية السيبرانية الدولية تقريباً على أنها أهداف عسكرية، وبالتالي - مع مراعاة قواعد القانون الدولي الإنساني الأخرى[3]- يمكن أن تكون عرضة للهجوم. في الواقع، ووفقاً لهذا الرأي، فإن الكابلات والعقد والموجهات والأقمار الصناعية التي تعتمد عليها العديد من الأنظمة المدنية ستعتبر جميعها أهدافاً عسكرية لأنها تؤدي وظيفة مزدوجة تتمثل في نقل المعلومات العسكرية. ومع اعتبار العديد من الاعيان في المجال السيبراني بهذا الشكل أهدافاً عسكرية، فإن مبدأ التمييز - الذي يُنظر إليه على أنه القاعدة الأساسية لحماية المدنيين من الأخطار الناشئة عن الأعمال العدائية - يصبح إلى حد كبير مجرداً من قيمته الحمائية. وأي حماية يمكن أن يوفرها القانون

الأحمر، مقدمة إلى فريق العمل المفتوح العضوية، المعنى بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الامن الدولي، وإلى فريق الخبراء الحكوميين المعنى بالارتقاء بسلوك الدول المسؤول في ميدان الفضاء السيبراني في سياق الامن الدولي، نوفمبر 2019 ، ص 6 ، متاح على الرابط :

icrc_ihl_and_cyber_operations_during_armed_conflict_ar.pdf (تاريخ الإطلاع: 2024/9/11)

[1] Ibid, p 19.

[2] Tallinn Manual, Commentary on Rule 39, para. 1.

[3] حيث اشارت اللجنة الدولية للصليب الأحمر في تقرير حول القانون الدولي الإنساني والعمليات السيبرانية السابق الإشارة إليه الى انه ذا لم تعد أجزاء معينة من البنية التحتية للفضاء السيبراني محمية بصفتها أعيان مدنية خلال النزاعات المسلحة، سيظل أي هجومً عليها محكوماً بالحظر المفروض على الهجمات العشوائية وقواعد التناسب والاحتياطات أثناء الهجوم.

الدولي الإنساني للبنية التحتية السيبرانية المدنية وللأنظمة والخدمات المدنية التي تعتمد عليها، ستكون مستمدة من مبدأي التناسب والاحتياط.[1]

ويسوق لنا النزاع الروسي الاوكراني مثال واضح في هذا السياق، حيث قامت أوكرانيا بتطوير مواقع الخدمات الحكومية وحولتها من مجرد شبكة خدمات عامة إلى منصة لتقديم خدمات عسكرية، من هذه الخدمات السماح للأوكرانيين المدنيين بتقديم صور ومقاطع فيديو موثقة بالموقع لرصد القوات العسكرية الروسية، وهذه البيانات يتم تجميعها على خريطة مرئية توفر للمسؤولين الاستخباراتيين الأوكرانيين معلومات قيمة تساعدهم في الدفاع والقيام بالضربات المضادة.[2]

حتى البنية التحتية السيبرانية المدنية التي لا تستخدم للأغراض المزدوجة، قد تتعرض للضرر بسبب الترابط في الفضاء السيبراني. فالفضاء السيبراني يتميّز بالتوصيل بين نظم الحواسيب. ويتألف هذا الفضاء من عدد لا يُحصى من نظم الحواسيب المتصلة ببعضها البعض في أرجاء العالم. فتتصل نظم الحواسيب العسكرية بالنظم التجارية والمدنية وتعتمد عليها كلياً أو جزئياً. هذا الترابط يجعل من الصعب، إن لم يكن من المستحيل، تنفيذ هجوم سيبراني يستهدف البنية التحتية العسكرية دون التأثير على الأهداف المدنية. فمثلاً من شأن استخدام دودة [3] تتكاثر

---

[1] Eitan Diamond ,"Applying International Humanitarian Law to Cyber Warfare, op.cit, pp. 77–78.

[2] Drew Harwell, , instead of consumer software, Ukraine's tech workers build apps of war,

The Washington Post, March 24, 2022, Available at;
https://www.washingtonpost.com/technology/2022/03/24/ukraine-war-apps-russian-invasion/

[Accessed Aug 10. 2024].

[3] الديدان (بالإنجليزية: Worms) هي نوع من برامج الكمبيوتر الضارة التي تنتشر وتتكاثر عبر الشبكات، وتستنسخ نفسها دون تدخل المستخدم، وتسبب الضرر للأنظمة والشبكات المصابة.

ولا يمكن السيطرة عليها، أن تتسبب في أضرار كبيرة في بنية تحتية مدنية أن يشكل انتهاكاً للقانون الدولي الإنساني. ولتجنب هذه النتيجة، ووفقاً للحظر المفروض على الهجمات العشوائية،[1] يُحظر على أطراف النزاع استخدام الأسلحة السيبرانية التي تكون عشوائية بطبيعتها والتي لا يمكن الحد من آثارها الضارة.[2]

علاوة على ذلك، يجب على أي طرف محارب ينوي شن هجوم سيبراني أن يتحقق أولاً من أنه في الظروف المعطاة، يمكن توجيه السلاح السيبراني المستخدم وتوجيهه بالفعل نحو هدف عسكري، وأن آثاره يمكن أن تكون محدودة وفق ما تتطلبه قواعد القانون الدولي الإنساني.[3]

وفقا للمادة 4/51/ج من البروتوكول الإضافي الأول يحظر استخدام وسيلة قتال لا يمكن حصر آثارها، والتي من شأنها أن تصيب الأهداف العسكرية والاعيان المدنية دون تمييز، وإذا نظرنا الى تأثيرات الهجوم السيبراني نجد أنها قد تكون غير مؤكدة أو غير متوقعة إلى حد كبير. نظرًا لأن بعض أدوات الهجوم، مثل الديدان والفيروسات، يمكن أن تنتشر عالميًا، فهناك خطر حقيقي من الأضرار الجانبية حيث تنتشر هذه العوامل بشكل لا يمكن السيطرة عليه. فقد تسببت دودة موريس في نوفمبر 1988، في أضرار جسيمة للإنترنت الناشئة، على الرغم من أن هذا لم يكن بالتأكيد نية منشئها، كما تسعى الهجمات السيبرانية بشكل مباشر إلى تغيير أداء الأنظمة الإلكترونية شديدة التعقيد، مما قد يؤثر بدوره على سلوك الأنظمة المادية الأخرى شديدة التعقيد مثل البنى التحتية. إن سلوك الأنظمة المعقدة، بشكل عام، غير مفهوم

---

[1] المادة 4/51 من البروتوكول الإضافي الأول .

[2] كورديولا درويغ، الحرب السيبرانية والقانون الدولى الإنساني: كيف نحمى المدنيين من الآثار العرضية لهجوم الكتروني؟، مجلة الإنساني، اللجنة الدولية للصليب الأحمر، العدد 52، 20 مارس 2011م. متاح على الرابط : الحرب السيبرانية والقانون الدولي الإنساني: كيف نحمي المدنيين من الآثار العرضية لهجوم إلكتروني؟ - مجلة الإنساني | مجلة الإنساني(icrc.org) (تاريخ الاطلاع: 2024/9/1).

[3] المادة 4/51/أ، ج من البروتوكول الإضافي الأول .

جيدًا؛ على سبيل المثال، لم يتم تفسير الأسباب الفعلية لبعض حالات انقطاع التيار الكهربائي (العرضي) المنتشرة على نطاق واسع بشكل مرضٍ، فقد يؤدي سلوك النظام غير المتوقع إلى نتائج أخرى غير تلك التي قصدها المهاجم.[1]

أخيرًا، قد لا يعرف المهاجمون السيبرانيين على وجه اليقين مدى الضرر الذي قد يلحق بالأنظمة الإلكترونية.

تثير القائمة الواسعة للأهداف العسكرية في ساحة المعركة السيبرانية تساؤلات حول الحدود الجغرافية للنزاع المسلح. فالعمليات السيبرانية يمكن أن تستخدم البنية التحتية السيبرانية الموجودة في أي مكان في العالم، وقد تشمل آلاف أو حتى ملايين أجهزة الحاسوب في مواقع متنوعة حول العالم.

إذا اعتبرت كل هذه البنية التحتية هدفاً عسكرياً، فإن النزاع المسلح الذي ينطوي على حرب سيبرانية يمكن أن يمتد ليشمل كل ركن من أركان الأرض. وبالتالي، ستصبح كل حرب سيبرانية حرباً عالمية محتملة في الفضاء السيبراني.[2]

في النزاعات المسلحة الدولية، ستكون العمليات السيبرانية مقيدة بموجب قوانين الحياد، والتي ستحد من حق الدول المتحاربة في مهاجمة البنية التحتية الواقعة في إقليم دولة محايدة في تلك الحالات التي تفشل فيها الدولة المحايدة نفسها في إنهاء انتهاكات الحياد الصادرة من إقليمها، وعندما تشكل هذه الانتهاكات تهديداً خطيراً

[1] Jeffrey Hunker, *Cyber War and Cyber Power: Issues for NATO Doctrine*. NATO Defense College, 2010, p6 , *JSTOR*, http://www.jstor.org/stable/resrep10354. Accessed 20 Sept. 2024.

[2] TALLIN MANUAL, Commentary on Rule 21.

وفورياً لأمن الدولة المهاجمة، وعندما لا يكون هناك بديل آخر ممكن وفي الوقت المناسب.[1]

[1] See, Tallinn Manual, supra note 3, Chapter 7, in particular the Commentary on Rule 94.cited on Diamond, Eitan. "Applying International Humanitarian Law to Cyber Warfare, op.cit, p78.

الخاتمة

إن ساحة المعركة السيبرانية، بما تحمله من تحديات غير مسبوقة، تلقي بظلالها القاتمة على أحد أعمدة القانون الدولي الإنساني الراسخة - ألا وهو مبدأ التمييز. فهذا المبدأ الجوهري، الذي طالما شكّل حصناً منيعاً لحماية المدنيين واعيانهم في خضم النزاعات، يجد نفسه اليوم على حافة الهاوية في مواجهة الهجمات السيبرانية، مما يثير المخاوف من ان يقوض هذا النوع من النزاعات مبدأ التمييز، ويقوده الى نهايته، ومن هذا المنطلق تناولنا في هذه الدراسة التحديات التي يفرضها هذا الميدان الحديث على تطبيق مبدأ التمييز، وخلصنا من ذلك لعدد من النتائج والتوصيات.

النتائج:

1- غياب التعريفات الواضحة والدقيقة للمفاهيم المتعلقة بالحرب السيبرانية يخلق فراغًا قانونيًا يعرض المدنيين للخطر أثناء النزاعات، مما يتعارض مع الهدف الأساسي للقانون الدولي الإنساني. لذا، فإن تطوير إطار قانوني شامل يتكيف مع تحديات الفضاء السيبراني أصبح ضرورة ملحة لضمان حماية المدنيين وتطبيق مبدأ التمييز في ساحة المعركة السيبرانية.

2- يشكل تصنيف المقاتلين السيبرانيين تحدياً كبيراً في إطار القانون الدولي الإنساني التقليدي. فالمعايير المعتمدة لتحديد صفة المقاتل في الحروب التقليدية لا تنطبق بسهولة على المشاركين في العمليات السيبرانية. فالمقاتل السيبراني قد لا يحمل سلاحاً ملموساً، ولا يرتدي زياً عسكرياً محدداً، ولا يتواجد فعلياً في ساحة المعركة التقليدية. بل إنه قد يكون مدنياً يعمل من مكان بعيد عن مناطق النزاع، مستخدماً مهاراته التقنية لشن هجمات إلكترونية قد تكون لها آثار مدمرة تضاهي أو تفوق الأسلحة التقليدية، هذا التباين يخلق صعوبات جمة في تطبيق مبدأ التمييز.

3-كشفت الدراسة عن تحدٍ جوهري في تطبيق مبدأ التمييز خلال النزاعات السيبرانية، يتمثل في سهولة مشاركة المدنيين في الأعمال العدائية دون الحاجة إلى

أسلحة تقليدية. فقد أظهرت النتائج أن المدنيين يمكنهم المشاركة في الهجمات السيبرانية باستخدام أجهزة الحاسوب المنزلية، مع إمكانية إخفاء هوياتهم أو انتحال شخصيات أخرى. هذا الأمر يجعل من الصعوبة بمكان التمييز بين المقاتلين والمدنيين في الفضاء السيبراني.

4- يتسع مفهوم المشاركة المباشرة في الأعمال العدائية بشكل كبير في سياق الحرب السيبرانية، ليشمل مراحل متعددة تبدأ من الإجراءات التحضيرية وتنتهي بإخفاء الآثار الرقمية بعد الهجوم. هذا التوسع في المفهوم يؤدي إلى زيادة نسبة المدنيين الذين قد يُعتبرون أهدافاً مشروعة مقارنة بالحروب التقليدية. وعليه، فإن تطبيق مبدأ التمييز في الفضاء السيبراني يواجه تحديات جمة تتطلب إعادة تقييم وتكييف القواعد القانونية الحالية لتتناسب مع طبيعة هذا النوع الجديد من النزاعات.

5- أدت الحرب السيبرانية إلى تلاشي الحدود الفاصلة بين المقاتلين والمدنيين، الأمر الذي ينذر بعواقب وخيمة. فمع استمرار هذا النهج، ستتبلور لدى أطراف النزاعات المسلحة قناعات مغلوطة تنظر إلى جميع المدنيين على أنهم متورطون في الأعمال العدائية، مما سيؤدي حتمًا إلى تقويض القيود المفروضة على استهدافهم. وعلى المدى البعيد، سيفضي هذا التحول المقلق إلى انحسار مبدأ التمييز شيئًا فشيئًا، مخلفًا وراءه سلسلة من التداعيات الخطيرة التي ستمس صميم تفسير جميع قواعد القانون الدولي الإنساني المنبثقة عنه.

6- يواجه مبدأ التمييز في الفضاء السيبراني تحديًا كبيرًا في توفير الحماية اللازمة للبنية التحتية المدنية الإلكترونية والمنشآت المدنية المرتبطة بها. وتنبع هذه الإشكالية من الطبيعة المزدوجة التي تتسم بها غالبية البنى التحتية السيبرانية، ومن ان البنية التحتية المدنية يحقق تدميرها ميزة عسكرية.

7- ساهم الدليل التفسيري للجنة الدولية للصليب الأحمر بشكل كبير في توضيح مفهوم المشاركة في الأعمال العدائية، مزيلاً الكثير من الغموض الذي كان يحيط بهذه

المسألة. غير أن القوى العسكرية الكبرى لم تعلن بعد موقفها الرسمي تجاه استنتاجات هذه الوثيقة، سواء بالموافقة أو الرفض. وعلى الرغم من أهمية الدليل في تسليط الضوء على القضايا الخلافية وتفصيلها، إلا أن الشكوك لا تزال قائمة حول بعض جوانبه. كما أنه من غير الواضح كيفية تطبيق إرشاداته عملياً في ساحات المعارك الفعلية. ويزداد هذا الغموض حدة عندما يتعلق الأمر بتطبيق هذه الإرشادات في ساحات المعارك الافتراضية.

8- يظل مبدأ التمييز راسخًا لا يقبل المساومة في خضم المشهد المتغير للحروب المعاصرة، سواء أكانت تدور رحاها في الميادين المادية أم في الفضاءات الرقمية. وفي ظل استمرار التطور التكنولوجي في رسم حدود جديدة للنزاعات، يغدو التمسك بهذا المبدأ الجوهري أكثر إلحاحًا وأهمية من أي وقت مضى. فكلما اتسعت آفاق الصراع وتعقدت أدواته، ازدادت الحاجة إلى صون هذا المبدأ الأخلاقي والقانوني الذي يشكل حجر الزاوية في حماية الإنسانية وسط غبار المعارك المتصاعد، وهو ما يثير مسؤولية المجتمع الدولي عن تكييف القانون الدولي الإنساني مع تعقيدات الفضاء السيبراني للحفاظ على قدسية الحياة البشرية وحماية البنية التحتية المدنية الحيوية التي يعتمد عليها المجتمع الحديث.

9- غياب قانون دولي متفق عليه ومعتمد لما هو مسموح به عسكريًا في الفضاء السيبراني مما أدى الى تفاقم التكهنات حول كيفية تطبيق القانون الدولي الإنساني بصورته الحالية على النزاعات السيبرانية، فالفراغ القانوني الحالي في مجال الحرب السيبرانية والتطورات المتسارعة للإنترنت، أدت إلى عدم وجود إطار قانوني واضح يحكم الصراعات في الفضاء السيبراني، مما يزيد من صعوبة التعامل مع التحديات الناشئة عن طبيعة ساحة المعركة السيبرانية.

10-هناك فضاء سيبراني واحد فقط تتقاسمه القوات المسلحة مع المستخدمين المدنيين وكل شيء متشابك ومترابط. مما يضعنا امام تحديات ضمان توجيه هذا النوع من

الهجمات السيبرانية ضد المقاتلين والأهداف العسكرية، وبالتالي تحييد المدنيين أو الأعيان المدنية المحميين بموجب القانون الدولي الإنساني.

التوصيات:

1- ضرورة استخدام القدرات السيبرانية بطريقة تتوافق مع مبادئ القانون الدولي الإنساني، بصفة خاصة مبدأ التمييز، فيجب بذل كل جهد ممكن للتحقق من شرعية الأهداف، واختيار الوسائل والتكتيكات التي تقلل الضرر المدني، وإصدار تحذيرات للسكان المدنيين متى كان ذلك ممكناً. كما يمكن توظيف القدرات السيبرانية في جمع المعلومات الاستخبارية وإصدار التحذيرات، بما يعزز حماية المدنيين في النزاعات المسلحة.

2- نوصى بتطوير برامج تدريبية شاملة للقوات المسلحة والمدنيين على حد سواء، تهدف إلى رفع الوعي بالأمن السيبراني وتعزيز فهم الالتزامات القانونية في هذا المجال لتعزيز تطبيق مبدأ التمييز في هذا السياق الجديد، ولتعزيز قدرة العسكريين على اتخاذ القرارات الأخلاقية والقانونية السليمة في سياق العمليات السيبرانية.

3- ندعو إلى عقد مؤتمر دولي سنوي لمناقشة التطورات في مجال الحرب السيبرانية وتأثيرها على القانون الدولي الإنساني، بهدف ضمان استمرارية تطوير الأطر القانونية بما يتماشى مع التقدم التكنولوجي المتسارع.

4. ضرورة تطوير وتحديث القواعد القانونية الدولية المتعلقة بمبدأ التمييز لتتلاءم مع طبيعة الحروب السيبرانية، وذلك من خلال صياغة بروتوكول إضافي خاص بالنزاعات السيبرانية يحدد بوضوح معايير تصنيف المشاركين في العمليات السيبرانية وحدود مشاركة المدنيين فيها.

5. إنشاء آلية دولية متخصصة لتقييم وتصنيف الهجمات السيبرانية وتحديد متى تصل إلى مستوى النزاع المسلح، مع وضع معايير واضحة لتحديد المشاركة المباشرة في الأعمال العدائية في السياق السيبراني.

6. تعزيز التعاون الدولي في مجال تبادل المعلومات والخبرات التقنية المتعلقة بالهجمات السيبرانية، وتطوير قدرات الدول على تحديد مصادر الهجمات وهوية المهاجمين، مما يسهل تطبيق مبدأ التمييز في الفضاء السيبراني.

المراجع:

أولاً: المؤلفات باللغة العربية

1- الكتب:

- بدر الدين عبد الله حسن حمد، القانون الدولي الإنساني، مكتبة المتنبي، الدمام، 1444ه.

- حسين على الدرديري ، القانون الدولي الإنساني(ولادته- نطاقه- مصادره)، دار وائل للنشر، ط1 ، 2012م.

- عامر الزمالي، التفرقة بين المقاتلين وغير المقاتلين وصلتها بالنظام الأساسي للمحكمة الجنائية الدولية ، منشور في كتاب المحكمة الجنائية الدولية وتوسيع نطاق القانون الدولي الإنساني، جامعة دمشق واللجنة الدولية للصليب الاحمر، 2004.

- هشام بشير، إبراهيم عبد ربه إبراهيم، المدخل لدراسة القانون الدولي الإنساني، المركز القومي للإصدارات القانونية، القاهرة ، ط1 ، 2012م .

2- الرسائل العلمية:

- العقون ساعد، مبدأ التمييز بين المقاتلين وغير المقاتلين وتحديات النزاعات المسلحة المعاصرة، رسالة ماجستير، جامعة الحاج لخضر بباتنة، كلية الحقوق، قسم العلوم القانونية، 2008-2009م.

- شوقي سمير، محكمة العدل الدولية والقانون الدولي الإنساني، رسالة ماجستير، جامعة الجزائر، كلية الحقوق ، 2007/2006

3- الدوريات :

- إسحاق صلاح أبو طه، المقاتل الشرعي وغير الشرعي وفقاً لقواعد القانون الدولي الإنساني، مجلة الدراسات القانونية والسياسية، مج 4، ع 2018،2.

- القانون الدولى الإنساني والعمليات السيبرانية خلال النزاعات المسلحة، ورقة موقف اللجنة الدولية للصليب الأحمر، مقدمة إلى فريق العمل المفتوح العضوية، المعنى بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الامن الدولي، وإلى فريق الخبراء الحكوميين المعنى بالارتقاء بسلوك الدول المسؤول في ميدان الفضاء السيبراني في سياق الامن الدولي، نوفمبر 2019.

- جون مارى هنكرتس ، لويز دوزوالد- -بك ، القانون الدولي الإنساني العرفي، اللجنة الدولية للصليب الأحمر، المجلد الأول: القواعد ، القاهرة ، 2007.

- حيدر كاظم علي، مبدأ التمييز بين المدنيين والمقاتلين (دراسة في ضوء أحكام القانون الدولي الإنساني)، مجلة الكلية الاسلامية الجامعة، مج 1، ع22، 2013.

- روابحى عمر، إشكالية تحديد مفهوم المقاتل الشرعي في النزاعات المسلحة غير المتكافئة، مجلة معارف: قسم العلوم القانونية، السنة الحادية عشر- العدد 21- ديسمبر 2016.

- كورديولا درويغ، الحرب السيبرانية والقانون الدولى الإنساني: كيف نحمى المدنيين من الآثار العرضية لهجوم الكتروني؟، مجلة الإنساني، اللجنة الدولية للصليب الأحمر، العدد 52، 20 مارس 2011م.

- مايكل شميت، الحرب بواسطة شبكات الاتصال: الهجوم على شبكات الحاسوب والقانون في الحرب، المجلة الدولية للصليب الأحمر، 2002.

- محمد أحمد سليمان عيسى، المبادئ الأساسية التي تحكم النزاعات المسلحة في الشريعة الإسلامية والقانون الدولي الإنساني، أعمال المؤتمر العلمي الدولي: القانون الدولي الإنساني في ضوء الشريعة الإسلامية، ضمانات التطبيق والتحديات المعاصرة، غزة: الجامعة الإسلامية - كلية الشريعة والقانون واللجنة الدولية للصليب الأحمر، 2015.

- معماش صلاح الدين، مبدأ التمييز في القانون الدولي الإنساني واستعمال الطائرات بدون طيار، دائرة البحوث والدراسات القانونية والسياسية، جامعة أمحمد بوقرة، الجزائر، مج6، ع1، 2022.

- ياسين محمد أحمد بونة، الهجمات السيبرانية: الحرب الرقمية التي تجاوزت الحدود الجغرافية، مجلة شمال افريقيا للنشر العلمي، الاكاديمية الافريقية للدراسات المتقدمة، مج1، ع 4، ديسمبر 2023، ص 162 .

ثانياً: المؤلفات باللغة الإنجليزية

-Ahmad Khalil, Challenges to the principle of distinction in cyber warfare: Navigating international humanitarian law compliance, Prawo I Wiez; Law & Social Bonds, June 2024.

- Ahmad Khalil & Mohamad bitarn, Navigating legal frontiers in cyber warfare: insights from the russia-ukraine conflict, Vol 14, No2, June 2024.

-Ahmed Aubais Al fatlawi, Beyond the Battlefield: Navigating the Legal Challenges of Civilian Cyber Participation in Modern Warfare, ATSK Journal of Law, Vol 1, Issue 1, Article 5, August 2024.

- Andy Manoske, ‘How Does Cyber Warfare Work’, (Forbes, 18 July, 2013).

- Benjamin Mueller , *THE LAWS OF WAR AND CYBERSPACE: On The Need For A Treaty Concerning Cyber Conflict* . LSE IDEAS, Jun 2014.

-Dan-Iulian Voitasec, Cyber Hostilities: Civilian Direct Participation, Challenges of the Knowledge Society, 2016.

-David Turns, Cyber Warfare and the Notion of Direct Participation in Hostilities, Journal of Conflict & Security Law, Oxford University Press 2012.

- David Turns, Cyber Warfare and the Notion of Direct Participation in Hostilities, Journal of Conflict & Security Law, Vol. 17 No. 2,2021.

-David Wallace, Shane Reeves, and Trent Powell, Direct Participation in Hostilities in the Age of Cyber: Exploring the Fault Lines, Harvard National Security Journal , Vol. 12, 2021.

- Eitan Diamond , "Applying International Humanitarian Law to Cyber Warfare." *Law and National Security: Selected Issues*, edited by Pnina Sharvit Baruch and Anat Kurz, Institute for National Security Studies, 2014.

- Evangelia Linaki, Cyber Warfare and International Humanitarian Law:a Matter of Applicability, Journal of International Law of Peace and Armed Conflict, Vol 27, April 2014.

-François Delerue ,Civilian Direct Participation in Cyber Hostilities, Journal promoted by the Law and Political Science Department, Issue 19 (October, 2014).

-Guyonneau, Rudy, and Arnaud Le Dez. “Artificial Intelligence in Digital Warfare: Introducing the Concept of the Cyberteammate.” *The Cyber Defense Review*, Vol. 4, No. 2, 2019.

- Harrison Dinniss, Cyber Warfare, and the Laws of War, Cambridge University Press, Cambridge, 2012.

-Jeffrey Hunker, *Cyber War and Cyber Power: Issues for NATO Doctrine*. NATO Defense College, 2010.

- Kubo Macak, Mauro Vignati, Civilianization of Digital Operations: A Risky Trend, Lawfare, Wednesday, April 5, 2023.

-Kubo Macak, Will the centre hold? Countering the erosion of the principle of distinction on the digital battlefield, International Review of the Red Cross, 105 (923), 2023.

- Leanne Christine Van Breda, The effectiveness of the principle of distinction in the context of cyber warfare, A dissertation submitted in partial fulfilment for the Degree of LL M in International law, University of Johannesburg, 2014.

-Luzzatto, Cadet Andrew. “Regulating Cyber Warfare Through the United Nations.” *The Cyber Defense Review*, Vol. 7, No. 4, 2022.

- Marco Roscini, Cyber Operations and the Use of Force in International Law, Oxford University Press, Oxford, 2014.

- Mačák, Kubo, “Unblurring the Lines: Military Cyber Operations and International Law.” *Journal of Cyber Policy* 6 (3), 2021.

- Matheson, Colton. “From Munitions to Malware: A Comparative Analysis of Civilian Targetability in Cyber Conflict.” *Journal of Law & Cyber Warfare*, vol. 7, no. 2, 2019.

-Michael N. Schmitt, Military Necessity and Humanity in International Humanitarian Law: Preserving the Delicate Balance, 50 VA.J. INT’L L. 2010.

- Michael N. Schmitt, Cyber Operations and the Jus in Bello: Key Issues, *Naval War College International Law Studies, 2011.*

- Michael N. Schmitt, “THE LAW OF CYBER TARGETING.” *Naval War College Review*, vol. 68, no. 2, 2015.

- Mohammed Naqib Ishan Jan, Mohammad Hisham Mohammad Kamal, IHL and the challenges of civilian involvement in armed conflict: examining the crux of the notion of direct participation in hostilities, *International Journal of Business, Economics and Law, Vol. 4, Issue 3 (June)*, 2014.

-Negrea Petru-Cristian, Cyber Conflict and International Relations: A Comprehensive Analysis of Cyber Deterrence

Strategies in Contemporary Geopolitics, PhD thesis, February 2024.

- Sabin Guțan, The Meaning of the Term Noncombatant in International Humanitarian Law – Interpretation of the Provision of Article 37/1/c of the Additional Protocol I of Geneva of 1977. International conference Knowledge-Based Organization, Vol.28, 2022.

- Saman Iftikhar, Cyberterrorism as a global threat: a review on repercussions and countermeasures, PeerJ Computer Science, January 15, 2024. 10:e1772.

- Sean Watts, The Notion of Combatancy in Cyber Warfare, International Conference on Cyber Conflict (ICCC), 05-08 June 2012.

- Shannon Bosch, the international humanitarian law notion of direct participation in hostilities: a review of the ICRC interpretive guide and subsequent debate , African Journals Online, vol 17, No 3 , Sep 17, 2014.

- Sharona Mann, legal challenges in the realm of cyber warfare, J. INT'L L. & POL. ONLINE FORUM, March, 2020.

-Stephenie Gosnell Handler, The new Cyber Face of Battle: Developing a legal Approach to Accommodate Emerging Trends in Warfare, in: Stanford Journal of International Law, Vol 48, 2012.

-Tomasz Andrzej Lewandowski, can mouse clicking be seen as involvement in armed conflict? Some notes on the direct participation in hostilities in cyberspace, Przegląd Prawniczy Uniwersytetu im. Adama Mickiewicza, June 2013.

-Urban Praprotnik, Principle of Distinction in Cyber Warfare, Contemporary Military Challenges, Vo.26,I.2, June 2024.

- US Army Training & Doctrine Command, DCSINT Handbook No. 1.02, Critical infrastructure threats and terrorism at VI1-2,15 August 2005.

-Vasileios Karatzias, *Direct Participation of Civilians in Cyber* , Available at; https://www.academia.edu/21147788/Direct_Participation_of_Civilians_in_Cyber_Hostilities_in_times_of_Armed_Conflict

- Zhixiong Huang and Yaohui Ying, The application of the principle of distinction in the cyber context: A Chinese perspective, International Review of the Red Cross (IRRC), 2020, 102 (913).

ثالثاً: الوثائق الدولية

- اعلان سان بطرسبرج الموقع في التاسع والعشرين من نوفمبر 1868 في شأن حظر استعمال قذائف معينة في وقت الحرب.

- اتفاقيات جنيف الأربع لعام 1949 .

- البروتوكولين الإضافيين لعام 1977م.

- النظام الأساسي للمحكمة الجنائية الدولية لعام 1998 .

- دليل تالين بشأن القانون الدولي المطبق على الحروب السيبرانية (النسخة المترجمة للعربية)، بالتعاون مع حلف شمال الأطلسي، وبدعمٍ من فريق مؤلف من خبراء السيبرانية، واللجنة الدولية للصليب الأحمر والقيادة السيبرانية الأميركية تحرير مايكل شيمت، ترجمة على محمد كاظم الموسوي، 2017.

- نيلس ميلزر، الدليل التفسيرى لمفهوم المشاركة المباشرة في العمليات العدائية بموجب القانون الدولي الإنساني، اللجنة الدولية للصليب الأحمر، الطبعة العربية الاولي، المركز الإقليمي للإعلام، القاهرة، مارس، 2010م.

رابعا: القواميس اللغوية

- القاموس العملي للقانون الانساني، تأليف: فرانسواز بوشيه- سولنييه، ترجمة: محمد مسعود، مراجعة: د. عامر الزمالي ومديحة مسعود، الناشر: دار العلم للملايين، 2006.

- Oxford Dictionary, https://en.oxforddictionaries.com/definition/cyberwarfare

- US Department of Defense, 'Dictionary of Military and Associated Terms'(8 November 2010 as amended through 15 February 2012) Joint Publication.

-Tallinn Manual on the International Law Applicable to Cyber Warfare – prepared by the International Group of Experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence, Cambridge University Press, 2013.

-Nils Melzer, Interpretive Guidance on the Notion of Direct Participation in the Hostilities Under International Humanitarian Law, International Committee of the Red Cross, (2009) .

- ICRC, Fourth Expert Meeting on the Notion of Direct Participation in Hostilities: Summary Report, Geneva,27–28 November 2006.

خامسا: المقالات الصحفية الالكترونية

- حسن فياض، الهجمات السيبرانية من منظور القانون الدولي الإنساني، مجلة الدفاع الوطني، ع 114، أكتوبر، 2020 .

متاح على الرابط : الهجمات السيبرانية من منظور القانون الدولي الإنساني | الموقع الرسمي للجيش اللبناني (lebarmy.gov.lb)

- اللجنة الدولية للصليب الأحمر، الحرب السيبرانية: القانون الدولي الإنساني يوفر طبقة إضافية من الحماية، سبتمبر 2019. متاح على الرابط: https://2u.pw/yBD7b6t0 .

-Dan Sabbagh , Ukrainians use phone app to spot deadly Russian drone attacks, The Guardian, October 29, 2022. Available at; . https://2u.pw/vov9QQ9g

- Drew Harwell, instead of consumer software, Ukraine’s tech workers build apps of war,

The Washington Post, March 24, 2022. Available at:

https://www.washingtonpost.com/technology/2022/03/24/ukraine-war-apps-russian-invasion/

سادساً: الاحكام القضائية

- فتوى محكمة العدل الدولية بشأن مشروعية استخدام الأسلحة النووية أو التهديد باستخدامها لعام 1996م، منشورات الأمم المتحدة.

-Prosecutor v. Tadic, case no. IT-94-1. Decision on defence motion for interlocutory appeal on jurisdiction. 127 (Oct 2, 1995).