International Journal of Law Research and Studies (IJLRS)
Vol. (4), No. (10)
IJLRS
October 2025
المجلة الدولية للبحوث والدراسات القانونية
الإصدار (4)، العدد (10)

عناصر تطبيق مبدأ التّناسب في الهجمات السّيبرانيّة والاحتياطات اللازمة

محمد عبدالكريم سالم*، جورج عرموني
قسم القانون العام، كلية الحقوق، الجامعة الإسلامية، لبنان
*alknani445@gmail.com

المستخلص

يُعدّ مبدأ التّناسب في الهجمات السّيبرانيّة إطارًا قانونيًّا وأخلاقيًّا جوهريا يهدف إلى موازنة الأثر العسكري المشروع مع الضّرر المحتمل على المدنيّين والأعيان المدنيّة الحيوية، يقوم هذا المبدأ على الحدّ من استخدام القوّة الإلكترونيّة كقوة جديدة ضمن الفضاء السيبراني بما يمنع الآثار غير الضروريّة أو المفرطة، ويشمل تقييم العواقب غير المباشرة مثل تعطيل البنى التحتيّة الحيويّة أو الخدمات الأساسيّة. إنّ تطبيقه يتطلّب تقديرًا دقيقًا وحقيقياً لمدى فعاليّة الهجوم الذي تقوم به القوة العسكرية مقابل المخاطر التي تنتج عنه، واعتماد تدابير احتياطيّة لتقليل الأضرار الناتجة عنه، التي لها الأثر البالغ على المدنيين والبنى التحتية الحيوية، بما يحافظ على الشرعيّة الدوليّة ويعزّز المسؤوليّة القانونيّة والأخلاقيّة في الفضاء السّيبراني الذي كما عرفنا أنه فضاء جديد ذو طبيعة جديدة، لذلك من المهم جداً تطبيق مبدأ التناسب وبشكل دقيق على الهجمات السيبرانية.

الكلمات المفتاحيّة: مبدأ التّناسب، الهجمات السّيبرانيّة، القانون الدولي الإنساني، الأضرار الجانبيّة، الأعيان المدنيّة، البنى التحتيّة الحيويّة، الشرعيّة، المسؤولية القانونيّة، الأخلاقيّات، الفضاء السّيبراني.

Elements of applying the principle of proportionality in cyber attacks

Mohammed Abdulkarim Salem*, George Armoni
Department of Public Law, Faculty of Law, Islamic University, Lebanon
alknani445@gmail.com*

Abstract

The principle of proportionality in cyberattacks is a legal and ethical framework that aims to balance the legitimate military impact with the potential damage to civilians and vital civilian objects. This principle is based on reducing the use of electronic force as a new force within cyberspace, to prevent unnecessary or excessive effects, and includes assessing indirect consequences such as disrupting vital infrastructure or basic services. Its application requires an accurate and real

assessment of the effectiveness of the attack carried out by the military force against the risks resulting from it, and the adoption of reserve measures to minimise the damage resulting from it, which have a profound impact on civilians and vital infrastructure, in order to preserve international legitimacy and enhance legal and moral responsibility in cyberspace, which, as we know, is a new space of a new nature, so it is very important to apply the principle of proportionality accurately to cyber-attacks.

Keywords: Proportionality Principle, Cyber Attacks, International Humanitarian Law, Collateral Damage, Civilian Objects, Vital Infrastructure, Legitimacy, Legal Responsibility, Ethics, Cyberspace.

المقدمة

مثلما بيّنا أهميّة "مبدأ التّناسب"، الذي يُعدّ من المبادئ الأساسيّة في "القانون الدّولي الإنساني "إذ أن هذا المبدأ يعد الأساس القانوني أو الضابطة القانونية للحد من الأضرار التي تسبب معاناة وموت ودمار للمدنيين والبنى التحتية الحيوية للسكان المدنيين التي وفر لها القانون الدولي الحمة الكبيرة وخصص لها الحد الأدنى من فرض الوضع الإنساني، ويقتضي عند تطبيقه على "الهجمات السّيبرانيّة" مراعاة التّوازن ما بين تحقيق "الميزة العسكريّة المشروعة" والحدّ من الأضرار العرضيّة المفرطة على المدنيين والأعيان المدنيّة؛ وأنّ هذا التّطبيق يرتكز على تقدير طبيعة الأهداف المُستهدفة، وتقدير حجم الأضرار المحتملة، والوسائل والأساليب المستخدمة في إطار "الهجمات السّيبرانيّة"، وبما يضمن التزام الأطراف المتحاربة بضبط القوة السّيبرانيّة ضمن حدود الضّرر المعقول الذي لا يخرج عن الأطر القانونيّة المسموح بها في القانون الدولي الإنساني، من هذا المنطلق سنبيّن تحقق الميزة العسكريّة ومن ثم الضّرر العرضي الذي يحدد الأطر القانونية لكدى انتهاك قواعد القانون الدولي الإنساني، لا سيما في ظل الحرب الجديدة في الفضاء السيبراني والتي تحدد السلوكيات التي من خلال انتهاك الميزة العسكري والضرر العرضي المفرط الموجب للمسؤولية الدولية.

أهمية البحث

إن الأهمية تأتي عن طريق ما تمثله الهجمات السيبرانية من تحدي كبير كحرب جديدة ضمن الفضاء الجديد، وهو الفضاء السيبراني الذي يتسم بالتعقيد، لذلك يحتاج إلى بحث معمق وتحليل للنصوص القانونية لتكييف هذه الهجمات والحد منها.

إشكالية البحث

إن إشكالية البحث تتمحور بكيفية معالجة الهجمات السيبرانية من حيث تحقق الميزة العسكرية والحد من الضرر العرضي المفرط في ظل تطبيق مبدأ التناسب، لا سيما أن الهجمات السيبرانية وما تتسم به من تعقيد من حيث طبيعتها وآلياتها كحرب جديدة، لذلك مهم جداً البحث بكل ما يعالج الحد من آثار هذه الهجمات وتطبيق مبدأ التناسب.

منهج البحث

سيتم اعتماد منهج البحث التحليلي ذلك لكونه الأنسب لموضوع دراستنا من حيث تحليل كل ما يتعلق بمبدأ التناسب من حيث النصوص القانونية الدولية والإجراءات العملية ذات العلاقة به.

خطة البحث

تقسم الدراسة على مبحثين الأول يتناول عناصر تطبيق مبدأ التناسب في الهجمات السيبرانية وهو قسمناه على مطلبين الأول يتناول تحقق الميزة العسكرية والثاني الضرر العرضي المفرط، أما المبحث الثاني يتناول الأهداف المشروعة والاحتياطات الواجبة، الذي قسمناه على مطلبين الأول يتناول الأهداف المشروعة أما الثاني الاحتياطات الواجبة في أثناء الهجمات السّيبرانيّة.

المبحث الأول: عناصر تطبيق مبدأ التناسب في الهجمات السيبرانية

إن مفهوم عناصر تطبيق مبدأ التناسب مهمة في مجال الهجمات السيبرانية لا سيما أن الهجمات السيبرانية تعد من الحروب المعقدة والجديدة، إذ لابد من بيانها بشكل تفصيلي، وهي الميزة العسكرية والضرر العرضي التي سنبينها وكما يلي.

قسمنا هذا المبحث إلى مطلبين؛ يستعرض أوّلهما: تحقق الميزة العسكرية؛ يليه ثانيهما مبينًا: الضرر العرضي (المفرط).

المطلب الأول: تحقق الميزة العسكريّة:

إنّ "الميزة العسكريّة" هي تلك المتأتية من الهجوم، والتي يقابلها استبعاد ميزة ليست عسكريّة بطبيعتها، وعلى وجه الخصوص الميزة الاقتصاديّة أو السّياسيّة أو النّفسيّة؛ وعلى سبيل المثال: إنّ الهجوم السّيبراني على قطاع عمل مدني، ظنًا من المهاجم أنّه سيُضعف بشكل عام الدّولة المعادية، لن يؤدّي بالضّرورة إلى ميزة عسكريّة بالمعنى المطلوب، بل ولا يُعد هدفًا عسكريًا، لأنّه لا يقدم مساهمة فعّالة في العمل العسكري؛ ففي التّوصيف كـ "هدف عسكري" يجب أن تكون الميزة العسكريّة التي يحتمل أن تنتج: واضحة [1].

إنّ "قواعد القانون الدّولي الإنساني" لم تنصّ على تعريفٍ للمقصود بـ "الميزة العسكريّة"؛ إلّا أنّ المادة (52/2) من البروتوكول الإضافي الأوّل: اشترطت أن تكون هذه الميزة "أكيدة" مع اقتصار". الهجمات على الأهداف العسكريّة فحسب، والتي يُحقق تدميرها التامُّ أو الجزئي أو الاستيلاء عليها أو تعطيلها في الظّروف السّائدة حينذاك ميزة عسكريّة أكيدة". كذلك تتطلّب المادَّة (51/5/ب) من البروتوكول الإضافي الأوّل: أن تكون الميزة العسكريّة (ملموسة ومباشرة)؛ وهو ما يُعتبر معيارًا أقوى ممّا تبنَّته المادة (52/2) سابقة الذّكر؛ إذ يفرض قيودًا أكثر صرامة على المهاجم عند توقُّعه إحداث أضرار عرضيَّة نتيجة الهجوم المزمع القيام به؛ ونتيجة لذلك يجب أن نكون الميزة المقصود تحقيقها هامة وقريبة الحدوث نسبيًّا. أمّا المزايا التي يصعب إدراكها أو تلك التي ستظهر على المدى الطّويل فقط: فيجب تجاهلها. ما يعني بالتّالي أن تكون "الميزة العسكريّة الملموسة والمباشرة" ذات "فائدة حقيقيّة وقابلة للقياس [2].

إنّ مفهوم "الميزة العسكريّة الملموسة والمباشرة" غير محدّد في "القانون الإنساني الدّولي" -كما بينا أعلاه؛ إلّا أنّ تقييم "الميزة العسكريّة الملموسة والمباشرة" مهم بشكل خاص، لأنّه يؤثر على المستوى المسموح به من الضّرر العرضي، ويُحدّد ما إذا كان الهجوم غير متناسب، ومحظور بالتّالي بموجب "القانون الإنساني الدّولي". وعلى هذا النّحو من المهم استكشاف ملامح هذه الفكرة بغية تحقيق المزيد من الدّقة لـ "مبدأ التّناسب" [3].

لقد حدّد "القانون الدولي الإنساني"، شروطًا معينة، وبموجبها يمكن اللجوء إلى "الضّرورة العسكريّة" كونها تحقق هدفاً عسكريّاً، وهي كما يلي [4]:

- أن يكون هذا التّجاوز موقتًا ومرتبطاً بمدة قيام هذه الضّرورة.
- أن يكون على أهداف محددة.
- أن يكون الغرض منها تحقيق ميزة عسكريّة أكيدة.

كذلك أكّد نصّ الفقرة (ب/٢-المادة ٥٧) من البروتوكول الإضافي الأوّل لعام ١٩٧٧، على أنّه: "يُلغى أو يُعلَّق أيّ هجوم، إذا ما تبيّن أنّ الهدف المقصود منه ليس هدفًا عسكريًا، أو أنّه مشمول بحماية خاصة، أو أنّ الهجوم قد يُتوقع منه إحداث خسائر في أرواح المدنيين أو إلحاق الإصابة بهم، أو الإضرار بالأعيان المدنيّة، أو أن يُحدّث خلطًا من هذه الخسائر أو الأضرار. وذلك بصفة عرضيّة تُفرط في تجاوز ما يُنتظر أن يسفر عنه هذا الهجوم من ميزة عسكريّة مباشرة". كما وأكدت القاعدة (٥٠) من (دليل تالين) لعام ٢٠١٣، على حظر "الهجمات السّيبرانيّة" التي تعامل عددًا من الأهداف العسكريّة السّيبرانية المميزة والمفصولة بشكل واضح، بصورة مماثلة باعتبارها هدفًا واحدًا، في البنية التّحتيّة السّيبرانيّة المُستخدمة في المقام الأوّل للأغراض المدنيّة، إذ اما كان من شأن ذلك الإضرار بالأشخاص والأعيان المحميين. هذا إضافة إلى حظرها "الهجمات السّيبرانيّة" المتوقع منها أن تسبب أضرارًا عرضيّة في أرواح المدنيين، أو

الإصابة لهم، أو الإضرار بالأعيان المدنيّة، أو أن يحدث مزيجًا من ذلك، والتي من شأنها أن تكون مفرطة بالنّسبة لـ "لميزة العسكريّة الملموسة والمباشرة" المتوقعة من ذلك الهجوم [5].

إذًا، يعتمد "مبدأ التّناسب" على تحقيق التّوازن ما بين أمرين أساسيّين، هما: 1-الميزة العسكريّة المتوقعة من أعمال القتال من جهة؛ 2-الخسائر التي تُلحقها هذه العمليات بالمدنيين والأعيان المدنيّة من جهة أخرى؛ ويُشترط في "الميزة العسكريّة" أن تكون متوقعة وتتحقق عادة من خلال السّيطرة على جزء من الإقليم أو تدمير القوات العسكرية للعدو أو إضعافها؛ وأن تكون هذه الميزة ملموسة ومباشرة؛ ومن ثم تظهر إشكاليات تطبيق هذا المبدأ على "الهجمات السّيبرانيّة" في أنّ برمجة تلك العمليات الإلكترونيّة ليس في مقدورها تطبيق "مبدأ التّناسب"، لاسيّما إذا ما علمنا أنّ "معادلة التّناسب" تُعدّ معادلة صعبة ودقيقة حتى في أثناء إدارة العمليات الحربيّة التّقليدية؛ فتحقيق المهمة القتاليّة وإحراز النّصر: هدف أساسي للقوات العسكريّة؛ وتنفيذ القوانين وضبط التّدمير وعدم إلحاق أضرار مفرطة بالخصم: التزام قانوني واجب النّفاذ، ويحتاج بالتّالي إلى قائد عسكري متمكن يُسويّ ميزان هذه المعادلة. والأمر بدون شكّ يزداد تعقيدًا إذا ما تعلق بـ "الهجمات السّيبرانيّة" [6].

يلعب "مبدأ التّناسب في المجال السّيبراني" دورًا أكثر وضوحًا في العمليات العسكريّة الهجوميّة؛ فأحد شروط هذا المبدأ هو أن ينطوي القرار بشأن عمل عسكري على الموازنة بين "الميزة العسكريّة" المتوقعة وبين الخسائر المدنيّة المحتملة التي ستنجم عن العمل العسكري المحدّد، وذلك تطبيقًا لـ "مبدأ التناسب" بشكل كافٍ في تحديد ما إذا كان يمكن اعتبار الهجوم مبررًا.

ينصّ "تعريف الميزة العسكريّة حول "مبدأ التّناسب والضّرورة" في القانون على أنّه: يمكن اعتبار "الميزة العسكرية": أيّة "نتيجة لهجوم يُعزّز بشكل مباشر العمليات العسكريّة الوديّة أو يعوق عمليات العدو، مثل تعطيل المقاتلين المعارضين، وتدمير معداتهم، وحرمانهم من فرص الهجوم، وخلق فرص لمهاجمتهم". كذلك يمكن النّظر في مصطلح "الميزة العسكرية" من خلال نهج "كل حالة على حدة" أو على النّهج التراكمي؛ إذ يشير الأوّل إلى الهدف العسكري المحدّد لإجراء معين، في حين يشير الأخير إلى الطريقة التّراكميّة التي سيساهم بها بالفعل في تحقيق الأهداف الاستراتيجيّة العامة [7].

المطلب الثاني: الضّرر العرضي (المفرط):

من البديهي أن تُخلّف "الهجمات السّيبرانيّة" أضرارًا عرضيّة، لكنّها قد تكون جسيمة وتفوق بآثارها الأضرار النّاتجة عن الهجمات الحركيّة التّقليديّة؛ أمّا الضّرر العرضي فهو نتيجة غير مقصودة للهجوم على هدف عسكري مشروع؛ وفهم معنى "الإفراط" جوهري في تحديد ما إذا "مبدأ التناسب" قد خُرِق أم تمت مراعاته؛ لذلك و "إن كان "مفهوم التّناسب" مطلقًا من حيث اعتباره شرطًا أساسيًا لمشروعيّة الهجمات المسبّبة لخسائر عرضيّة: فإنّ "مبدأ الإفراط" هو مبدأ نسبيّ؛ إذ لم يضع "القانون الدّولي الإنساني" حدًا

موضوعيًا يُعتمد على تجاوزه لتحديد تحقق صفة الإفراط من عدمها [8]؛ لكنّ هذا الإفراط قد يمسّ المدنيين والأعيان المدنيّة بشكل واسع، لأنّ الطّبيعة المترابطة للبنية التحتيّة الرّقمية مختلفة -وكما بيناها سابقا-. لذلك يكتسب "مفهوم الضرر العرضي" أهميّة كبيرة في ظلّ "القانون الدّولي الإنساني"، إذ يُعدّ معيارًا أساسيًا لتفعيل "مبدأ التّناسب" الذي يوجب التّوازن ما بين "الميزة العسكريّة" المؤكّدة وحدود الضّرر المسموح به. ولذا: إنّ تقدير الأضرار العرضيّة في "الفضاء السّيبراني" يظل تحديًا معقدًا يتطلب منهجيّة دقيقة وقدرة على التّنبؤ بالآثار غير المباشرة، والتي قد تتخطى حدود الدّولة المستهدفة.

إنّ احتساب "مبدأ التّناسب" يرتبط بـ "الضّرر العرضي" اللاحق بالمدنيين والأعيان المدنيّة، ولذلك لا يتمُّ احتساب الضّرر المقصود بالأهداف العسكريّة من إصابة أو وفيات ما بين المقاتلين أو المدنيين المشاركين بشكل مباشر في الأعمال العدائيّة، والذين يجوز استهدافهم خلال مدّة مشاركتهم في هذه الأعمال العدائيّة؛ كما أنّ آثار "الهجمات الإلكترونيّة" قد تكون أوليّة تُؤثّر على البيانات والبرامج التي تعرّضت للهجوم، وقد تكون ثانويّة تُؤثّر على البنية التحتيّة الموجودة في النّظام أو الشّبكات المستهدفة، وقد تكون آثارًا من الدّرجة الثّالثة، وهي التي تتعلّق بالأشخاص المتضرّرين من تدمير أو بعجز النّظام أو البنية التحتيّة التي تعرّضت للهجوم. وبالتّالي، إنّ كلًّا من الآثار الأوليّة والثّانويّة، والآثار من الدّرجة الثالثة: يتمُ احتسابها جميعًا عند فحص مسألة "الضرر العرضي" كنتيجة محتملة للهجوم [9]. بالمقابل، وفي الواقع، إنّ الآثار المتوقعة للعمليّة الحركيّة تكون واضحة بشكل عام لتوقعها وتقييمها وإدارتها، في حين أنّ التّرابط ما بين الأنظمة السّيبرانيّة والفيزيائيّة السّيبرانيّة: قد يصعب التّنبؤ بآثاره المباشرة وغير المباشرة والجانبيّة، ممّا يجعل النُهج التقليديّة غير فعّالة لتقدير الأضرار الجانبيّة؛ كذلك هي فكرة تحديد "الضرر" والنّظر فيه بوضوح داخل المجال السّيبراني: أمرٌ صعب في الواقع؛ وعلى سبيل المثال: كيف للمرء أن يُقدّر الأضرار النّاتجة عن انقطاع اتصال الشبكة النّاجم عندما يستغل المهاجم ثغرة برمجيّة؟ كيف يمكن للمرء تقييم وزن التّأثير الجانبي للتّدخل السّيبراني على القيم التي لا يمكن قياسها [10]؟ هذا ما سنبينه بشكل تفصيلي في "التّحديات العمليّة لمبدأ التناسب" ضمن الفصل القادم، وعندما نبيّن معيار غموض الضّرر.

إنّ من شروط تحقيق "مبدأ التّناسب" في استخدام القوة خلال النّزاع المسلح ما أوردته الفقرة (٥/ب من المادة (٥١) في البروتوكول الإضافي الأوّل لعام ١٩٧٧، إذ أكّدت على أنّ الأضرار التي تحدث في الهجوم المتوقع منه إحداث خسائر عرضيّة في أرواح المدنيين، إصابة المدنيين، الإضرار بالأعيان المدنيّة أو مزيجًا منها: سيكون هجومًا مفرطًا فيما يتعلق بـ "الميزة العسكريّة المباشرة والملموسة" المرتقبة. كذلك أكّدت المادة (٥٧) من البروتوكول أعلاه: على إلغاء وتعليق أيّ هجوم، إذا ما تبين أنّ الهدف المقصود ليس عسكريًا أو له حماية خاصة، أو أنّ الهجوم قد يتوقع منه إحداث خسائر في أرواح المدنيين أو إلحاق الإصابة بهم، أو الإضرار بالأعيان المدنيّة، أو خلطًا من هذه الخسائر أو الأضرار، وذلك بصفة عرضيّة [11].

أمّا "إلحاق الضّرر بالأعيان المدنيّة" فيقصد به الضّرر المعطّل لقيمة شيء ما، أو للانتفاع به؛ بذلك يتضح أنّ "الضّرر" الذي يتوجب أخذه بالحسبان: لا يشتمل على الضّرر المادي فحسب، بل ويتضمن أيضًا الخواص الوظيفيّة للبنية الأساسيّة المدنيّة حتى في حالة انتفاء الضّرر المادي؛ وبالإشارة إلى "الهجمات السّيبرانيّة" ينبغي الإقرار بأنّ هذه الهجمات حين تتسبب بإلحاق الضّرر بالبنيّة الأساسيّة المدنيّة وتسبب تعطيلًا مؤقتًا، فإنّ "مبدأ التناسب" تعترضه قيود عدة، وهي [12]:

قدر من الشّك بشأن ما يمكن اعتباره أضرارًا عرضيّة مفرطة تلحق بالأعيان المدنيّة مقارنة بـ "الميزة العسكريّة الملموسة والمباشرة"؛ إذ تبدو النّتائج التي تبيّن أنّ الأضرار العرضيّة اللاحقة بالبنيّة الأساسيّة المدنيّة مفرطة: قليلة ومتباعدة -مقارنة بـ "الميزة العسكريّة"-؛ من ثم يجب توقع الأضرار العرضيّة في أغلب الحالات حتى وإن صّعُب تقييم حجمها.

وجوب أن تؤخذ التّوقعات للأضرار بعين الاعتبار حتى إذ اما كانت طويلة الأمد أو أنّها أضرار على المستويين الثّاني والثّالث.

أمّا "مبدأ التّناسب" فيتعامل مع الآثار النّاجمة عن "الهجمات السّيبرانية" التي لا تستهدف المدنيين عمدًا، لكنّها تسبب الضّرر للأعيان المدنيّة أو الموت أو الإصابة للمدنيين، على الرّغم من توجيهها إلى هدف عسكري مشروع. ولِذا سيتم تخصيص فرع حول "تأثيرات الهجمات السّيبرانيّة في حساب التّناسب"، وما لها من إحداث ضرر مادي، أو تدمير للبيانات التّشغيليّة تتم فيها إعاقة الحاسوب أو النّظام أو الشّبكة؛ سيتم تضمين الضّرر في تقييم التّناسب.

أيضًا، ومن الإشكاليّات التي طرحها البروفيسور أحمد عبيس الفتلاوي، والتي تثيرها "الهجمات السّيبرانيّة"، وتحديدًا ما يتعلق منها بالتّناسب: ما الموقف من التّأثيرات "غير المباشرة"، والتي يمكن توقعها بشكل معقول على المدنيين والأعيان المدنيّة؟ أجاب البروفيسور بالقول: يوجد الآن اتفاق عام على أنَّ مثل هذه الآثار يجب أن تؤخذ في الحسبان مقابل إعمال "مبدأ التّناسب"؛ أمّا المدى الذي يجب أن تؤخذ فيه هذه التّأثيرات في الحسبان، فهو أمر لازال غير واضح المعالم؛ وبعبارة أخرى: هل سيكون من الدّرجة الثّانية أم الثّالثة، أو حتى الأعلى من ذلك؛ كما و يتوجب على مسؤولي التّخطيط للهجوم أو اتخاذ القرار بالتّنفيذ، وبالضّرورة: أن يتوصلوا لقراراتهم استناداً إلى تقييم المعلومات من المصادر المتاحة لهم في الظّروف السّائدة [13].

إنّ التّأثيرات غير المباشرة تُعرّف بأنّها: النّتائج المتأخرة أو البعيدة عن الدّرجة الثّانية فصاعدًا، والتي تنشأ من خلال أحداث أو آليات وسطيّة في المجال السّيبراني؛ وستشمل هذه الآثار الأضرار التي لم تكن مقصودة من الهجوم، كما لو تمّ الهجوم على نظام كومبيوتري عسكري وأدّى إلى إيقاف تشغيل النّظام، ثم تنتشر

البرامج الضّارة أيضًا في الأنظمة المدنيّة فتغلقها، وذلك بسبب الرّوابط ما بين الأنظمة العسكريّة والمدنيّة [14].

أيضًا، يؤكّد عنصر "الضّرر العرضي" في إطار المادة (8) من "النّظام الأساسي للمحكمة الجنائيّة الدّوليّة": على عموميّة هذا المفهوم في تحديد مشروعيّة الهجمات المسلحة؛ إذ اعتبرت الفقرة (2-ب-4) من المادة أعلاه، شنّ الهجوم المتعمد مع العلم بأنّه (سيسفر عن خسائر تبعية في الأرواح أو عن إصابات بين المدنيين أو عن إلحاق أضرار مدنيّة أو إحداث ضرر واسع النّطاق وطويل الأجل وشديد للبيئة الطّبيعيّة: يكون إفراطه واضحًا بالقياس إلى مجمل المكاسب العسكريّة المتوقعة الملموسة المباشرة)؛ إذًا، إنّ الهجمات التي تُنفذ مع العلم بأنّ لها نتائج وآثارًا تسبب الخسائر في أرواح المدنيين أو أضرارًا عرضيّة مفرطة مقارنةً بـ "الميزة العسكريّة المؤكدة": تُعدّ جريمة حرب [15].

يُعدّ "الضّرر العرضي" (Collateral Damage) محورًا مهمًا وأساسيًا في مضمون "مبدأ التّناسب" حسب القانون الدّولي الإنساني العرفي"، والذي نصّت القاعدة (14) منه على حظر "الهجوم المتوقع". منه أن يسبّب بصورة عارضة خسائر في أرواح المدنيين أو إصابات بينهم أو أضرارًا بالأعيان المدنيّة، أو مجموعة من هذه الخسائر والأضرار؛ ويكون مفرطًا في تجاوز ما يُنتظر أن يُسفر عنه من ميزة عسكريّة ملموسة ومباشرة"؛ هذا فضلاً عن تأكيد القاعدة (15) على توخي الحرص الدّائم في إدارة العمليات العسكريّة، وعلى تفادي إصابة السّكان المدنيين والأشخاص المدنيين، والأعيان المدنيّة؛ وأن تُتخذ جميع الاحتياطات العمليّة لتجنب إيقاع خسائر في أرواح المدنيين، أو إصابتهم، أو الإضرار بالأعيان المدنيّة بصورة عارضة، وتقليلها على أيّ حال إلى الحدّ الأدنى [16].

كذلك كانت إعادة تفسير الضّرر من قبل خبراء (دليل تالين) ليشمل تدخلًا كبيرًا في الوظائف؛ إذ توسعت إعادة التفسير لمفهوم "الضّرر" ليشمل الأعمال التي تُعطّل، وبشكل كبير، الحياة اليوميّة للمدنيين؛ أو "العنف" الذي يشمل التّأثير التّخريبي نفسه، فمجرد رفض بعض الخدمات يمكن أن يوصف في نهاية المطاف بأنّه ضرر؛ لكنّ النّهج البديل قد يكون توسيع نطاق الأشخاص أو الأشياء أو الأنشطة المحميّة، كما هو مقترح. لذلك يكون المرشح الواضح لإعادة التّفسير، هو: مفهوم "الكائن" فيما يتعلق بالبيانات [17].

المبحث الثاني: الأهداف المشروعة والاحتياطات الواجبة

يُعتبر تحديد الأهداف التي تتسم بمشروعيّة استهدافها: أحد أهم المعايير الأساسيّة في "القانون الدّولي الإنساني"؛ لاسيّما وأنّ النّزاع المسلح بالأصل يستهدف المقاتلين والمواقع العسكريّة، مقابل تكريس الحماية للمدنيين والأعيان الحيويّة؛ ففي مقابل يوجب "القانون الدّولي الإنساني" التزامًا قانونيًا ثابتًا على الأطراف كافة باتخاذ الاحتياطات الواجبة في أثناء الهجمات والدّفاع أيضًا، بهدف تقليل "الضّرر العرضي".

قسمنا هذا المبحث على مطلبين؛ يستعرض أوّلهما: الأهداف المشروعة؛ يليه ثانيهما مبينًا: الاحتياطات الواجبة في أثناء الهجمات السّيبرانيّة.

المطلب الأوّل: الأهـــداف المشـروعـــــة:

ومثلما بينا سابقاً: يتوجب أن تكون الهجمات مشروعة ويُحظر استهداف المدنيين والأعيان الحيويّة؛ ومع ذلك، ثمة ما يجوز ضربه كالأشخاص والأهداف العسكريّة؛ فالأشخاص الذين يجوز استهدافهم يُشكّلون أحد تطبيقات "مبدأ التّمييز" في النّزاعات المسلحة، حيث يُلزِم "القانون الدّولي الإنساني" أطراف النّزاع بالفصل ما بين المقاتلين والمدنيين لضمان حماية من لا يشارك في الأعمال العدائيّة. لاحقًا، ومع تطور أساليب القتال وظهور الهجمات السّيبرانيّة: أصبحت مسألة تحديد الفئات المستهدفة أكثر تعقيدًا وصعوبة؛ ممّا يفرض تدقيقًا أكبر في معيار المشاركة المباشرة في الأعمال العدائيّة، ومن هذه المشروعة هم **الأشخاص الجائز استهدافهم، إذ** أن تحديد الأشخاص الذين يجوز استهدافهم في العمليات العسكريّة، ومن ضمنها "الهجمات السّيبرانية" باعتبارها إحدى النّزاعات الحديثة أو الحروب الجديدة- كما بيناها سابقاً-، والتي تُعدّ نزاعًا مسلحًا إذا ما انطبقت عليها المعايير القانونيّة الدّوليّة الاتفاقيّة- أيضًا أشرنا إليها سابقاً-، وأبرزها تطبيق "مبدأ التمييز" ما بين المقاتل والمدني؛ من ثم سنبيّن المقاتل والعسكري النّظامي في القوات المسلحة كفئات يبيح "القانون الدولي" استهدافها استثناءً من قواعد الحماية بحظر الاستهداف.

لقد أوجب تأمين الاحترام والحماية للسّكان والأعيان المدنيّة: إلزام أطراف النّزاع وفي كلّ الأوقات بالتّمييز ما بين السّكان المدنيين والمقاتلين، وكذلك ما بين الأعيان المدنيّة والأهداف العسكريّة؛ وأن يكون توجيه العمليات الهجوميّة ضدّ الأهداف العسكريّة حصرًا من دون غيرها. هذا المبدأ الإلزامي أورده البروتوكول الإضافي الأوّل لاتفاقيات جنيف عام ١٩٧٧ في نصّه على أن (تعمل أطراف النّزاع على التّمييز بين السّكان المدنيين والمقاتلين وبين الأعيان المدنيّة والأهداف العسكريّة، ومن ثم توجه عملياتها ضدّ الأهداف العسكريّة دون غيرها من أجل تأمين احترام السّكان المدنيين والأعيان المدنيّة)؛ أيضًا أكّدت "محكمة العدل الدوليّة" على أنّه: لا يجوز توجيه الهجمات إلّا نحو المقاتلين والأهداف العسكريّة فقط"؛ وهذا يعني أنّ الأهداف المسموح بها عند تخطيط وتنفيذ العمليات الإلكترونيّة: هي العسكريّة حصرًا؛ كأجهزة الكمبيوتر أو النّظم الحاسوبيّة المُستخدمة في العمليات العسكريّة؛ أي لا يجوز توجيه الهجمات نحو نظم حاسوبيّة متعلقة بالمنشآت المدنيّة. إنّ تطبيق هذا المبدأ يتسم بالتّعقيد لأنّ طبيعة "الهجمات السّيبرانيّة ونظامها: عكس ما هي عليه في الهجمات التّقليديّة الحركيّة؛ فالمقاتل السّيبراني يكون غالبًا بعيدًا عن المكان المستهدف. وهذا ما يؤكّد أنّ تطبيق قاعدة "التّمييز" ما بين المدنيين والمقاتلين أمرٌ في غاية الصّعوبة [18].

إذًا، وعلى العموم، إنّ الاستهداف المشروع للأشخاص والأعيان في أثناء "الحرب السّيبرانية"، كهدف أساسي تحمله "قواعد القانون الدّولي الإنساني" من خلال أحكامها: هو حماية الأفراد؛ فهؤلاء هم المعنيون بالقواعد القانونيّة المقرّرة لحمايتهم تجاه الظّروف الاستثنائيّة التي قد تواجههم في أوطانهم، من مثل الحرب والنّزاع المسلح غير الدّولي والاضطرابات الدّاخليّة. كما وتجدر الإشارة إلى أنّ "قواعد القانون الدّولي الإنساني"، وخصوصًا التي تضمنتها اتفاقيّة جنيف الرّابعة لسنة ١٩٤٩ والبروتوكول الإضافي الثّاني سنة ١٩٧٧: تعني المدنيين بالتّحديد، أي غير المشاركين في الأعمال المسلحة ما بين أطراف النّزاع. يُعدّ اعتماد قواعد حماية السّكان المدنيين من آثار الحرب: من أضخم إنجازات "القانون الدّولي الإنساني؛ وقد خُصص بابٌ كامل في البروتوكول الأوّل لحماية السّكان المدنيين، وحيث يخضع الأطفال والنّساء في حمايتهم لتلك القواعد، باعتبارهم أشخاصًا مدنيين لا يشاركون في الأعمال العدائيّة (19). لكنّ المنطق القانوني الذي يدعم النّهج التقييدي: لا يزال بعيد المنال؛ إذ لا يَعتمد "مفهوم الهجوم" بأي شكل من الأشكال على تعريف الأهداف العسكريّة؛ بل وعلى العكس من ذلك، إنّ توجيه عمليات ضارة ضدّ المدنيين والأعيان المدنيّة وغيرهم من الأشخاص أو الأشياء المحميّة: لا يقل عن هجوم أو توجيه لنفس العمليات ضدّ المقاتلين أو المدنيين المشاركين مباشرة في الأعمال العدائيّة أو الأهداف العسكريّة؛ بالتّالي، وبمجرد أن تصبح العمليّة بمثابة هجوم: تنشأ مسألة ما إذا كان الهدف عسكريًا، على سبيل المثال: غالباً ما تقوم القوات العسكريّة بعمليات استخبارات ومراقبة واستطلاع ضدّ الأنشطة المدنيّة والعسكريّة على حد سواء -الأولى لتطوير نمط تقييمات الحياة التي من شأنها تسهيل الامتثال لـ "قاعدة التّناسب"، شرط اتخاذ الاحتياطات اللازمة في الهجوم؛ أمّا الاستطلاع فمن أجل جمع المعلومات لضرب الهدف بشكل فعّال [20].

أمّا الأشخاص المدرجين ضمن الأهداف العسكريّة المشروعة، فهم المقاتلون وأعضاء الجماعات المسلحة المنظّمة والمدنيون المشاركون بشكل مباشر في الإعمال العدائيّة؛ في حين أنّ المدنيين والموظفين والعاملين ضمن المجال الطّبي والدّيني، والمقاتلين العاجزين عن القتال بسبب الجروح أو المرض أو القبض أو الاستسلام أو أي سبب آخر: يتوجب أن تتم حمايتهم [21]. وبالتّالي: ينبغي لمعيار الإنسانيّة أن يكون حاضرًا كأحد الشّروط لـ "مبدأ الضّرورة العسكريّة" [22].

تنصّ الفقرة (1 -المادة 43) من البروتوكول الإضافي الأوّل عام 1977 لاتفاقيات جنيف عام 1949 على أنّه: "تتكون القوات المسلحة التّابعة لطرف في النّزاع، من كافة القوات المسلحة والمجموعات والوحدات النّظاميّة التي تكون تحت قيادة مسؤولة عن سلوك مرؤوسيها". هذا المفهوم الواسع والوظيفي للقوات المسلحة النّظاميّة: هو أشمل من المفهوم الضّمني الوارد في اتفاقيّة لاهاي عام 1907، واتفاقيات جنيف الأربع عام 1949م"؛ كما أنّ هذه القوات لها الحق في ممارسة أعمال القتال مع العدو [23].

ضمن السّياق أيضًا، يُعرّف المقاتلون بأنّهم: "الأشخاص الذين يخوّلهم طرف في نزاع مسلح استخدام القوة، تنفيذًا للعمليات العدائيّة في ميدان النزاع"؛ ويتطلب تعريف المقاتل الشّرعي وفق "القانون الدّولي

الإنساني" مستوى من مسؤوليّة المنظمة أو قيادة الدّولة. هذه السّمات موجودة داخل الدّول التي لديها قوات مسلحة تمتلك قدرات سيبرانيّة، حيث أنشأت العديد من البلدان فروعًا أو وحدات سيبرانيّة خاصة بها داخل القوات المسلحة؛ على سبيل المثال لا الحصر: لدى الولايات المتحدة الأمريكيّة القيادة السّيبرانيّة للجيش الأمريكي (V.S. Army Cyber Command)؛ ومثلها أنشأ جيش التّحرير الشّعبي الصّيني قسمًا أو فريقًا سيبرانيًا يسمى "الجيش الأزرق"؛ ودولة النّرويج لديها "الدّفاع السّيبراني" الذي يقوم بإنشاء وتشغيل وحماية أنظمة اتصالات القوّات المسلحة والبنية التّحتيّة الرّقميّة [24].

بالرجوع إلى المدنيين وفقدانهم الحماية من الهجمات المباشرة، وجعلهم أهدافًا مشروعة: يتمّ الأمر في حالتين متناقضتين، الأولى -اعتبار المدني مشاركًا مباشرةً في العمل العدائي؛ الثّانيّة -عدم اعتباره من فئة المدنيين بموجب "القانون الدولي الإنسان"؛ ولا توجد فئة ثالثة بموجب "قواعد القانون الدّولي الإنساني"، فإمّا أن يكون الشّخص مدنيًا ومتمتعًا بالحماية في حال عدم مشاركته المباشرة في العمل العدائي؛ وإمّا أن يكون مقاتلًا وفاقدًا للحماية من الهجمات المباشرة.

إنّ المشاركة المباشرة للمدني، والتي تتصف بالعفويّة أو غير المنتظمة أو المتقطعة أو حتى بالمشاركة المباشرة المتكررة: لا تجعل من هذا المدني فئة ثالثة في "القانون الدّولي الإنساني"، بل ويفقد الحماية الممنوحة له طوال فترة مشاركته، ولا يستعيدها إلّا عند انفصاله عن العمليات العدائيّة وإذا لم يشكّل خطرًا [25].

لقد حدّدت الفقرة (٣ -المادة ٥١)، من البروتوكول الإضافي الأوّل عام 1977، الظّروف والشّروط التي يفقد فيها المدني صفته المدنيّة ليدخل ضمن قانون الحرب باعتباره مقاتلاً، حيث نصت على أنّه: (يتمتع الأشخاص المدنيون بالحماية التي يوفرها هذا القسم، ما لم يقوموا بدور مباشر في الأعمال العدائيّة، وعلى مدى الوقت الذي يقومون خلاله بهذا الدّور)؛ وتُعدّ حماية "الصّفة المدنيّة" ذات أهميّة خاصة، لأنّ من شأنها المساعدة في الحدّ من إلحاق الأضرار بالمدنيين، وجعل الأهداف العسكريّة مباشرة للهجوم.

أيضًا، وبالرّجوع إلى صفة "المدني"، فقد يمتلك الفرد خبرة في العمل على الحاسوب، وقد يشارك في الهجوم، من دون أن يحمل الصّفة العسكريّة الرّسميّة، ممّا قد يساعد في بقاء الصّفة المدنيّة والحماية من الهجوم، وباعتبارها مشاركة مباشرة من هذا المدني في الهجوم [26]؛ أي المشاركة المباشرة ضمن العمليات العدائيّة والتي تسبّب الضّرر الفعلي، أي أنّ المدني المشارك يصبح هدفًا مشروعًا [27]. بالمقابل، هناك رأي أخر يعتبر أنّ فعل المشاركة المباشرة، وإن لم يلحق ضررًا بالطّرف الآخر: قد حقق منفعة لأحد الأطراف؛ أي أنّ المشاركة مباشرة لوجود علاقة عمل بين ما قام به المدني وبين العمليات العدائيّة [28].

ضمن شروط اعتبار المدني مشاركًا مباشرًا، هناك ثلاث معايير وجوبيّة [29]، وهي:

- تلبية حدّ معين من الضّرر (عتبة الضّرر).

- التّرابط السّببي المباشر ما بين الفعل المعني بالضّرر والضّرر المباشر.
- كون الفعل مصممًا لدعم أحد أطراف النّزاع وإلحاق الضّرر بالطّرف الآخر في النّزاع (العلاقة بالعمل الحربي).

أما من هذه الأهداف المشروعة بعد الأشخاص هي الأهداف العسكريّة، إذ يواجه "المفهوم الحديث للحرب" تحديًا في تعريف "الهدف العسكري"، لاسيّما وأن طبيعة الحرب قد تغيرت بشكل كبير؛ ومن ثم فإنّ استخدام "هجمات الفضاء السّيبراني" يمكنه توسيع مجال الحرب والعمل على نشر أسلحة "الفضاء السّيبراني"، وذلك مقارنة بالقواعد الأخرى التّقليديّة التي تقيد انتشار الأسلحة التّقليديّة واستخدامها. لقد تطورت أساليب القتال والحرب، بل وأصبحت متعديّة للحدود والمكان والزّمان، ولو كان ذلك خارج نطاق العمليات العسكريّة. بالتّالي، ونتيجة لهذا التّطور، اقتضت الحاجة وضع قواعد تكفل حماية المدنيين والأعيان المدنيّة ضدّ آثار الحروب وأضرارها، من خلال القيود والضّوابط التي يستعان بها في التّمييز بين الأهداف العسكريّة والأعيان المدنيّة، وبين المحاربين وغير المحاربين؛ ففي "حرب الفضاء السّيبراني" تصبح مسألة التّفريق بين من يقاتل أو من لا يقاتل صعبة حيث لا أسرى ولا جرحى، وإنّما مرافق وأنظمة لا تعمل، أو دمار ذاتي من دون تدخل مباشر كالقصف والتدمير التّقليدي [30].

إنّ "الفضاء السّيبراني" يتميز بالارتباط ما بين نُظم الحواسيب؛ ويتألف هذا الفضاء من عدد لا يحصى لنُظم الحواسيب المتصلة بعضها ببعض في أرجاء العالم؛ وغالبًا ما يبدو أنّ نُظم الحواسيب العسكريّة تتصل بالنُظم التّجارية والمدنيّة، وتعتمد عليها كليًا أو جزئيًا. وبالتّالي، قد يكون من المستحيل شنّ "هجوم سيبراني" على بنية تحتيّة عسكريّة وجعل الآثار مقتصرة على الهدف العسكري فحسب؛ ذلك أنّ المعضلة تكمن بوجود العديد من البنى التّحتيّة الإلكترونيّة الحاليّة ذات الاستخدام المزدوج بطبيعتها، ولن يتغير هذا في المستقبل؛ على سبيل المثال: يمكن مدّ شبكة الاتصالات العسكريّة جزئيًا عبر الكابلات مع وسائط أخرى تُستخدم أيضًا لحركة المرور المدنيّة؛ وغالبًا ما تعتمد الأسلحة على البيانات النّاتجة عن نظام تحديد المواقع العالمي (GPS)، والذي يخدم أغراضًا مدنيّة مثل الملاحة [31].

أمّا الأساس القانوني للأهداف العسكريّة من الأعيان فقد تضمنته المادة (٢ /٥٢) من البروتكول الإضافي الأوّل عام 1977، ومبيّنة أنّ الأهداف العسكريّة تنحصر بالمواقع التي لها مساهمة فعّالة في العمل العسكري، والتي يحقق تدميرها "ميزة عسكريّة أكيدة"؛ كذلك اعتبرت المادة أعلاه في الفقرة (3) أنّ الأعيان المدنيّة تُكّرس لأغراض مدنيّة، وبالتالي لا يمكن أن تُستخدم أو تساهم مساهمة فعّالة في العمل العسكري [32].

توضح صياغة المادة أعلاه (2/ 52) وجوب أن تكون هناك علاقة واضحة ما بين الهدف المحتمل والعمل العسكري. كما ويشير مصطلح (العمل العسكري) إلى القدرات القتاليّة للعدو في الحرب؛ وتتأسس العلاقة

من خلال المعايير الأربعة للطّبيعة والموقع والغاية والاستخدام؛ أمّا الطّبيعة فتشير إلى الطّابع المتأصل للهدف، مثل السلاح؛ فالأعيان التي ليس لها طبيعة عسكريّة قد تقدم أيضًا مساهمة فعّالة في العمل العسكري بحكم موقعها الخاص أو غايتها أو استخدامها الحالي [33].

بهذا الصّدد أيضًا، أشار (دليل تالين للحرب السّيبرانية) في القاعدة (٣٨) منه، إلى أنّ الأهداف العسكريّة المتعلقة بالأعيان هي تلك التي تسهم مساهمة فعّالة في العمل العسكري بطبيعتها أم مرقعها أم بغرضها أم باستخدامها، والتي يحقق تدميرها الكلّي أو الجزئي "ميزة عسكريّة أكيدة"؛ والأهداف العسكريّة للهجمات على شبكات الحاسوب يمكن أن تضمّ الحواسيب وشبكاتها والبنى التّحتية المعلوماتيّة [34].

أمّا المقصود بـ "المساهمة الفعّالة، فهو: "وجوب أن يُسهم الهدف مساهمة فعّالة في العمل العسكري، وضمن معايير عدة"، هي:

- المعيار الأوّل: الأهداف حسب طبيعتها -هناك أعيان عسكرية بطبيعتها وهناك أعيان مدنيّة بطبيعتها، مثلاً مباني ومعسكرات القوات المسلحة والمطارات العسكريّة والطائرات الحربيّة ومخازن الأسلحة والذخائر التّابعة للقوات العسكريّة والآليات العسكريّة: هي أعيان عسكريّة بطبيعتها. بالمقابل، الأعيان المدنية بطبيعتها هي التي لا تسهم بطبيعتها في العمليات العسكريّة؛ إذ تشمل المساكن والمستشفيات وأعيانًا مدنيّة لا تُستخدم لأغراض عسكريّة، إضافة إلى الأعيان المشمولة بحماية خاصة وتكفل الشّارات والعلامات المميزة لهذه الحماية، والتي لا يجوز أن تكون هدفًا للهجوم [35].

  ضمن السّياق أيضًا، وعند الرّجوع إلى "الهجمات السّيبرانية" وربطها بالأهداف حسب طبيعتها نجد أنّ هذا المعيار يركّز على أهداف عسكريّة في أصلها -كما بينا أعلاه-؛ وبذلك تُعدّ أجهزة الكمبيوتر العسكريّة والبنية التّحتيّة الإلكترونيّة العسكريّة أهدافًا عسكريّة تنسجم مع المعيار أعلاه [36].

- المعيار الثّاني: الأهداف حسب موقعها -هناك بعض الأعيان التي لا تكون لها وظيفة عسكرية بطبيعتها، إلّا أنّ موقعها يقدّم مساهمة فعّالة في العمل العسكري؛ فالموقع هو المنطقة الجغرافيّة ذات الأهميّة العسكريّة، سواء باستخدامه من قبل الطرف المهاجم أو بحرمان الخصم من ذلك الاستخدام. وتبعاً لذلك يُعتبر حرمانه تحقيقًا للميزة العسكريّة.

  أمّا في "الهجمات السّيبرانية"، فأهميّة مثل تلك المواقع لا تكمن في الاستخدام الفعلي لها، وإنّما في موقعها الذي يجعل مساهمتها فعّالة في العمل العسكري، وتصبح بالتّالي هدفًا عسكريًا مشروعًا؛ على سبيل المثال: إنّ القيام بالهجمات على شبكات الحاسوب لاستهداف نظام الإشراف والمراقبة وجمع البيانات (SCADA) الخاصة بخزان للماء يقع في منطقة جغرافية يتوقع استخدامها من قبل الخصم، والتّسبب في إطلاق الماء إلى تلك المنطقة بغية حرمان الخصم من ذلك الاستخدام: يبرر

القيام بشنّ مثل تلك الهجمات، لأنّ فائدة تلك المنطقة من الناحية العسكريّة تجعلها هدفًا عسكريًا صحيحا [37].

- المعيار الثّالث: الأهداف حسب غرضها -وهنا يشير الاستخدام المستقبلي المزمع لشيء ما، إلى أنّه لا يستخدم العين لأغراض عسكريّة، ومن المتوقع أن يستخدم مستقبلا؛ فبمجرد وضع الهدف يتضح هذا الغرض ولا يحتاج المهاجم إلى الانتظار لكي يتحول هدفًا عسكريًا من خلال الاستخدام إذا كان الغرض قد تبلور بالفعل بدرجة كافية، أي أنّه لا يستخدم حاليّا، لكن قد يستخدم مستقبلاً؛ ومثال ذلك: قد تتوفر معلومات بأنّ الطرف المعادي اشترى أنظمة حاسوب، وقد تستخدم لأغراض عسكريّة، وبذلك تكون هدفاً عسكريًا [38].

بعد أن بينا المعايير الخاصة بالمساهمة العسكريّة الفعليّة مع تحقق "شرط الميزة العسكريّة" -والذي فصلناه في فقرة سابقة من هذا المبحث -نجد أنّ المعيار الأخير، أي معيار الهدف بحسب غرضه: يتسم بالتّعقيد لكونه يفرض حالة من التّوقع، وهذا أمرٌ صعب في "الهجمات السّيبرانيّة"، أو لبناء النّتائج عليه ومن ثم توجيه الضّربات السّيبرانيّة أو العمليات الهجوميّة.

إنّ تحديد الأهداف العسكريّة قد تمّ بيانه وفق المعايير المذكورة أعلاه، ولكنّ السّؤال الأهم هو حول كيفيّة التّحديد وشروطه إذا ما كانت الأعيان ذات استخدام مزدوج؟ والجواب هو أنّ استخدام هذه الأعيان لأغراض مدنيّة وعسكريّة على حدّ سواء: يجعلها هدفًا مشروعًا بسبب استخدامها للغرض العسكري؛ وخير مثال هو الأعيان المدنيّة كالمحطات الخاصة بالطّاقة مثل الكهرباء والمياه التي تمدّ الوحدات العسكريّة، ومساعدتها في العمليات [39]؛ والصّعوبة تكمن هنا في تحديد أي جزء من هذه الأعيان يستخدم للأغراض العسكريّة؛ ومن ثم إنّ تحديدها كهدف عسكري مشروع له عواقب إنسانيّة وخيمة. لذلك تحتاج إلى دقة وتركيز في التّحديد، ومن ثم تخضع لـ "مبدأ التّناسب".

المطلب الثاني: الاحتياطات الواجبة في أثناء الهجمات السّيبرانيّة:

تُعتبر الاحتياطات الواجبة من القواعد المهمة والأساسيّة في "القانون الدّولي الإنساني"، إذ تهدف إلى تحجيم الأضرار العرضيّة التي قد تلحق بالأعيان المدنيّة أو بالأشخاص الذين لا يشاركون مباشرة في الأعمال العدائيّة؛ ومع ازدياد استخدام "الفضاء السّيبراني في النّزاعات المسلحة"، اكتسبت هذه القاعدة بُعدًا خاصًا يستلزم مواءمة القواعد التّقليديّة مع "طبيعة الهجمات السّيبرانيّة"، لما تتميز به من سرعة وانتشار وصعوبة التّنبؤ بنتائجها؛ ومن ثمّ، إنّ احترام الاحتياطات الواجبة في هذا المجال: يُعدّ حجر الزّاوية لضمان "تطبيق التّناسب والتمييز"، وتحقيق التّوازن ما بين تحقيق الأهداف العسكريّة المشروعة وحماية المدنيين. وتتمثل هذه الاحتياطات الواجبة في أثناء الهجوم وقبل الهجوم، إذ تكون **الاحتياطات في أثناء الهجوم** تطبيقاً لقواعد "القانون الدّولي الإنساني" يعني: ضمان الامتثال لقاعدتي "التّمييز والتّناسب"،

وضمان توخّي الحرص الدّائم في إدارة العمليات العسكريّة تفاديًا لإصابة المدنيين والأعيان المدنيّة؛ لذلك فرض "القانون الدّولي الإنساني" على أطراف النزاع المسلح اتخاذ الاحتياطات في الهجوم، أي اتخاذ كلّ التدابير الممكنة للتّأكد من أن الهدف المراد مهاجمته هدف عسكري؛ وذلك بفعل الاحتياطات الممكنة عند اختيار وسائل وأساليب الهجوم، بقصد تفادي الأضرار العرضيّة المتوقعة، أو التّقليل منها إلى أقل حدّ ممكن، والامتناع عن شنّ هجوم قد ينتهك "مبدأ التناسب"، وإلغاء الهجوم أو تعليقه إذا ما اتضح أنّ الهدف ليس عسكريًا، أو مشمول بحماية خاصة، أو أنّ الهجوم يتوقع منه انتهاك "مبدأ التّناسب". ما يعني بالتّالي أنّ لهذه القواعد أهميّة بالغة، سواء منها قاعدة "التناسب" أو سواها من قواعد الاحتياط، لاسيّما وأنّها تقتضي إجراء تقييم للأضرار العرضيّة المتوقع أن تنجم عن الهجوم [40]. وللتفصيل الأوسع نجد:

أنّ البروتوكول الإضافي الأوّل لعام 1977 ينصّ على "مبدأ التّناسب" في المادة (5/51)؛ إذ يحظر الهجمات العشوائية التي قد تسبب خسائر وأضرارًا مفرطة للمدنيين والأعيان المدنيّة مقارنةً بـ "الميزة العسكريّة" المتوقعة. كذلك تؤكد المادة (2/57) ضرورة اتخاذ الاحتياطات كافة والممكنة للتّحقق من أنّ الأهداف ليست مدنيّة أو محميّة؛ وتشدّد على اختيار وسائل وأساليب الهجوم التي تقلّل الأضرار العرضيّة بالمدنيين والأعيان المدنيّة؛ ويُلزم المهاجم بالامتناع عن أيّ هجوم يتوقّع أن يُحدِث خسائر مفرطة لا تتناسب مع المكسب العسكري. كذلك يُلغى أو يُعلّق الهجوم إذا ما تبيّن أنّ الهدف ليس عسكريًا أو يُحدث خلطًا من هذه الخسائر والأضرار، وذلك بصفة عرضيّة تفرط في تجاوز ما يُنتظر أن يسفر عن ذلك الهجوم من "ميزة عسكريّة ملموسة ومباشرة" [41].

أيضًا، هناك نقاش فقهي حول عبارة (يمكن أن يُتوقع منه) في المواد (51-5ب) والمادة (57-2-أ وب) من البروتوكول المذكور أعلاه؛ إذ يشير النّص إلى أنّ هذه العبارة ليست محددة بزمان أو مكان معين؛ كذلك رفض المؤتمر الدّبلوماسي تقييد الأضرار العرضيّة بالآثار المباشرة قرب الهدف العسكري؛ ووفقًا لـ (درويغيه -Droighe) فإنّ الأضرار طويلة الأمد أو ذات الآثار غير المباشرة: يجب أن تؤخذ بالحسبان. كما ويرى (ساسولي -Sassoli) و(كاميرون -Cameron) أنّ الهجوم على الأعيان ذات الاستخدام المزدوج يشمل الأضرار النّاتجة عن تدميرها وأيّة أضرار تبعيّة يمكن توقّعها في المناطق المجاورة، بما في ذلك التّداعيات الارتداديّة.

بالمقابل، هناك اتجاه يفسر أحكام المواد (51) و(57) -وهو طبعاً التّفسير الهادف -من خلال "مبدأ التناسب" والاحتياطات في الهجوم ضمن سياق البروتوكول الإضافي الأوّل عام 1977؛ وباعتبارها أحكام تؤكّد حماية السّكان المدنيين والأعيان المدنيّة من أخطار العمليات العسكريّة؛ فرغم السّماح ببعض الأضرار العرضيّة: يجب ألّا تكون مفرطة مقارنةً بـ "الميزة العسكرية"، مع مراعاة الآثار الارتداديّة المتوقعة؛ فضلًا عن وجوب تفسير الأضرار العرضيّة في ضوء الأغراض الإنسانيّة التي تقضي بتوفير أقصى حماية ممكنة للمدنيين. كذلك يتعزز هذا المبدأ في مواد أخرى مثل المادتين (54) و(56) لكونهما تحظران

استهداف الأعيان الحيويّة ضمانًا لأمن السّكان المدنيين وبقائهم بعيدًا عما قد ينجم من آثار متوقعة إذ ما لحقت بها أضرار أو تدمير [42].

إنّ تنفيذ العمليات العسكريّة يوجب توخي العناية الدّائمة بغية تجنيب السّكان المدنيين والأعيان المدنيّة أيّ خطر من الإصابة المفرطة؛ وتشمل هذه الاحتياطات التي تقتضيها مبادئ "القّانون الدّولي الإنساني" بذل الجهد المستطاع للتّحقق من الأهداف عسكريّة؛ وأن تتخذ جميع الاحتياطات الواجبة عند تخير وسائل وأساليب القتال تفاديًا للإضرار بصفة عرضيّة -كما بينا أعلاه-؛ وفي الحرب الإلكترونيّة: قد تشمل الاحتياطات تصميم خريطة بشبكة الخصم، والتي تكون عادة جزءًا من تصميم الهجمات على شبكات الحاسوب؛ وإذا ما كانت المعلومات غير كاملة: توجّب اقتصار الأهداف على المتاحة. وهذا ما يتطلب خبرة تقنيّة [43].

إن من الأهميّة القصوى، وفقًا لـ "مبادئ القانون الدّولي الانساني": وجوب التزام القائم بالهجوم باتخاذ التّدابير إلى أقصى حدّ ممكن تفاديًا للضرر العرضي الذي يطال البنى التّحتيّة المدنيّة المحميّة؛ وهو ما يتطلب التّحقق من النّظم التي تتعرض للهجوم والأضرار المحتملة، التي قد تنجم عن هذه الهجمات؛ وهذا يعني أنّ أيّ هجوم يسبب إصابات أو أضرارًا مدنيّة يجب إلغاؤه، فضلًا عن التّأكد من نظم الحاسوب واستقلالها عن الأعيان المدنيّة [44].

إنّ "مبدأ التّناسب" الوارد في المادتين (51) و(57) من البروتوكول الإضافيّ الأوّل لاتفاقيات جنيف لعام 1949: ينطبق على حالات الهجوم المسلح؛ وإنّ "مفهوم الهجوم المسلح" -كما مرّ بنا -لم يعد مقتصرًا على القوة الحركيّة؛ فقد يُحدث "الهجوم السّيبراني" آثارًا ضارة على دولة ما بشكل موازٍ للأثر الذي يُحدِثهُ الهجوم التّقليدي؛ وهذا الأثر الضّار هو الذي يحدّد نوع الهجوم أكثر من الهجوم ذاته. إذًا، تتوجب مراعاة المعايير التي يتطلبها "مبدأ التناسب" في الهجوم؛ أولها: معيار الرّعاية الدائمة أو المتواصلة كما عبرت عنها المادة (57) من البروتوكول الإضافي الأوّل، والتي جاءت بعنوان (الاحتياطات في الهجوم)؛ إذ تفرض الفقرة (1) من المادة المذكورة شرطًا قانونيًا عامًا على العمليات العسكريّ، ويتمثل في ممارسة ما يُعبّر عنه بـ "الرّعاية الدّائمة، بالرّغم من أنَّ هذا المصطلح غير معرَّف سواء في المادة (57) أو في تعليق "اللجنة الدوليّة للصليب الأحمر"، أو بصورة عامة في خطاب الاعتماد؛ إلّا أنّ التّطبيق الدقيق لهذا المبدأ يُشير، وأقّله، إلى أنّ القائد لا يمكنه تجاهل الآثار التي تصيب السّكان المدنيين [45].

أيضًا، يُشدّد (دليل تالين) على أهميّة توفر الخبرة التّقنيّة الخاصة عند تطبيق "مبدأ الاحتياط في الهجمات السّيبرانيّة" نظرًا لتعقيدها وارتفاع احتمالات الإضرار بالنّظم المدنيّة؛ بالتّالي، وإذا لم تكن لدى المسؤولين خبرة فعليهم الاستعانة بالخبراء التقنيين وإلّا اقتضى الأمر الامتناع عن الهجوم عند غياب القدرة على تقييم الأضرار المحتملة. كذلك تثير الهجمات الإلكترونية الدّفاعيّة الآليّة تحديات خاصة لأنّها تستهدف أجهزة

متعددة من دون تمييز بين طبيعتها المدنيّة أو العسكريّة، ممّا يتطلب من الدّول توخي الحذر في مشروعيتها؛ وقد ينطوي "مبدأ الاحتياط" أيضًا على الالتزام باستخدام الوسائل الإلكترونيّة إذا ما كانت أقل ضررًا من العمليات الحركيّة التّقليديّة، ومع ذلك، لا يوجد حتى الآن اتفاق دولي واضح بشأن إلزام الأطراف المتحاربة بهذا الالتزام.

كما أنّ "مبدأ الاحتياط" يتضمن التزامًا بعدم التّقيد بمبدأ "التّمييز والتناسب" فحسب، بل وباتخاذ كلّ التدابير المستطاعة تجنبًا لإحداث الخسائر في أرواح المدنيين، أو الأضرار بالأعيان المدنيّة، وذلك بصفة عرضيّة؛ وفي هذه الحالات، يعني "مبدأ الاحتياط" ضمنًا أنّ القادة ينبغي لهم اختيار أقلّ الوسائل ضررًا، ما دامت متاحة في زمن الهجوم، من أجل تحقيق هدفهم العسكري [46].

أما الالتزام بالتّدابير الوقائيّة تعد أيضاً من الاحتياطات الواجبة، إنّ الالتزام بالتّدابير الوقائيّة مهم جدًا لمواجهة التّأثيرات النّاجمة عن "الهجمات السّيبرانية"؛ ويقضي "مبدأ الاحتياطات" بأن تسعى أطراف النّزاع، قدر الإمكان، إلى نقل ما تحت سيطرتها من السّكان المدنيين والأعيان المدنيّة عن المناطق المجاورة للأهداف العسكريّة، أو اتخاذ تدابير أخرى لحمايتهم من أخطار العمليات العسكريّة؛ كما ويوصي (دليل تالين) بتطبيق إجراءات عمليّة عن طريق فصل البنية التّحتيّة الإلكترونيّة الأساسيّة العسكريّة عن المدنية، وعزل النّظم الحاسوبيّة الحيويّة عن الإنترنت، واتخاذ تدابير مسبقة لضمان الإصلاح الفوري للأضرار؛ ويشمل ذلك تسجيل الرّقمي للأعيان الثّقافيّة بهدف حمايتها وإعادة إعمارها عند/ بعد التّدمير. غالبًا ما تُؤكد المبادئ على ضرورة الفصل ما بين الشّبكات العسكريّة والمدنيّة كوسيلة وقاية أساسيّة، واستخدام تدابير مكافحة الفايروسات لحماية النّظم المدنيّة التي قد تتناثر بالأضرار أو بالتّدمير في أثناء الهجوم على البنيّة الأساسيّة الإلكترونيّة المدنيّة [47].

أيضًا، وضمن السّياق نفسه، أشارت القاعدة (59) من (دليل تالين للحرب السّيبرانيّة) إلى ضرورة أن تتخذ أطراف النزاع، قدر المستطاع، احتياطات ضروريّة لحماية المدنيين والأعيان المدنيّة من الأخطار النّاجمة عن الهجمات على شبكات الحاسوب، استنادًا إلى المادة (58/ج) من البروتوكول الإضافي الأوّل عام 1977، والتي تُعد من القواعد العرفيّة في "القانون الدّولي الإنساني"؛ كذلك هي القاعدة (57) من الدليل والمادة (57) تتعلق باحتياطات الدّفاع ضدّ آثار الهجمات؛ وأكدت اللجنة الدّوليّة للصليب الأحمر أنّ هذه التّدابير تشمل بناء الملاجئ وحفر الخنادق، نشر التّحذيرات وتنظيم الدّفاع المدني؛ وفي مجال "الهجمات السّيبرانيّة" تتضمن الاحتياطات عزل الشّبكات الإلكترونيّة العسكريّة عن المدنية، دعم البيانات بنسخ احتياطيّة، وتطوير وسائل الحماية من الفيروسات والهجمات الإلكترونيّة. ومع ذلك، تظلّ هذه الاحتياطات مقيدة بما هو ممكن عمليًا مع مراعاة الظّروف الإنسانيّة والعسكريّة [48].

إنّ تقليل فرص تعرض البُنى التّحتيّة الحيويّة للهجمات السّيبرانيّة من خلال تحديد الجهات المختصة بالحماية محليًا من أثار الهجمات، مثلما هي الحال في الولايات المتحدة حيث تختص "القيادة السّيبرانية" بحماية الأنظمة العسكريّة بينما تتولى وزارة الأمن الدّاخلي حماية القطاع الخاص: تبرز جميعها أهميّة واجب الحماية للمدنيين وتحقيق الرّدع السيبراني عبر سنّ القوانين وتطبيقها بفعّالية، خاصةً مع التّوسع في استخدام التّكنولوجيا ضمن مختلف القطاعات.

أمّا مظاهر هذه الحماية في الدّول العربية فأبرزها تجربة مصر من خلال "قانون مكافحة جرائم تقنيّة المعلومات" رقم 175 لسنة 2018، والذي ينظّم التّعاون الدّولي وتبادل المعلومات لمنع الجرائم الإلكترونيّة. كما ويشير مفهوم نّص القانون أعلاه في المادة (4) منه إلى أنّ الأمن السّيبراني: يشمل الإجراءات والتّدابير التّقنية والأدوات المستخدمة لحماية الشّبكات والبيانات من الهجوم، بما يضمن سلامة المعلومات وخصوصيتها وسرّيتها [49].

إنّ "مبدأ التّناسب"، ورغم ما يواجه من صعوبة التّحديات التقنيّة والقانونيّة المتعلقة بصعوبة تقدير الأضرار والخسائر: قابلٌ للتّطبيق في سياق "الهجمات السّيبرانية"؛ إذ يقوم هذا المبدأ في "القانون الدّولي الإنساني" على وجوب أن تكون الإجراءات العسكريّة متناسبة مع الهدف العسكري المشروع، وأن تقلل قدر الإمكان من الأضرار الإنسانيّة والعرضيّة. وبناءً عليه، يمكن تفعيل هذا المبدأ في "الحرب السّيبرانية" عبر الخطوات التّالية [50]:

- تحديد الهدف المشروع للإجراءات العسكريّة في الهجمات السّيبرانيّة.
- تحليل الأضرار المحتملة لتلك الإجراءات على المدنيين والممتلكات والبنية التّحتيّة الحيويّة، مع الأخذ في الاعتبار الأضرار الجانبيّة المحتملة أيضًا.
- تقييم البدائل الممكنة لتحقيق الهدف بطرق تقلل الأضرار الإنسانيّة والماديّة.
- اتخاذ الإجراءات العسكريّة التي تحقق الهدف بأقل قدر ممكن من الأضرار البشريّة والماديّة، وفقًا لـ "معايير التناسب".
- مراقبة وتقييم النّتائج للتأكد من عدم وقوع أضرار غير متناسبة مع الهدف المرجو.
- الالتزام بالتّعاون مع الجهات المعنية، بما فيها الجهات الإنسانيّة، للحدّ من الآثار السّلبيّة والخسائر النّاتجة عن الهجمات السّيبرانيّة.

لكن، ورغم أنّ التزام الأطراف بهذا المبدأ يسهم في التّخفيف من الأضرار الإنسانيّة والماديّة في النّزاعات السّيبرانيّة: تبقى الإشكاليّة الرّئيسية في القدرة على تحديد مصادر الهجمات وتأثيرها الفعلي.

الخاتمة

بعد أن أنهينا دراستنا بما يخص عناصر تطبيق مبدأ التناسب وبيان الميزة العسكرية وحصول الضرر العرضي المفرط، ومن ثم بيان الاحتياطات اللازمة للحد من انتهاك مبدأ التناسب والتسبب بدمار السكان المدنيين وحصول الضرر المفرط قد وصلنا إلى مرحلة الخاتمة وتضمينها أبرز النتائج ومن ثم وضع المقترحات على ضوء ذلك وكالآتي:

النتائج

1. إنّ مبدأ التّناسب في الهجمات السّيبرانيّة يشكّل أحد أبرز الأسس التي تضمن تقييد استخدام القوّة الإلكترونيّة ضمن إطار قانوني وأخلاقي يحافظ على التوازن بين الضرورة العسكريّة والاعتبارات الإنسانيّة.
2. أن الميزة العسكرية هي تلك المتأتية من الهجوم، والتي يقابلها استبعاد ميزة ليست عسكرية بطبيعتها، وعلى وجه الخصوص الميزة الاقتصادية أو السياسية أو النفسية، فمثلاً الهجوم على قطاع حيوي مدني ظناً من الجهة المعادية أنه سيؤدي لضعف الدولة عسكرياً، بل يحتاج الهجوم السيبراني على الهدف أن يحقق ميزة عسكرية بحيث الهدف له مساهمة عسكرية فعالة.
3. أن التطوّر السريع في أدوات الفضاء الرّقمي وتعقيداته، تزداد الحاجة إلى تطبيق صارم لهذا المبدأ، لما له من دور محوري في تقليل الخسائر غير المبرّرة والحدّ من تداعيات قد تمسّ حياة المدنيّين أو تعطل الخدمات الحيويّة التي يعتمدون عليها.
4. أن تجنب الضرر العرضي له أهمية كبيرة في النزاعات الحديثة، التي تتسم يتطور الوسائل والأساليب، وعلى وجه الخصوص في الهجمات السيبرانية، التي قد تسبب أضرار جسيمة وضرر عرضي مفرط مدمر، يؤدي إلى انتهاك قواعد القانون الدولي الإنساني.
5. أن اتخاذ الاحتياطات الوقائية للحد من الآثار التي تسببها الهجمات السيبرانية، يمثل واجباً أخلاقياً والتزاماً قانونياً في إطار القانون الدولي الإنساني، بالتالي إن أخذ هذه الاحتياطات هي تقليل منم الأضرار العرضية والخسائر الإنسانية والمادية عن طريق تعزيز القدرة على كشف الهجمات والتصدي لها.

المقترحات

1. من الضروري إيجاد آليات أكثر واقعية للحد من استخدام القوة الإلكترونية عن طريق تقييدها بشكل قانوني.
2. من الضروري جداً تكثيف الاجتماعات للأوساط القانونية الدولية لصياغة نصوص جديد تلائم طبيعة الهجمات السيبرانية.

3. من الضروري جداً تكثيف الآليات التدريبية والتطويرية للقادة العسكريين لأجل إنفاذ قواعد القانون الدولي الإنساني بما ينسجم مع الحرب السيبرانية، والتصدي للهجمات السيبرانية لتجنب حصول الضرر المفرط الذي يؤدي إلى دمار المدنيين والأعيان الحيوية التي بدورها تسبب انتهاك صارخ لمبدأ التناسب.
4. من الضروري جداً تطوير آليات اتخاذ الاحتياطات بما ينسجم مع خصوصية الحرب الجديدة، إذ أن الهجمات السيبرانية تحتاج إلى جهد تقني وعملي لتقييم الواقع والضرر المتوقع.

هوامش البحث

(1) الموصلّي، نور أمير: الهجمات السّيبرانيّة في ضوء القانون الدّولي الإنساني، رسالة ماجستير، الجامعة الافتراضيّة السّوريّة، 2021، ص39.

(2) الشّرقاوي، محمود حسين: الهجمات السّيبرانيّة في ضوء أحكام القانون الدّولي الإنساني، ط1، دار النّهضة العربية، القاهرة، 2022، ص536.

(3) Ommittee International De La Croix Rouge & Université Laval, op. cit 9.

(4) كاطع، زهراء حسين: الإطار القانوني للضرورة العسّكر في ضوء الهجمات السّبرانيّة، رسالة ماجسيتر، معهد العلمين للدراسات العليا، قسم القانون، العراق، 2023، ص103.

(5) رمضان، إبراهيم السيد أحمد: مواجهة الهجمات السّيبرانيّة في ضوء أحكام القانون الدّولي، مجلة العلوم القانونيّة والاقتصاديّة، العدد الأوّل، السّنة السّابعة والسّتون، 2025ص1797.

(6) نجيب، نسيب: الحرب السّيبرانيّة من منظور القانون الدّولي الإنساني، المجلة النّقديّة للقانون والعلوم السّياسيّة، كليّة الحقوق والعلوم اليّياسيّة -جامعة تيزي وزو، الجزائر، المجلد 16، العدد 4، 2021 ص231.

(7) Célestine de Zeeuw, The Principle of Proportionality in Military Cyber Operations (Master's thesis, Leiden University, Institute of Security and Global Affairs, Crisis and Security Management, 12 January 2020), p34.

(8) السّبيني، معاوية محمد معتز: المسؤوليّة الجزائيّة عن التّسبب عمدًا بخسائر عرضيّة في النّزاعات المسلحة الدّوليّة "دراسة تطبيقيّة على قضية ستانيسلاف غالتيش أمام محكمة يوغسلافيا السّابقة"، رسالة ماجستير، الجامعة الافتراضيّة السّوريّة، 2024، ص9.

(9) الشّرقاوي، محمود حسين: الهجمات السّيبرانيّة في ضوء أحكام القانون الدّولي الإنساني، مرجع سابق، ص541.

(10) Romanosky, Sasha and Zachary Goldman. "Understanding Cyber Collateral Damage." Journal of National Security Law & Policy, 9 (2017): p 233.

(11) كلنتر، زهراء عماد محمد: المسؤوليّة الدّولية الناشئة عن الهجمات السّيبرانيّة K ط1، مكتبة القانون المقارن، بغداد، 2022، ص138.

(12) دوريجي، كوردولا: لا تقترب من حدود فضاني الإلكتروني: الحرب الإلكترونيّة والقانون الدولي الإنساني وحماية المدنيين، مختارات من المجلة الدوليّة للصّليب الأحمر مجلد ٤، العدد، ص573 وما بعدها.

(13) الفتلاوي، أحمد عبيس؛ الغزي، قاسم محمد مهدي: الدّليل إلى فهم الهجمات السّيبرانيّة العدوانيّة" دراسة في إطار مواجهة قانونيّة وسياسيّة فاعلة، ط1، منشورات زين الحقوقيّة، بيروت، 2025، ص256 وما بعدها.

(14) جنديل السّراي، مهند عجب: الهجمات السّيبرانيّة والأسلحة الذّاتيّة في ظلّ مبدأ التّناسب، مجلة واسط للعلوم الإنسانيّة، مجلد 21، العدد 2، 2025، ص295.

(15) المادة (8 -الفقرة (2) -(ب- 4) من النّظام الأساسي للمحكمة الجنائيّة الدّوليّة عام 1998.

(16) السبيني، معاوية محمد معتز: المسؤوليّة الجزائيّة عن التّسبب عمدًا بخسائر عرضيّة في النّزاعات المسلحة الدّوليّة "دراسة تطبيقيّة على قضية ستانيسلاف غالتيش أمام محكمة يوغسلافيا السّابقة"، مرجع سابق، ص17.

(17) Schmitt, op. cit, P.204.

(18) محمود، لمى عبد الباقي؛ كيطان، إسراء ناصر: المسؤوليّة الدّوليّة عن الأضرار التي تحدثها الهجمات الإلكترونيّة، مجلة العلوم القانونيّة، مجلد 36، العدد الخاص الجزء الثاني -2021، ص345.

(19) حميد ابراهيم، عبد القادر: الحرب السّيبرانيّة في القانون الدّولي الإنساني، رسالة ماجستير، الجامعة الإسلاميّة -كليّة الحقوق، بيروت -لبنان، عام 2022، ص71.

(20) Schmitt, op. cit. P. 197.

(21) الحديثي، صلاح عبد الرّحمن؛ عزيز حسن، كاميران: التفصيل الشّامل لتطوّر القواعد القانونيّة الخاصة بالحرب السّيبرانيّة، ط1، المجموعة العلميّة للطباعة والنّشر والتّوزيع، مصر، 2021، ص206.

(22) Hans peter Garser-International Humanitarian law - Law an Introduction" in Hans Haug Humanity for all' ICRC. And Red Crescent Movements - Henry Donant Institute Haupt- 1993- p 17.

(23) مليرز، نيلس: المشاركة المباشرة في الأعمال العدائيّة، المجلة الدّوليّة للصليب الأحمر، الطّبعة العربيّة الأولى -2010، ص22 وما بعدها.

(24) موصلي، نور أمير: الهجمات السّيبرانيّة في ضوء القانون الدّولي الإنساني، مرجع سابق، ص350.

(25) الموسوي، علي محمد كاظم: المشاركة المباشرة في الهجمات السّيبرانيّة، ط1، المؤسسة الحديثة للكتاب، بيروت، 2019م، ص119.

(26) مهران، خالد محمود محمد: الإشكالات الخاصة بالاستخدام غير المشروع للفضاء الإلكتروني في إطار القانون الدّولي، أطروحة دكتوراه، جامعة أسيوط، كليّة الحقوق، 2023، ص234.

(27) Hans peter Garser-international Humanitarian law -Law An Introduction" in Hans Haug Humanity for all' ICRC. And Red Crescent Movements -Henry Donant Institute Haupt- 1993- p 17.

(28) David turns: Cyberwarefare and the Notion of Direct Participation in Hostilities, Journal of iro conflict & Security law, Oxford University, Press, Press, Vol, p 295-296.

(29) الفتلاوي، أحمد عبيس؛ مهدي الغزي، قاسم محمد: الدّليل إلى فهم الهجمات السّيبرانيّة العدوانيّة" دراسة في إطار مواجهة قانونيّة وسياسيّة فاعلة، مرجع سابق، ص301.

(30) مهران، خالد محمود محمد: الإشكالات الخاصة بالاستخدام غير المشروع للفضاء الإلكتروني في إطار القانون الدّولي، مرجع سابق، ص230.

(31) فياض، حسن: الهجمات السّيبرانيّة من منظور القانون الدّولي الانساني، مجلة الدّفاع الوطني اللبناني، العدد 114 ،2020، ص25.

(32) تنصّ المادة (52) من البروتكول الإضافي الأوّل عام 1977، على: 2 -تُقصر الهجمات على الأهداف العسكريّة فحسب. وتنحصر الأهداف العسكريّة فيما يتعلق بالأعيان على تلك التي تسهم مساهمة فعّالة في العمل العسكري سواء أكان ذلك بطبيعتها أم بموقعها أم بغايتها أم باستخدامها، والتي يحقق تدميرها التّام أو الجزئي أو الاستلاء عليها أو تعطيلها في الظّروف السّائدة حينذاك ميزة عسكريّة أكيدة. 3 -إذا ثار الشّك حول ما إذا كانت عين ما، تكرّس عادّة لأغراض مدنيّة مثل مكان العبادة أو المنزل أو أيّ مسكن آخر أو مدرسة، إنّما تُستخدم في تقديم مساهمة فعّالة للعمل العسكري، يفترض أنها لا تُستخدم كذلك.

(33) دوريجي، كوردولا: لا تقترب من حدود فضائي الإلكتروني: الحرب الإلكترونيّة والقانون الدولي الإنساني وحماية المدنيين، مرجع سابق، ص562.

(34) ثامر أحمد، سراب: الهجمات على شبكات الحاسوب في القانون الدّولي الإنساني، أطروحة دكتوراه، جامعة النّهرين كليّة الحقوق، 2015، ص222.

(35) عبد الباقي محمود، لمى؛ أحمد، مروة إبراهيم: الهدف العسكري المشروع وأهم المبادئ التي تحكمه في القانون الدّولي الإنساني، مجلة العلوم والقانون، مجلد 30 عدد 2، 2015 ص701.

(36) موصلي، نور أمير: الهجمات السّيبرانيّة في ضوء القانون الدّولي الإنساني، مرجع سابق، ص38.

(37) ثامر أحمد، سراب: الهجمات على شبكات الحاسوب في القانون الدّولي الإنساني، مرجع سابق، ص223.

(38) موصلي نور أمير: الهجمات السّيبرانيّة في ضوء القانون الدّولي الإنساني، مرجع سابق، ص 38 وما بعدها.

(39) دوريجي، كوردولا: لا تقترب من حدود فضائي الإلكتروني: الحرب الإلكترونيّة والقانون الدولي الإنساني وحماية المدنيين، مرجع سابق، ص563.

(40) روبنسون، ايزابيل؛ نول، إيلين: التّناسب في الاحتياطات الواجب اتخاذها في الهجوم: التّداعيات والآثار الارتداديّة لاستخدام الأسلحة المتفجرة في المناطق المأهولة بالسّكان، مختارات من المجلة الدّوليّة للصليب الأحمر، 97، 319، 2016، ص111.

(41) الموسوي، صائب محمد: الحرب السّيبرانيّة على ضوء مبادئ القانون الدّولي الإنساني، أطروحة دكتوراه، الجامعة الإسلاميّة، كليّة الحقوق، قسم القانون العام، 2023، ص223.

(42) روبنسون، ايزابيل؛ نول، إيلين: التّناسب في الاحتياطات الواجب اتخاذها في الهجوم: التّداعيات والآثار الارتداديّة لاستخدام الأسلحة المتفجرة في المناطق المأهولة بالسّكان، مرجع سابق، ص113.

(43) دوريجي، كوردولا: لا تقترب من حدود فضائي الإلكتروني: الحرب الإلكترونيّة والقانون الدولي الإنساني وحماية المدنيين، مرجع سابق، ص573.

(44) مهران، خالد محمود محمد: الإشكالات الخاصة بالاستخدام غير المشروع للفضاء الإلكتروني في إطار القانون الدّولي، مرجع سابق، ص261.

(45) جنديل السراي، مهند عجب: الهجمات السّيبرانيّة والأسلحة الذّاتيّة في ظلّ مبدأ التّناسب، مرجع سابق، ص293

(46) دوريجي، كوردولا: لا تقترب من حدود فضائي الإلكتروني: الحرب الإلكترونيّة والقانون الدولي الإنساني وحماية المدنيين، مرجع سابق، ص574 وما بعدها.

(47) دوريجي، كوردولا: لا تقترب من حدود فضائي الإلكتروني: الحرب الإلكترونيّة والقانون الدولي الإنساني وحماية المدنيين، مرجع سابق، ص575.

(48) ثامر أحمد، سراب: الهجمات على شبكات الحاسوب في القانون الدّولي الإنساني، مرجع سابق، ص269.

(49) الشّرقاوي، محمود حسين: الهجمات السّيبرانيّة في ضوء أحكام القانون الدّولي الإنساني، مرجع سابق، ص566.

(50) الموسوي، صائب محمد ناظم: الحرب السّيبرانيّة على ضوء مبادئ القانون الدّولي الإنساني، مرجع سابق، ص277.

المصادر

أولاً: الكتب:

1. الشّرقاوي، محمود حسين: الهجمات السّيبرانيّة في ضوء أحكام القانون الدّولي الإنساني، ط1، دار النّهضة العربية، القاهرة، 2022.

2. الحديثي، صلاح عبد الرّحمن؛ عزيز حسن، كاميران: التفصيل الشّامل لتطوّر القواعد القانونيّة الخاصة بالحرب السّيبرانيّة، ط1، المجموعة العلميّة للطباعة والنّشر والتّوزيع، مصر، 2021.

3. كلنتر، زهراء عماد محمد: المسؤوليّة الدّولية الناشئة عن الهجمات السّيبرانيّة، ط1، مكتبة القانون المقارن، بغداد، 2022.

4. الفتلاوي، أحمد عبيس؛ الغزي، قاسم محمد مهدي: الدّليل إلى فهم الهجمات السّيبرانيّة العدوانيّة "دراسة في إطار مواجهة قانونيّة وسياسيّة فاعلة، ط1، منشورات زين الحقوقيّة، بيروت، 2025.

5. الموسوي، علي محمد كاظم: المشاركة المباشرة في الهجمات السّيبرانيّة، ط1، المؤسسة الحديثة للكتاب، بيروت، 2019.

ثانياً: الرسائل والأطاريح:

1. الموصلّي، نور أمير: الهجمات السّيبرانيّة في ضوء القانون الدّولي الإنساني، رسالة ماجستير، الجامعة الافتراضيّة السّوريّة، 2021.

2. كاطع، زهراء حسين: الإطار القانوني للضرورة العسّكر في ضوء الهجمات السّبرانيّة، رسالة ماجستير، معهد العلمين للدراسات العليا، قسم القانون، العراق، 2023.

3. السّبيني، معاوية محمد معتز: المسؤوليّة الجزائيّة عن التّسبب عمدًا بخسائر عرضيّة في النّزاعات المسلحة الدّوليّة "دراسة تطبيقيّة على قضية ستانيسلاف غالتيش أمام محكمة يوغسلافيا السّابقة"، رسالة ماجستير، الجامعة الافتراضيّة السّوريّة، 2024.

4. حميد ابراهيم، عبد القادر: الحرب السّيبرانيّة في القانون الدّولي الإنساني، رسالة ماجستير، الجامعة الإسلاميّة -كليّة الحقوق، بيروت -لبنان، عام 2022.

5. مهران، خالد محمود محمد: الإشكالات الخاصة بالاستخدام غير المشروع للفضاء الإلكتروني في إطار القانون الدّولي، أطروحة دكتوراه، جامعة أسيوط، كليّة الحقوق، 2023.

6. ثامر أحمد، سراب: الهجمات على شبكات الحاسوب في القانون الدّولي الإنساني، أطروحة دكتوراه، جامعة النّهرين كليّة الحقوق، 2015.

7. الموسوي، صائب محمد: الحرب السّيبرانيّة على ضوء مبادئ القانون الدّولي الإنساني، أطروحة دكتوراه، الجامعة الإسلاميّة، كليّة الحقوق، قسم القانون العام، 2023.

ثالثاً: المجلات:

1. رمضان، إبراهيم السيد أحمد: مواجهة الهجمات السّيبرانيّة في ضوء أحكام القانون الدّولي، مجلة العلوم القانونيّة والاقتصاديّة، العدد الأوّل، السّنة السّابعة والسّتون، 2025.

2. نجيب، نسيب: الحرب السّيبرانيّة من منظور القانون الدّولي الإنساني، المجلة النّقديّة للقانون والعلوم السّياسيّة، كليّة الحقوق والعلوم اليّياسيّة -جامعة تيزي وزو، الجزائر، المجلد 16، العدد 4، 2021.

3. دوريجي، كوردولا: لا تقترب من حدود فضاني الإلكتروني: الحرب الإلكترونيّة والقانون الدولي الإنساني وحماية المدنيين، مختارات من المجلة الدوليّة للصّليب الأحمر مجلد ٤، العدد.

4. جنديل السّراي، مهند عجب: الهجمات السّيبرانيّة والأسلحة الذّاتيّة في ظلّ مبدأ التّناسب، مجلة واسط للعلوم الإنسانيّة، مجلد 21، العدد 2، 2025.

5. محمود، لمى عبد الباقي؛ كيطان، إسراء ناصر: المسؤوليّة الدّوليّة عن الأضرار التي تحدثها الهجمات الإلكترونيّة، مجلة العلوم القانونيّة، مجلد 36، العدد الخاص الجزء الثاني، 2021.

6. مليرز، نيلس: المشاركة المباشرة في الأعمال العدائيّة، المجلة الدّوليّة للصليب الأحمر، الطّبعة العربيّة الأولى -2010.

7. مهران، خالد محمود محمد: الإشكالات الخاصة بالاستخدام غير المشروع للفضاء الإلكتروني في إطار القانون الدّولي، أطروحة دكتوراه، جامعة أسيوط، كليّة الحقوق، 2023.

8. فياض، حسن: الهجمات السّيبرانيّة من منظور القانون الدّولي الانساني، مجلة الدّفاع الوطني اللبناني، العدد 114, 2020.

9. عبد الباقي محمود، لمى؛ أحمد، مروة إبراهيم: الهدف العسكري المشروع وأهم المبادئ التي تحكمه في القانون الدّولي الإنساني، مجلة العلوم والقانون، مجلد 30 عدد 2، 2015.

10. روبنسون، ايزابيل؛ نول، إيلين: التّناسب في الاحتياطات الواجب اتخاذها في الهجوم: التّداعيات والآثار الارتداديّة لاستخدام الأسلحة المتفجرة في المناطق المأهولة بالسّكان، مختارات من المجلة الدّوليّة للصليب الأحمر، 97، 319، 2016.

رابعاً: الاتفاقيات:

1. المادة (8 -الفقرة (2) -(ب- 4) من النّظام الأساسي للمحكمة الجنائيّة الدّوليّة عام 1998.
2. المادة (52) من البروتكول الإضافي الأوّل عام 1977.

خامساً: المصادر باللغة الإنكليزية:

1. Ommittee International De La Croix Rouge & Université Laval.

2. Célestine de Zeeuw, The Principle of Proportionality in Military Cyber Operations (Master's thesis, Leiden University, Institute of Security and Global Affairs, Crisis and Security Management, 12 January 2020).
3. Romanosky, Sasha، and Zachary Goldman. "Understanding Cyber Collateral Damage." Journal of National Security Law & Policy, 9 (2017): p 233.
4. Michael N. Schmitt ،"Rewired Warfare: Rethinking the Law of Cyber Attack،" International Review of the Red Cross 96 ،no. 893 (2014).
5. Hans peter Garser-International Humanitarian law -Law an Introduction" in Hans Haug Humanity for all' ICRC. And Red Crescent Movements - Henry Donant Institute Haupt-1993- p 17.
6. Hans peter Garser-international Humanitarian law -Law an Introduction" in Hans Haug Humanity for all' ICRC. And Red Crescent Movements - Henry Donant Institute Haupt-1993- p 17.
7. David turns: Cyberwarfare and the Notion of Direct Participation in Hostilities, Journal of Conflict & Security law, Oxford University, Press، Press, Vol, p 295-296.