

القانون الإنساني

بين الحرب السيبرانية والأسلحة المستقلة

Humanitarian Law: Between Cyber Warfare and Autonomous Weapons

د. علاء الدين بومرعي

الجامعة الإسلامية في لبنان

alaadinbumeri@gmail.com

DOI: <https://doi.org/10.63939/JIES.2025-Vol7.N20.62-79>

الملخص

يتناول هذا البحث إشكالية انطباق قواعد القانون الدولي الإنساني على أنماط النزاعات المسلحة المعاصرة، ولا سيما الحرب السيبرانية وأنظمة الأسلحة المستقلة، في ظل التطور التكنولوجي المتسارع الذي غير طبيعة وسائل وأساليب القتال. فقد أصبحت الدول تعتمد بشكل متزايد على الهجمات السيبرانية لاستهداف البنى التحتية الحيوية والأهداف العسكرية، وعلى أنظمة أسلحة مستقلة تعمل دون تدخل بشري مباشر، بهدف تقليل الخسائر البشرية وتحقيق تفوق عسكري أكبر. غير أن هذا التحول يثير تحديات قانونية عميقة تتعلق بمدى قدرة هذه الوسائل الحديثة على الامتثال لمبادئ القانون الإنساني الدولي، وفي مقدمتها مبادئ التمييز، والتناسب، والضرورة العسكرية، واتخاذ الاحتياطات اللازمة أثناء الهجوم.

يركّز البحث، في شقّه الأول، على الحرب السيبرانية بوصفها شكلاً جديداً من أشكال النزاع المسلح، ويحلل مدى خضوع العمليات السيبرانية لقواعد القانون الدولي الإنساني، ولا سيما مبدأ التمييز بين المدنيين والمقاتلين، في ظل الطبيعة المزدوجة للفضاء السيبراني وصعوبة تصنيف الأهداف السيبرانية، فضلاً عن الإشكاليات المرتبطة بإسناد المسؤولية القانونية عن الانتهاكات الناتجة عن الهجمات السيبرانية، نتيجة صعوبة تحديد الفاعلين الحقيقيين ومصادر الهجمات.

أما في الشق الثاني، فيتناول البحث انطباق القانون الإنساني الدولي على أنظمة الأسلحة المستقلة، ويبيّن التحديات التي تفرضها هذه الأنظمة على إمكانية احترام المبادئ الإنسانية الأساسية، نظراً لغياب الإدراك الإنساني والضمير الأخلاقي في عمليات اتخاذ القرار الآلي. كما يناقش البحث إشكالية "فجوة المسؤولية" التي قد تنشأ عند ارتكاب انتهاكات للقانون الإنساني باستخدام هذه الأنظمة، ويحلل أوجه المسؤولية المحتملة، سواء على عاتق الدول، أو القادة العسكريين، أو المبرمجين، أو الجهات المصنّعة.

ويخلص البحث إلى أن قواعد القانون الدولي الإنساني، رغم أنها وُضعت في سياق الحروب التقليدية، لا تزال قابلة للتطبيق على النزاعات الحديثة، بما فيها الحرب السيبرانية واستخدام الأسلحة المستقلة، غير أن ذلك

يستلزم تفسيراً مرناً لهذه القواعد وتطويرها بما ينسجم مع مستجدات النزاعات المعاصرة. كما يؤكد البحث على ضرورة تعزيز الأطر القانونية الدولية، ووضع آليات تنظيمية أكثر وضوحاً وفاعلية، لضمان حماية المدنيين، ومنع الإفلات من العقاب، والحفاظ على الطابع الإنساني للنزاعات المسلحة.

الكلمات المفتاحية: القانون الدولي الإنساني، الحرب السيبرانية، الأسلحة المستقلة، مبدأ التمييز، حماية المدنيين، المسؤولية الدولية، النزاعات المسلحة المعاصرة، الهجمات السيبرانية.

Abstract

This study examines the applicability of international humanitarian law (IHL) rules to contemporary forms of armed conflict, particularly cyber warfare and autonomous weapon systems, in light of the rapid technological developments that have fundamentally transformed the means and methods of warfare. States have increasingly resorted to cyber operations to target critical infrastructure and military objectives, as well as to autonomous weapon systems that operate without direct human intervention, with the aim of reducing human casualties and achieving greater military superiority. However, this shift raises profound legal challenges concerning the ability of these modern means of warfare to comply with the core principles of international humanitarian law, foremost among them the principles of distinction, proportionality, military necessity, and the obligation to take precautions in attack.

In its first part, the study focuses on cyber warfare as a novel form of armed conflict and analyzes the extent to which cyber operations are subject to the rules of international humanitarian law, particularly the principle of distinction between civilians and combatants. This analysis is conducted in light of the dual-use nature of cyberspace and the difficulty of classifying cyber targets, in addition to the challenges related to the attribution of legal responsibility for violations resulting from cyber attacks, given the difficulty of identifying the actual perpetrators and the sources of such attacks.

In its second part, the study addresses the application of international humanitarian law to autonomous weapon systems and highlights the challenges these systems pose to compliance with fundamental humanitarian principles, due to the absence of human judgment and moral agency in automated decision-making processes. The study further discusses the issue of the “responsibility gap” that may arise when violations of international humanitarian law are committed through the use of such systems, and analyzes the potential forms of responsibility, whether borne by states, military commanders, programmers, or manufacturers.

The study concludes that, although the rules of international humanitarian law were originally developed in the context of traditional warfare, they remain applicable to modern conflicts, including cyber warfare and the use of autonomous weapons. Nevertheless, this applicability requires a flexible interpretation and further development of these rules in order to align them with the realities of contemporary armed conflicts. The study also emphasizes the need to strengthen international legal frameworks and to establish clearer and more effective regulatory mechanisms to ensure the protection of civilians, prevent impunity, and preserve the humanitarian character of armed conflicts.

Keywords: International Humanitarian Law; Cyber Warfare; Autonomous Weapons; Principle of Distinction; Civilian Protection; International Responsibility; Contemporary Armed Conflicts; Cyber Attacks.

المقدمة

يَشْهَدُ العالم، اليوم، نزاعات تَسْتَعْمِلُ فيها الدول أساليب حربية حديثة، ووسائل قتالية هائلة التّعقيد، بات المدنيين عُرضَةً للقتل، أو الجرح، والأعيان المدنية لا تُمَيِّزُها الهجمات القتالية عن الأهداف العسكرية، وأصبح القانون الإنساني الدولي وأحكامه، بِسَببِها، وَجْهًا لَوَجْهٍ مع تحديات جسام، وعلى مَحَكِّ الصلاح لهذه المُواجهة، وفي نَظَرِ مُعْظَم أطرافها قيداً يُرجى التخلّص منه، ومن أعبائه.

ولا شكّ في أن الحرب السيبرانية تلك النوع من الحروب المستجدة على مستوى أنواع النزاعات المسلحة وأساليبها ووسائلها، باتت اليوم تشكل هاجساً لدى الدول، وباتت واقعاً يُقلق أمن واستقرار أي دولة مهما كانت حصانتها كبيرة أمام أية هجمات سيبرانية، ومهما كان تقدمها العلمي والتقني هائلاً. فالمهاجمون مهما كانت صفاتهم أصبحوا قادرين على خرق الاحتياطات الأمنية لأية دولة بفضل القدرات المتوفرة لديهم والتطور المستمر في الفضاء السيبراني ومجال الذكاء الاصطناعي.

ويضاف، اليوم، إلى الحرب السيبرانية والأسلحة التقليدية، أنواع أسلحة جديدة هي الأسلحة المستقلة عن البشر في تشغيلها، والقادرة على القتال بمفردها في ساحة المعركة مزودة بوسائل القتال كالمقاتلين البشريين. هذا النوع الجديد من الأسلحة بات اليوم، هاجساً للدول، أيضاً.

ويبدو أن تعاظم القدرات القتالية للدول وتنوعها، وتطورها، أصبح يُشكل تحدياً أمام ما يقتضيه القانون الإنساني الدولي من تلك الدول أثناء النزاع المسلح، فتطبيق هذا القانون وفرض مبادئه على أطراف النزاع لم يعد كما كان الحال سابقاً مع الأسلحة التقليدية، وعندما كان البشر هم مَنْ يخضون القتال ويشاركون في الأعمال العدائية. وأمام هذا الواقع بات لزاماً بحث تلك التحديات أمام تطبيق القانون الإنساني، فالحرب السيبرانية والأسلحة المستقلة باتت تشكل عائقاً أمام فرض القانون، ولذلك كانت هذه الدراسة محاولةً لكشف الواقع الذي فرضه استخدام الهجمات السيبرانية بين الدول، واستعمال الأسلحة المستقلة أو «الروبوتية»، ومحاولةً لدراسة مدى انطباق القانون الإنساني أثناء استخدام هذا النوع الجديد من الأساليب والوسائل القتالية، بالإضافة إلى تحديد الجهات التي تكون مسؤولةً عن انتهاك القانون الإنساني أثناء استخدام هذه الوسائل والأساليب الحربية الحديثة.

وتحت وطأة استخدام الحرب السيبرانية والأسلحة المستقلة أثناء النزاع المسلح، وما قد تسببه من

انتهاكات للقانون الإنساني الدولي، وما شكلته من تحديات أمام تطبيق هذا القانون فإنه يمكن طرح الإشكالية التالية: ما مدى انطباق القانون الإنساني على الحرب السيبرانية والأسلحة المستقلة؟

وللإجابة عن هذه الإشكالية، لا بدّ من رسم إطار قانوني واضح ركيزته الأساسية القانون الإنساني الدولي بما فيه من مبادئ أساسية يجب على الدول مراعاتها والعمل بها، ومحاسبة الأشخاص الذين ينتهكون هذه المبادئ أثناء النزاع المسلح.

وانطلاقاً مما تقدم، تم تقسيم هذه الدراسة إلى قسمين وفق ما يلي:

1. تطبيق القانون الإنساني أثناء الحرب السيبرانية والمسؤولية عن انتهاكه.

2. انطباق القانون الإنساني على أنظمة أسلحة المستقلة وتحديات فرض المسؤوليات القانونية.

1. تطبيق القانون الإنساني أثناء الحرب السيبرانية والمسؤولية عن انتهاكه.

الحرب السيبرانية مجموعة من الهجمات الإلكترونية المتبادلة تُشنّ في الفضاء السيبراني من قبل أطراف متنازعة، سواء كانت دولاً أو جهات حكومية أو غير حكومية، وتستهدف أنظمة المعلومات وشبكات الحاسوب الخاصة بالطرف المستهدف، وتتخذ هذه الهجمات شكل برامج إلكترونية ضارة أو فيروسات حاسوبية، وتهدف إلى تعطيل أو تدمير هذه الأنظمة، أو سرقة البيانات السرية، أو شلّ الأنظمة الحيوية التي تُشغّل المرافق العامة للدولة المستهدفة أو قواتها المسلحة، كالأنظمة المالية والملاحية، مما يُشكل تهديداً مباشراً للأمن القومي وحياة المواطنين.

هذه الحرب تُحدث تأثيراً كبيراً على تطبيق القانون الإنساني، لما لها من قدرة على استهداف المدنيين والأعيان المدنية، والمقاتلين والأهداف العسكرية، على حدّ سواء، دون تمييز بين هؤلاء وأولئك، وهي تُشكل تحدياً على مستوى إسناد المسؤولية عن الانتهاكات التي قد تنتج عن تنفيذ هجمات سيبرانية تطلّ بنى تحتية حيوية، ومرافق يُستخدمها المدنيون، كمحطات الطاقة، أو المطارات، أو غيرها.

ومن المسلم به أنه لا يجوز لأطراف أية حرب أن يخوضوها دون أن يلتزموا بتطبيق مبادئ القانون الإنساني أثناء تنفيذ هجماتهم على العدو، والحرب السيبرانية واحدة من هذه الحروب، وهي تستلزم تطبيق هذه المبادئ بشكل صارم لأن تأثيرها واسع على حياة الناس. وهنا يمكن طرح السؤال التالي: هل تنطبق مبادئ القانون الدولي الإنساني، ولا سيما مبدأ التمييز، فعلاً، على الحرب السيبرانية؟ وهل الالتزام به سهل، في حال كان تطبيقه ممكناً؟ وما التحديات التي ترتب عن تطبيقه أثناء شنّ هجمات سيبرانية؟ هذه الأسئلة تجعل قضية تطبيق مبدأ التمييز أثناء الحرب السيبرانية تحتاج بحثاً.

أما القضية الأخرى التي تحتاج بحثاً، أيضاً، فهي مشكلة إسناد المسؤولية عن انتهاكات للقانون الإنساني الدولي قد تُرتكب بسبب شنّ هجمات سيبرانية. وهذه المشكلة تظهر بسبب عدم القدرة على تحديد الأشخاص الذين يُنفذون هذه الهجمات، لأنهم غير معروفين عند عدوّهم، وهم لا يُعلنون عن أنفسهم. ولأن الدول لا تكشف هويّة الأشخاص الذين تتعاقد معهم في مجال الفضاء السيبراني، وشنّ الهجمات السيبرانية؛ فهويّة هؤلاء الأشخاص تبقى مخفية إلا عن القادة المسؤولين عنهم.

وفي هذا المبحث لا بدّ من البحث في قضية تطبيق مبدأ التمييز في الحرب السيبرانية، وفي مشكلة إسناد المسؤولية، وذلك في المطلبين الآتيين:

1.1. التمييز بين المدنيين والمقاتلين أثناء الحرب السيبرانية.

2.1. إسناد المسؤولية عن انتهاك القانون الإنساني جراء الحرب السيبرانية.

1.1. التمييز بين المدنيين والمقاتلين أثناء الحرب السيبرانية.

الحرب السيبرانية حرب ذات دافع سياسي⁽²⁷⁾، تركز على هجمات سيبرانية ميدانها الفضاء السيبراني، وتأخذ شكل برامج إلكترونية ضارة، أو فيروسات، وتهدف إلى تعطيل أنظمة المعلومات، والشبكات الانترنت، أو سرقة البيانات السريّة، أو شلّ الأنظمة المشغلة للعديد من المرافق الحيوية التابعة للدولة، أو لقواتها المسلحة، وتُشكّل تهديداً للأمن القومي في الدولة⁽²⁸⁾.

ولقد حظيت الحرب السيبرانية بتغطية إعلامية واسعة نتيجةً للهجمات السيبرانية ضدّ دول عديدة، منها أستونيا وإيران، وعلى الرغم من كون هذا النوع من الحروب ليس شائعاً بين الدول، إلا أنّ بعض الهجمات التي حصلت مؤخراً أتت في سياق نزاعات سياسية بين دول متعادلة. وإنّ دولاً كثيرة تعمل على تقوية نفسها في الفضاء السيبراني، وتعمل على امتلاك أدوات الحرب السيبرانية، وتقنياتها، تحسباً لنشوب هكذا حرب في المستقبل.

وإنّ نطاق هذه الحرب واسع جداً، وهي تُتيح للمخططين العسكريين مجموعة واسعة من الإجراءات التي قد تُنفذ ضدّ أطراف معادية. وإنّ الفضاء السيبراني، بمكوناته من أجهزة الكمبيوتر والإنترنت وغيرها، يخدم مجالين هما: المجال المدني، والمجال العسكري، وهذا يَحْتِمُ أن يتمّ استخدام هذا الفضاء بشكل مُتناسق من قبل المدنيين والعسكريين، وإنّ أيّ محاولة لعرقلة استخدام هذا الفضاء نتيجة الحروب السيبرانية التي قد تنشأ بين

(27) Paulo Shakarian and others, *Introduction to Cyber-warfare A Multidisciplinary Approach*, (USA: Syngress, Elsevier, 2013, p. 2).

(28) Richard A. Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, (New York: Harper Collins, 2010), p. 6.

الدول، أو التي قد تنشأ نتيجة هجمات إرهابية، سوف تكون انعكاساتها على المدنيين رهيبة، وسوف تطال حياتهم المعيشية، وتؤثر على حقوقهم الإنسانية⁽²⁹⁾. وهذا ما يؤثر المخاوف بشأن ما إذا كان من الممكن للحرب السيبرانية عملياً أن تمثل لمبادئ القانون الدولي الإنساني، ولا سيما مبدأ التمييز.

ومن الثابت عملياً، أنه لا يمكن خوض حروب دون تطبيق القانون الإنساني الدولي، ودون أن يلتزموا بتطبيق مبدأ التمييز أثناء تنفيذ هجماتهم على العدو، فالقانون الدولي الإنساني، الذي يُعرف بـ«قانون النزاعات المسلحة»، أو بـ«قانون الحرب»، يتكوّن من قواعد قانونية تُنظّم سير الحروب، وأهمّ هذه القواعد، ما ورد منها في اتفاقيات جنيف الأربع، وفي بروتوكولها الإضافيين.

هذه القواعد، على الرغم من أهميتها، لا يُذكر أيّ منها الحرب السيبرانية، لأنها وُضعت في زمانٍ لم يكن فيه حروبٌ تُخاض في الفضاء السيبراني بواسطة أجهزة الكمبيوتر، والإنترنت، من خلف مكاتب مريحة في أماكن بعيدة عن ساحات القتال.

وبما أن الحرب السيبرانية باتت واقعاً جديداً يهتمّ به المجتمع الدولي، والمخططون العسكريون باتوا يُدركون تهديدها، وفُرَص وقوعها، فلا بدّ من وجود قانون يُنظّم سيرها، وشؤونها. هذا القانون يمكن أن يكون القانون الدولي الإنساني، الذي يرمي سائر النزاعات المسلحة، وشؤونها، عامةً، والذي يُعدّ جزءاً من القواعد القانونية الدولية التي تحظى بتوافق دولي حولها.

ولكن ما يعترض هذه الإمكانية هو أن المجتمع الدولي لم يتوصّل، بعد، إلى توافق في الآراء بشأن تطبيق القانون الدولي الإنساني على هذا النوع من الحرب. فقد حذّرت بعض الدول، مثلاً، من أن العمليات السيبرانية قد تؤدي إلى تصعيد سباق التسلح، ورأت: إن القانون الدولي المعاصر لا يمتلك أية وسيلة تساهم في تنظيم شؤون استخدام هذا السلاح، وشؤون تطوّره، ورأى آخرون أن إطار القانون الدولي الإنساني الحالي غير مناسب للتعامل مع نموذج الحرب السيبرانية الجديد، ودعوا إلى وضع اتفاقية دولية جديدة تُنظّم استخدامها. أما البعض الآخر فقد رأى أن الإطار القانوني للقانون الدولي الإنساني الحالي يمكن أن ينطبق على الحرب السيبرانية عن طريق القياس، أي أنه لا حاجة إلى تطوير قواعد سلوك الدول في الفضاء السيبراني، أو إلى إعادة ابتكار القانون الدولي العرفي، كما أن القواعد الدولية الحالية ليست بالية، والمعايير الدولية الطويلة الأمد التي تُوجّه سلوك الدولة، في أوقات السلم والنزاع، تنطبق على الفضاء السيبراني⁽³⁰⁾.

(29) أنظر هيربرت لين، النزاع السيبراني والقانون الدولي الإنساني، مختارات من المجلة الدولية للصليب الأحمر، عدد 886، المجلد 94، (صيف 2012)، ص 517 وما بعدها.

(30) *International Strategy for Cyberspace, Prosperity, Security, and Openness in a Networked World* the White House Washington, USA, May, 2011, p. 9.

وينطبق قانون الحرب على أيّ نزاع مسلح دولي أو غير دولي؛ والنزاع المسلح الدولي يقع عندما تكون هناك أعمال عدائية، تشمل، أو تقتصر على العمليات السيبرانية، التي تحدث بين دولتين أو أكثر⁽³¹⁾. أما النزاع المسلح غير الدولي فيقع عندما يكون هناك عنف مسلح مطوّل، يشتمل، أو يقتصر على العمليات السيبرانية، التي تحدث بين القوات المسلحة الحكومية، وقوات جماعة مسلحة واحدة أو أكثر، أو بين هذه الجماعات. وهذا يعني أنّ النزاع السيبراني يقع عندما تجري أعمال عدائية متبادلة في الفضاء السيبراني، بين جهات دولية أو غير دولية. ولكنّ أنشطة الأفراد، والكيانات غير المرتبطة بالنزاع المسلح، لا ينطبق عليها قانون الحرب (القانون الدولي الإنساني)⁽³²⁾. وبالتالي، عندما يَشُنُّ فردٌ، أو مجموعةٌ من الأفراد، هجمة سيبرانية على هدف معين، ولا يكون لهذه الهجمة صلة بنزاع مسلح، فإنّ مثل هذا الموقف لا يُنظّمه القانون الدولي الإنساني.

ويجدر الانتباه إلى أن تطبيق القانون الدولي الإنساني على الهجمات السيبرانية يمكن أن ينطوي على معضلة، سببها وجود صعوبات تتعلق بتحديد حدوث عملية سيبرانية، وتحديد منشئها، وبالغرض المقصود منها، وبتأثيراتها الدقيقة، ولكنّ هذه المعضلة لا تمنع تطبيق القانون الدولي الإنساني⁽³³⁾.

وبما أنّ مبدأ التمييز ينطبق على العمليات التي تُعدّ هجمات عسكرية فقط، فإنّه في غياب معايير واضحة تُحدّد ما إذا كانت العمليات السيبرانية هجمات أم لا، سيظلّ من الصعب على أطراف النزاع التي تُستخدّم العمليات السيبرانية تحديد الظروف التي ينطبق فيها مبدأ التمييز أثناء تنفيذ هذه العمليات. وبما أنّ القانون الدولي الإنساني يحتاج إلى إيجاد توازن بين حماية المدنيين والأعيان المدنية من جهة، وضمان عدم تقييد العمليات السيبرانية العسكرية بشكل غير معقول من جهة ثانية؛ فإنّ الحاجة إلى توضيح تصنيف العمليات بين هجمات، وغير هجمات، تبقى مُلِحَّةً لكي تعرف الدول ما العمليات التي يُسمَح بها، بموجب القانون الدولي الإنساني، وما تلك التي لا يُسمَح بها، لأن غياب هذا الوضوح يُصعّب تطبيق مبدأ التمييز، وهنا لا بدّ من التمييز بين أشكال العمليات السيبرانية، فلا يمكن أن تُعدّ عمليات تُسبّب إزعاجاً للمدنيين هجمات، وبالمقابل يجب أن تُعدّ العمليات التي تؤدي إلى آثار تَمَسّ حياة المدنيين وتُسبّب لهم المعاناة هجمات، ويجب أن يُطبّق عليها مبدأ التمييز بين المدنيين والمقاتلين.

أمّا كثرة المرافق ذات الاستخدام المزدوج فتجعل تطبيق مبدأ التمييز بين الأهداف العسكرية والأعيان المدنية، أثناء الهجمات السيبرانية، عملاً صعباً جداً، فالعديد من المرافق التي تُعدّ، تقليدياً، مدنيةً من المرجح أن

(31) 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 Defense Centre of Excellence, General editor: Michael N. Schmitt, (New York: Cambridge University Press, 2013, rule 30, p. 91_92).

(32) Ibid, para 7, p. 69.

(33) Ibid, para 9, p. 70.

تصبح أهدافاً دائمة أثناء الحرب السيبرانية، نظراً لاعتماد العالم الحديث على شبكات الكمبيوتر، والإنترنت، لتشغيل المرافق العامة، والاتصالات، والعمليات الاقتصادية، والتجارية، وهذا ما يزيد احتمال أن يصبح المدنيون والأعيان المدنية عُرضة للهجمات السيبرانية أكثر من ذي قبل. وإذا لم يكن هناك وسيلة للفصل بين المرافق ذات الاستخدام المدني والاستخدام العسكري تصبح كلّ المرافق المدنية عُرضة للهجوم السيبراني المُعادي. لذلك يجب أن يستجيب القانون الدولي الإنساني لِثُل هذه التحديات عن طريق تكييف مبدأ التمييز معها.

2.1. إسناد المسؤولية عن انتهاك القانون الإنساني جراء الحرب السيبرانية.

عندما يتعلق الأمر بالنشاط السيبراني، فإنّ العالم يعيش في ما يُسمى «حالة من عدم السلام»، أيّ حالة من التنافس بين الدول وسطَ طيفٍ يقع أسفل عتبة العنف المدّمر مادياً، لكن آثاره الضارة تتجاوز مستوى المنافسة المسموح به في زمن السلم⁽³⁴⁾.

والكثير من الدول، اليوم، قادر على استخدام الأدوات السيبرانية بشكل فاعل، نظراً إلى أن الأجهزة، والتقنيات السيبرانية، أصبحت أكثر تقدماً، وأكثر انتشاراً، وبعض هذه الدول قادرٌ على شنّ هجمات سيبرانية يصُعب معها تحديد الحدّ الفاصل بين آثار بعضها الذي لا يصل إلى مستوى القوة المسلحة، وبعضها الآخر الذي يصل إلى مستوى القوة المسلحة. ويبدو أنّ كثيراً من الدول، والجهات الفاعلة غير الحكومية يستخدم الهجمات السيبرانية للإفلات من العقاب، ولعلّهم أنّ هجماته السيبرانية، على الأرجح، لن تؤدي إلى أن يرذّ الخصم عليها، ردّاً حركياً مسلحاً.

وإنّ التقلبات في عملية تحديد المسؤولية عن الهجمات السيبرانية داخل المجتمع الدولي، وإمكانية الوصول إلى قواعد إسناد صارمة تُشكّل كلّها تحدياً قانونياً كبيراً. والتحدّي القانوني المتعلق بإسناد الهجمات السيبرانية غير الشرعية يُعدّ مشكلة يجب حلّها، لأنّ عملية الإسناد تهدف إلى تحديد الأفعال غير الشرعية، وإلى تحديد المسؤولية عنها.

وبالاعتماد على قواعد لجنة القانون الدولي، تتمثل نقطة الانطلاق، في السياق السيبراني، في كَوْن الدولة تتحمّل مسؤولية دولية عن الفعل الذي يُعزى إليها المتعلق بالفضاء السيبراني⁽³⁵⁾.

وتتحمل الدول المسؤولية عن أيّ فعل غير شرعي متعلق بالساير يقوم به بعض مسؤوليها، أو بعض التابعين لها من وكلاء، أو مقاولين، أو جهات فاعلة غير حكومية، ما دامت تُسيطر على أفعال هؤلاء سيطرةً

⁽³⁴⁾ Lucas Kello, *The Virtual Weapon and International Order*, (Great Britain: Yale University press New Haven and London, 2017, p. 78).

⁽³⁵⁾ *Tallinn Manual 2.0 On the International law applicable to Cyber Operations*, Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defense Centre of Excellence, General editor Michael N. Schmitt, (USA: Cambridge University Press, 2017, Rule 14, p. 84).

فعلية⁽³⁶⁾. ولا يمكن للدول أن تهرب من المسؤولية القانونية عن الأفعال غير الشرعية التي ترتكبها عبّر وكلاء⁽³⁷⁾.

وفي نطاق الهجمات السيبرانية التي تأتي في سياق نزاع دولي مسلح، وهي قد تطوي أفعالاً غير شرعية، وانتهاكات للقانون الإنساني الدولي، فإن الجهة التي تتحمل المسؤولية هي الدولة. وإن أحد الشروط الأساسية لتحصيل المسؤولية الدولية لدولة ما، هو أن يُعزى السلوك غير الشرعي إلى هذه الدولة بموجب القانون الدولي⁽³⁸⁾.

ومع مرور الوقت، تتطور الآليات التقنية، والقانونية التي تسمح بتحديد مستوى مشاركة دولة ما في عمليات سيبرانية للإعلان عن أنّ هذه الدولة مسؤولة قانوناً عن عمل سيبراني. فالدول، اليوم، أكثر قدرة على إسناد الهجمات السيبرانية مما كانت عليه قبلاً سنوات خلت. ومع ذلك، فإن البيئة التقنية تتسم بالديناميكية، وبالتحسّن المستمر، إذ إنّ الأدوات التقنية الجديدة تعمل باستمرار إمّا على تحسين قدرات الإسناد، وإمّا على إعاقتها. فالغش، والقدرة على التخفي، وعلى تطوير العمليات السيبرانية يؤديان إلى تعقيد عملية الإسناد، وعملية الاستجابة، خصوصاً عندما يكون هناك حاجة إلى استجابة فورية، ضدّ دولة تُعدّ الجاني المشتبه فيه الذي قام بالعملية السيبرانية⁽³⁹⁾.

ومع استمرار العلاقات الدولية السيبرانية، تستفيد بعض الدول المتقدّمة، التي لديها القدرات السيبرانية الهجومية عالية المستوى، من عدم وجود قواعد صريحة تساهم في إسناد مسؤولية إليها إذا ما قامت بعمليات سيبرانية ضدّ دول ضعيفة. وفي الوقت نفسه، إنّ الخلّ في عملية الإسناد الحاصل بين الدول القوية، والدول الضعيفة، يُعادل سباق التسلح الذي يأخذ شكل سباق بين التقدّم في الكشف عن المسؤول، والتهرب من الكشف عن هذا المسؤول. وهذا التهرب أصبح، اليوم، سهلاً، لذلك يمكن للدول التي ليس لديها قدرات إسناد متقدّمة أن تستمرّ في إخفاء نفسها، بشكل موثوق به⁽⁴⁰⁾.

ونظراً إلى أنّ معظم الدول المتقدّمة سيبرانياً تُدرك مخاطر التصعيد السيبراني، فإن لدى هذه الدول

(36) Tallinn Manual 2.0, op. cit, Rule 15, p. 87.

(37) Ibid, Rule 17, p. 92_95.

(38) يُراجع المواد 1 حتى 11، من مشاريع المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دولياً، تقرير لجنة القانون الدولي إلى الجمعية العامة عن أعمال دورتها الثالثة والخمسين، حولية لجنة القانون الدولي، م. 2، ج. 2، (الأمم المتحدة: 2001، ص 32).

(39) Brian J. Egan, *Remarks on International Law and Stability in Cyberspace*, Berkeley Journal of International Law, vol. 35, Issue 1, (2017), p. 177.

(40) *Cyber Strategy, Summary*, U.S. Department of Defense, (USA, 2018), p. 1. (https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF) (last site visit november 2025).

سبباً وجيهاً لتكون أكثر شفافية بشأن عملية الإسناد، وأكثر مَيلاً إلى تبادل المعلومات المتاحة لديها حول العمليات السيبرانية مع الدول غير المتقدمة سيبرانياً. ولكن مخاوف الدول حول الكشف عن مصادر استخباراتها، وعن الأساليب التقنية المتبعة في عمليات الإسناد، ما زالت تُعدّ عائقاً أمام القيام بعمليات إسناد المسؤولية بشكل شفاف. وأخيراً، يبدو أنّ هناك حاجة إلى وضع معايير دولية تُوضّح طرق الإسناد، وتُنظّمها، بشكل يُساعد الدول في الكشف عن مصادر الهجمات، وفي تحديد المسؤول عن الانتهاكات، والأفعال غير الشرعية.

2. انطباق القانون الإنساني على أنظمة أسلحة المستقلة وتحديات فرض المسؤوليات القانونية.

الاستقلال في أنظمة الأسلحة، يعني قدرة هذه الأنظمة على اختيار الأهداف، والتعامل معها، بشكلٍ مستقل عن أيّ مشغّل بشري، وذلك بناءً على الاستنتاجات التي تستخلصها من المعلومات المُجمّعة فيها، ومن قيودها المبرمجة مُسبقاً. وأنظمة الأسلحة المستقلة ليست أسلحة المستقبل فحسب، بل أسلحة الحاضر أيضاً، لأنها موجودة اليوم، ومُستخدَمة. هذه الحقيقة لها آثار عميقة على النقاش حول قانونية استخدام هذه الأسلحة. والسؤال الحاسم ليس حول ما إذا كان ينبغي حظر بعض هذه الأسلحة، أم لا، بل كيف يمكن استخدام القانون على أفضل وجه من أجل تنظيمها؟

وقد رأى بعض الباحثين أنه من المستحيل تطوير أنظمة أسلحة يمكنها الامتثال لقواعد القانون الإنساني الدولي، لأن مصطلحات القانون الإنساني الدولي كالمدنيين، والمقاتلين، والمشاركة المباشرة في الأعمال العدائية، وما إلى ذلك، لا تخضع لتعريفات دقيقة، يمكن برمجتها، وترجمتها إلى شيفرات، وتضمينها في آلة⁽⁴¹⁾. وأمام هذا الواقع يَرْتَبِئ سؤالان: هل يمكن أن ينطبق القانون الإنساني الدولي الحالي على هذه الأنظمة؟ وهل يمكن تحديد المسؤولين عن الهجمات التي تؤدي إلى انتهاك القانون الإنساني؟ وللإجابة عن هذين السؤالين تم تقسيم هذا المبحث إلى المطلبين الآتيين:

1.2. انطباق القانون الإنساني على أنظمة الأسلحة المستقلة.

2.2. المسؤولية عن انتهاك مبادئ القانون الإنساني أثناء استعمال الأسلحة المستقلة.

1.2. انطباق القانون الإنساني على أنظمة الأسلحة المستقلة.

إنّ أنظمة الأسلحة المستقلة التي يُطلق عليها اسم «الروبوتات القاتلة»، أو «الروبوتات المستقلة القاتلة»، أو «أنظمة الأسلحة الذاتية التشغيل»، تتّصف بأنها:

— أنظمة أسلحة تتمتع بالاستقلالية في عملها، وتعمل دون مُشغّل بشري، أو بإشراف مُشغّل بشري يُتخلّى

(41) Thompson Chengeta, *Measuring autonomous weapon systems against international humanitarian law rules*, Journal of law and cyber warfare, Editor-in-Chief, Daniel B. Garrie, Partner, Law & Forensics, Vol. 5, Issue 1, (Summer 2016), p. 63.

عن إشرافه بَعْدَ تنشيط نظام السلاح⁽⁴²⁾.

- تمتلك استقلالية الخيار في اختيار الأهداف أثناء النزاع المسلح، وفي استخدام القوة المميتة ضدها.
 - تمتلك مواصفات تقنية وفنية، وذكاءً صناعياً يُمكنها من تعلُّم كيفية التصرف في ميدان النزاع، ومن تكيف عملها مع المتغيرات التي تطرأ على أرض النزاع.
 - قدرة على اتخاذ الإجراءات اللازمة أثناء النزاع، وتحديد طريقة التصرف دون الاعتماد على مُشغِّل بشري. وقادرة على تحديد الأهداف، والاشتباك معها، ثم مهاجمتها⁽⁴³⁾.
- وفي أيِّ حال من الأحوال، قد تكون المزايا والمواصفات التي تتمتع بها أنظمة الأسلحة المستقلة، دوافع إلى استخدام هذه الأنظمة، ولكن على الرغم من ذلك تبقى هذه الأنظمة خاضعة لمبادئ القانون الدولي الإنساني، ويجب أن تكون قادرة على الالتزام بمبادئه.
- ومن الجلي أن اتفاقيات جنيف، وبروتوكولها الإضافيين لا تتحدث عن أنظمة الأسلحة المستقلة، لأنه لم يكن لهذه الأنظمة وجود عند وُضْع هذه الاتفاقيات، ولم يكن يَخْطُر ببال واضعها أن حروباً سوف تُخاض بواسطة وسائل حربية غير بشرية تستطيع الواحدة منها المحاربة كأنها مقاتل بشري بحدِّ ذاته، ومَنْ يستعملها من البشر يُراقب عملها من بعيد، ويتدخل فيه حينما يريد.
- ولكن ليس هناك شك في أن تطوير الأسلحة، واستخدامها في النزاعات المسلحة، والالتزام بإجراء مراجعات قانونية أثناء دراسة سلاح جديد، أو تطويره، أو حيازته، أو اقتنائه، أعمال تخضع للقانون الإنساني الدولي، وفقاً لما تقتضيه المادة 36 من البروتوكول الإضافي الأول⁽⁴⁴⁾. وهذا ينطبق على أنظمة الأسلحة المستقلة التي يجب أن تكون قادرة على التكيف مع مبادئ: أخذ الاحتياطات اللازمة، والتناسب، والتمييز، المعنيّة بالتخفيف من آثار الحرب على المدنيين.

ومبادئ القانون الإنساني، لا يمكن أن تلتزم بها أنظمة الأسلحة المستقلة، لأن هذه المبادئ تحتاج إلى

(42) كريستوف هاينز، تقرير المقرر الخاص المعني بحالات الإعدام خارج نطاق القضاء أو بإجراءات موجزة أو تعسفاً، مجلس حقوق الإنسان، الدورة 23، 9 نيسان 2013، الأمم المتحدة، A/HRC/23/47، الفقرة 37، ص 10.

(43) SEE. *MIND THE GAP*, The Lack of Accountability for Killer Robots, The International Human Rights Clinic (IHRC), Harvard Law School, Human Rights Watch, USA, (2015), p. 6.

(44) المادة 36 من البروتوكول الأول، شريف عتلم، محمد ماهر عبد الوهاب، موسوعة اتفاقيات القانون الدولي الإنساني، النصوص الرسمية للاتفاقيات والدول المصدقة والموقعة، ط. 6، (القاهرة: إصدار بعثة اللجنة الدولية للصليب الأحمر بالقاهرة، 2002)، ص 283.

قُدرة الإنسان على جمع المعلومات، وتحليلها، والتعامل مع واقع النزاع بناءً على ما يستوجبه الضمير الإنساني القويم، ولأنها تتضمن تعقيدات لا يمكن أن تُضَمَّن في برامج هذه الأنظمة، ومن هذه التعقيدات: تعريف المدنيين، والمقاتلين، ومفهوم المشاركة المباشرة في الأعمال العدائية.

لذلك فإنَّ نشر أنظمة أسلحة مستقلة لا تقدر على التمييز بين المدنيين والمقاتلين يُعدّ انتهاكاً للقانون الإنساني الدولي، وأمرًا لا يُمكن قَبوله في بيئات النزاعات المسلحة الفوضوية التي يُمكن أن يكون فيها المدنيون جزءاً من ساحة النزاع، لأنَّ قرارات استهداف المقاتلين، أو المدنيين تحتاج إلى الضمير الإنساني القويم، ولا يمكن تفويض هذه القرارات إلى أنظمة أسلحة لا يُعرف مدى قُدرتها على التعامل مع واقع النزاعات المتغيّر.

وتصُعب ترجمة بعض جوانب القانون الدولي الإنساني، كي تُضَمَّن في برنامج كمبيوتر، ومن هذه الجوانب التوجيه التفسيري الذي وَضَعته اللجنة الدولية للصليب الأحمر بشأن مفهوم المشاركة المباشرة في الأعمال العدائية، أو التفسيرات المختلفة التي وَضَعتها بعض الدول لهذا المفهوم؛ ففي سياقات النزاعات اليوم، يُشارك المدنيون بشكل مباشر في الأعمال العدائية، مما يجعل تطبيق مبدأ التمييز صعباً على الجنود العاديين، فما حال الأسلحة المستقلة⁽⁴⁵⁾؟

وإذا كان لا بدّ من برمجة روبوت، فإنه لا يمكن، في أي حال من الأحوال، أن يُبرَمَج على أن «هذا يعتمد على كذا»، أو على أن «يُسْتَخْدَم حكماً منطقياً»، وبعبارة أخرى، لا يمكن أن تَتِمَّ برمجته على أنَّ الإجراء المناسب يعتمد على موقف محدد دون توضيح الإجراء الذي يجب أيُّ يتَّخذ في هذا الموقف؛ وتبقى الحاجة إلى وضوح كيف يتصرف هذا الروبوت أولويةً عند وَضْع برنامج كمبيوتر عن العوامل التي يعتمد عليها قرار الاستهداف، وكيفية تحديد تلك العوامل⁽⁴⁶⁾.

وترتسم أمام استخدام أنظمة الأسلحة المستقلة مشكلةٌ تتعلق بالقُدرة على تصنيف العمل الذي يقوم به المشارك في الأعمال العدائية بأنه مشاركةٌ مباشرة، وليس مشاركةً غير مباشرة.

وفي كثير من الحالات، يمكن أن يشارك شخص ما بشكل غير مباشر في المجهود الحربي الذي يقوم به أفراد القوات المسلحة، لكنَّ هذه المشاركة لا تؤدي إلى فقدانه الحماية من الاستهداف. ومن الأمثلة على هذه المشاركة، المشاركة في إنتاج الأسلحة، وبيعها، ونقلها، وتوفير الأموال، والإدارة، والدعم السياسي، وصيانة البنية التحتية العسكرية، وفي هذه الحالة تحتاج أنظمة الأسلحة المستقلة، ولا سيما تلك التي لا تخضع لتحكُّم بشريّ ذي معنى بعد تنشيطها، إلى ذكاء اصطناعي مكافئ للذكاء البشري كي تتمكن من التمييز بين المشاركة المباشرة في

(45) Marco Sassóli, Autonomous Weapons and International Humanitarian Law: Advantages, Open Technical Questions and Legal Issues to be Clarified, International Law Studies, U.S Naval College, vol. 90, (2014), p. 313.

(46) Marco Sassóli, op. cit, p. 329.

الأعمال العدائية، والمشاركة غير المباشرة، وهذا التمييز يُعدّ تمييزاً نوعياً⁽⁴⁷⁾.

أما القيود الزمنية المتعلقة بموعد استهداف المدني المشارك مباشرة في الأعمال العدائية فتُمثّل فكرة يصعب تضمينها في نظام سلاح مستقل، لأن المدني ليس سوى هدف مشروع في الوقت الذي يُشارك فيه في القتال، ولكن هذا القيد الزمني يُعدّ عند بعض الباحثين شرطاً غير عادل لأنه يُتيح لبعض المدنيين أن يكونوا مُزارعين في النهار، ومقاتلين في الليل، من أجل أن يَفِرّوا من استخدام القوة غير الشرعي. وفي هذه الحالة ليس بإمكان نظام سلاح مستقل أن يتمكّن من فهم واقع المدنيين الذين يشاركون في العمليات العدائية ليلاً ويَكفّون عنها نهاراً، وليس بإمكانه تحديد أيّ خيار سيتخذه عند استهداف هؤلاء المدنيين.

ويطرح شرطُ مهاجمة المدنيين أثناء مُدّة مشاركتهم في الأعمال العدائية، فقط، تحدّيات خاصة في مجال مكافحة الإرهاب. لأنه في بعض الحالات يُعدّ الإرهابيون مدنيين، وبسبب سرّيّة عملياتهم، فإنه من الصعب، إن لم يكن من المستحيل، تحديد النقطة التي يمكن للمرء أن يقول فيها: إنهم يشاركون مباشرة في الأعمال العدائية. ففي العمليات التي قامت بها بعض الدول ضدّ الإرهاب، بواسطة طائرات بلا طيار (Drones)، مثلاً، لم يكن استهداف الإرهابيين على أساس المشاركة المباشرة في الأعمال العدائية فحسب، بل على أساس عضويتهم في منظمة إرهابية، أيضاً، أو على أساس الاشتباه في عضويتهم. فقد تمّ تنفيذ هجمات، من قبل بعض الدول، ضدّ الإرهابيين المُشتَبَه بهم، خارج ساحة المعركة، حيث تمّ توجيه هذه الهجمات في سلسلة من المناطق المضطّربة، أو الخارجة على القانون، في عدد من البلدان في جميع أنحاء الشرق الأوسط⁽⁴⁸⁾.

واستهداف الأفراد على أساس أنهم أعضاء في منظمة إرهابية معيّنة، أو أعضاء مُشتَبَه بهم، يتعارض مع مبدأ التمييز⁽⁴⁹⁾. وقد يكون لهذا استهداف تداعيات على أمن المدنيين؛ ولهذا السبب، يجب الاعتراض على استخدام أنظمة أسلحة مستقلة من أجل القيام بعمليات الاستهداف، ويجب التحذير من هذه الأنظمة المستقلة التي يمكن أن تكون أشدّ خطراً على المدنيين من الطائرات بلا طيار (Drones).

2.2. المسؤولية عن انتهاك القانون الدولي الإنساني أثناء استخدام أنظمة الأسلحة المستقلة.

إن استخدام أنظمة أسلحة مستقلة لا يُسيطر عليها البشر أثناء النزاعات المسلحة، بدلاً من أسلحة يُسيطر عليها البشر، وعدم القدرة على تحديد الجهة المسؤولة عن أيّ انتهاك يحصل أثناء استخدام هذه

(47) Autonomous weapon systems: technical, military, legal and humanitarian aspects, expert meeting, International Committee of the Red Cross, Geneva, Switzerland, (26 to 28 March 2014). p. 7_8.

(48) Anthony Dworkin, *Drones and targeted killing: defining a european position*, European council of foreign relations, Policy brief, (July 2013), p. 1.

(49) Genevieve Lennon and Clive Walker, *Routledge Handbook of Law and Terrorism*, first edition (United Kingdom, London: Taylor & Francis Ltd, 2015, p. 58).

الأنظمة، أمران قد يؤديان إلى ما يمكن أن يُسمى فجوة المسؤولية.

وقد لَحَّصَ بعض الخبراء العقبات التي تَحُولُ دون قُدرة أنظمة الأسلحة المستقلة على الامتثال لقواعد القانون الدولي الإنساني، بما يأتي: الموثوقية، وعدم اليقين بمآلات التشغيل في غياب الإشراف البشري، ومخاطر التداخل، وقابلية الكشف (أي إمكانية اختراق البرنامج بناءً على هجوم سيبراني)، والتأخر في معالجة الخوارزميات في الحالات المُعقَّدة، والتأخر في البحث في مفاهيم التعلُّم الذاتي، والتقويم الذاتي والتدريب، وتطوير الذكاء الاصطناعي، سواء بَعْدَ التصنيع، أم عَبرَ الفضاء السيبراني. هذه العقبات التي تُفرض نفسها على عمل الأنظمة المستقلة تُعدّ عائقاً كبيراً في طريق إمكانية تحديد المسؤولية عن الانتهاكات التي قد تحصل أثناء استخدام هذه الأنظمة في النزاعات المسلحة، وهذا ما يستدعي وجود اتجاه إلى حَظَر هذه الأنظمة.

وفي مقابل ذلك ظهرت آراء تتصور أنه في سياق الحرب ليس هناك واقع مثالي، ولا يُعدّ وجود ثغرات في المسؤولية، حُجّةً لِحَظَر استخدام هذه الأنظمة. وبدلاً من هذا الحظر، يجب القبول بحتمية فجوات المسؤولية في سياق الحرب، بنفس الطريقة التي يُقْبَلُ فيها مثل هذه الفجوات في المواقف الأخرى، ومثال هذه المواقف: انهيار جسر تسبب بحادث مميت، فقد نجد أنفسنا في موقف لا يمكن فيه مُساءلة أحد، وبالتالي، إذا تمّ بناء الجسر وفقاً للتشريعات والقواعد والمعايير، وإذا لم يكن من الممكن تَوَقُّع الظروف التي أدّت إلى انهياره، على الرغم من الحسابات الدقيقة، فإننا نقبل أن هناك فجوة طبيعية في المسؤولية قد تأتي على شكل تسامح هندسي (Engineering Tolerance)⁽⁵⁰⁾.

وبالانتقال إلى واقع تنظيم أنظمة الأسلحة المستقلة، فإن هناك مشكلة تتعلق بالقدرة على تحديد مسؤولية المُستخدِم (المسؤولية الجنائية)، ومسؤولية الجهة التي صنعت هذه الأنظمة (مسؤولية المنتج)⁽⁵¹⁾. فنَشُر أنظمة أسلحة مستقلة لا يعني أن الجهة الرئيسية التي نشرتها يمكن أن تَتَجَنَّب المسؤولية، ويُقاس هذا على قضية، استخدام الأطفال على أنهم جنود، هذا الأمر الذي لا يخلق فجوة في المسؤولية، حيث يَتِمّ إسناد المسؤولية إلى القائد المسؤول عن استخدامهم⁽⁵²⁾.

وهنا يمكن أن تكون المسؤولية مخصصة لمستوى الجنرال أو الرئيس، الذي يُقرّر نَشْر نظام سلاح مستقل مُميت أو عدم نَشْرِهِ، وبعد ذلك، يَتِمّ تحميله المسؤولية إذا حدث خطأ ما. وكذلك، يمكن القول: إنَّ أيّ

(50) Vincent C. Müller and Thomas W. Simpson, Autonomous Killer Robots Are Probably Good News, Sociable Robots and the Future of Social Relations, Frontiers in Artificial Intelligence and Applications, vol. 273, los press, (2014), p. 304.

(51) Vincent C. Müller and Thomas W. Simpson, Killer Robots: Regulate, Don't Ban, BSG Policy Memo, (November 2014). (<https://philpapers.org/archive/MLLKRR.pdf>) (last site visit november 2025).

(52) Müller and Simpson, Killer Robots, op. cit.

نموذج يُحدّد سلسلة مسؤوليات بمعزلٍ عن الأطراف المعنية بانتهاكات قد تحصل أثناء نزاع مسلح لا ينبغي أن يُوضَّع مُسَبِّقاً، بل ينبغي أن تُراعى، عند وَضْعِهِ، إمكانية أن تتحمّل تلك الأطراف المسؤولية عن تلك الانتهاكات. وليس غريباً عن الواقع أن يُحمّل مبدأ مسؤولية القيادة عن الإهمال قائداً ما المسؤولية عن عدم منعه ارتكاب انتهاك ما، أو عن عدم معاقبته المُرتكِب. والمواقف التي يعجز فيها القائد عن منع أيّ عمل غير شرعي يقوم به مرؤوسه، يتحمل المسؤولية نيابةً عنهم لأنّ من المفترض أن يكون للقائد سيطرة فعّالة، وأن يكون له قدرة على منع المخالفات المحتملة. وبالتالي، فإنّ مسؤولية القيادة تستوجب، عندما يتعلق الأمر بأنظمة الأسلحة المستقلة، منظوراً إنسانياً، وتساوياً عمّا إذا كان القادة العسكريون في وَضْعٍ يسمح لهم بفهم برمجة هذه الأنظمة المُعقّدة فهماً يُبرّر مسؤوليتهم الجنائية.

وإذا لم يكن بالإمكان، عملياً، العثور على قائد، أو مُبرمج، أو صانع، ليكون مسؤولاً عن الانتهاكات، فإنّه يُخشى أن تكون هناك فجوة في تحمّل المسؤولية من شأنها أن تُتيح الإفلات من العقاب بسبب استخدام أنظمة الأسلحة المستقلة.

وهنا يمكن وَضْعُ إعلانٍ سياسيٍّ دوليٍّ يؤكد أمراً أساسياً مفاده أن من مسؤولية البشر: (أ) اتخاذ القرارات النهائية في ما يتعلق باستخدام القوة، و(ب) التحكم في منظومات الأسلحة الذاتية التشغيل⁽⁵³⁾. ويمكن أن يُعقَّب ذلك وَضْعُ مدوّناتٍ لقواعد السلوك، ومزيدٍ من تدابير بناء الثقة. وتضمن هذه المدوّنات وظيفة استعراضٍ للتكنولوجيا الحربية المتطورة. ولكن هذا الإعلان السياسي ينبغي أن يكون خطوة مرحلية تُسبق إبرام صكٍّ مُلزم قانوناً يمكن أن يتخذ شكل بروتوكول جديد يُضاف إلى اتفاقية الأسلحة التقليدية.

الخاتمة

تناولت هذه الدراسة موضوع الحرب السيبرانية والأسلحة المستقلة في إطار القانون الإنساني الدولي، وقد ركزت على مدى انطباق هذا القانون على استخدام هذا النوع الجديد من الحروب والوسائل القتالية الحديثة، وركزت على تحديد المسؤوليات عن انتهاك هذا القانون جراء استخدام هذه الأسلحة وأساليب القتال التي لم تلاحظها اتفاقيات جنيف والبروتوكولات الإضافية أثناء وضع نصوصها في عام 1949 وما بعده.

وانطلاقاً مما تناولته هذه الدراسة، يمكن القول في إطار ما وصلت إليه من نتائج: إنه في سياق الحرب السيبرانية يجب أن يَتِمَّ تصنيف العمليات السيبرانية بين هجمات، وغير هجمات، لكي تُعرّف الدول ما العمليات

(53) تقرير اجتماع 2018 لفريق الخبراء الحكوميين المعني بالتكنولوجيات الناشئة في مجال منظومات الأسلحة الفتاكة الذاتية التشغيل، جنيف، 9_13 نيسان/أبريل 2018 و 27 - 31 آب/أغسطس 2018، (CCW/GGE.1/2018/3)، الفقرة 48، ص 27_28.

التي يُسَمَح بتوجيهها ضدّ العدو، بموجب مبادئ القانون الإنساني الدولي عامة، وما تلك التي لا يُسَمَح بها.

أما في ما يتعلق بمبادئ القانون الإنساني الدولي ولا سيما: التمييز، والتناسب، والضرورة العسكرية، وأخذ الاحتياطات اللازمة أثناء الهجوم، فإن هذه المبادئ تتضمن تعقيدات كثيرة كتعريف المقاتلين، وتعريف الأهداف العسكرية، ومفهوم مشاركة المدنيين المباشرة في الأعمال العدائية، ومفهوم أخذ الاحتياطات اللازمة أثناء الهجوم، وغيرها من المفاهيم المعقّدة. هذه التعقيدات تحتاج إلى قدرات الإنسان على جمع المعلومات، وتحليلها، والتعامل مع واقع النزاع المسلح بناءً على ما يستوجبه الضمير الإنساني القويم، وهذه القدرات الإنسانية ليست مُتَوَفِّرة لأنظمة الأسلحة المستقلة، لذلك، فإنّ هذه الأنظمة لا يُمكن أن تلتزم بمبادئ القانون الإنساني، وما تتضمنه من مفاهيم مُعقّدة.

وأما في ما يتعلق بالمسؤولية عن انتهاك القانون الإنساني الدولي، فإنّ الدول تُعدّ الجهة التي يمكن أن تتحمّل المسؤولية عن الهجمات السيبرانية التي تأتي في سياق نزاع دولي مسلح، والتي تنطوي على أفعال غير شرعية، وعلى انتهاكات للقانون الإنساني. أمّا المسؤولية عن الانتهاكات التي قد تنتج عن استخدام أنظمة الأسلحة المستقلة، فالجهات التي يمكن أن تتحمّلها كثيرة، أبرزها: الأشخاص الذين يقومون ببرمجة هذه الأنظمة، والقادة والجنود الذين يُنْشِرونها، والدول التي تُجيز استخدامها.

وفي الختام، لا بدّ من القول: إن استخدام أسلحة جديدة واستعمال أساليب قتالية حديثة لم يتمّ ذكرها ضمن قواعد القانون الإنساني الدولي العرفي، واتفاقيات جنيف، يجب أن يكون يتوافق مع هذه القواعد المعمول بها، فهي كافية للدول لتسترشد بها في حروبها، ولكي تتجنب استهداف المدنيين وتخفيف آلام الحرب عنهم. ولا بدّ، أيضاً، من تطوير قواعد القانون الإنساني بما يتناسب مع مستجدات الحروب ووسائلها.

قائمة المراجع

- تقرير اجتماع 2018 لفريق الخبراء الحكوميين المعني بالتكنولوجيات الناشئة في مجال منظومات الأسلحة الفتاكة الذاتية التشغيل، جنيف، 13_9 نيسان/أبريل 2018 و 27 - 31 آب/أغسطس 2018، (CCW/GGE.1/2018/3).
- شريف عتلم، ومحمد ماهر عبد الوهاب، موسوعة اتفاقيات القانون الدولي الإنساني، النصوص الرسمية للاتفاقيات والدول المصدقة والموقعة، ط. 6، (القاهرة: إصدار بعثة اللجنة الدولية للصليب الأحمر بالقاهرة، 2002).
- كريستوف هاينز، تقرير المقرر الخاص المعني بحالات الإعدام خارج نطاق القضاء أو بإجراءات موجزة أو تعسفاً، مجلس حقوق الإنسان، الدورة 23، 9 نيسان 2013، الأمم المتحدة، A/HRC/23/47.

- مشاريع المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دولياً، تقرير لجنة القانون الدولي إلى الجمعية العامة عن أعمال دورتها الثالثة والخمسين، حولية لجنة القانون الدولي، م. 2، ج. 2، (الأمم المتحدة: 2001).
- هيربرت لين، النزاع السيبراني والقانون الدولي الإنساني، مختارات من المجلة الدولية للصليب الأحمر، عدد 886، المجلد 94، (صيف 2012).
- Anthony Dworkin, *Drones and targeted killing: defining a european position*, European council of foreign relations, Policy brief, (July 2013).
- Autonomous weapon systems: technical, military, legal and humanitarian aspects, expert meeting, International Committee of the Red Cross, Geneva, Switzerland, (26 to 28 March 2014).
- Brian J. Egan, *Remarks on International Law and Stability in Cyberspace*, Berkeley Journal of International Law, vol. 35, Issue 1, (2017).
- *Cyber Strategy*, Summary, U.S. Department of Defense, (USA, 2018) (https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF) (last site visit november 2025).
- Genevieve Lennon and Clive Walker, *Routledge Handbook of Law and Terrorism*, first edition (United Kingdom, London: Taylor & Francis Ltd, 2015).
- *International Strategy for Cyberspace*, Prosperity, Security, and Openness in a Networked World the White House Washington, USA, May, 2011.
- Lucas Kello, *The Virtual Weapon and International Order*, (Great Britain: Yale University press New Haven and London, 2017).
- Marco Sassóli, *Autonomous Weapons and International Humanitarian Law: Advantages, Open Technical Questions and Legal Issues to be Clarified*, International Law Studies, U.S Naval College, vol. 90, (2014).
- *MIND THE GAP*, The Lack of Accountability for Killer Robots, The International Human Rights Clinic (IHRC), Harvard Law School, Human Rights Watch, USA, (2015).
- Paulo Shakarian and others, *Introduction to Cyber-warfare A Multidisciplinary Approach*, (USA: Syngress, Elsevier, 2013).
- Richard A. Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, (New York: Harper Collins, 2010).
- *Tallinn Manual 2.0 On the International law applicable to Cyber Operations*, Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defense Centre of Excellence, General editor Michael N. Schmitt, (USA: Cambridge University Press, 2017).
- *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 Defense Centre of Excellence, General editor: Michael N. Schmitt, (New York: Cambridge University Press, 2013).

- Thompson Chengeta, *Measuring autonomous weapon systems against international humanitarian law rules*, Journal of law and cyber warfare, Editor-in-Chief, Daniel B. Garrie, Partner, Law & Forensics, Vol. 5, Issue 1, (Summer 2016).
- Vincent C. Müller and Thomas W. Simpson, *Autonomous Killer Robots Are Probably Good News*, Sociable Robots and the Future of Social Relations, Frontiers in Artificial Intelligence and Applications, vol. 273, Ios press, (2014).
- Vincent C. Müller and Thomas W. Simpson, *Killer Robots: Regulate, Don't Ban*, BSG Policy Memo, (November 2014). (<https://philpapers.org/archive/MLLKRR.pdf>) (last site visit november 2025).