القانون الدولي الإنساني والحرب السيبرانية في النزاعات المسلحة غير الدولية

مقدم من الباحث

محمد صبحي حسن علي الفار
مدرس مساعد بقسم القانون الدولي العام
كلية الحقوق جامعة الزقازيق

أمل عمرو عبدالغني
مدرس مساعد بقسم القانون الدولي العام
كلية الحقوق جامعة الزقازيق

المقدمة

شهد العالم في العقود الأخيرة تطوّرًا تكنولوجيًّا مذهلًا أدّى إلى إعادة تشكيل طبيعة النزاعات المسلّحة، فلم تعد الحروب مقتصرة على المواجهات التقليدية فحسب، بل امتدّت لتشمل هجماتٍ تُدار عبر الفضاء الإلكتروني. وفي خضمّ تزايد الاعتماد على التقنيات الرقمية والتواصل الشبكي، باتت الهجمات السيبرانية عنصرًا محوريًّا في النزاعات المسلحة غير الدولية (NIACs)، نظرًا لقدرتها على شلّ البنية التحتية الحيويّة وإضعاف الاقتصادات الوطنية وتهديد الأمن والاستقرار على نطاق واسع.

يُسلّط هذا البحث الضوء على الإطار القانوني الدولي الذي يحكم الهجمات السيبرانية في النزاعات المسلحة غير الدولية، مستندًا في الأساس إلى مبادئ القانون الدولي الإنساني (IHL) وقواعده. ورغم وضوح تلك المبادئ—كوجوب التمييز بين الأهداف العسكرية والأعيان المدنية، ومراعاة مبدأ التناسب، واحترام الضرورة العسكرية—إلا أنّ تطبيقها في المجال السيبراني لا يخلو من تحدّياتٍ معقّدة، أبرزها صعوبة تحديد المسؤولية القانونية عن الهجوم السيبراني وصعوبة إثبات نسبة الهجوم إلى دولةٍ أو طرفٍ بعينه، علاوة على غموض الإطار المحدود الذي يُنظّم دور الفاعلين من غير الدول في النزاعات السيبرانية.

ضمن هذا السياق، يستعرض البحث عددًا من الحالات الدراسية التي تُبيّن مدى خطورة الهجمات السيبرانية، مثل الهجمات التي طالت البنية التحتية الأوكرانية، فضلًا عن أبعاد الحرب النفسية وحرب المعلومات في العالم الافتراضي. كما يبحث في مدى التزام الجماعات المسلّحة غير التابعة للدول بقواعد القانون الدولي الإنساني، والتحدّيات الناشئة عن افتقارها لصفة "الدولة" في نظر المجتمع الدولي.

ولأجل تعزيز الحماية القانونية في هذا المجال، يتناول البحث جملةً من التوصيات، أبرزها: تحديث المعاهدات الدولية القائمة لتشمل العمليات السيبرانية صراحةً، وتطوير آليّات قانونية متخصّصة في هذا النوع من الحروب الرقمية، وتفعيل دور المحاكم الدولية—وبالأخص المحكمة الجنائية الدولية (ICC)—في محاسبة المنتهكين. ويُختتم البحث بالتشديد على ضرورة مواصلة التعاون الدولي وتكثيف الجهود التشريعية والرقابية، ضمانًا لإرساء قواعدٍ أكثر وضوحًا وصلابةً في ميدان النزاعات السيبرانية.

وعلي هدي ما سبق سيتم تقسيم البحث علي النحو التالي:

المبحث الأول: دور الجهات المسلحة من غير الدول في النزاعات المسلحة غير الدولية (NIACs)

المطلب الأول: الإطار القانوني لمسؤولية الجهات المسلحة من غير الدول

المطلب الثاني: الآثار الناجمة عن الهجمات السيبرانية

المبحث الثاني: القانون الدولي الإنساني (IHL) والهجمات السيبرانية في النزاعات المسلحة غير الدولية (NIACs)

المطلب الأول: لمحة عامة عن النزاع المسلح غير الدولي (NIAC) والإطار القانوني للقانون الدولي الإنساني

المطلب الثاني: دور الجهات المسلحة من غير الدول في النزاع المسلح غير الدولي (NIAC)

المبحث الأول

دور الجهات المسلحة من غير الدول في النزاعات المسلحة غير الدولية (NIACs)

يستدعي الخوض في دور الجهات المسلحة من غير الدول في النزاعات المسلحة غير الدولية (NIACs) استحضار السياق التاريخي والقانوني لتطوّر هذه الجهات وطبيعة انخراطها في الأعمال العدائية. فقد شهدت العقود الأخيرة تنامياً ملحوظاً لنفوذ المجموعات المسلحة التي لا تتبع لدولةٍ بعينها، سواءٌ كانت تعمل بصورةٍ منظَّمة ولها بنية هرمية واضحة، أم تتبع أساليب لامركزية يصعب تتبُّعها أو محاسبة مكوِّناتها. وينبع هذا التوسّع من عدّة عوامل، أبرزها سهولة حصول تلك الجهات على الموارد المالية واللوجستية عبر الأسواق السوداء، إضافةً إلى تسخيرها الأدوات التكنولوجية الحديثة – وخصوصاً الهجمات السيبرانية – في تنفيذ أنشطتها. وفي ظلّ هذا الواقع، تتفاقم التحدّيات أمام المجتمع الدولي والأطراف الرسمية لجهة مساءلة هذه الكيانات وردعها عن ارتكاب انتهاكاتٍ جسيمة للقانون الدولي الإنساني.

على أنّ الدور المتعاظم للجهات المسلحة من غير الدول لم يعد يقتصر على تنفيذ العمليات القتالية التقليدية، كالكمائن أو الهجمات على مواقع عسكرية أو مدنية، بل بات يمتد إلى الفضاء السيبراني الذي أصبح جزءاً لا يتجزأ من حروب العصر الحديث. وتتجلّى خطورة هذا التطوّر في قدرته على تسهيل تنفيذ عملياتٍ رقمية تستهدف البنى التحتية الحيوية

للخصوم، من دون أن تترك أثراً مادياً يُمكِّن من كشف الفاعلين أو تحرّكاتهم. كما تتعدّد دوافع تلك الجهات، فقد تسعى أحياناً إلى تحقيق مصالح سياسية أو اقتصادية أو عقائدية، ما يضفي المزيد من التعقيد على مسألة تصنيف أنشطتها ومساءلتها.

وعليه، تستدعي هذه التحوّلات توضيحاً دقيقاً للإطار القانوني الذي يضبط سلوك الجهات المسلحة من غير الدول، سواءٌ على صعيد القانون الدولي الإنساني أو القانون الدولي العام. وهو ما يُبرِز أهمية دراسة طبيعة المسؤولية القانونية الملقاة على عاتق هذه الجهات في النزاعات المسلحة غير الدولية، وخصوصاً عندما تستخدم الحرب السيبرانية كوسيلةٍ لتحقيق أهدافها. ومن شأن الوقوف عند الأُطر التعاهدية والعرفية، كالمادة ٣ المشتركة من اتفاقيات جنيف لعام ١٩٤٩ والبروتوكول الإضافي الثاني، أن يبيّن مدى شمولية أو قصور المنظومة القانونية حيال الممارسات السيبرانية. فالاضطراب الناجم عن غموض أحكام القانون في المجال الرقمي يحفّز البعض على استغلال هذه الثغرات لتحقيق مكاسب على حساب قواعد القانون الدولي.

وانطلاقاً من هذه الأهمية، يأتي المطلب الأول بعنوان: "الإطار القانوني لمسؤولية الجهات المسلحة من غير الدول"، ليُحاوِل رسم حدود المسؤولية وبيان الأسس التي يقوم عليها إلزام تلك الجهات باحترام قواعد النزاعات المسلحة وحقوق الإنسان. وتتزايد ضرورة تحديد هذا الإطار القانوني في ضوء ارتفاع وتيرة الهجمات السيبرانية، نظراً إلى ما يكتنف

تلك الهجمات من صعوباتٍ في التكييف القانوني وفي تحديد معايير الانتهاك وصور المسؤولية الجنائية المحتملة.

ويُمهّد هذا بدوره للمطلب الثاني الذي يتناول "الآثار الناجمة عن الهجمات السيبرانية"، إذ إنّ تسليط الضوء على هذه الآثار يُظهِر كيف يمكن للاعتداءات الرقمية أن تُلحِق ضرراً واسع النطاق بالبُنى التحتية الحيوية والأنظمة العسكرية والمدنية على السواء. ومن ثمّ، فإنّ الربط بين ضرورة تحديد المسؤولية القانونية للجهات المسلحة من غير الدول وإيضاح الآثار الخطيرة للهجمات السيبرانية يهدف إلى توضيح مدى الحاجة إلى تطوير أُطُر تشريعية جديدة ومعايير متقدّمة لضبط هذه الأعمال والحدّ من تبعاتها. إنّ التطرّق إلى هذه الجوانب مجتمعةً يتيح فهماً أشمل لدور الجهات المسلحة من غير الدول في النزاعات المسلحة غير الدولية، ويؤكّد ضرورة تكاتف الجهود الدولية لبلورة أحكامٍ قانونية فعّالة تُراعي تطوّر الأدوات القتالية وتنوّع الفاعلين في المشهد المعاصر.

المطلب الأول

الإطار القانوني لمسؤولية الجهات المسلحة من غير الدول

طبيعة الهجمات السيبرانية

يُعَدُّ أحد أهم الأسباب التي دفعت المجتمع الدولي للاهتمام بالحرب السيبرانية وأدواتها هو الاستغلال المتزايد للفضاء السيبراني. ويبدو أنّ

تاريخ ٢٤ فبراير ٢٠٢٢ سيُسجَّل في التاريخ بوصفه نقطة تحوُّل مهمة في العالم المعاصر، إذ تجسِّد الهجمات السيبرانية ضد أوكرانيا الطبيعة المتطوِّرة للصراعات الحديثة. وتؤكد هذه الهجمات على الدور المتنامي للفضاء السيبراني باعتباره ساحةً للقتال، كما تُظهِر أنّ إمكانية إحداث اضطرابات واسعة النطاق تتطلَّب تعزيز الأُطر القانونية الدولية لتنظيم سلوك الدول في الفضاء السيبراني. وتبرز تلك الهجمات السيبرانية وغيرها الحاجة الملحّة إلى التعاون الدولي من أجل مواجهة التحديات الناشئة عن العمليات السيبرانية خلال النزاعات المسلحة وبعد انتهائها. ويُعَدّ الإقرار بخطورة هذه التهديدات مسألةً ضروريةً للحفاظ على الاستقرار العالمي في عالمٍ بات يعتمد على الوسائل الرقمية بصورة متزايدة.

تعريف مصطلح "الهجمات السيبرانية"

يُشتَق مصطلح "سيبر (Cyber) "من كلمة "سيبرنيتيك " (Cybernetic)التي تدلّ على علم الاتصال ونظرية التحكم، والذي يركّز بشكل خاص على الدراسة المقارنة لأنظمة التحكم الآلي (كالجهاز العصبي والدماغ والأنظمة الميكانيكية–الكهربائية للاتصالات). كما يرتبط هذا المصطلح بثقافة الحاسوب (مثل الإنترنت والواقع الافتراضي وغيرها) والشبكات الحاسوبية. وهو مستمدٌّ من الكلمة الإغريقية "kybernetes"التي تعني "قائد الدفّة" أو "الحاكم"، ويُستَخدَم عادةً

كبادئة لوصف المفاهيم المرتبطة بالحاسوب وتقنية المعلومات والإنترنت، بحيث يشير إلى كل ما يتعلَّق بـ:

- **الأنظمة الرقمية** :كل ما يخصُّ شبكات الحاسوب والبرمجيات والتكنولوجيا.
- **البيئات الافتراضية** :الأنشطة والتفاعلات التي تدور في الفضاء السيبراني.
- **الأمن السيبراني** :حماية الأنظمة والشبكات من التهديدات السيبرانية.

على سبيل المثال، يُستخدم مصطلح "سيبر" في عبارات مثل الأمن السيبراني والجريمة السيبرانية والهجوم السيبراني والحرب السيبرانية، وجميعها ترتبط بالمجال الرقمي أو الافتراضي.

وقد استُخدِم مصطلح "سيبر" على نحو واسع في **دليل تالين** (Tallinn Manual) للإشارة إلى الأنشطة والعمليات والبيئات المرتبطة بالفضاء السيبراني، والذي عرّفه الدليل بأنّه "النطاق العالمي ضمن بيئة المعلومات، والمتكوّن من شبكة مترابطة من أنظمة المعلومات والبُنى التحتية، بما في ذلك الإنترنت وشبكات الاتصالات ونُظُم الحاسوب والمعالجات والمتحكّمات المضمَّنة". ويعكس هذا التعريف الطبيعة

المترابطة والرقمية للفضاء السيبراني بوصفه وسطاً لإجراء العمليات السيبرانية[1].

يرتبط مصطلح "سيبر" أيضاً بمفاهيم أخرى، منها "العمليات السيبرانية". فالمفهوم السيبراني يشمل الإطار التكنولوجي والنظري الذي يستند إليه ما يُنفَّذ في الفضاء السيبراني من أنشطة. وهذا يشمل استخدام شبكات الحاسوب والبنية التحتية الرقمية ونُظُم المعلومات لتحقيق أهداف محدَّدة. أمّا العمليات السيبرانية، فهي التطبيق العملي لتلك المفاهيم في سياق تنفيذ أنشطة هجومية أو دفاعية أو استخباراتية في الفضاء السيبراني. وتتبع العلاقة الجوهرية بين المفهوم والعمليات من اعتماد الأخيرة على الأسس المفاهيمية السيبرانية لضمان فعاليتها. فعلى سبيل المثال، إن فهم الثغرات في الشبكات (وهو مفهوم سيبراني رئيسي) يمكِّن من تنفيذ عمليات مثل اختراق الشبكات أو نشر البرمجيات الخبيثة. ويُعَدّ التمييز بين "السيبر" بوصفه نطاقاً و"العمليات السيبرانية" بوصفها أنشطةً داخله مهماً لمعالجة المسائل القانونية والأخلاقية المترتبة على هذه الأفعال. علاوةً على ذلك، يؤكّد **دليل تالين ٢,٠ بشأن القانون الدولي المنطبق على العمليات السيبرانية** على كيفية تأثير مبادئ السيادة والولاية القضائية والحياد، في التخطيط للعمليات السيبرانية وتنفيذها في بيئة رقمية عالمية.

بالنسبة لتحديد مفهوم "الهجوم" في القانون الدولي، يُعرَّف مصطلح "الهجوم" بأنّه "أفعال عنيفة ضد الخصم، سواء أكانت هجومية أم

[1] Michael N. Schmitt (Ed.) – "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations"

دفاعية". وقد نشأ هذا التعريف من المادة ٤٩ من البروتوكول الإضافي الأول لاتفاقيات جنيف، ويُعتبر هذا التعريف من القواعد العرفية في القانون الدولي. وتكتسب هذه القاعدة أهمية بالغة كون العديد من قواعد قانون النزاعات المسلحة بشأن إدارة العمليات العدائية لا تُطبّق إلا على الأفعال التي تندرج تحت مفهوم "الهجمات". فعلى سبيل المثال، يُحظَر استهداف المدنيين والأعيان المدنية، لكن هذه القواعد لا تسري على العمليات السيبرانية التي لا ترقى إلى مستوى "الهجمات". ومن ثمّ، قد يكون بعض العمليات السيبرانية التي تستهدف السكان المدنيين مباحاً من منظور قانوني، مثل معظم العمليات النفسية التي تُنفَّذ عبر الوسائل السيبرانية كمنصات التواصل الاجتماعي.

يشير استخدام مصطلح "هجوم" في القانون الدولي إلى إطارين قانونيين مختلفين. في الإطار الأول، الذي يُعرَف بـ"القانون الناظم لاستخدام القوة " (Jus ad Bellum)، تُحدَّد الشروط التي يجوز للدولة بموجبها استخدام القوة ضد دولة أخرى، ويُعَدّ "الهجوم المسلَّح" عاملاً أساسياً يبرّر حق الدولة في الدفاع عن نفسها وفقاً للمادة ٥١ من ميثاق الأمم المتحدة. وعلى صعيد العمليات السيبرانية، يثور جدلٌ حول ما إذا كانت الهجمات السيبرانية التي تُفضي إلى دمار كبير أو آثار وخيمة يمكن تصنيفها بوصفها "هجمات مسلَّحة" تبرِّر بدورها استخدام القوة.

في المقابل، يركِّز الإطار الثاني "القانون الدولي الإنساني (Jus in Bello)" على كيفية إدارة العمليات العسكرية بعد نشوب النزاع المسلَّح.

ويُعرَّف "الهجوم" هنا بأنّه أي فعل عنيف ضد الخصم، سواء أكان هجومياً أم دفاعياً. وعلى هذا الأساس، يُطرَح السؤال عمّا إذا كانت الهجمات السيبرانية التي لا تُخلِّف ضرراً مادياً يُمكن أن تصل إلى مستوى "الهجوم" بالمعنى المقصود في هذا التعريف، وما إذا كانت تستلزم تطبيق قواعد القانون الدولي الإنساني.

ويُبرِز التمييز بين "القانون الناظم لاستخدام القوة "(Jus ad Bellum) و"القانون الدولي الإنساني "(Jus in Bello) مدى تعقيد المسائل القانونية المتعلقة بالعمليات السيبرانية في الوقت المعاصر[1].

تتسم الهجمات السيبرانية بطبيعةٍ فريدةٍ من حيث الوسائل والغايات؛ فهي تُشنّ في الفضاء الرقمي عبر أدواتٍ إلكترونية تهدف إلى التسلُّل أو التعطيل أو إلحاق الأذى بالأنظمة والشبكات. وغالباً ما يكون تركيز هذه الهجمات منصبّاً على بياناتٍ رقميةٍ وأصولٍ غير ماديةٍ، دون الحاجة إلى وجودٍ مادي على الأرض. فعلى سبيل المثال، يعتمد هجوم الحرمان من الخدمة (DDoS) على إغراق الأنظمة بالطلبات والبيانات لتعطيلها، من دون إحداث تدميرٍ مادي ملموس. وفي المقابل، ترتبط الهجمات التقليدية باستخدام وسائل القوة العسكرية كالأسلحة والمواد المتفجرة، ما يُسفر عادةً عن دمارٍ ماديٍّ واضح مثل تدمير المباني أو إيقاع خسائر بشرية[2].

[1] Michael. N. Schmitt, "“Attack” as a term of art in international law: The cyber operations context," 2012 4th International Conference on Cyber Conflict (CYCON 2012), Tallinn, Estonia, 2012, pp. 1-11.

[2] Schmitt, M. N. (Ed.). (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press.

وتنعكس هذه الفروق في طبيعة كلٍّ من الهجمات السيبرانية والتقليدية على الآثار المترتبة عليها. إذ تَتَّسم الهجمات السيبرانية بانعكاساتٍ واسعة النطاق، وإن كانت غالباً غير مباشرة، وتشمل تعطيل الخدمات الحيوية كالكهرباء والرعاية الصحية، أو إلحاق خسائرٍ اقتصادية، أو التسبّب في عدم استقرارٍ مجتمعيٍّ من دون وقوع تدميرٍ مادي فوري. فعلى سبيل المثال، قد يؤدي اختراق شبكةٍ كهربائيةٍ إلى انقطاعٍ للتيار يستمر لساعاتٍ أو أيام، ويؤثر على ملايين المدنيين. أمّا الهجمات التقليدية، فتخلف آثاراً مباشرةً وملموسةً عادةً، كوقوع إصاباتٍ في صفوف المدنيين والعسكريين أو تدميرٍ للبنية التحتية، ما يتطلّب جهوداً للإغاثة وإعادة الإعمار قد تمتد لفتراتٍ طويلة.

وعلى الصعيد القانوني والأخلاقي، تُلقي الهجمات السيبرانية بظلالٍ من الشك على إمكانية تطبيق مبادئ القانون الدولي الإنساني، خصوصاً فيما يتعلق بالتمييز بين المقاتلين والمدنيين. ذلك أنّ الأفراد الضالعين في هذه الهجمات قد يكونون مختبئين وراء شاشات الحاسوب في مواقعٍ بعيدة، ما يصعّب تحديد هوياتهم وطبيعة انتماءاتهم. وبناءً عليه، يتعذّر أحياناً تقييم مدى الالتزام بمبدأ التمييز ومبدأ التناسب في تنفيذ الهجمات السيبرانية. أمّا الهجمات التقليدية، وبحكم طبيعتها المادية، فتخضع لقواعد القانون الدولي الإنساني بصورةٍ أوضح، إذ يُمكن رصد المواقع المستهدفة وتقدير

الأضرار بدقّة نسبية، ما يسهّل عملية تقييم مدى التزام الأطراف المتحاربة بالالتزامات القانونية المفروضة عليهم[1].

ثمّة فروقٌ جوهرية بين النزاع المسلَّح الدولي والنزاع المسلَّح غير الدولي. ففي حالة النزاع المسلَّح الدولي، تسري اتفاقيات لاهاي لعام ١٩٠٧، واتفاقيات جنيف الأربع لعام ١٩٤٩، والبروتوكول الإضافي الأوّل لتلك الاتفاقيات. أمّا في حالة النزاع المسلَّح غير الدولي، فيسري في الأساس القانون التعاهدي المتمثل بالمادة ٣ المشتركة بين اتفاقيات جنيف لعام ١٩٤٩ والبروتوكول الإضافي الثاني، علماً بأنّ هذا الأخير لا يسري إلا على الدول الأطراف فيه وفي حالات معينة من النزاعات غير الدولية. وبصورة عامة، فإنّ الجزء الأكبر من قواعد القانون الدولي العرفي المنطبقة على النزاعات الدولية يتجاوز نظيره المنطبق على النزاعات غير الدولية.[٢] ويُعَدّ النزاع المسلَّح دولياً قائماً في الحالات الآتية:

١. عندما تقع أعمال عدائية بين القوات المسلحة أو الجهات الرسمية في الدول.

٢. أثناء احتلال دولة لأراضي دولة أخرى.

٣. عندما تفرض إحدى الدول سيطرتها على جماعة مسلَّحة منظَّمة تقاتل دولةً أخرى.

[1] Dinstein, Y. (2016). The Conduct of Hostilities Under the Law of International Armed Conflict. Cambridge University Press.

[2] Taddeo, M. (2018). "The Challenges of Cyber Operations During Armed Conflicts." International Review of the Red Cross, 100(1-2), 229-246.

٤. أخيراً، هناك حالة تقتصر على الدول الأطراف في البروتوكول الإضافي الأوّل، وتشمل الجماعات المناضلة من أجل حق تقرير المصير (وفقاً للجنة الدولية للصليب الأحمر).

وفي سياق النزاعات المسلحة، تُعَدّ الهجمات السيبرانية أفعالاً تُنفَّذ عبر الفضاء السيبراني بهدف إلحاق الضرر أو الإرباك أو تحقيق مكسب على حساب البنى التحتية الرقمية للخصم، وغالباً ما تشكّل جزءاً من العمليات العسكرية الأوسع نطاقاً. وقد تستهدف هذه الهجمات البنى التحتية الحيوية أو أنظمة الاتصالات أو شبكات الجيش، سعياً لتحقيق أهداف تتراوح بين التجسُّس والتعطيل والتدمير المادي. وتطرح هذه الهجمات تساؤلات معقَّدة بموجب القانون الدولي الإنساني، ولا سيّما في مسألة اعتبارها "هجمات" وفق مفهوم القانون الدولي الإنساني ومدى توافقها مع مبادئ التمييز والتناسب والضرورة العسكرية.

فعلى سبيل المثال، قد يُعَدّ الهجوم السيبراني على شبكة الكهرباء في دولة ما أثناء نزاع مسلَّح هجوماً مباشراً على بنية تحتية مدنية، إذا كان يفتقر إلى الضرورة العسكرية أو ينتهك مبدأ التمييز بين الأهداف المدنية والعسكرية.

وتجدر الإشارة هنا إلى الحالة الواضحة التي تتمثل في استخدام الحرب السيبرانية في النزاع العسكري الأوسع بين روسيا وأوكرانيا الذي بدأ عام ٢٠١٤، حيث قامت روسيا بضمِّ شبه جزيرة القرم إثر استفتاء مثير للجدل دانته غالبية المجتمع الدولي، بما في ذلك أوكرانيا. وقد شكّل هذا

الضمّ بدايةً لسلسلة من العمليات العسكرية، من بينها الدعم الروسي لقوات انفصالية في شرق أوكرانيا. وكان الهجوم على شبكة الكهرباء الأوكرانية جزءاً من استراتيجية شاملة تهدف إلى إضعاف قدرة أوكرانيا على العمل بوصفها دولة ذات سيادة. ويمثّل ذلك مثالاً على أساليب "الحرب الهجينة" التي تتبناها روسيا، والتي تمزج بين العمليات السيبرانية والأساليب العسكرية التقليدية لزعزعة استقرار أوكرانيا.

وبموجب القانون الدولي، تُعدّ الهجمات التي تستهدف البُنى التحتية الحيوية، مثل شبكة الطاقة لأي دولة، مندرجةً ضمن الأعمال العدائية في حالة النزاع المسلَّح. والهجوم السيبراني على شبكة الكهرباء الأوكرانية يتّسق مع أحكام القانون الدولي الإنساني الذي يحكم أساليب ووسائل الحرب. فوفقاً للبروتوكول الإضافي الأوّل لاتفاقيات جنيف لعام ١٩٧٧، يُحظَر استهداف البنى التحتية المدنية، ومنها شبكات الطاقة، ما لم تكن هناك ضرورة عسكرية واضحة ومباشرة. ورغم أنّ هذا الهجوم لم يتضمّن عملاً عسكرياً مادياً مباشراً، فقد صُمِّم ليشلّ قدرة أوكرانيا على الاستمرار في أداء وظائفها، مما يجعله جزءاً من الحملة العدائية الأكبر في النزاع الدائر.

ومن أكثر أنواع الهجمات السيبرانية شيوعاً:

١. **البرمجيات الخبيثة(Malware)**

تُشير هذه الهجمات إلى أي نوع من البرمجيات الضارة المصممة لإلحاق الضرر أو التلف بحاسوب أو خادم أو عميل أو شبكة

حاسوبية و/أو بالبنية التحتية، دون علم المستخدم النهائي. ويقوم المهاجمون السيبرانيون بإنشاء واستخدام وبيع البرمجيات الخبيثة لأسبابٍ متعددة، ولكن غالباً ما يُوظَّف هذا النوع من الهجمات في سرقة المعلومات الشخصية أو المالية أو التجارية. ورغم اختلاف دوافعهم، فإنّ المهاجمين السيبرانيين غالباً ما يركّزون تكتيكاتهم وتقنياتهم وإجراءاتهم على الوصول إلى بيانات الاعتماد والحسابات ذات الصلاحيات العالية لتنفيذ مآربهم.

مثال :هجوم الفدية WannaCry الذي وقع في عام ٢٠١٧، حيث طال مئات الآلاف من الحواسيب عالمياً، واستهدف خصوصاً المنظّمات التي لم تثبّت تحديثات أمنيّة بالغة الأهمية. استغلّ WannaCry ثغرةً في نظام مايكروسوفت ويندوز تُعرَف باسمEternalBlue ، والتي تسرّبت من أدوات الاختراق التابعة لوكالة الأمن القومي الأميركية[1].(NSA)

٢. **التصيّد الاحتيالي(Phishing)**

يُعَدّ التصيّد الاحتيالي شكلاً شائعاً من الهجمات السيبرانية التي تستهدف الأفراد عبر البريد الإلكتروني أو الرسائل النصية أو المكالمات الهاتفية أو غير ذلك من وسائل التواصل. ويهدف المهاجم في هذا النوع إلى خداع المتلقّي ودفعه إلى القيام بالإجراء المراد تنفيذه، مثل الكشف عن معلوماتٍ مالية أو بيانات

[1] Kaspersky Lab. (2017). WannaCry Ransomware Attack: The Critical Security Patch You Need

اعتماد الأنظمة أو أي معلومات حسّاسة أخرى. وباعتباره شكلاً رائجاً من الهندسة الاجتماعية، ينطوي التصيّد الاحتيالي على استغلال الأساليب النفسية والخداع، بحيث ينتحل المهاجم صفة جهةٍ موثوقة بهدف إقناع المستخدمين باتخاذ إجراءات معيّنة. وغالباً ما تشمل هذه الإجراءات النقر على روابط تقود إلى مواقع وهمية، أو تنزيل وتثبيت ملفاتٍ خبيثة، أو الإفصاح عن معلوماتٍ خاصّة مثل أرقام الحسابات المصرفية أو بيانات البطاقات الائتمانية.

٣. **هجوم الحرمان من الخدمة(Denial-of-Service – DoS)**

يُعدّ هذا النوع محاولةً خبيثةً لتعطيل أو إيقاف الأداء الطبيعي لخادمٍ أو خدمةٍ أو شبكةٍ مستهدفة، وذلك من خلال إغراقها بسيلٍ من الطلبات غير الشرعية التي تؤدي إلى تعطّلها. ويُفضي ذلك إلى بطء الخدمة أو تراجع الاستجابة أو فقدان الوصول إليها تماماً بالنسبة للمستخدمين الشرعيين. ويمكن أن تتسبب هذه المحاولات الخبيثة في إحداث شلل للمواقع الإلكترونية، وتعطيل الخدمات، وإلحاق أضرار مالية وسمعية جسيمة بالجهة المستهدفة. وتستخدم هجمات الحرمان من الخدمة آليات وأدوات متنوعة قادرة على إحداث اضطراب كبير في الخدمات، ولكن يمكن الحدّ من آثارها عن طريق الإجراءات الأمنية المناسبة كاستخدام الجدران النارية (Firewalls) وأنظمة الكشف عن الاقتحام (Intrusion Detection Systems)، وتحديد معدّلات استقبال

الطلبات، بالإضافة إلى خدمات الحماية المتخصصة ضد هجمات الحرمان من الخدمة .(Anti-DDoS) ويستدعي هذا الأمر اعتماد استراتيجيات متقدمة للرصد والتصدي، نظراً لاستمرار وتيرة تلك الهجمات بشكل مكثّف.

المطلب الثاني
الآثار الناجمة عن الهجمات السيبرانية

يتميّز الفضاء السيبراني بتعرّضه لهجمات سيبرانية تستهدف شبكات المؤسّسات الأمنية والعسكرية، وذلك في ظلّ غياب التدابير الكافية للحفاظ على الأمن السيبراني للدول وقطاعاتها ومرافقها، وعدم تحقيق المستويات الأمنية المطلوبة. ومن الجدير بالذكر أنّه يصعُب تحديد نطاق الهجمات السيبرانية بدقّة نظراً لاتساعها، وفي ظلّ التطور التكنولوجي الراهن، باتت تمتدّ لتشمل شتى الميادين، بما يمنحها القدرة على التأثير في حركات الملاحة الجوية والبحرية والتلاعب بالأنظمة المعتمدة على الإحداثيات الجغرافية والرقمية. كما يمكنها التأثير في منظومات المرافق العامة وتعطيلها، كما حدث في ٧ يناير ٢٠٢٤، إذ تعرّضت شاشات الوصول والمغادرة في مطار رفيق الحريري الدولي في بيروت لهجومٍ سيبراني، حيث استُبدِلَت محتويات الشاشات برسائل تنتقد "حزب الله" وأمينه العام، متهمةً الحزب بتهريب الأسلحة عبر المطار ومحذّرةً من توريط لبنان في

نزاعات إقليمية. كما حملت الرسائل شعار مجموعةٍ تدعى "hezboallah"والتي نفت لاحقاً أي صلة لها بالهجوم. وقد تسبّب الهجوم في تعطيل نظام مناولة الحقائب(BHS) ، ما اضطرّ سلطات المطار إلى تطبيق خططٍ بديلة لضمان سلاسة العمليات.

شهد مطار رفيق الحريري الدولي في بيروت حادثة اختراق سيبرانية خطيرة، استهدفت الأنظمة الرئيسية التي تُشغِّل الشاشات ولوحات المعلومات الخاصة بالرحلات الجوية. وقد دفع ذلك السلطات اللبنانية إلى طلب المساعدة من خبراء ألمان وفرنسيين، فتعاون هؤلاء الخبراء مع الجيش اللبناني والأجهزة الأمنية لإعادة برمجة الأنظمة المتضررة. وعلى أثر هذه الجهود، عادت الشاشات إلى حالتها الطبيعية واستؤنفت العمليات في المطار تدريجياً. وفي موازاة ذلك، باشرت مديرية المخابرات في الجيش اللبناني وقوى الأمن الداخلي تحقيقاً موسعاً في الحادثة، حيث استجوبت موظفين مسؤولين عن الأنظمة المُختَرقة. وقد شدّد معالي وزير الأشغال العامة والنقل، الدكتور علي حمية، على أهمية تعزيز إجراءات الأمن السيبراني للحيلولة دون وقوع هجمات مماثلة مستقبلاً، مؤكداً أنّ مثل هذه الواقعة تشكّل خرقاً خطيراً لأمن لبنان الوطني، وتستدعي تكاتف مختلف الجهات لمواجهة أي تهديد قد يمسّ استقرار البلاد.

لا تقتصر تداعيات الهجمات السيبرانية على قطاع أو اثنين، بل تمتد لتشمل عدة قطاعات حيوية تمثّل عماد الدولة ومجتمعها. وتأتي البنية

التحتية في مقدمة الأهداف السيبرانية، إذ يسعى منفّذو هذه الهجمات إلى تدمير الأنظمة أو شلّها لإحداث اضطرابات داخلية وتعطيل المؤسسات الرئيسية. ويشمل ذلك أنظمة التحكّم المركزي وموارد الطاقة والقطاع المالي وقطاعي الاتصالات والمواصلات، فضلاً عن مرافق المياه. وباعتبار أنّ هذه القطاعات هي بمثابة الأعمدة الأساسية لعمل الدولة، فإنّ اختراقها أو إتلافها يمكن أن يخلق حالة من الفوضى وعدم الاستقرار تُعرّض الأمن الوطني للخطر وتنعكس سلباً على الحياة اليومية للمواطنين.

إلى جانب ذلك، يتأثّر القطاع الاقتصادي تأثراً بالغاً في حال تعرّضه لهجماتٍ سيبرانية، خاصةً عندما تطال الهجمات النظم المصرفية والمالية. إذ قد تُفضي هذه العمليات إلى سرقة مبالغ مالية ضخمة أو تعطيل تحويلات مصرفية حسّاسة، وهو ما يُفقد المستثمرين ثقتهم بالقطاع المالي في البلد المتضرر، ويدفعهم للعزوف عن الاستثمار فيه. وتتفاقم التبعات بتزايد معدلات البطالة نتيجة انكماش الأنشطة الاقتصادية، فضلاً عن التراجع المُحتمل للعملة الوطنية وارتفاع تكلفة الاقتراض، ما يخلق دوامةً من المصاعب قد يصعب الخروج منها في وقت قصير[1].

وعلى الصعيد السياسي والأمن القومي، أصبحت الهجمات السيبرانية وسيلةً ناجعة في الصراعات الجيوسياسية المعاصرة، حيث تتيح للدول – أو الجهات المدعومة حكومياً – التدخّل في شؤون دول أخرى من دون أن

[1] Lyons, Marty. United states. Homeland security . threat Assessment of cyber warfare. Washington, D.C, 2005. Web

تترك أثراً مادياً واضحاً. وتُعَدّ محاولة التدخّل في الانتخابات الرئاسية الأميركية عام ٢٠١٦، المنسوبة إلى جهات روسية رسمية، مثالاً صارخاً على توظيف الفضاء السيبراني للتأثير في الرأي العام وزرع الشكوك في المسارات الديمقراطية. كما تُظهِر حملات التجسّس السيبراني، مثل "Operation Cloud Hopper"المنسوبة إلى جهات صينية، كيف يمكن لمثل هذه الاختراقات أن تسرّب معلومات حسّاسة من الحكومات والشركات الكبرى، وتُستَثمر لاحقاً في تحقيق مكاسب استراتيجية أو اقتصادية.

أما القطاع العسكري، فيمثّل واحداً من أخطر القطاعات التي يمكن أن تُستهدَف بهجمات سيبرانية، كونه يشكّل خط الدفاع الأول عن أي دولة. فالاعتماد المتزايد على الأنظمة التكنولوجية في المنظومات العسكرية يفتح الباب أمام إمكانات التخريب الرقمي الذي قد يعطّل قنوات الاتصال بين المنشآت العسكرية وقادتها، أو يُصدر أوامر خاطئة إلى الأسلحة الموجّهة والطائرات المسيّرة، مع تغيير إحداثيات الأهداف لتستهدف مواقع داخل الدولة ذاتها. وقد تؤول هذه الفوضى الرقمية إلى خسائر جسيمة في الأرواح وإلى أضرار مادية جسيمة لا تقلّ عن تلك الناجمة عن الحروب التقليدية.

في ضوء ما سبق، يتّضح أنّ الآثار التي تُخلّفها الهجمات السيبرانية لا تقلّ خطورةً عن آثار الحروب التقليدية، إذ تقوّض مبادئ الإنسانية والقانون الدولي، وتهدّد الأسس التي يستند إليها نظام الأمن الجماعي ودور الأمم

المتحدة والمنظمات الدولية. كما أنّها تفرض تحدّيات جديدة على نظام روما الأساسي المُنشِئ للمحكمة الجنائية الدولية، بما يعكس الحاجة إلى تطوير مفاهيم قانونية وأطر تنظيمية دولية أكثر فعالية قادرة على توفير الحماية اللازمة للدول والأفراد من هذا النوع من العدوان، والحفاظ على الأمن والسلم الدوليين في عالم يزداد اعتماداً على التكنولوجيا الرقمية.

المبحث الثاني

القانون الدولي الإنساني (IHL) والهجمات السيبرانية في النزاعات المسلحة غير الدولية (NIACs)

يشهد العالم تطوراً متسارعاً في التكنولوجيا وازدياداً في القدرات السيبرانية، الأمر الذي غيّر شكل الحروب جذرياً وأدخل تحديات جديدة على الأطر القانونية التي تنظم النزاعات المسلحة. ومن أبرز هذه التحديات كيفية انطباق أحكام القانون الدولي الإنساني (IHL) على الهجمات السيبرانية أثناء النزاعات المسلحة. فالقانون الدولي الإنساني، الذي ينظم سلوك الأعمال العدائية ويهدف إلى حماية من لا يشاركون مشاركةً مباشرة في الأعمال العدائية، لم يجرِ بعد تكييفه بالكامل لمواجهة تعقيدات الحروب السيبرانية.

يُعرَف القانون الدولي الإنساني أيضاً باسم "قانون النزاعات المسلحة" أو "قانون الحرب"، ويتألف من مجموعة قواعد قانونية دولية ترمي إلى الحدّ من الآثار المترتبة على النزاع المسلح. ويتمثّل غرضه الرئيس في حماية الأفراد الذين لا يشاركون، أو لم يعودوا قادرين على المشاركة، في الأعمال العدائية، علاوةً على تنظيم سبل القتال بهدف تجنّب المعاناة غير الضرورية.

بالنسبة للجنة الدولية للصليب الأحمر (ICRC)، لا جدال في أنّ القانون الدولي الإنساني يسري على العمليات السيبرانية أثناء النزاعات المسلحة ويقيّدها، تماماً كما ينظم استخدام أيّ سلاح أو وسيلة أو أسلوبٍ آخر في النزاع المسلح، سواءٌ كان حديثاً أو قديماً. وينطبق ذلك بغضّ النظر عمّا إذا اعتُبر الفضاء السيبراني نطاقاً جديداً للحرب شأنه شأن الجوّ والبرّ والبحر أو الفضاء الخارجي، أم نُظر إليه بوصفه نطاقاً مختلفاً من صنع الإنسان، أم حتى إن لم يُعَدّ نطاقاً بالمعنى الحرفي. وعند تصديق الدول على معاهدات القانون الدولي الإنساني، فإنّها تفعل ذلك لتنظيم النزاعات الراهنة والمستقبلية، وقد اشتملت هذه المعاهدات على قواعد تستشرف ظهور وسائل وأساليب قتال جديدة، بافتراض أنّ القانون الدولي الإنساني سينطبق عليها.[١]

[1] ICRC,InternationalHumanitarianLawandtheChallengesofContemporaryArmedConflicts, 31IC/11/5.1.2, Geneva, 2011 (ICRC Challenges Report 2011), pp. 36–37, available at: www.icrc.org/en/doc/assets/files/redcross-crescent-movement/31st-international-conference/31-int-conference-ihl-challenges-report-11-5-

وعلى سبيل المثال، لو لم ينطبق القانون الدولي الإنساني على وسائل وأساليب الحرب المستقبلية، لما كان ضرورياً إخضاعها للمراجعة القانونية في ضوء القواعد السارية بموجب المادة ٣٦ من البروتوكول الإضافي الأوّل لعام ١٩٧٧. كما تحظى هذه النتيجة بدعم قوي في الرأي الاستشاري الصادر عن محكمة العدل الدولية بشأن مشروعية التهديد أو استخدام الأسلحة النووية؛ إذ أشارت المحكمة إلى أنّ المبادئ والقواعد الراسخة في القانون الدولي الإنساني والمنطبقة في النزاع المسلح تنطبق على "جميع أشكال الحرب وجميع أنواع الأسلحة"، بما فيها "أسلحة المستقبل". وفي نظر اللجنة الدولية للصليب الأحمر، ينطبق هذا الموقف نفسه على استخدام العمليات السيبرانية خلال النزاعات المسلحة. وترحب اللجنة الدولية للصليب الأحمر بتزايد تأكيد الدول والمنظمات الدولية على سريان أحكام القانون الدولي الإنساني على العمليات السيبرانية أثناء النزاعات المسلحة، وكذلك بالحوار حول كيفية انطباقه. ويجوز للدول أيضاً أن تقرر فرض قيود إضافية على ما هو منصوص عليه في القانون القائم أو تطوير قواعد مكملة، لا سيّما لتوفير حماية أكبر للمدنيين والبنى التحتية المدنية من آثار العمليات السيبرانية. وترى اللجنة الدولية للصليب

1-2en.pdf ;ICRC,International Humanitarian Law and the Challenges of Contemporary Armed Conflicts,32IC/ 15/11, Geneva, 2015 (ICRC Challenges Report 2015), p. 40, available at: www.icrc.org/en/download/file/15061/32ic-report-on-ihl-and-challenges-of-armedconflicts.pdf ; ICRC, International Humanitarian Law and the Challenges of Contemporary Armed Conflicts, 33IC/19/9.7, Geneva, 2019 (ICRC Challenges Report 2019), p. 18, available at: https://rcrcconference.org/app/uploads/2019/10/33IC-IHL-Challengesreport_EN.pdf. 484

الأحمر أنّ أي قواعد جديدة ينبغي أن تستند إلى الإطار القانوني القائم وتعززه، بما يشمل القانون الدولي الإنساني. وفي الحالات التي لا تغطيها القواعد النافذة للقانون الدولي الإنساني، فإنّ المدنيين والمقاتلين يستمرون في التمتع بالحماية المنصوص عليها في "بند مارتنز" (Martens Clause)، الذي ينصّ على أنّهم يظلون تحت حماية ومقتضيات المبادئ المستمدة من القانون الدولي العرفي، ومن مبادئ الإنسانية، وإملاءات الضمير العام.[١]

ومن المهم التأكيد على أنّ تأكيد تطبيق القانون الدولي الإنساني على العمليات السيبرانية خلال النزاعات المسلحة لا يضفي شرعيةً على الحروب السيبرانية ولا يشجّع عسكرة الفضاء السيبراني، بل يفرض حدوداً معيّنة على تلك العسكرة عبر حظر تطوير قدرات عسكرية سيبرانية تنتهك القانون الدولي الإنساني.

وعلاوةً على ذلك، يبقى أيّ استخدام للقوة من جانب الدول—سيبرانياً كان أم عسكرياً تقليدياً—خاضعاً لميثاق الأمم المتحدة والقواعد العرفية ذات الصلة، لا سيّما حظر استخدام القوة. فلا بدّ من تسوية المنازعات الدولية بالطرق السلمية، في الفضاء السيبراني كما في سائر المجالات. ومع أنّ بعض جوانب القانون المنطبق ما زالت غير محسومة، فلا شكّ في

[1] Jean-Marie Henckaerts and Louise Doswald-Beck (eds), Customary International Humanitarian Law, Vol. 1: Rules, Cambridge University Press, Cambridge, 2005 (ICRC Customary Law Study), Rules 70, 71, available at: https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1. See also AP I, Art. 36. 4

انطباق القانون الدولي الإنساني عندما تُنفّذ عملية سيبرانية بموازاة أو دعماً لعمليات عسكرية "جسدية" أو "تقليدية" في سياق نزاع مسلّح قائم.

المطلب الأول

لمحة عامة عن النزاع المسلح غير الدولي (NIAC) والإطار القانوني للقانون الدولي الإنساني

يستند تصنيف النزاع على أنه نزاعٌ مسلّحٌ غير دولي (NIAC) في المقام الأول إلى المادة ٣ المشتركة بين اتفاقيات جنيف الأربع لعام ١٩٤٩ وإلى البروتوكول الإضافي الثاني (AP II) المعتمد عام ١٩٧٧. حيث تحدّد المادة ٣ المشتركة الحدّ الأدنى من المعايير الإنسانية في النزاعات "التي ليست لها صبغة دولية"، وتوجب على جميع أطراف النزاع، بما في ذلك الجهات من غير الدول، معاملة المدنيين والأشخاص الذين أصبحوا خارج القتال (hors de combat) معاملةً إنسانيةً. وتتمتع هذه المادة باعتراف شبه عالمي ويُنظر إليها على نطاق واسع بوصفها جزءاً من القانون الدولي العرفي. أمّا البروتوكول الإضافي الثاني فيبني على هذه الأسس عبر النصّ على حماية أشمل لضحايا النزاعات المسلحة غير الدولية، مقرراً أنّ أحكامه تسري في الحالات التي تشن فيها جماعاتٌ مسلحة معارضة أو كياناتٌ مسلحةٌ منظّمةٌ أعمال عنفٍ طويلة الأمد ضد حكومةٍ ما، شريطة أن تسيطر تلك الجماعات على إقليمٍ ما سيطرة كافية تتيح لها القيام بعملياتٍ عسكريةٍ مستمرة.

وعلى الرغم من هذا التقنين، غالباً ما يثور الجدل بشأن ما إذا كان ينبغي الاعتراف بوجود نزاع مسلّح غير دولي داخل حدود دولة ما. إذ قد تصف الدولة المواجهات الجارية بأنّها مجرد قضية "إنفاذ للقانون" أو اضطراب داخلي، متردّدةً في الاعتراف بصفة النزاع المسلّح خشية منح الجماعات المسلحة شرعيةً أو استجلاب رقابةٍ خارجية. بيد أنّ الاجتهاد القضائي للمحكمة الجنائية الدولية ليوغوسلافيا السابقة (ICTY)، ولا سيما في قرارها في قضية (Tadić)، قد بيّن أنّ النزاع المسلّح يتحقق متى توافرت "أعمال عنفٍ مسلّحة طويلة الأمد" بين السلطات الحكومية وجماعاتٍ مسلحة منظّمة (أو فيما بين الجماعات نفسها)، شريطة أن تبلغ تلك الجماعات مستوىً من التنظيم يمكّنها من تنفيذ عمليات عسكريةٍ مستدامة. وقد أسهم هذا المعيار المعروف بـ"اختبار تاديتش" في الحدّ من الغموض القانوني، مؤكداً أنّ العبرة ليست بما تعلنه الدول، وإنما بحقيقة توفّر الشروط التي تجعل النزاع خاضعاً للقانون الدولي الإنساني.

ورغم أنّ المبادئ الجوهرية للقانون الدولي الإنساني—بشأن تقييد وسائل وأساليب القتال وحماية من لا يشاركون في الأعمال العدائية ومنع المعاناة غير الضرورية—تنطبق على النزاعين الدولي وغير الدولي على السواء، فإنّ المنظومة التعاهدية الخاصة بالنزاعات غير الدولية أقل تفصيلاً. فلا تُعيد المادة ٣ المشتركة والبروتوكول الإضافي الثاني نسخَ جميع الأحكام التفصيلية المضمّنة في الآليات المنظمة للنزاعات الدولية، مثل البروتوكول الإضافي الأوّل (AP I). بيد أنّ القانون الدولي العرفي

يسدّ الكثير من الثغرات، مؤكداً تطبيق القواعد الأساسية بشأن التمييز والتناسب والمعاملة الإنسانية سواء أكان النزاع دولياً أم داخلياً.

وقد تتضمن النزاعات المسلحة غير الدولية المعاصرة كذلك عناصر تتجاوز الحدود الوطنية، ما يشكّل تحدياً أمام التعريفات التقليدية؛ إذ قد تتدخل قوى خارجية في النزاع بشكل مباشر أو عبر تقديم الدعم لأحد الأطراف، فيتحوّل النزاع "المحلي" إلى طابع دولي. كما قد يمتد العنف إلى دولٍ مجاورة، ويخلق أزمةً إقليمية أوسع نطاقاً. وتضغط هذه التطورات على الإطار القانوني القائم وتجعل الهيئات القضائية وواضعي السياسات والجهات الإنسانية بحاجةٍ إلى إعادة تقييم كيفية الحفاظ على حماية أحكام القانون الدولي الإنساني عند تداخل الحدود بين النزاعين الداخلي والدولي. وتعكس هذه التحديات التوتر الكامن بين ضرورة الحفاظ على سيادة الدولة ووجوب حماية الأفراد من مآسي الحرب.

ويرتكز القانون الدولي الإنساني على مجموعةٍ من المبادئ الجوهرية التي تهدف إلى الحدّ من المعاناة الإنسانية وصون كرامة الأشخاص المتأثرين بالنزاع. ورغم أنّ هذه المبادئ نشأت أساساً في سياق النزاعات المسلحة الدولية (IACs)، إلا أنها تنطبق كذلك على النزاعات المسلحة غير الدولية. وقد أكّد القانون الدولي العرفي وبعض النصوص التعاهدية، مثل المادة ٣ المشتركة، امتداد هذه المبادئ إلى النزاعات الداخلية.

مبدأ التمييز هو الجوهر في القانون الدولي الإنساني، إذ يلزم أطراف النزاع بالتفريق دائماً بين المقاتلين وغير المقاتلين (المدنيين). فيُحظَر

قطعياً توجيه هجماتٍ متعمدة ضد المدنيين أو الأعيان المدنية. إلا أنّه في النزاعات غير الدولية، قد يصعب تحديد الأهداف المشروعة حين لا يرتدي المقاتلون زياً مميزاً، أو يندمجون مع السكان المدنيين، أو يستخدمون تكتيكاتٍ مرتجلة. ورغم هذه التعقيدات العملية، يبقى المبدأ ثابتاً: أي استهداف مقصود للمدنيين لتحقيق غايات عسكرية أو سياسية يُعدّ خرقاً للقانون الدولي الإنساني، على غرار ما بيّنته قضايا مثل (Prosecutor v. Stanislav Galić) أمام المحكمة الجنائية الدولية ليوغوسلافيا السابقة، حيث أدانت المحكمة الهجمات على سراييفو التي استهدفت إرهاب السكان المدنيين.

أمّا مبدأ التناسب، وهو الركيزة الثانية، فيلزم بأن لا تتجاوز الخسائر المحتملة في صفوف المدنيين أو الأعيان المدنية الفائدة العسكرية المتوقّعة من العملية. حتى لو تبيّن أنّ الهدف مشروع، ينبغي أن يكون استخدام القوة مناسباً. وقد أوضحت المحكمة الجنائية الدولية ليوغوسلافيا السابقة، في سياق دراستها لحوادث القنص والقصف في المدن المحاصرة، أنّ استخدام تكتيكاتٍ تُلحق أضراراً مفرطة بالمدنيين مقارنة بالهدف العسكري المنشَدّ يُشكّل انتهاكاً جسيماً للقانون الدولي الإنساني.

ويأتي مبدأ الضرورة العسكرية ليفرض أنّ المقاتلين لا يُقدِمون إلا على الإجراءات اللازمة لتحقيق هدفٍ عسكري مشروع، شريطة ألا يحظرها القانون الدولي الإنساني. ولا يجوز تحت أي ظرف التذرع بالضرورة

العسكرية لتبرير أفعال مثل التعذيب أو العقاب الجماعي أو غيرها من جرائم الحرب.

وأخيراً، فإنّ واجب المعاملة الإنسانية يُحتّم حماية الأشخاص الذين لا يشاركون، أو لم يعودوا قادرين على المشاركة، في الأعمال العدائية— سواء كانوا مدنيين أو أسرى حرب أو مقاتلين جرحى—والحرص على عدم تعريضهم للمعاناة كلما كان ذلك ممكناً. وتحظر المادة ٣ المشتركة والبروتوكول الإضافي الثاني على وجه الخصوص أفعال القتل والتعذيب والتشويه والمعاملة اللاإنسانية أو المهينة في النزاع المسلّح غير الدولي. وفي قضايا أمام المحكمة الجنائية الدولية (ICC)، ولا سيما (Prosecutor v. Jean-Pierre Bemba Gombo) و (Prosecutor v. Bosco Ntaganda)، جرت ملاحقة قادةٍ من الجهات المسلحة من غير الدول جنائياً عن جرائم واسعة النطاق ارتُكبت بحق سكانٍ محليين، شملت الاغتصاب والقتل والاستعباد الجنسي.[١]

ورغم وضوح هذه الضوابط، تواجه النزاعات المسلحة غير الدولية صعوبات لا تُرى عادةً في الحروب بين الدول. فقد تنكر الحكومات انطباق القانون الدولي الإنساني، متمسّكةً بكون مبادئ إنفاذ القانون كافية، بينما قد تتجاهل الجهات المسلحة من غير الدول تلك القواعد ولا تخضع

[1] International Criminal Court. (n.d.). Prosecutor v. Bosco Ntaganda. Case No. ICC-01/04-02/06. Retrieved from https://www.icc-cpi.int/pages/record.aspx?docNo=ICC-01/04-02/06-2359

لأحكام المعاهدات الرسمية. وبناءً عليه، يبقى الالتزام بمبادئ التمييز والتناسب والضرورة والمعاملة الإنسانية موضع تحدٍ مستمر في سياق النزاعات الداخلية.

يواجه تطبيق القانون الدولي الإنساني في النزاعات المسلحة غير الدولية جملةً من العقبات السياسية والعملية والقانونية التي تحول دون ضمان إنفاذه على نحوٍ متسقٍ وعام. وتبرز في هذا السياق مشكلة إحجام الدول عن الاعتراف بوجود نزاعٍ مسلّحٍ غير دولي على أراضيها. إذ قد يعني التصنيف الرسمي للنزاع على هذا النحو إقراراً ضمنياً من الحكومة بوجود خصومٍ تتجاوز صفتهم مجرد "مجرمين"، وقد ينطوي ذلك على منحهم مكانةً أعلى أو استجلاب اهتمامٍ دولي.

ومن جهة أخرى، فإنّ الجماعات المسلحة من غير الدول تُشكّل تحدياً في ضمان الامتثال للقانون الدولي الإنساني نظراً إلى أنّها ليست أطرافاً موقِّعةً عادةً على الاتفاقيات ذات الصلة. ورغم انطباق القواعد العرفية والمادة ٣ المشتركة عليها، فإنّ قادة هذه الجماعات قد يرفضون القانون الدولي الإنساني أو يجهلون أُسُسه القانونية، معتبرين إياه مفروضاً عليهم من الخارج. كما تتسم بنية كثيرٍ من هذه الجماعات بالتشظي، إذ تعمل فصائل متعددة أو خلايا مختلفة دون هيكل قيادة مركزي صارم، ما يجعل التنسيق على أساسٍ قانوني أمراً عسيراً.

وفي النزاعات التي تُصنّف فيها إحدى الجماعات المسلحة كمنظمة إرهابية، يبرز تداخل القانون الدولي الإنساني مع قوانين مكافحة

الإرهاب، ما يمثّل عائقاً آخر. فعند إدراج جماعة ما في قوائم الإرهاب، قد تُجرّم التشريعات الوطنية أو الدولية أيّ شكلٍ من التفاوض أو التواصل معها، ما يعوق الحوارات الضرورية لتحسين حماية المدنيين والأسرى، ويعرقل عمل منظمات الإغاثة بما فيها اللجنة الدولية للصليب الأحمر، التي تعتمد غالباً على قنوات اتصال محايدة مع جميع الأطراف المتحاربة.

وتفرض التحولات التكنولوجية مزيداً من التعقيد على الالتزام بالمبادئ الأساسية للقانون الدولي الإنساني. إذ كثيراً ما تتداخل المنشآت المدنية مع البنية التحتية العسكرية في الساحات الحضرية، وقد تتيح التكنولوجيا تنفيذ هجماتٍ خفية أو مُسيّرة عن بُعد، ما يضاعف احتمالات الخطأ في الاستهداف. فعلى سبيل المثال، قد تؤدي الهجمات السيبرانية على البنى التحتية الحيوية إلى تعطيل إمدادات المياه أو السجلات الطبية، من دون قدرةٍ واضحة على التمييز بين الأنظمة العسكرية والمدنية. ويزيد الغموض في الفضاء السيبراني من صعوبة إسناد المسؤولية (Attribution)، ما يعيق إثبات الصلة بين الهجوم وجماعةٍ مسلّحةٍ معيّنة، ويحدّ من إمكانية المحاسبة.

كما يُعَدّ قصور آليات الإنفاذ عاملاً جوهرياً في إشكالية التطبيق. ففي حين أنّ جرائم الحرب والجرائم ضد الإنسانية يجوز ملاحقتها دولياً أو داخلياً، تتطلّب الملاحقة القضائية الناجحة توافر الأدلة وشهادات الشهود، وأيضاً القبض على المشتبه بهم. وفي المناطق غير المستقرة أو عديمة القانون، قد لا تتوافر هذه الشروط. وفي حين تُعدّ المحكمة الجنائية الدولية (ICC)

آليةً دوليةً لملاحقة مرتكبي الجرائم الخطرة، فإنّ سلطاتها القضائية محدودة كما أنها بحاجةٍ للتعاون مع الدول، وهو ما قد لا يتوافر، لا سيما إن كانت للدول مصالح سياسية أو استراتيجية في النزاع.

وتعكس هذه العوائق، المتغلغلة في السياقات المحلية والدولية، واقع النزاعات المسلحة غير الدولية، بما يؤكّد أنه رغم وجود التزامات وحظرٍ واضح في نصوص القانون الدولي الإنساني، فإنّ الامتثال الفعلي لها يبقى رهيناً بعوامل شتّى حين تتواجه الدول والجهات المسلحة غير الحكومية وأساليب الحرب المتطورة في مسرحٍ واحد. وتبيّن هذه الحالة ضرورة استمرار الجهود الدولية في الدعوة والتوضيح القانوني وإيجاد وسائل مبتكرة لضمان ألا تتحوّل مبادئ القانون الدولي الإنساني إلى مجرد بياناتٍ رمزية، وإنما تحظى بالقوة الفعلية لحماية حياة المدنيين.

طالما استُخدمت الحرب النفسية في النزاعات المسلحة بغرض إضعاف إرادة العدو للقتال، وتعطيل قدرته على اتخاذ القرار، وبث الذعر في صفوفه. وفي النزاعات المسلحة غير الدولية، تتخذ هذه التكتيكات أبعاداً جديدة مع انتشار التكنولوجيا الرقمية ومنصّات التواصل الاجتماعي على نحوٍ واسع. إذ تتجاور الأساليب التقليدية—مثل بث الرسائل عبر مكبرات الصوت أو توزيع المنشورات الورقية—مع نشر مقاطع الفيديو على الإنترنت، وتدبير حملات تشويهٍ رقمية، وبثّ دعايةٍ مدروسةٍ على مواقع التواصل الاجتماعي. ومع أنّ هذه الأساليب قد تمنح أطراف النزاع

مكاسب تكتيكية ملموسة، فإنها تنطوي على مخاطر جسيمة تطال السكان المدنيين العالقين وسط دوامة العمليات النفسية.

وقد أتاحت منصّات "فيسبوك" و"تويتر" وغيرها من التطبيقات إمكان إيصال رسائل ترويعية أو مضلّلة إلى جمهورٍ عالمي في غضون دقائق معدودة، ما يضاعف الأثر النفسي على كلٍّ من المدنيين والمقاتلين. وفي كثيرٍ من النزاعات المسلحة غير الدولية، تنشر الجماعات المسلحة محتوىً عنيفاً لإرهاب خصومها، في حين قد تنشر الحكومات رواياتٍ (صحيحة أو مفبركة) لجرائم تُنسب للعدو بغرض حشد الدعم الشعبي أو قمع الاعتراضات. ومع أنّ التأثير على ذهنية الخصم كان ولا يزال جزءاً من الاستراتيجية العسكرية، فإنّ سرعة التواصل الرقمي واتساع نطاقه قد بلغ حداً غير مسبوق.

ويُحظَر تعمّد استهداف المدنيين بأعمال أو تهديداتٍ غايتها الرئيسية بثّ الذعر، عملاً بالمادة ٥١(٢) من البروتوكول الإضافي الأوّل، التي تنصّ على حظر ترويع السكان المدنيين، وتجسد مبدأً عرفياً أشمل. ورغم أنّ هذا البروتوكول يُطبق من حيث الأصل على النزاعات الدولية، فقد أكّدت المحكمة الجنائية الدولية ليوغوسلافيا السابقة في قضية (Prosecutor v. Stanislav Galić) أنّ ترهيب المدنيين، من خلال إطلاق النار عليهم أو

قصفهم بشكلٍ يستهدف إخافتهم، يُعدّ انتهاكاً للقانون الدولي الإنساني بصفةٍ أعم.[١]

وتناولت قضية (Galić) حصار سراييفو، حيث شنّ جيش صرب البوسنة هجماتٍ متواصلة على المدنيين، وخلصت المحكمة إلى أنّ بثّ الرعب في أوساط المدنيين كان هدفاً عملياً صريحاً، وليس مجرد أثرٍ جانبي لاستهدافٍ مشروع. ويُظهر هذا المثال كيف أنّ توظيف الخوف بوصفه أداةً رئيسية، بدلاً من كونه نتيجة عرضية للهجوم على أهدافٍ عسكرية مشروعة، ينتهك المبادئ الإنسانية الأساسية.[٢]

وفي النزاعات المسلحة غير الدولية الحديثة، بات الانتقال من الترهيب المادي إلى الرقمي يزيد من وطأة هذه الانتهاكات، إذ يكفي لجماعةٍ مسلحةٍ نشر مقاطع مصوّرةٍ لعقوباتٍ عنيفة، أو تدبير حملاتٍ إلكترونيةٍ تمجّد سفك الدماء أو توجّه تهديداتٍ ضد السكان المدنيين. وقد يعاني المدنيون جراء القلق الممتدّ أو النزوح القسري أو التفكك الاجتماعي، لا سيما إذا اقترنت التهديدات الرقمية بأفعال عنفٍ على الأرض. فضلاً عن ذلك، فإنّ غياب القدرة على تحديد مصدر الحملات النفسية عبر الإنترنت

[1] Chainoglou, K. (2016). Psychological warfare. In Max Planck Encyclopedia of Public International Law. Max Planck Institute for Comparative Public Law and International Law

[2] International Criminal Tribunal for the former Yugoslavia. (n.d.). Prosecutor v. Stanislav Galić. Case No. IT-98-29-T. Retrieved from https://www.icty.org/x/cases/galic/tjug/en/gal-tj031205e.pdf

وكثرة استخدام الحسابات المجهولة يعرقلان جهود المحاسبة. ورغم أنّ اللجنة الدولية للصليب الأحمر وغيرها من المنظمات الإنسانية تحثّ الأطراف دوماً على تجنّب ترويع المدنيين، فإن البيئة المتسارعة في العالم الرقمي تقتضي وضع إرشاداتٍ أوضح وآليات تنفيذٍ أكثر دقة. وتسعى اللجنة الدولية للصليب الأحمر عبر التواصل المباشر مع الجماعات المسلحة إلى تعميق الاحترام للقانون الدولي الإنساني حتى في السياقات التكنولوجية المتقدّمة، بيد أنّ مدى فاعلية هذه المساعي على أرض الواقع يظل رهناً بعوامل عديدة.[١]

تتسع حرب المعلومات لتشمل ما هو أكثر من مجرد الترهيب النفسي، وإن كانت تتقاطع معه كثيراً. ففي النزاعات المسلحة غير الدولية، يمكن أن يُعادل التحكم في تدفق المعلومات أو توجيهها فعالية العمليات الهجومية نفسها. إذ قد تؤدي أساليب الدعاية والتضليل وصياغة السرديات بعناية إلى تشكيل الرأي العام المحلي والدولي، وتأجيج الكراهية، ودفع العنف ضد فئاتٍ بعينها، ليصل الأمر أحياناً إلى انتهاكات فادحة لحقوق الإنسان أو حتى الإبادة الجماعية.

ويحمي القانون الدولي الإنساني المدنيين ليس فقط من الأذى المادي، بل ومن أشكال التعرّض التي تنال من كرامتهم أيضاً. فتضمن اتفاقيات جنيف الثالثة والرابعة، على سبيل المثال، أحكاماً تمنع عرض أسرى الحرب

[1] Additional Protocol I (1977), Articles 57(2)(a)(iii) and 57(2)(b); ICRC, Study on Customary International Humanitarian Law, 2005, Rules 18 and 19.

والمحتجزين على العامة بقصد إذلالهم. وقد وُضع هذا المنع في الأصل ليتماشى مع الظروف الإعلامية التقليدية، لكنه يمتد منطقياً إلى البيئات الرقمية حيث يمكن بثّ مقاطع مهينة أو اعترافاتٍ قسريةٍ على وسائل التواصل الاجتماعي، ما يُعرّض المحتجز لامتهان الكرامة ويحرّض الجمهور على الانتقام أو يفاقم من حدّة العنف. وعليه، فإنّ المبدأ القاضي بعدم جواز إخضاع الأفراد لمعاملة مهينة أو إثارة انتباه الرأي العام بطرقٍ تقلّل من احترام آدمية الأفراد يظل قائماً، سواءٌ في بثٍ إذاعي أو تلفزيوني أو عبر بثّ مباشر على منصّة "فيسبوك".

وفي قضية (Prosecutor v. Radovan Karadžić)، تبرز بوضوحٍ محورية دور الإعلام في إذكاء النزاعات، حيث استغلّ كاراديتش الدعاية لشيطنة المجتمع البوسني المسلم، وبث الخوف والكراهية اللذين مهّدا لوقوع فظائع إبّان حرب البوسنة. وبينما تناولت هذه القضية جانباً مما صنّفته المحكمة نزاعاً دولياً، إلا أن استنتاجاتها تنطبق على سياق النزاعات الداخلية أيضاً، حيث غالباً ما تُستهدف مجموعاتٌ عرقية أو دينية أو سياسية داخل البلد الواحد بالتحريض الدعائي.

وفي عصرنا الرقمي، يؤدي الانتشار السريع للمحتويات—مثل الفيديوهات والصور والميمات والمنشورات—إلى تضخيم تأثير حرب المعلومات. وقد يتعرّض السكان المدنيون لوابلٍ من الرسائل التي تُضلّل أو تُحرّض أو تُرهّب، ما يضاعف الانقسامات المجتمعية القائمة. كما يمكن تعطيل وصول المساعدات الإنسانية إذا انتشرت معلومات كاذبة

حول أهداف العاملين في المجال الإنساني، فتمنع السكان من قبول الإغاثة أو تحبط مساعي إنشاء ممرات آمنة. وعندما تحوَّل "الآخر" إلى شرٍ مطلقٍ، يُقوَّض بذلك السعي للامتثال للقانون الدولي الإنساني ويُشكَّك في جدواه، سواء من حيث حماية الأسرى أو الانخراط في مفاوضات السلام.

وتُفاقِم الفجوات التنظيمية هذه المخاوف؛ إذ على الرغم من أن الدول والجهات المسلحة من غير الدول تظل ملتزمةً بأحكام القانون الدولي الإنساني، فإنّ شركات التكنولوجيا ليست ملزمةً مباشرةً بقواعده. كما أنّ شروط الخدمة وضوابط المحتوى في منصّاتها، إلى جانب القوانين الوطنية والإقليمية، تؤثر في سرعة إزالة المحتوى الضار أو الإشارة إليه كتحريضٍ. وقد دعت اللجنة الدولية للصليب الأحمر وغيرُها من الخبراء الدولَ إلى وضع أطرٍ قانونيةٍ أكثر فعالية للحدّ من النتائج الإنسانية السلبية لحرب المعلومات، مؤكّدين أنّ سرعة وقوّة التواصل الرقمي في عصرنا يستلزمان رقابةً أشد وضوحاً ومبادئ معياريةً أشد تحديداً. وفي غياب مثل هذه الأطر، يخشى أن تطغى فوضوية ساحات القتال الرقمية على مبادئ حماية المدنيين المنصوص عليها في القانون الدولي الإنساني.

إذا كانت حرب المعلومات تهدف إلى التأثير في تصوّرات الخصوم، فإنّ الحرب السيبرانية تتيح التسبب بآثار مادية واسعة النطاق أو انهيار البنى التحتية دون إطلاق رصاصة واحدة. وتشهد نزاعات متنامية—بما فيها النزاعات المسلحة غير الدولية—استخدام عملياتٍ سيبرانية يمكنها تخريب شبكات الكهرباء أو منشآت الرعاية الصحية أو نظم الاتصالات،

مخلّفةً الفوضى لدى المقاتلين والمدنيين على حدّ سواء. وتثير هذه التطورات أسئلةً جوهرية بشأن كيفية تفسير مبادئ القانون الدولي الإنساني—كالتمييز والتناسب والضرورة—وتطبيقها في النطاق الرقمي.

وقد أكّدت محكمة العدل الدولية (ICJ) في رأيها الاستشاري بشأن مشروعية التهديد أو الاستخدام للأسلحة النووية أنّ القانون الدولي الإنساني يسري على "جميع أشكال الحرب"، ما يشكّل أساساً لمدّ نطاق أحكامه إلى الفضاء السيبراني. ويعني هذا أنّ أي عمليةٍ سيبرانية تُنفّذ في نزاعٍ مسلحٍ غير دولي، تماماً كما في النزاع المسلح الدولي، ينبغي أن تلتزم بقواعد الحظر على استهداف المدنيين أو إلحاق الضرر المفرط مقارنةً بالميزة العسكرية المتوقعة. غير أنّ تطبيق هذه القواعد عملياً ليس بالأمر اليسير، إذ غالباً ما يعتمد المدنيون والعسكريون على البنية التحتية الإلكترونية نفسها، دون وجود خط واضح يُفرّق بين الأنظمة المستخدمة للخدمات العامة الحيوية وتلك المخصصة للأغراض القتالية.[١]

ويعزّز عنصر صعوبة إسناد الهجمات (Attribution) من درجة التعقيد؛ إذ عادةً ما تمرّ الهجمات السيبرانية عبر خوادم في ولاياتٍ قضائيةٍ متعدّدة ويجري تنفيذها مع إخفاء الهوية، ما يجعل اكتشاف المهاجم وتأكيد هويته تحدياً قانونياً. وفي حال عدم توافر أدلةٍ قاطعة تربط

[1] International Court of Justice (1996). Advisory Opinion on the Legality of the Threat or Use of Nuclear
Weapons. Retrieved from https://www.icj-cij.org/en/case/95/advisory-opinions

الاختراق السيبراني بجماعةٍ مسلّحةٍ معيّنة وتثبت ارتكابه في سياق النزاع، فإنّ الضحايا يجدون أنفسهم أمام محدودية سبل الانتصاف، وتنخفض احتمالية مساءلة الفاعلين. كما يغدو إثبات مسؤولية القيادة أو التواطؤ في الهجمات السيبرانية عمليةً شاقة، خصوصاً إن كانت الهجمات من تنفيذ مجموعات قرصنة (هاكرز) فضفاضة الارتباط.

وتقود اللجنة الدولية للصليب الأحمر جهوداً للتأكيد على أنّ القيود الإنسانية المفروضة على الحروب تنطبق كذلك على العمليات السيبرانية. ومع تزايد التقارير عن انخراط نزاعات عديدة—وخاصة في منطقة الشرق الأوسط—في عناصرٍ سيبرانية، تتعالى الأصوات المطالبة بمواءمة القانون الدولي الإنساني مع هذا النوع الناشئ من الحروب. فإمكان تعطيل كامل البنية التحتية لدولةٍ ما بضغطة زر واحد يفاقم الخوف من أن تكون الخسائر الجانبية أو العرضية التي قد تَلحَق بالمدنيين أضعاف ما يجنيه الجانب العسكري من مكاسب. على سبيل المثال، يُمكن أن يتسبب الهجوم على شبكات الكهرباء بحرمان المستشفيات ومحطات معالجة المياه والمنشآت الحيوية الأخرى من الطاقة، مُعرّضاً حياة أعداد هائلة من المدنيين للخطر. ورغم أنّ اتفاقيات جنيف القائمة لا تتناول الحرب السيبرانية تحديداً، فإنه يمكن تفسير مبادئها بما يغطّي هذه الحالات. لكن المسألة الحاسمة هي ما إذا كان راسمو السياسات والقادة

العسكريون والجهات المسلحة غير الحكومية سيختارون الالتزام بهذه التفسيرات، أم سيستغلون الغموض لحصد مكاسبٍ تكتيكية.[1]

المطلب الثاني

دور الجهات المسلحة من غير الدول في النزاع المسلح غير الدولي (NIAC)

تمثِّل الجهات المسلحة من غير الدول، بما فيها الميليشيات والمتمردين والمنظمات المصنفة إرهابية، أطرافاً رئيسية في العديد من النزاعات المسلحة غير الدولية (NIACs). وتُسلّط مشاركتها الضوء على المسألة الخلافية المتعلقة بكيفية إلزام مجموعات لا تخضع للهيكلية الرسمية للدول بالتقيد بقواعد قانونية لم تكن طرفاً في إبرامها. ومع ذلك، فإنّ القانون الدولي العرفي والمادة ٣ المشتركة في اتفاقيات جنيف تُلزم جميع الأطراف في النزاع باحترام الحد الأدنى من المعايير الإنسانية.

تُظهِر القضايا المنظورة أمام المحكمة الجنائية الدولية (ICC) وغيرها من المحاكم الدولية إمكانية مساءلة الجهات المسلحة من غير الدول عن انتهاكات جسيمة للقانون الدولي الإنساني (IHL). فعلى سبيل المثال، تناولت قضيتا Prosecutor v. Jean-Pierre Bemba Gombo وProsecutor v. Bosco Ntaganda الجرائم المرتكبة في جمهورية

[1] International Committee of the Red Cross (2019). Avoiding civilian harm from military cyber operations
during armed conflicts. Geneva: ICRC. Retrieved from https://www.icrc.org/en/download/file/96008/thepotential-human-cost-of-cyber-operations.pdf

الكونغو الديمقراطية من قبل جماعات مسلحة ارتكبت منهجياً جرائم قتل واغتصاب وقامت بتجنيد أطفال للقتال. وقد أكّدت المحاكم المعنية أنّ العمل خارج إطار حكومة معترف بها لا يعفي القادة من المسؤولية عن ارتكاب جرائم حرب. ويمكن تطبيق مبدأ مسؤولية القادة (Command Responsibility) إذا تقاعس القادة عن منع الانتهاكات التي يرتكبها مرؤوسوهم أو معاقبتهم عليها.[1]

ورغم إمكانيات المساءلة الرسمية هذه، فإنّ الإنفاذ العملي يمثّل تحدياً كبيراً. إذ غالباً ما تعمل الجماعات المسلحة في مناطق نائية أو تفتقر إلى سيادة القانون، ما يجعل وصول الأجهزة الوطنية والدولية إليها محدوداً. وقد تمتنع بعض الدول عن اعتقال مشتبه بهم يتمتعون بنفوذ محلي أو بدعمٍ واسع، أو ربما تدعم تلك الدول بعض المجموعات لأسباب جيوسياسية، الأمر الذي يثبط جهود الإنفاذ المحايد. وعلاوة على ذلك، قد تتصف بعض الجماعات المسلحة نفسها باللامركزية الشديدة، فلا يتسنّى تحديد بنية قيادية متكاملة يمكن محاسبتها بصورة شاملة.

تُدرك اللجنة الدولية للصليب الأحمر (ICRC) هذه الصعوبات، وقد طوّرت استراتيجيات لإشراك الجهات المسلحة من غير الدول في حوارٍ حول القانون الدولي الإنساني. ومن خلال مناقشاتٍ سرية وبرامج تدريبية

[1] Djukić, D., & Pons, N. (Eds.). (24 Sep. 2018). The Companion to International Humanitarian Law. Leiden,
The Netherlands: Brill | Nijho

وتوزيع كتيّبات قانونية مصممة خصيصاً للميليشيات والجماعات المتمردة، تسعى اللجنة الدولية إلى إقناعها بأنّ التقيّد بالمعايير الإنسانية يمكن أن يضفي شرعيةً على قضيتها ويقلّل من الإضرار بالمدنيين. ورغم ما تنطوي عليه هذه المشاركة من حساسية—ولا سيما عند تصنيف تلك الجماعات كمنظمات إرهابية—فقد أسفرت أحياناً عن التزامات إيجابية، مثل التعهّد بوقف تجنيد الأطفال أو احترام العاملين في المجال الطبي. وبالرغم من أنّ بعض الفصائل قد لا تلتزم عملياً بهذه التعهدات، فإنّ مجرّد إقرارها يشي بأنّ للسلطة الأخلاقية والقانونية للقانون الدولي الإنساني أثراً ممكناً على الجهات المسلحة من غير الدول في ظروفٍ معينة.

وتُشكّل قوانين مكافحة الإرهاب عائقاً آخر، إذ يمكنها تقييد أو حتى تجريم محاولات الجهات المحايدة التحاور مع الجماعات المصنفة إرهابية. ومع أنّ غرض هذه القوانين قطع قنوات الدعم المادي للعناصر العنيفة المتطرفة، فإنها قد تعرقل في الوقت ذاته المفاوضات الإنسانية الضرورية، فتمنع إقامة ممراتٍ آمنة أو تبادل الأسرى أو عقد هدنٍ موضعية. ويؤدي هذا أحياناً إلى ترسيخ دائرة العنف أكثر فأكثر، فيتراجع تطبيق معايير القانون الدولي الإنساني إلى الهامش. ويظل الموازنة بين اعتبارات الأمن المشروع والحاجة إلى تخفيف معاناة المدنيين مهمة حساسة تواجه الدول والمنظمات الدولية والمنظمات غير الحكومية على حدٍّ سواء.

رغم تعدّد العوائق التي تعرقل تطبيق القانون الدولي الإنساني في النزاعات المسلحة غير الدولية—من الغموض بشأن تصنيف النزاع إلى ظهور العمليات السيبرانية—فإنّ هناك فرصاً حقيقية لتعزيز الامتثال. ولعلّ أحد السبل الممكنة يكمن في تحديث المعاهدات الدولية القائمة لتتناول على نحوٍ أوضح قضايا مثل الهجمات السيبرانية وحملات التضليل المعلوماتي. ومع أنّ البروتوكول الإضافي الثاني يتطرق إلى الجوانب الرئيسة للنزاع المسلّح غير الدولي، إلا أنّ صياغته تسبق العصر الرقمي، الأمر الذي يفسح مجالاً للدول لتوضيح الأحكام المتعلقة بالأساليب الحديثة في إدارة النزاعات أو توسيع نطاقها. وقد يساهم وضع معايير صريحة تتعلق بالعمليات السيبرانية أو الدعاية الرقمية في تقديم إرشاداتٍ أوضح لأطراف النزاع بشأن السلوك المسموح، مما يحدّ من الغموض الذي قد يؤدي إلى الانتهاكات.

أما إذا حالت العقبات السياسية دون تعديل المعاهدات الراسخة، فقد يكون وضع صكوك قانونية جديدة موجَّهة تحديداً لبعض أساليب الحرب خطوةً ممكنة. فعلى سبيل المثال، يمكن لاتفاقٍ دوليٍ ينظّم الحرب السيبرانية أن ينصّ بوضوح على كيفية التمييز بين الأهداف المدنية والعسكرية في الفضاء الافتراضي، إلى جانب وضع آليات للتحقيق وتحديد المسؤولية. وبالمثل، قد يُساعد صكٌّ خاصٌّ بـ"حرب المعلومات" (Information Warfare) على توضيح حدود الدعاية وحظر التحريض على الإبادة الجماعية أو الجرائم ضد الإنسانية عبر الوسائط الرقمية. ورغم أنّ

التفاوض حول مثل هذه الصكوك لا يخلو من التعقيد، فإنّها قد تعزّز المساءلة وتشكل مرجعاً لتشريعاتٍ وطنية.

وعلاوةً على الإطار التشريعي، يمكن للمبادرات التثقيفية أن تُحدث أثراً عملياً في تعزيز امتثال القانون الدولي الإنساني. فمن خلال ضمان فهم القوات المسلحة الرسمية والجهات المسلحة غير الحكومية على السواء للمبادئ الأساسية—التمييز والتناسب والضرورة والمعاملة الإنسانية— يمكن التخفيف من النزعة إلى اعتبار كلٍّ من الخصوم وغير المقاتلين أهدافاً مشروعة. وعادةً ما تقوم اللجنة الدولية للصليب الأحمر والأمم المتحدة ومنظمات غير حكومية مختلفة بتقديم تدريباتٍ للقوات العسكرية الحكومية. أما توسيع هذه التدريبات أو تكييفها لتشمل الجماعات المتمرّدة، فينطوي على مخاطر سياسية وأمنية، إلا أنّ استعداد بعض الجماعات المسلحة للانخراط في المسار الإنساني يشير إلى إمكان تحقيق تقدّم في هذا الصدد

وبأي حال، فإنّ تعزيز الامتثال يستلزم أيضاً دعم آليات المساءلة. فقد أثبتت المحكمة الجنائية الدولية وغيرها من المحاكم أنّ بإمكانها ملاحقة فاعلين من غير الدول في النزاعات المسلحة غير الدولية بسبب الانتهاكات الجسيمة. ويجب الحرص على تعاون الدول مع هذه الهيئات، واعتقال المشتبه بهم، والحفاظ على الأدلة المتصلة بالجرائم، بهدف التصدي لخطر الإفلات من العقاب. كما يمكن للإصلاحات القانونية الداخلية أن تمنح المحاكم الوطنية صلاحية محاكمة جرائم الحرب

المرتبطة بالنزاعات المسلحة غير الدولية، ما يشكّل مكمِّلاً للولاية القضائية الدولية.

وبالنسبة للتكنولوجيا، فبإمكانها أن تؤدي دوراً إيجابياً في الحدّ من أضرار النزاع، رغم ما تخلقه من تهديدات جديدة. إذ يمكن الاستفادة من صور الأقمار الصناعية وتقنيات البلوك تشين (Blockchain) في حفظ السجلات وتحليلات البيانات المتقدّمة لتحسين إيصال المساعدات الإنسانية ومراقبة الأوضاع على أرض المعركة وتوثيق جرائم الحرب بدقة أكبر. وإذا ما استُخدمت هذه الأدوات بأخلاقيات مسؤولة، يمكن أن تساعد في تعزيز الحماية الإنسانية عبر صعوبة إخفاء الانتهاكات أو إنكارها. كما يمكن تشجيع المجتمعات المحلية ومنظمات المجتمع المدني على الإبلاغ عن الانتهاكات عبر منصات رقمية آمنة، مما يزيد من قدرة آليات المساءلة على رصد تلك الانتهاكات.

وفي المحصلة، إنّ تعزيز القانون الدولي الإنساني في نزاعات العصر الحديث غير الدولية يحتاج إلى مقاربةٍ متعددة المحاور تشمل تطوير الآليات القانونية، والحرص على التدريب المتعمّق، وتعزيز آليات المساءلة، وتوظيف التكنولوجيا بأسلوبٍ مبتكر، والانخراط الإيجابي مع جميع الأطراف. ورغم التحديات الكبرى التي تواجه هذه المبادرات، خصوصاً في الدول الهشة أو التي تعاني نزاعاتٍ مستمرة، فإنها تمثّل في النهاية التزاماً عالمياً للتخفيف من وحشية الحرب. وتُعدّ اللجنة الدولية

للصليب الأحمر فاعلاً محورياً في هذه الجهود، حيث تذكّر الحكومات وقادة المتمردين والرأي العام على الدوام بأنّه حتى في غياهب النزاع الداخلي، لا بدّ أن تظل القيم الإنسانية هي البوصلة الحاكمة.

الخاتمة

لقد أفضى التطور في أساليب الحرب إلى توظيفٍ متعاظمٍ للتقنيات الرقمية، ما ولّد تحدياتٍ غير مسبوقة للأمن الدولي وللأطر القانونية الساعية إلى التخفيف من ويلات النزاع. وقد تناولت هذه الدراسة الطبيعة المتعددة الأوجه للهجمات السيبرانية في سياق النزاعات المسلحة غير الدولية (NIACs)، مُبرزةً آثارها العميقة على القطاعات الاقتصادية والبنى التحتية الحيوية والقطاع العسكري. ومع تزايد وتيرة هذه الهجمات وتطورها، يزداد خطر تعطيل الخدمات الأساسية وزعزعة الاقتصادات وتقويض الأمن الوطني، ما يؤكد الحاجة الملحّة إلى بلورة آليات قانونية متينة لتنظيم هذه الأفعال.

وركّزت الدراسة على مدى انطباق القانون الدولي الإنساني على العمليات السيبرانية. فرغم احتفاظ مبادئ القانون الدولي الإنساني—مثل التمييز والتناسب والضرورة والمعاملة الإنسانية—بوجاهتها الأساسية، فإنّ تطبيقها في الفضاء السيبراني تعترضه تعقيداتٌ جمّة. إذ تجعل صعوبة إسناد الهجمات السيبرانية والفصل غير الواضح أحياناً بين الأهداف المدنية والعسكرية، فضلاً عن الطبيعة اللامركزية لبعض الجهات المسلحة غير الحكومية، مسألة إنفاذ القانون الدولي الإنساني شديدة

التعقيد. وتتفاقم هذه المعوّقات في النزاعات المسلحة غير الدولية، حيث غياب الأطر القانونية الشاملة وتردّد الدول في الاعتراف بطابع النزاع، ما يُضعف الامتثال للمعايير الإنسانية

علاوةً على ذلك، أبرزت الدراسة الدور المحوري للجهات المسلحة من غير الدول في النزاعات المسلحة غير الدولية وصعوبة ضمان التزامها بالقانون الدولي الإنساني. فبالنظر إلى طبيعتها المتشظية وسريّة عملياتها، وكونها في أحيانٍ كثيرة خارج نطاق الالتزام القانوني الرسمي، تبرز الحاجة إلى أساليب مبتكرة لتعزيز احترام القواعد الإنسانية. وتشمل تلك الأساليب الحوار والتعليم بدعمٍ من منظمات كاللجنة الدولية للصليب الأحمر، التي تمثل وسيلةً أساسية لترسيخ الامتثال لهذه القواعد بين جميع أطراف النزاع.

ومن أجل مجابهة هذه التحديات، يصبح من الضروري تحديث المعاهدات الدولية القائمة، بحيث تشمل العمليات السيبرانية والحرب الرقمية بشكلٍ صريح، وتقدِّم توجيهاتٍ أوضح بشأن التمييز بين الأهداف المدنية والعسكرية في الفضاء الافتراضي. كما يمكن تطوير صكوك قانونية متخصصة تُعنى تحديداً بالهجمات السيبرانية وحرب المعلومات، بما يضع قواعد تفصيلية ويؤسس لآليات تحقيق وإسناد المسؤولية، لسدّ الفراغات التنظيمية. ويظلّ تعزيز آليات المساءلة بتقوية دور الهيئات الدولية كالمحكمة الجنائية الدولية (ICC) أمراً حاسماً، لا سيما عبر

الارتقاء بقدرات جمع الأدلة وضمان تعاون الدول في ملاحقة جرائم الحرب التي تندرج فيها الأبعاد السيبرانية.

وتمثل المبادرات التعليمية محوراً مهماً في هذه المنظومة. فتعزيز البرامج التدريبية في القانون الدولي الإنساني لتشمل السيناريوهات السيبرانية يمكّن الفاعلين الرسميين وغير الرسميين من اكتساب فهمٍ معمّقٍ للمبادئ الإنسانية في السياق الرقمي. كما أنّ توظيف التقنيات المتقدّمة، مثل أنظمة البلوك تشين لحفظ المستندات بأمان، وصور الأقمار الصناعية لرصد مدى الامتثال، قد يعزّز جهود تطبيق المعايير القانونية وحماية المدنيين من آثار الحرب السيبرانية.

ويبقى توطيد التعاون الدولي مسألةً لا غنى عنها. إذ يؤدي تنسيق الجهود بين الدول والمنظمات الدولية والقطاع الخاص دوراً حاسماً في تطوير معاييرٍ سيبرانية مشتركة وتعزيز الدفاعات السيبرانية الجماعية. وقد يُسهم دعم الجهات المسلحة من غير الدول عبر قنواتٍ محايدة في دفعها نحو التقيّد بالقانون الدولي الإنساني، ما قد يضفي قدراً من الشرعية على جهودها ويخفف من معاناة المدنيين.

إن التداخل بين الحرب السيبرانية والقانون الدولي الإنساني في النزاعات المسلحة غير الدولية يشكّل حقل بحث متطوّر بسرعة، ويتطلب قدراً متصاعداً من الاهتمام الأكاديمي ومن القرارات السياسية الاستباقية. وينبغي للأبحاث المستقبلية أن تركّز على مزيدٍ من التحديد القانوني للإطار المنظّم للعمليات السيبرانية، واستكشاف دور التقنيات المستحدثة

في تأجيج الهجمات السيبرانية أو الحدّ منها، وتقييم مدى فاعلية تطبيق القانون الدولي الإنساني في سيناريوهات الصراع الواقعية. علاوةً على ذلك، يظلّ السعي إلى تعزيز التعاون والتوافق الدوليين حول معايير الفضاء السيبراني أمراً حاسماً لتوحيد الجبهة الدولية في مواجهة إساءة استغلال هذا الفضاء في النزاعات.

ومع استمرار تطور ساحات القتال بفعل المنجزات التكنولوجية، تزداد ضرورة تكييف القانون الدولي الإنساني وتعزيزه. وإنّ ضمان امتداد أحكام القانون الدولي الإنساني لتشمل الهجمات السيبرانية في النزاعات المسلحة غير الدولية ليس مجرد مطلبٍ قانوني، بل هو واجبٌ أخلاقيٌّ يهدف إلى صون الإنسانية وسط التعقيدات التي تميّز الحروب المعاصرة. وبالتصدي للتحديات واغتنام الفرص التي أوردتها هذه الدراسة، يمكن للمجتمع الدولي أن يتمسّك بمبادئ الإنسانية والعدالة، حتى في أكثر البيئات القتالية حداثةً واضطراباً.