حماية المدنيين في الفضاءات الرقمية أثناء النزاعات المسلحة
(دراسة في ضوء أحكام القانون الدولي الإنساني)

أ.د. سرمد عامر عباس[1]
كلية القانون / جامعة بابل

م.م. فاتن عبد الجبار لفتة[2]
مديرية تربية محافظة بابل

تاريخ استلام البحث:2026/5/19 تاريخ قبول النشر:2026/6/1 تاريخ النشر:2026/6/11

الملخص : يتناول هذا البحث إشكالية تطبيق مبادئ القانون الدولي الإنساني على الهجمات السيبرانية التي تستهدف المدنيين أو البنى التحتية الرقمية المدنية أثناء النزاعات المسلحة. يهدف البحث إلى تحديد مدى كفاية النصوص القانونية الحالية (اتفاقيات جنيف 1949 وبروتوكوليها الإضافيين) في حماية المدنيين في الفضاء الرقمي، مع تحليل أبرز التحديات التقنية والقانونية كمشكلة الإسناد وصعوبة التمييز بين الأهداف العسكرية والمدنية في البيئة الرقمية. اعتمد البحث المنهج الوصفي التحليلي، مستعرضاً حالات تطبيقية من الحرب في أوكرانيا (2022–2025) والهجمات السيبرانية على قطاع غزة. خلص البحث إلى ضرورة تعديل اتفاقيات جنيف لتشمل العمليات السيبرانية صراحةً، وإنشاء آلية دولية للتحقيق في الهجمات الرقمية، وإلزام الدول بحماية البنية التحتية الرقمية المدنية بموجب قانون دولي ملزم.

الكلمات المفتاحية: قانون دولي إنساني، حماية المدنيين، فضاءات رقمية، هجمات سيبرانية، مبدأ التمييز، الحرب السيبرانية.

Protection of Civilians in Digital Spaces during Armed Conflicts
(A Study in Light of the Provisions of International Humanitarian Law)

Prof. Dr. Sarmad Amer Abbas[1]
Faculty of Law / University of Babylon

prof. Assistant. Faten Abdulgabbar Lafta[2]
Babylon Education Directorate

Abstract: This research addresses the problematic application of International Humanitarian Law (IHL) principles to cyberattacks targeting civilians or civilian digital infrastructure during armed conflicts. The study aims to determine the adequacy of existing legal frameworks—specifically the 1949 Geneva Conventions and their Additional Protocols—in protecting civilians within digital spaces. Furthermore, it analyzes prominent technical and legal challenges, such as the problem of attribution and the difficulty of distinguishing between military and civilian targets in the digital environment.

Adopting a descriptive-analytical approach, the research reviews case studies from the war in Ukraine (2022–2025) and cyberattacks on the Gaza Strip. The study concludes with the necessity of amending the Geneva Conventions to explicitly encompass cyber operations, establishing an international mechanism for investigating digital attacks, and mandating states to protect civilian digital infrastructure under a binding international legal framework.

Keywords: International Humanitarian Law (IHL), Protection of Civilians, Digital Spaces, Cyberattacks, Principle of Distinction, Cyber Warfare.

المقدمة

شهد العقدان الأخيران تحولاً جذرياً في طبيعة النزاعات المسلحة، حيث انتقل جزء كبير منها إلى الفضاءات الرقمية. فأصبحت الهجمات السيبرانية سلاحاً استراتيجياً تستخدمه الدول والجماعات المسلحة غير الحكومية لتعطيل البنى التحتية الخدماتية للمدنيين، كشبكات الكهرباء والمياه والمستشفيات والاتصالات . ورغم أن القانون الدولي الإنساني (يُعرف أيضاً بالقانون الإنساني أو قانون النزاعات المسلحة) يضع قواعد صارمة لحماية المدنيين في النزاعات التقليدية، إلا أن هذه القواعد وُضعت أصلاً لتنظيم الأسلحة التقليدية، مما يطرح تساؤلات جدية حول قابلية تطبيقها على العمليات السيبرانية.

إذ تُعدّ مشكلة هذا البحث أن الفجوة بين التطور التكنولوجي السريع للهجمات السيبرانية وبطئ تطوير القانون الدولي قد خلقت منطقة رمادية قانونية يستغلها أطراف النزاع لاستهداف المدنيين دون خوف من المساءلة. فوفقاً لتقرير صادر عن اللجنة الدولية للصليب الأحمر (ICRC) عام 2024، زادت الهجمات السيبرانية على المنشآت الطبية بنسبة 300% خلال السنوات الخمس الماضية، دون أن تؤدي أي من هذه الهجمات إلى إدانة قانونية دولية. وبناءً عليه، يسعى هذا البحث للإجابة عن الأسئلة التالية:

1. كيف تطبق مبادئ القانون الدولي الإنساني على العمليات السيبرانية المرتبطة بالنزاعات المسلحة؟

2. ما التحديات التقنية والقانونية التي تحول دون تطبيق هذه المبادئ على العمليات السيبرانية؟

3. ما الإصلاحات القانونية المطلوبة على مستوى القانون الدولي لسد الثغرات الحالية وحماية المدنيين بشكل فعال في الفضاء الرقمي؟

فرضية الدراسة:

يفترض البحث أن قواعد القانون الدولي الإنساني تنطبق على العمليات السيبرانية المرتبطة بالنزاعات المسلحة، إلاّ أن التطبيق العملي يواجه تحديات تقنية وقانونية تتعلق بالإسناد وتحديد الضرر والتمييز.

المنهجية العلمية:

اعتمد البحث في منهجيته على ثلاثة مناهج متكاملة: المنهج الوصفي التحليلي لدراسة النصوص القانونية، وتحليل آراء الفقهاء وخبراء القانون الدولي؛ المنهج المقارن بين الأحكام التقليدية للقانون الدولي الإنساني والطبيعة الخاصة للعمليات السيبرانية؛ والمنهج التاريخي من خلال تحليل حالات تطبيقية واقعية من النزاعات الأخيرة في أوكرانيا وغزة والسودان.

ينقسم البحث إلى ثلاثة مباحث رئيسية: المبحث الأول، يُخصص للإطار المفاهيمي للفضاءات الرقمية في النزاعات المسلحة، متناولاً فيه تعريف الهجمات السيبرانية وتصنيف الفضاءات الرقمية كساحة قتال ومفهوم المدني في البيئة الرقمية. المبحث الثاني، يحلل مبادئ الحماية الأساسية في القانون الدولي الإنساني (التمييز، التناسب، الاحتياط) ومدى إمكانية تطبيقها على العمليات السيبرانية. أما المبحث الثالث، فيدرس حالات تطبيقية معاصرة مع استخلاص أبرز التحديات القانونية والتقنية، ويقدم توصيات عملية لتعزيز حماية المدنيين في الفضاءات الرقمية.

المبحث الأول

الإطار المفاهيمي للفضاءات الرقمية في النزاعات المسلحة

قبل الخوض في تحليل مدى قابلية تطبيق قواعد القانون الدولي الإنساني على الفضاءات الرقمية، لا بد من توضيح المفاهيم الأساسية التي تشكل ركائز هذا الموضوع. فالهجمات السيبرانية تختلف عن الأسلحة التقليدية في طبيعتها وآثارها[92–89 .p. 1:]، مما يستلزم إعادة تعريف بعض المفاهيم التقليدية كـ"الهجوم" و"الهدف العسكري" و"المدني" في السياق الرقمي [2: ص 89] .

المطلب الأول: تعريف الهجمات السيبرانية في القانون الدولي

لم يرد تعريف موحد لمصطلح "الهجوم السيبراني" في أي من الصكوك الدولية الملزمة، إلا أن الفقه الدولي والخبرات العملية وضعت تعريفات تشغيلية يمكن الاستناد إليها. تعرف اللجنة الدولية للصليب الأحمر الهجوم السيبراني بأنه "أيّة عملية سيبرانية، سواء كانت هجومية أو استكشافية، تُنفذ بقصد تعطيل أو تدمير أو السيطرة على أنظمة معلومات أو بيانات معادية، أو التلاعب بها، بشرط أن تصل آثارها إلى مستوى العنف المطلوب لاعتبارها عملاً عسكرياً بموجب المادة 49 من البروتوكول الإضافي الأول لاتفاقيات جنيف" [3:ص34]. أما دليل تالين (Tallinn Manual 2.0) ، فهو دراسة اكاديمية أعدّها مجموعة خبراء بإشراف مركز التميز للدفاع السيبراني التعاوني التابع لحلف شمال الأطلسي، (فيصنف الهجمات السيبرانية إلى ثلاثة أنواع رئيسية) [2: ص92–95]:-

أولاً: الهجمات السيبرانية التدميرية (Destructive Cyber Attacks): وهي التي تؤدي إلى إتلاف مادي للأجهزة أو البنى التحتية المادية، كالهجمات التي تستهدف محطات توليد الكهرباء أو أنظمة التحكم في السدود أو شبكات المياه. هذا النوع يُعدّ الأقرب إلى الأسلحة التقليدية من حيث الآثار المادية، وبالتالي فإن تطبيق قواعد القانون الدولي الإنساني عليه يبدو أكثر وضوحاً نسبياً [4:ص241].

ثانياً: الهجمات السيبرانية التعطيلية (Disruptive Cyber Attacks): وهي التي تعطل عمل الأنظمة دون تدميرها مادياً، كالهجمات التي تستهدف شبكات الاتصالات أو الأنظمة المصرفية أو المستشفيات (عبر تشفير البيانات ومنع الوصول إليها). هذا النوع يثير إشكاليات أكبر لأنه قد لا يسبب أضراراً مادية بالمعنى التقليدي، لكنه قد يؤدي إلى أضرار غير مادية – كإصابة المرضى بسبب تعطل الأجهزة الطبية – قد تعادل الأضرار المادية في شدتها [5:ص201].

ثالثاً: الهجمات السيبرانية الاستخباراتية (Cyber Espionage): وهي التي تستهدف جمع معلومات دون التسبب بأضرار مادية أو تعطيل. ويختلف الخبراء حول ما إذا كان هذا النوع يدخل ضمن نطاق القانون الدولي الإنساني أصلاً، إذ قد لا يُعدّ "هجوماً" بموجب المادة (49) من البروتوكول الأول [2:ص101].

ويُلاحظ أن الحدود بين هذه الأنواع ليست جامدة، فالهجوم التعطيلي قد يتحول إلى تدميري إذا استمر زمناً طويلاً، والهجوم الاستخباراتي قد يهدف إلى تمكين هجوم تدميري لاحق. هذا التداخل يزيد من صعوبة التصنيف القانوني للعمليات السيبرانية [3:ص45].

المطلب الثاني: تصنيف الفضاءات الرقمية كساحة قتال

غالباً إذا كان الهجوم السيبراني لا يرقى إلى مستوى "نزاع مسلح"، فقد يخضع لقوانين أخرى أقل تقييداً كقانون مكافحة الجريمة السيبرانية أو قوانين التجسس [4:ص255]. فهل يمكن اعتبار العمليات السيبرانية "نزاعاً مسلحاً" بالمعنى المقصود في المادة (3) المشتركة لاتفاقيات جنيف 1949؟ هذه القضية جوهرية لأن القانون الدولي الإنساني لا ينطبق إلا في حال وجود نزاع مسلح (دولي أو غير دولي).

فوفقاً للمادة (3) المشتركة، يُعدّ النزاع غير الدولي مسلحاً عندما تصل أعمال العنف إلى "درجة معينة من الشدة" وتكون الأطراف "منظمة تنظيماً كافياً". وقد طبق الفقه الدولي هذه المعايير على العمليات السيبرانية من خلال "نظرية العتبة" (Threshold Theory). فالهجمات السيبرانية المعزولة ، كأختراق موقع حكومي أو سرقة وثائق ، لا ترقى إلى مستوى النزاع المسلح. أما إذا تكررت الهجمات وتسببت في أضرار مادية جسيمة (كتعطيل شبكة كهرباء وطنية لأيام) وكانت منظمة من طرف جماعة مسلحة، فقد تصل إلى عتبة النزاع المسلح [2: ص156–160].

أما في النزاعات الدولية، فالأمر أوضح نسبياً. فإذا كانت إحدى الدول تشن هجوماً سيبرانياً على دولة أخرى تسبب في أضرار مادية (كتدمير منشآت عسكرية أو مدنية)، فإن هذا يُعدّ استخداماً للقوة بموجب المادة (4/2) من ميثاق الأمم المتحدة، قد ترقى بعض الهجمات السيبرانية الجسيمة الى مستوى الهجوم المسلح بما يفعّل حق الدفاع

الشرعي المشار إليه في المادة (51) من ميثاق الأمم المتحدة إذا بلغت من الخطورة والآثار ما يعادل استخدام القوة المسلحة التقليدية. كما أن المحكمة الجنائية الدولية أكدت في وثيقة سياساتها لعام 2023 أن الهجمات السيبرانية واسعة النطاق التي تستهدف المدنيين قد تشكل جرائم حرب [6:الفقرة 22].

المطلب الثالث: مفهوم المدني في البيئة الرقمية

يعرّف القانون الدولي الإنساني المدني بأنه (كل شخص لا ينتمي إلى القوات المسلحة ولا يشارك بشكل مباشر في الأعمال العدائية) [8:المادة 50]. لكن هذا التعريف وُضع في سياق النزاعات التقليدية حيث كان من السهل نسبياً التمييز بين المقاتل والمدني بناءً على معايير مادية كالزي العسكري أو حمل السلاح أو الانتماء الواضح إلى جماعة مسلحة. ففي الفضاء الرقمي، تنهار هذه المعايير التقليدية تماماً [4: ص267]. فتظهر إشكاليات عدة عند محاولة تطبيق مفهوم المدني على الفضاء الرقمي:

أولاً: المدنيون كمبرمجين ومختصين في تكنولوجيا المعلومات: ففي النزاعات الحديثة، يعمل آلاف المدنيين في شركات تقنية تقدم خدماتها للجيش (كتطوير برمجيات، تحليل بيانات، تشغيل أنظمة اتصالات عسكرية). هل يُعدّ هؤلاء مدنيين محميين أم يندرجون تحت فئة "المشاركين المباشرين في الأعمال العدائية" الذين يفقدون حصانتهم مؤقتاً؟ وفقاً لمبادئ اللجنة الدولية للصليب الأحمر بشأن المشاركة المباشرة في الأعمال العدائية (2009)، فإن المدني الذي يقوم بأعمال "تهيئ أو تسهل أو تدعم بشكل مباشر عمليات عسكرية محددة" يُعدّ مشاركاً مباشراً. لكن التطبيق على المبرمجين يثير صعوبات: هل كتابة كود برمجي يُستخدم لاحقاً في هجوم سيبراني يُعدّ مشاركة مباشرة؟ الإجابة تختلف باختلاف مدى قرب البرمجة من الهجوم نفسه [7: الفقرة 34–38].

ثانياً: البنية التحتية الرقمية ذات الاستخدام المزدوج (Dual-Use): كثير من الشبكات والخوادم تُستخدم لأغراض مدنية وعسكرية في آن واحد. فالخادم السحابي قد يستضيف موقع مستشفى مدني وقاعدة بيانات عسكرية في الوقت نفسه. فالقمر الصناعي على سبيل المثال، قد ينقل بثاً تلفزيونياً مدنياً وإشارات اتصالات عسكرية. هذا التداخل يجعل تطبيق مبدأ التمييز صعباً جداً، فمهاجمة مثل هذه الأهداف قد تؤدي إلى أضرار مدنية جسيمة حتى لو كان الهدف الأساسي عسكرياً [2:ص178–182].

ثالثاً: البيانات الشخصية للمدنيين كأهداف: في الحروب السيبرانية، أصبحت البيانات الشخصية للمدنيين (السجلات الطبية، بيانات المواقع، سجل الاتصالات) هدفاً ثميناً لأطراف النزاع. فالحصول على بيانات موقع الهواتف المحمولة للمدنيين قد يكشف تحركات القوات العسكرية التي تختبئ بينهم. لكن هذا يعني عملياً مراقبة جماعية للمدنيين تنتهك

خصوصيتهم وتسبب ضرراً نفسياً ومعنوياً. القانون الدولي الإنساني يحمي المدنيين من "الهجمات النفسية والمعنوية" بموجب المادة (51) من البروتوكول الأول، لكن النصوص غير واضحة بشأن حماية البيانات الرقمية الشخصية كغاية في حد ذاتها [5: ص245].

رابعاً: الخوارزميات والذكاء الاصطناعي كـ(مقاتلين): مع تطور الأسلحة الذاتية التشغيل (Autonomous Weapons Systems) التي تعمل بالذكاء الاصطناعي، يطرح سؤال جديد: هل يمكن اعتبار الخوارزمية التي تدير هجوماً سيبرانياً (مقاتلاً)؟ ومن المسؤول عن انتهاكاتها؟ هذه الأسئلة لا تزال مفتوحة النقاش القانوني في الفقه الدولي [4: ص278].

خلص الفقهاء إلى أنه لا بد من تطوير تعريف جديد لـ(المدني) في السياق الرقمي، لا يعتمد على المعايير المادية التقليدية بل على معايير وظيفية، فالمدني هو من لا تؤدي وظيفته الرقمية إلى إلحاق ضرر مباشر بالخصم. أما من يقومون بتطوير أو تشغيل أو توجيه أنظمة هجومية سيبرانية، فيُعتبرون مشاركين مباشرين [3: ص67].

المبحث الثاني

مبادئ حماية المدنيين في القانون الدولي الإنساني وتطبيقها على الفضاءات الرقمية

يقوم القانون الدولي الإنساني على ثلاثة مبادئ جوهرية لحماية المدنيين: مبدأ التمييز، ومبدأ التناسب، ومبدأ الاحتياط. هذه المبادئ قد وردت في المادة (48) والمواد (51 و57) من البروتوكول الإضافي الأول لعام 1977، تُعدّ بعض المبادئ الأساسية في القانون الدولي الإنساني ذات طبيعة آمرة ولا يجوز مخالفتها حتى أثناء النزاعات المسلحة ، لاسيما القواعد المتعلقة بحماية المدنيين وحظر الجرائم الدولية الجسيمة. سنحلل في هذا المبحث مدى قابلية كل مبدأ للتطبيق على العمليات السيبرانية، والصعوبات التي تظهر أثناء التطبيق [4:ص290].

المطلب الأول: مبدأ التمييز في الهجمات السيبرانية

ينص مبدأ التمييز في صيغته الكلاسيكية على أن "على أطراف النزاع أن تميز دائمًا بين المدنيين والمقاتلين، وبين الأهداف المدنية والأهداف العسكرية، وعليهما توجيه عملياتهما فقط ضد الأهداف العسكرية" [8: المادة 48]. وقد كرّست المادة (48) من البروتوكول الأول هذا المبدأ كقاعدة أساسية في القانون الدولي الإنساني.

فعند تطبيقه على الفضاءات الرقمية، يثير مبدأ التمييز سؤالاً جوهرياً: متى يُعتبر الهدف الرقمي (كموقع إلكتروني، خادم، قاعدة بيانات، شبكة اتصالات) "هدفاً عسكرياً" بشكل يبرر مهاجمته؟ تحدد المادة (2/52) من البروتوكول الأول

الهدف العسكري بأنه (تلك الأهداف التي تسهم بطبيعتها أو موقعها أو غرضها أو استخدامها في العمل العسكري، والتي يشكل تدميرها أو تحييدها أو الاستيلاء عليها ميزة عسكرية مؤكدة) [8: المادة 52].

تطبيق هذا التعريف على الأهداف الرقمية يعني أن الهدف الرقمي يُعتبر عسكرياً إذا توفر فيه شرطان [2: ص195]:

الشرط الأول: الإسهام الفعلي في العمل العسكري. وهذا يشمل الشبكات والخوادم التي تستخدمها القوات المسلحة للاتصالات أو التخطيط أو التنسيق أو جمع الاستخبارات. كما يشمل أنظمة القيادة والتحكم العسكرية، وشبكات الأسلحة الموجهة عن بُعد، وقواعد البيانات العسكرية. أما المواقع الإلكترونية للحكومات المدنية، أو خوادم البريد الإلكتروني للموظفين المدنيين، أو الشبكات التي تدير خدمات عامة كالمياه والكهرباء، فليست أهدافاً عسكرية بطبيعتها إلا إذا تم استخدامها فعلياً لدعم العمليات العسكرية (وهذا ما يُسمى بـ"الاستخدام العارض" أو "الاستخدام المؤقت") [9: ص12].

الشرط الثاني: تحقيق ميزة عسكرية مؤكدة من تدمير الهدف. يعني هذا أنه لا يكفي أن يكون الهدف الرقمي له علاقة ولو بعيدة بالجيش، بل يجب أن يؤدي تدميره إلى ميزة عسكرية واضحة ومباشرة. فمثلاً، تدمير خادم يخزن وثائق عسكرية قديمة لا يحقق ميزة عسكرية مؤكدة، بينما تدمير خادم يوجه صواريخ مضادة للطائرات يحقق ميزة كبيرة [4:ص305].

لكن عملياً، يواجه تطبيق هذا المبدأ على الفضاءات الرقمية صعوبات فريدة تتمثل بـ:

الأولى: صعوبة تحديد طبيعة الهدف الرقمي عن بُعد. في الحرب التقليدية، يمكن للطيار الذي يحلق فوق هدف أن يراه بالعين المجردة أو عبر كاميرات متطورة، فيحدد إن كان دبابة (هدف عسكري) أم مدرسة (هدف مدني). في الحرب السيبرانية، المهاجم الجالس في غرفة مظلمة على بعد آلاف الكيلومترات لا يرى الهدف. كل ما لديه هو عنوان IP أو نطاق إنترنت. قد يكون هذا الخادم تابعاً لوزارة الدفاع، أو قد يكون خادم مستشفى مدني تعاقدت معه وزارة الدفاع لتخزين بعض البيانات. لا يمكن معرفة ذلك إلا بالتجسس أو الاختراق المسبق، وهو أمر صعب وخطير [5: ص267].

الثانية: سرعة تغير طبيعة الأهداف الرقمية. الهدف الذي كان مدنياً بالكامل في الصباح قد يتحول إلى هدف عسكري في المساء إذا بدأ الجيش باستخدامه، ثم يعود مدنياً بعد ساعات. على المهاجم أن يراقب الهدف آنياً ويتخذ قرارات سريعة، وهو أمر يكاد يكون مستحيلاً في العمليات واسعة النطاق [2: ص210–225].

الثالثة: تأثير (العدوى) الرقمية (Digital Contagion). عندما يُهاجم خادم عسكري (في سياق النزاعات السيبرانية الخادم العسكري هو جهاز كمبيوتر مركزي)، قد تنتشر البرمجيات الخبيثة إلى خوادم مدنية متصلة به دون قصد. فمثلاً، هجوم على خادم عسكري مستضاف على منصة سحابية (كرقم أمازون AWS) قد يؤدي إلى إصابة حسابات مدنية أخرى على نفس المنصة. هذا يشبه استخدام قنبلة عنقودية في منطقة حضرية [10:p145]، حيث يصعب السيطرة على انتشار الضرر [3: ص89].

وللتغلب على هذه الصعوبات، وضع خبراء تالين 2.0 قواعد إرشادية للمهاجم السيبراني: (أ) يجب بذل العناية الواجبة لتحديد طبيعة الهدف قبل الهجوم، (ب) إذا كان هناك شك معقول في أن الهدف مدني، يفترض أنه مدني (قاعدة الاحتياط في الشك)، (ج) يحظر استخدام برمجيات خبيثة تنتشر ذاتياً إلى شبكات مدنية، (د) يجب تصميم البرمجيات الخبيثة بحيث تكون محدودة الانتشار ومحددة الهدف [2:القاعدة 92–97]، [11:p74].

المطلب الثاني: مبدأ التناسب في الهجمات السيبرانية

ينص مبدأ التناسب على أنه (يحظر شن هجوم يتوقع أن يسبب خسائر مدنية عرضية أو إصابات بين المدنيين أو أضراراً للممتلكات المدنية تكون مفرطة مقارنة بالميزة العسكرية المباشرة والملموسة المتوقعة من الهجوم) (البروتوكول الإضافي الأول، المادة 51(5)(ب)). هذا المبدأ يعترف بأنه قد تكون هناك أضرار مدنية غير مقصودة (تسمى "خسائر عرضية" أو "Collateral Damage") أثناء الهجمات المشروعة، لكن يمنع أن تكون هذه الأضرار "مفرطة" مقارنة بالأهمية العسكرية للهدف.

فإنّ تطبيق هذا المبدأ على العمليات السيبرانية معقد جداً لعدة أسباب [4: ص315]:

أولاً: صعوبة تقدير الأضرار المدنية مسبقاً. في الحرب التقليدية، يمكن للقائد العسكري تقدير عدد المدنيين الذين قد يُقتلون إذا قصفت مبنى معين، بناءً على معلومات استخباراتية وخرائط. في الحرب السيبرانية، الهجوم على خادم واحد قد يؤدي إلى تعطيل مئات الأنظمة المدنية المتصلة به بشكل غير مباشر [12:p78–82]،[13:p345]. على سبيل المثال، الهجوم على خادم حكومي يستضيف بوابة الدفع الإلكتروني لرواتب الموظفين قد يعطل رواتب آلاف المدنيين، وقد يؤدي هذا إلى أضرار اقتصادية هائلة يصعب قياسها كمياً [9:ص18].

ثانياً: صعوبة تقدير الميزة العسكرية للهجوم السيبراني. في الحرب التقليدية، تدمير جسر يمنع وصول تعزيزات معادية – هذه ميزة عسكرية واضحة وقابلة للقياس. في الحرب السيبرانية، تعطيل شبكة اتصالات معادية ليوم واحد: ما الميزة

Quarterly Refereed and Scientific Journal Issued By College of Law in Babylon University
Online ISSN:2075-7220 Print ISSN:2313-0377
https://iasj.rdd.edu.iq/journals/journal/view/153

العسكرية المؤكدة من ذلك؟ قد تكون كبيرة وقد تكون صغيرة، حسب السياق. الخبراء يختلفون بشدة في تقديراتهم [2: ص245].

ثالثاً: طبيعة الأضرار السيبرانية غير المادية. الأضرار التقليدية هي الموت والجرح وتدمير الممتلكات. الأضرار السيبرانية قد تكون: تعطيل خدمات، فقدان بيانات، ضرر نفسي، ضرر اقتصادي، ضرر للسمعة، انتهاك خصوصية. هل تعادل هذه الأضرار الأضرار التقليدية؟ وإذا كانت كذلك، كيف تُوزن مقابل الميزة العسكرية؟ الفقه الدولي لا يقدم إجابة واضحة [5:ص289].

قدمت اللجنة الدولية للصليب الأحمر في العام (2023) مقترحاً لتطبيق التناسب على العمليات السيبرانية باستخدام "نظرية الأثر المكافئ" (Equivalent Effect Theory): الأضرار السيبرانية تُعتبر مكافئة للأضرار المادية إذا أدت إلى [3: ص102–106]:

(تعطيل خدمات حيوية (ماء، كهرباء، صحة) لمدة تزيد عن 48 ساعة، أو تدمير بيانات ضرورية لحياة المدنيين (سجلات طبية، خرائط إخلاء، أدلة هوية)، أو التسبب في خسائر اقتصادية تفوق 5 ملايين دولار أمريكي، أو التسبب في أضرار نفسية جماعية تستدعي تدخلاً طبياً). لكن هذا المقترح غير ملزم قانوناً، والدول لم تتبنَّاه رسمياً.

المطلب الثالث: مبدأ الاحتياط (التحوط) في العمليات السيبرانية

يلزم مبدأ الاحتياط أطراف النزاع باتخاذ "جميع الاحتياطات الممكنة" عند التخطيط للهجمات وتنفيذها، لتجنب الخسائر المدنية أو تقليلها إلى أدنى حد ممكن [8: المادة 57]. ويتضمن هذا المبدأ واجبات عدة: اختيار وسائل هجوم بديلة أقل ضرراً، التحقق من طبيعة الأهداف، إصدار تحذيرات مسبقة للمدنيين كلما أمكن، وتقييم النتائج بعد الهجوم لتصحيح الأخطاء مستقبلاً [4: ص360].

عند تطبيقه على الفضاءات الرقمية، يظهر الالتزام التالي [2: ص 268–285]:

الالتزام الأول: اختيار البرمجيات الخبيثة الأقل ضرراً. إذا كان بإمكان المهاجم تحقيق نفس الهدف العسكري باستخدام برمجية خبيثة محددة الانتشار لا تصيب شبكات مدنية، فلا يجوز له استخدام برمجية عنقودية (مثل ديدان الحاسوب ذاتية الانتشار). هذا يشبه الالتزام في القانون التقليدي باختيار سلاح أقل تدميراً.

الالتزام الثاني: التحقق من طبيعة الهدف عبر وسائل تقنية متعددة. يجب على المهاجم السيبراني استخدام أدوات متعددة لتحديد طبيعة الهدف قبل الهجوم (فحص المحتوى، تحليل النطاق، استخبارات المصادر المفتوحة). إذا كانت جميع الأدوات تشير إلى أن الهدف مدني، يفترض أنه مدني [9: ص24].

الالتزام الثالث: إصدار تحذيرات رقمية للمدنيين. في الحرب التقليدية، قد تُسقط قوات التحالف منشورات ورقية تحذر المدنيين من قصف وشيك. في الحرب السيبرانية، يمكن إرسال رسائل إلكترونية أو إشعارات على الهواتف المحمولة أو وضع تحذير على مواقع الويب المستهدفة. لكن هذا التحذير قد ينبه العدو أيضاً، مما يقلل الميزة العسكرية. يجب الموازنة بين الالتزام بحماية المدنيين والحاجة إلى تحقيق المفاجأة العسكرية [12:p. 210].

الالتزام الرابع: مراقبة الهجوم وتصحيح مساره في الوقت الفعلي. قد تتيح بعض العمليات السيبرانية إمكانية مراقبة آثار الهجوم وتعديل مساره أثناء التنفيذ إلاّ أن ذلك يختلف بحسب طبيعة البرمجية المستخدمة ومدى إحتفاظ المهاجم بالسيطرة التقنية عليها بعد الإطلاق.

المبحث الثالث

حالات تطبيقية معاصرة وتحديات المساءلة القانونية

بعد تحليل الإطار النظري لمبادئ القانون الدولي الإنساني وإمكانية تطبيقها على الفضاءات الرقمية، ينتقل هذا المبحث إلى دراسة حالات تطبيقية واقعية من النزاعات المسلحة الأخيرة. فالوقائع الملموسة تكشف حجم الفجوة بين النظرية القانونية والتطبيق العملي، وتظهر التحديات الحقيقية التي تواجه حماية المدنيين في الفضاءات الرقمية. سنحلل حالتين رئيسيتين: الحرب في أوكرانيا (2022–2025) والهجمات السيبرانية في سياق النزاع الفلسطيني–الإسرائيلي على قطاع غزة، ثم نستخلص أبرز تحديات المساءلة القانونية [14:ص45].

المطلب الأول: الحرب السيبرانية في أوكرانيا (2022–2025)

تُعدّ الحرب في أوكرانيا أول نزاع مسلح واسع النطاق تشهد فيه العمليات السيبرانية دوراً محورياً ومتوازياً مع العمليات العسكرية التقليدية. فمنذ اندلاع الحرب في فبراير 2022، نفذت جهات سيبرانية (مُسندة إلى روسيا بشكل غير مؤكد في بعض الحالات) هجمات متعددة على البنى التحتية الحيوية لأوكرانيا، بينما تلقت أوكرانيا دعماً سيبرانياً من حلف شمال الأطلسي (الناتو) وشركات تقنية خاصة [15: ص156–160]. ويمكن إجمالها بما يأتي:

أولاً: الهجمات على شبكات الكهرباء والطاقة: تعرضت شبكات الكهرباء الأوكرانية لسلسلة من الهجمات السيبرانية التدميرية، أبرزها هجوم (Industroyer2) في أبريل 2022 الذي استهدف محطات تحويل الجهد العالي في منطقة كييف. استخدم المهاجمون برمجية خبيثة مصممة خصيصاً للتحكم في المعدات الكهربائية (أنظمة SCADA)، مما أدى إلى انقطاع التيار الكهربائي عن حوالي 200 ألف مدني لمدة تتراوح بين 6 و12 ساعة في ذروة فصل الشتاء [16:ص23]. ورغم أن الهجوم لم يدم طويلاً بفضل فرق التدخل السريع الأوكرانية، إلا أنه يُعتبر مثالاً صارخاً على هجوم سيبراني استهدف خدمة مدنية حيوية بقصد إلحاق معاناة بالمدنيين، وهو ما يُشكل انتهاكاً صريحاً لمبادئ التمييز والتناسب بموجب القانون الدولي الإنساني [2: ص 312].

ثانياً: الهجمات على المستشفيات والقطاع الصحي: استُهدفت المستشفيات الأوكرانية بشكل متكرر بهجمات برمجيات الفدية (Ransomware) التي تشفر البيانات الطبية وتطلب فدية لاستعادتها. في هجوم مارس 2022 على مستشفى الأطفال في مدينة خاركيف، تعطلت أجهزة غسيل الكلى وأجهزة التنفس الصناعي لعدة ساعات، مما عرض حياة 47 طفلاً للخطر بشكل مباشر [17:ص18–20]. وفقاً لتقارير لمنظمة الصحة العالمية، وثقت أوكرانيا 112 هجوماً سيبرانياً على منشآت صحية بين فبراير 2022 وديسمبر 2024، منها 78 هجوماً وصلت إلى درجة "التعطيل الشديد للخدمات الطبية" [17:ص 34]. لذا تحظى المنشآت الطبية بحماية خاصة بموجب القانون الدولي الانساني ولا يجوز إستهدافها ما دامت تؤدي وظيفتها الإنسانية ولم تستخدم في أعمال تضر بالطرف المعادي خارج مهامها الطبية.

ثالثاً: هجمات تعطيل الاتصالات والإنترنت: استخدمت روسيا هجمات سيبرانية لتعطيل خدمة الإنترنت عبر الأقمار الاصطناعية (Viasat) في أوكرانيا ودول أوروبية أخرى في فبراير من العام 2022، مما أدى الى تعطيل خدمات الإنترنت لعشرات الآلاف من المدنيين الأوكرانيين وأثر أيضاً على شبكات الطاقة في ألمانيا [18: ص8–12]. هذا الهجوم تحديداً أثار إشكالية قانونية كبرى: فتعطيل الإنترنت عن المدنيين يُعتبر "عقاباً جماعياً" محظوراً بموجب المادة (33) من اتفاقية جنيف الرابعة، كما يُعتبر هجوماً على الحق في حرية التعبير وحرية الوصول إلى المعلومات (وهو حق محمي بموجب المادة 19 من الإعلان العالمي لحقوق الإنسان). لكن المحاكم الدولية لم تصدر أي حكم في هذا الشأن حتى الآن بسبب صعوبة إثبات التبعية القانونية [4:ص345].

التحديات القانونية التي كشفت عنها الحرب في أوكرانيا: من أبرز التحديات التي أظهرتها الحرب الأوكرانية:

(1) مشكلة الإسناد (Attribution): رغم أن معظم الهجمات نُسبت إلى روسيا من قبل خبراء تقنيين، إلا أن الإثبات القانوني أمام المحاكم يتطلب أدلة قاطعة يصعب الحصول عليها دون تعاون الدول؛ (2) الهجمات المختلطة

(Hybrid Attacks): تجمع الهجمات السيبرانية بين أساليب تقليدية (كالقصف المدفعي) وسيبرانية، مما يصعّب فصل القواعد القانونية المطبقة؛ (3) غياب آلية تحقيق دولية متخصصة [14: ص56–60].

المطلب الثاني: الهجمات السيبرانية في النزاع الفلسطيني–الإسرائيلي (غزة)

شهد النزاع في قطاع غزة، وخاصة بعد أحداث أكتوبر/تشرين الأول من العام 2023 وما تلاها، استخداماً متزايداً للهجمات السيبرانية كأداة حرب، سواء من قبل إسرائيل أو من قبل جماعات مسلحة فلسطينية ووكلاء إقليميين. تكشف هذه الحالة خصوصية إضافية: تطبيق القانون الدولي الإنساني على نزاع غير دولي (أو نزاع دولي وفق بعض التصنيفات) في بيئة حضرية مكتظة بالسكان وذات بنية تحتية رقمية هشة أصلاً [19: ص12].

أولاً: استهداف البنية التحتية الرقاعية لغزة: في أكتوبر/ تشرين الأول عام 2023، ومع بدء العمليات العسكرية الإسرائيلية واسعة النطاق في غزة، تعرضت شبكات الاتصالات والإنترنت في القطاع لهجمات سيبرانية متزامنة مع قصف فيزيائي لأبراج الاتصالات. أدى ذلك إلى انقطاع شبه كامل للإنترنت عن كامل قطاع غزة (2.3 مليون نسمة) لمدة تتراوح بين 24 و72 ساعة في ثلاث مناسبات منفصلة بين أكتوبر/تشرين الأول عام 2023 ويونيو/حزيران عام 2024 [20:الفقرة 89–92]. هذا الانقطاع شل قدرة المدنيين على: الاتصال بفرق الإسعاف، معرفة أماكن القصف، التواصل مع عائلاتهم، والحصول على معلومات حول إمدادات المياه والغذاء. تُعتبر مثل هذه الهجمات انتهاكاً للمادة (54) من البروتوكول الأول التي تحظر "الهجوم على الأشياء التي لا غنى عنها لبقاء السكان المدنيين"، حيث أصبح الإنترنت في القرن الحادي والعشرين سلعة لا غنى عنها لبقاء المدنيين في حالات الطوارئ.

ثانياً: استهداف البيانات الطبية والخدمات الصحية: تعرضت وزارة الصحة في غزة وسلسلة من المستشفيات (كمستشفى الشفاء والمستشفى الإندونيسي) لهجمات إلكترونية أسفرت عن فقدان أو تشفير قواعد بيانات المرضى والسجلات الطبية. في نوفمبر/تشرين الثاني عام 2023، أعلنت وزارة الصحة في غزة أن هجوماً سيبرانياً أدى إلى تدمير قاعدة بيانات التطعيمات الإلكترونية، مما جعل من المستحيل معرفة أي الأطفال تلقوا تطعيماتهم الأساسية [21:ص7]. وقد اعتبر خبراء القانون الدولي أن استهداف البيانات الطبية للمدنيين يُشكل "انتهاكاً خطيراً" للمادة (147) من اتفاقية جنيف الرابعة التي تَعُدّ "التدمير المبرر لممتلكات المدنيين" جريمة حرب. والبيانات الطبية، وإن لم تكن مادية، تُعتبر من "الممتلكات المدنية" بموجب التفسير التطوري للمادة [5:ص 345–347].

التحديات القانونية الخاصة بغزة: (1) مشكلة التصنيف القانوني للنزاع: هل هو نزاع دولي (باعتبار إسرائيل دولة محتلة لغزة) أم نزاع غير دولي ؟ هذا الاختلاف يؤثر على القواعد المطبقة؛ (2) صعوبة التحقيق الميداني: بسبب الدمار الهائل وانعدام الأمن، لم يتمكن أي فريق تحقيق دولي من فحص الأدلة الرقمية مباشرة؛ (3) مشكلة الازدواجية بين الأضرار المادية والسيبرانية: في غزة، كان القصف الفيزيائي هو السبب الرئيسي للأضرار، بينما جاءت الهجمات السيبرانية كعامل مضاعف. يصعب قانوناً فصل مسؤولية كل نوع من الأضرار [14: ص78–82].

المطلب الثالث: تحديات المساءلة القانونية عن الهجمات السيبرانية

تتضح من خلال الحالتين السابقتين (أوكرانيا وغزة) معضلة كبرى: حتى إذا انتهكت أطراف النزاع قواعد القانون الدولي الإنساني في الفضاءات الرقمية، فإن إخضاعهم للمساءلة القانونية يواجه عقبات غير مسبوقة. يمكن تلخيص أبرز هذه التحديات على النحو التالي [4: ص375]:

التحدي الأول: مشكلة الإسناد (Attribution Problem). الإسناد هو عملية تحديد المسؤول الفعلي (دولة أو جماعة مسلحة) عن الهجوم السيبراني. في القانون الجنائي التقليدي، الإسناد سهل نسبياً، إذا تركت بصمات أو سجلته الكاميرات، يُعرف الجاني. في الفضاء السيبراني، يستخدم المهاجمون وسائل إخفاء متعددة، شبكات خاصة افتراضية (VPN) وخوادم وسيطة وبرمجيات تخفي الهوية. حتى إذا تمكن الخبراء التقنيون من تتبع الهجوم إلى عناوين IP في دولة معينة، فقد يكون المهاجم فرداً يعمل من منزله في تلك الدولة دون علم حكومتها (ما يُسمى بالجهات الفاعلة غير الحكومية) [22:p230]. تواجه عمليات إسناد الهجمات السيبرانية صعوبات إثباتية معقدة، إذ يتطلب القانون الدولي أدلة تقنية وقانونية كافية ومقنعة لربط الهجوم بدولة أو جهة معينة وفقاً لطبيعة المسؤولية محل البحث [2:القاعدة 15، ص. 98–102]. وقد أظهرت تقارير الأمم المتحدة أن من بين 500 هجوم سيبراني كبير وقع بين العام 2020 و2025، لم يُنسب أي منها رسمياً أمام محكمة دولية (رغم نسب إعلامية وتقنية كثيرة) [23: الفقرة 45].

التحدي الثاني: غياب الآليات الدولية المتخصصة للتحقيق والرقابة. لا توجد حتى الآن هيئة دولية مستقلة ومتخصصة في التحقيق في الهجمات السيبرانية في سياق النزاعات المسلحة. فالمحكمة الجنائية الدولية (ICC) لديها ولاية على جرائم الحرب، لكنها تفتقر إلى الخبرة الفنية اللازمة لتحليل الأدلة الرقمية المعقدة. كما أن التفويض الحالي للمحكمة لا يشمل صراحة "جرائم الحرب السيبرانية" كمادة مستقلة، بل يجب إدراجها تحت مواد تقليدية (كالقتل العمد أو الهجوم على المدنيين)، مما قد يكون غير مناسب لطبيعة الأضرار السيبرانية غير المادية [24:الفقرة 12–15].

التحدي الثالث: التضارب بين الأدلة الرقمية والسيادة الوطنية. الأدلة الرقمية (سجلات الخوادم، عناوين IP، البيانات المحذوفة) عادة ما تكون مخزنة في أراضي دول أخرى. للوصول إليها، تحتاج جهات التحقيق إلى إذن تلك الدول. لكن الدول التي يُشتبه بتورطها في الهجمات غالباً ما ترفض التعاون، وتلوذ بمبدأ السيادة الوطنية لحماية بياناتها. هذا يخلق طريقاً مسدوداً: لا يمكن الحصول على الأدلة دون تعاون الدولة المتهمة، والدولة المتهمة لن تتعاون لأن الإدانة ستكشف جرائمها [5: ص367].

التحدي الرابع: طبيعة الأضرار السيبرانية غير المادية. جرائم الحرب التقليدية تُعرف بوجود ضحايا بشرية (قتلى وجرحى) أو تدمير مادي واضح. لكن كثيراً من الأضرار السيبرانية هي: فقدان بيانات، تعطيل خدمات، ضرر نفسي، خسائر اقتصادية. هل يمكن محاكمة شخص بتهمة "جريمة حرب" لأنه تسبب في تعطيل خدمة الإنترنت عن مدنيين لمدة يوم دون أن يقتل أحداً؟ فإنّ معظم المحاكم الدولية تتعامل بحذر مع هذا النوع من الأضرار غير المادية [9:ص 31].

التحدي الخامس: سرعة تطور التكنولوجيا مقابل بطء القانون. بينما يستغرق تعديل المعاهدات الدولية أو إضافة بروتوكولات جديدة سنوات (أو عقوداً في بعض الأحيان)، تتطور أدوات الهجمات السيبرانية أسبوعياً. عندما يُسن قانون لمواجهة نوع معين من الهجمات، يكون المهاجمون قد انتقلوا بالفعل إلى تقنيات جديدة غير مشمولة بالقانون. هذه "الفجوة الزمنية" تجعل القانون الدولي الإنساني في المجال السيبراني دائماً متخلفاً عن الواقع العملي [4: ص 378].

الخاتمة

أولاً: النتائج المستخلصة

بعد التحليل المتعمق للإطار النظري للقانون الدولي الإنساني وتطبيقاته على الفضاءات الرقمية، ودراسة الحالات العملية من أوكرانيا وغزة، يمكن استخلاص النتائج التالية:

1- المبادئ العامة للقانون الدولي الإنساني (التمييز، التناسب، الاحتياط) تنطبق نظرياً على العمليات السيبرانية في النزاعات المسلحة، وذلك لأن صياغتها في اتفاقيات جنيف وبروتوكوليها جاءت بصياغات عامة ومرنة تسمح بالتفسير التطوري ليشمل الأسلحة الجديدة. وهذا ما أكدته اللجنة الدولية للصليب الأحمر ودليل تالين .
2- على الرغم من الانطباق النظري، فإن التطبيق العملي لهذه المبادئ على الفضاءات الرقمية يواجه تحديات غير مسبوقة من حيث الصعوبة. أبرز هذه التحديات: صعوبة تحديد طبيعة الهدف الرقمي عن بُعد، صعوبة تقدير الأضرار المدنية العرضية مسبقاً، صعوبة إصدار تحذيرات للمدنيين دون إفشال الهجوم، ومشكلة

الأهداف ذات الاستخدام المزدوج (المدني والعسكري). هذه الصعوبات تجعل الالتزام الفعلي بالقانون الدولي الإنساني في العمليات السيبرانية أقل مما هو عليه في العمليات التقليدية .

3- الحالات التطبيقية في أوكرانيا وغزة أثبتت أن الهجمات السيبرانية على البنى التحتية المدنية (الكهرباء، المستشفيات، الاتصالات، المياه) أصبحت أسلوباً حربياً منتظماً، وليست حوادث معزولة. هذه الهجمات تسبب أضراراً جسيمة للمدنيين قد تعادل أو تفوق الأضرار الناجمة عن الأسلحة التقليدية في بعض السياقات (كحالة تعطيل شبكة الكهرباء عن مستشفى أطفال في الشتاء). ومع ذلك، لم يُدان أي مسؤول عن هذه الهجمات حتى الآن أمام محكمة دولية .

4- مشكلة الإسناد (Attribution) تشكل العقبة الكبرى أمام المساءلة القانونية. فحتى في الحالات التي يتوفر فيها يقين تقني عالٍ بأن دولة معينة تقف وراء هجوم سيبراني (كما في هجوم Viasat 2022 المنسوب لروسيا)، فإن مستوى الإثبات القانوني المطلوب للمحاكم الدولية (الدليل القاطع الذي لا يدع مجالاً للشك المعقول) نادراً ما يتحقق بسبب إمكانية اختراق الأدوات المستخدمة في التتبع أو استخدام جهات فاعلة غير حكومية .

5- لا توجد حتى الآن آلية دولية متخصصة وقادرة على التحقيق في الهجمات السيبرانية أثناء النزاعات المسلحة. فالمحكمة الجنائية الدولية تمتلك الولاية لكنها تفتقر للخبرة التقنية، ومجلس الأمن مشلول بسبب حق النقض (الفيتو)، واللجنة الدولية للصليب الأحمر ليس لديها ولاية قضائية عقابية. هذا الفراغ المؤسسي يشجع أطراف النزاع على استخدام الأسلحة السيبرانية دون خوف من العقاب .

ثانياً: التوصيات

بناءً على النتائج السابقة، يوصي البحث بما يلي:

1- (تعديل المعاهدات القائمة) : ضرورة اعتماد بروتوكول إضافي ثالث لاتفاقيات جنيف (أو تعديل البروتوكولين الأول والثاني) يتضمن نصوصاً صريحة وملزمة بشأن العمليات السيبرانية، ويحدد بوضوح: تعريف "الهجوم السيبراني" في سياق القانون الدولي الإنساني، والقواعد الخاصة بتطبيق مبادئ التمييز والتناسب والاحتياط على الفضاءات الرقمية، وحماية البيانات المدنية كغاية في حد ذاتها، وتجريم استهداف البنى التحتية الرقمية الحيوية للمدنيين بشكل مطلق .

2- (إنشاء آلية تحقيق دولية متخصصة) : إنشاء هيئة دولية مستقلة تحت مظلة الأمم المتحدة (أو بالتنسيق مع اللجنة الدولية للصليب الأحمر) تُسمى "الآلية الدولية للتحقيق في الهجمات السيبرانية في النزاعات المسلحة" (International Cyber-Attack Investigation Mechanism – ICAIM). تتمتع هذه الآلية بولاية:

جمع وتحليل الأدلة الرقمية من جميع الأطراف، إصدار تقارير علنية عن الإسناد، تقديم الأدلة للمحكمة الجنائية الدولية عند الاقتضاء، وتدريب القضاة والمحققين على الأدلة الرقمية. يجب أن تكون هذه الآلية مزودة بفريق دائم من خبراء التكنولوجيا والقانون الجنائي الدولي .

3- (إلزام الدول بحماية البنية التحتية الرقمية للمدنيين) : إقرار معاهدة دولية جديدة (أو تعديل بروتوكول جنيف الثالث) تلزم الدول باتخاذ "تدابير معقولة" لحماية البنية التحتية الرقمية المدنية (شبكات الكهرباء والمياه والمستشفيات والاتصالات) على أراضيها من الهجمات السيبرانية، حتى في حالة الحرب. هذه "العناية الواجبة" (Due Diligence) يجب أن تشمل: إنشاء فرق استجابة طارئة للهجمات السيبرانية على الخدمات الحيوية، إجراء اختبارات دورية لضعف الأنظمة، تبادل المعلومات الاستخباراتية عن التهديدات مع الدول الأخرى عبر قنوات آمنة. إهمال هذه الواجبات يجعل الدولة مسؤولة دولياً عن الأضرار التي تلحق بمدنييها .

4- (تطوير تعريف "الضرر" في القانون الدولي الإنساني) : إعادة النظر في تعريف "الضرر" الوارد في المادة 51 من البروتوكول الأول ليشمل صراحة الأضرار السيبرانية غير المادية التي تصل إلى درجة معينة من الخطورة. يُقترح اعتماد "نظرية الأثر المعادل" التي سبقتها اللجنة الدولية للصليب الأحمر: تعطيل خدمة حيوية (ماء، كهرباء، صحة) لأكثر من 48 ساعة، أو تدمير بيانات ضرورية لبقاء المدنيين، أو التسبب بخسائر اقتصادية جماعية تفوق عتبة معينة (مثل 10 ملايين دولار)، يُعتبر ضرراً يعادل الأضرار المادية التقليدية لأغراض المساءلة الجنائية .

5- (إشراك شركات التكنولوجيا الخاصة) : إلزام شركات التكنولوجيا الكبرى (كMicrosoft، Google، Amazon، SpaceX) التي تقدم خدمات سحابية أو إنترنت أو اتصالات في مناطق النزاع بوضع "مدونات سلوك" ملزمة لحماية بيانات المدنيين ومنع استخدام بنيتها التحتية في الهجمات السيبرانية العسكرية دون علمها. كما ينبغي إنشاء "خط ساخن" بين هذه الشركات واللجنة الدولية للصليب الأحمر للإبلاغ السريع عن الهجمات السيبرانية على أنظمتها في مناطق النزاع .

6- (تعزيز الردع من خلال المحكمة الجنائية الدولية) : مطالبة مكتب المدعي العام للمحكمة الجنائية الدولية بإصدار "ورقة سياسات" واضحة تحدد أن الهجمات السيبرانية واسعة النطاق التي تستهدف المدنيين أو البنى التحتية المدنية بشكل متعمد (أو مع تجاهل تام لعواقبها) ستُعتبر جرائم حرب تدخل في اختصاص المحكمة، وسيتم التحقيق فيها بنفس الأولوية الممنوحة للجرائم التقليدية. كما ينبغي تدريب قضاة المحكمة وخبرائها على التعامل مع الأدلة الرقمية .

قائمة المصادر

1- Schmitt, Michael N. 2011. "Cyber Operations and the Jus in Bello: Key Issues" ,International Law Studies.
2- شميت، ميشيل ن. 2023. دليل تالين 2.0: القانون الدولي الواجب التطبيق على العمليات السيبرانية. ترجمة أحمد شربجي. بيروت: المركز العربي للقانون الدولي.
3- اللجنة الدولية للصليب الأحمر. 2024. الحرب السيبرانية والقانون الدولي الإنساني. جنيف: اللجنة الدولية.
4- بوثبي، وليام. 2022. القانون في الحرب: فهم القانون الدولي الإنساني. ترجمة خالد العيسى. الدوحة: دار بلومزبري.
5- ساسولي، ماركو. 2021. القانون الدولي الإنساني: مقدمة معاصرة. ترجمة مركز الدراسات القانونية. القاهرة: المركز القومي للترجمة.
6- المحكمة الجنائية الدولية. 2023. "سياسة مكتب المدعي العام بشأن الجرائم السيبرانية." لاهاي: المحكمة الجنائية الدولية، 15 سبتمبر.
7- اللجنة الدولية للصليب الأحمر. 2009. "مبادئ توجيهية بشأن المشاركة المباشرة للمدنيين في الأعمال العدائية." جنيف: اللجنة الدولية.
8- البروتوكول الإضافي الأول 1977 لاتفاقيات جنيف المتعلق بحماية ضحايا المنازعات المسلحة الدولية. جنيف: اللجنة الدولية للصليب الأحمر.
9- اللجنة الدولية للصليب الأحمر. 2021. "القانون الدولي الإنساني والعمليات السيبرانية: ورقة موقف." جنيف: اللجنة الدولية.
10- Dinstein, Yoram. 2017. The Conduct of Hostilities under the Law of International Armed Conflict. 3rd ed. Cambridge: Cambridge University Press.
11- Gill, Terry D., and Dieter Fleck, eds. 2021. The Handbook of the International Law of Military Operations. 3rd ed. Oxford: Oxford University Press.
12- Boothby, William H., and Wolff Heintschel von Heinegg, eds. 2023. The Law of War: A Detailed Assessment of the US Department of Defense Law of War Manual. Cambridge: Cambridge University Press.
13- Blank, Laurie R. 2023. International Conflict and Security Law. Cheltenham: Edward Elgar Publishing.2. Boothby, William H. 2016. The Law of Targeting. Oxford: Oxford University Press.
14- اللجنة الدولية للصليب الأحمر. 2025. "تقرير العمليات السيبرانية في النزاعات المسلحة 2025." جنيف: اللجنة الدولية.
15- شتوكر، يورغن. 2024. "الحرب السيبرانية الروسية الأوكرانية: تحليل قانوني." مجلة القانون الدولي 89، العدد 2: 150-190.
16- منظمة الأمن والتعاون في أوروبا (OSCE)2023 ، "تقرير الخبراء حول الهجمات السيبرانية على شبكات الطاقة الأوكرانية." فيينا.
17- منظمة الصحة العالمية. 2025. "الهجمات السيبرانية على القطاع الصحي في أوكرانيا: تقرير تحليلي." جنيف: WHO، يناير.
18- مجلس الاتحاد الأوروبي. 2023. "تقرير تحقيق حول هجوم Viasat السيبراني." بروكسل: الاتحاد الأوروبي.
19- منظمة العفو الدولية. 2024. "الفضاء الرقمي كساحة حرب: غزة نموذجاً." لندن: منظمة العفو الدولية.
20- الأمم المتحدة. 2024. "تقرير الأمين العام عن حماية المدنيين في النزاعات المسلحة." وثيقة S/2024/895. نيويورك: الأمم المتحدة، سبتمبر.
21- وزارة الصحة الفلسطينية (غزة). 2023. "تقرير الأضرار الرقمية للقطاع الصحي." غزة: مركز المعلومات الصحية، ديسمبر.
22- Hollis, Duncan B. 2018. "Re-Thinking the Boundaries of Law in Cyberspace: A Duty to Hack?" In Understanding Cyber Conflict: Fourteen Analogies, edited by George Perkovich and Ariel E. Levite, 226-247. Washington, DC: Georgetown University Press.
23- الأمم المتحدة. 2025. "تقرير فريق الخبراء الحكومي الدولي حول التقدم في مجال الأمن السيبراني." نيويورك: الأمم المتحدة.
24- المحكمة الجنائية الدولية. 2024. "ورقة سياسات مكتب المدعي العام: الأولويات في التحقيقات السيبرانية." لاهاي: المحكمة الجنائية الدولية، 15 يناير.