Print ISSN: 2791-2248
Online ISSN: 2791-2256
مَجلّةُ تَسْنِيمِ الدَوليّة
للعُلومِ الإنسانيّةِ والاجتمَاعيّةِ والقانونيّةِ

العدد السابع عشر – حزيران – 2026 / June

الهجمات السيبرانية على جنوب لبنان في ضوء القانون الدولي الجنائي

م.م مريم نبيل عادي [1]

[1] جامعة القادسية/ كلية العلوم - العراق

maryam.nabeel@ijsu.edu.iq
maryam.nabeel@qu.edu.iq

ملخص. تعد الهجمات السيبرانية واحدة من أبرز التحديات المعاصرة التي تواجه الأمن القومي والسلم الإقليمي والدولي، خاصة في ظل التطور التكنولوجي المتسارع الذي يعيد صياغة مفاهيم الأمن والجريمة. يأتي هذا البحث لدراسة الهجمات السيبرانية التي استهدفت جنوب لبنان كنموذج يعكس تعقيد العلاقة بين الأمن السيبراني، القانون الدولي الجنائي، والسياسة الجيوسياسية. تتمثل خلفية البحث في تصاعد استخدام الوسائل السيبرانية كأدوات لتحقيق أهداف سياسية وعسكرية، سواء من قبل الجهات الحكومية أو غير الحكومية، مما يثير تساؤلات قانونية حول تصنيف هذه الهجمات وآليات معاقبتها. تكمن أهمية البحث في ضرورة تحديث الأطر القانونية الدولية لتواكب التطورات التكنولوجية وتعزز حماية المدنيين والبنى التحتية الحيوية. كما أن دراسة هذه الظاهرة في سياق جنوب لبنان تسلط الضوء على الفجوات القانونية التي تعيق تحقيق العدالة الجنائية الدولية في مواجهة الجرائم السيبرانية. يهدف البحث إلى تحقيق مجموعة من الأهداف، منها: تحليل مفهوم الهجمات السيبرانية في إطار القانون الدولي الجنائي، تقييم مدى توافق هذه الهجمات مع مبادئ القانون الدولي، مثل السيادة وعدم التدخل وحظر استخدام القوة، وتحديد الآثار القانونية لهذه الهجمات على المستوى الوطني والدولي. كما يسعى البحث إلى تقديم مقترحات عملية لتعزيز النظام القانوني الدولي في مكافحة الجرائم السيبرانية. اعتمدت منهجية البحث على المنهج التحليلي، حيث تم دراسة النصوص القانونية ذات الصلة، بما في ذلك اتفاقيات القانون الدولي الإنساني والاتفاقيات المتعلقة بالجرائم السيبرانية. كما تم إجراء تحليل مقارن بين القوانين الوطنية والدولية لاستكشاف كيفية تصنيف ومعاقبة الهجمات السيبرانية. أظهرت نتائج البحث أن

Print ISSN: 2791-2248
Online ISSN: 2791-2256
مَجلّةُ تَسْنِيمِ الدَوليّة
للعُلومِ الإنسانيّةِ والاجتمَاعيّةِ والقانونيّةِ

الهجمات السيبرانية التي تستهدف المدنيين أو البنى التحتية الحيوية قد ترقى إلى مستوى "الجرائم الدولية" إذا كانت تنطوي على انتهاكات للقانون الدولي الإنساني. كما أكدت الدراسة وجود فجوات قانونية في النظام الدولي الحالي تحول دون تحقيق مساءلة فعّالة بشأن هذه الجرائم. في الخاتمة، يشدد البحث على أهمية تعزيز التعاون الدولي لإنشاء إطار قانوني شامل يعالج التهديدات السيبرانية ويضمن تحقيق العدالة الجنائية كما يدعو إلى ضرورة تعزيز القدرات الوطنية والإقليمية لمكافحة الجرائم السيبرانية، خاصة في المناطق ذات الحساسية السياسية والأمنية مثل جنوب لبنان.

الكلمات الدلالية: الهجمات السيبرانية، لبنان، القانون الدولي الجنائي.

Abstract. Cyberattacks pose a major challenge to national security ،regional stability ،and international peace ،particularly with rapid technological advancements reshaping security and crime. This research focuses on cyberattacks in South Lebanon as a case study to explore the intersection of cybersecurity ،international criminal law ،and geopolitical dynamics. It highlights the growing use of cyber tools by state and non-state actors to achieve political and military goals ،raising legal questions about classifying and punishing such attacks**.** The significance of this research lies in the urgent need to update international legal frameworks to keep pace with technological developments and enhance the protection of civilians and critical infrastructure. Additionally ،studying this phenomenon within the context of South Lebanon highlights the legal gaps that hinder achieving international criminal justice in response to cybercrimes**.** The research aims to achieve several objectives ،including: analyzing the concept of cyberattacks within the framework of international criminal law ،assessing the compatibility of these attacks with principles of international law such as sovereignty ،non-intervention ،and the prohibition of the use of force ،and determining the legal implications of these attacks at both national and international levels. Furthermore ،the study seeks to propose practical recommendations to strengthen the international legal system in combating cybercrimes**.** The research methodology adopted an analytical approach ،examining relevant legal texts ،including international humanitarian law agreements and conventions related to cybercrimes. A comparative analysis was also conducted between national and international laws to explore how cyberattacks are classified and

Print ISSN: 2791-2248
Online ISSN: 2791-2256
مَجلّةُ تَسْنِيمِ الدَولِيّة
للعُلومِ الإنسانيّةِ والاجتمَاعيّةِ والقانونيّةِ

punished. The findings of the research indicate that cyberattacks targeting civilians or critical infrastructure may rise to the level of "international crimes" if they involve violations of international humanitarian law. The study also confirms the existence of legal gaps in the current international system that hinder effective accountability for such crimes. In conclusion ،the research emphasizes the importance of enhancing international cooperation to establish a comprehensive legal framework addressing cyber threats and ensuring criminal justice. It also calls for strengthening national and regional capacities to combat cybercrimes ، particularly in politically and security-sensitive areas such as South Lebanon.

Keywords: Cyberattacks ،Lebanon ،International Criminal Law

المقدمة

"لو كان العلم بالثريا لتناوله رجال من فارس"، قالها سيد الخلق واكرمهم، فكأنما أشار الى علمٍ، سيكون لحملته دورا فعالا في صنع التاريخ، ولعل اهل فارس استشفوا ذلك، فتصدروا لنيل دور الصدارة في مجال الاتصالات والامن السيبراني على مستوى الدول الإقليمية، باعتراف الخصوم قبل الحلفاء الذين اتفرط عقدهم في عصر القطبية السياسية الأحادية.

وفي ظل التحولات التكنولوجية المتسارعة التي يشهدها العالم، أصبحت الهجمات السيبرانية تشكل تهديداً جديداً ومتنامياً للأمن القومي والسلم الإقليمي والدولي. وقد أفرزت هذه الظاهرة تحديات غير مسبوقة أمام القانون الدولي العام، الذي يواجه صعوبة في اللحاق بالتطورات التقنية السريعة وتقنينها ضمن إطار قانوني واضح ومحدد. ومن بين المناطق التي تعرضت بشكل متزايد للهجمات السيبرانية، يأتي جنوب لبنان كنموذج يعكس تعقيد العلاقة بين الأمن السيبراني، القانون الدولي، والسياسة الجيوسياسية. اذ يعد جنوب لبنان منطقة ذات حساسية سياسية وأمنية خاصة. وفي السنوات الأخيرة، شهدت هذه المنطقة تصاعداً في استخدام الوسائل السيبرانية كأداة لتحقيق أهداف سياسية وعسكرية، سواء من قبل الجهات الحكومية أو الجهات غير الحكومية. ويشكل هذا الواقع الأساس لطرح تساؤلات قانونية وفقهية حول كيفية تصنيف مثل هذه الهجمات في إطار القانون الدولي العام، وما إذا كانت ترقى إلى مستوى "الاستخدام العدائي للقوة" أو حتى "العمل العسكري"، وبالتالي تخضع لأحكام ميثاق الأمم المتحدة وقواعد القانون الدولي الإنساني.

إن فهم هذه القضية لا يقتصر فقط على تحليل النصوص القانونية، بل يتطلب أيضاً النظر في السياقات السياسية والتاريخية التي تحيط بهذه الهجمات، بالإضافة إلى تقييم مدى فعالية الأطر القانونية الحالية في التعامل مع التهديدات السيبرانية. ومن خلال هذا البحث، نسعى إلى تقديم رؤية شاملة ومتكاملة حول كيفية معالجة القانون الدولي للتحديات الجديدة التي تفرضها الهجمات السيبرانية على جنوب لبنان، مع تقديم مقترحات عملية لتعزيز النظام القانوني الدولي في هذا المجال.

أولا- إشكالية البحث

تُشكل الهجمات السيبرانية التي تستهدف المدنيين أو البنية التحتية الحيوية في جنوب لبنان إشكالية قانونية معقدة في إطار تطبيق أحكام القانون الدولي الإنساني والقانون الدولي الجنائي. فمع تصاعد وتيرة الاعتداءات الرقمية عبر الحدود وازدياد الأدلة على تورط جهات أجنبية في تنفيذ عمليات اختراق واستهداف لأنظمة حيوية مدنية، يطرح تساؤل جوهري حول مدى إمكانية اعتبار هذه الأعمال انتهاكات للقواعد الدولية المنظِّمة لحماية المدنيين أثناء النزاع المسلح. ويثير هذا الواقع تحديات قانونية تتعلق بتأهيل تلك الهجمات كأفعال مجرمة بموجب القانون الدولي، خاصةً إذا أدت إلى إحداث ضرر جسيم بالمنشآت الأساسية التي تمس حياة السكان أو تهدد سلامتهم الجسدية أو الاقتصادية. ومن ثمَّ، تظهر الحاجة إلى تحليل دقيق لقدرة نظام روما الأساسي والمحكمة الجنائية الدولية على مساءلة مرتكبي هذه الأعمال باعتبارها جرائم دولية، في ظل غياب نصوص واضحة تتناول بصفة مباشرة طبيعة الهجمات السيبرانية وآثارها المترتبة عليها، مما يولِّد فجوة تشريعية تتطلب التفاتة من الفقه والقضاء الدوليين لسد الثغرات وتعزيز مبدأ المحاسبة في الفضاء الرقمي الجديد.

ثانيا- فرضيات البحث

يمكن أن يُفترض في هذا البحث أن الكيان الصهيوني قد ارتكب خروقات للقانون الدولي الإنساني والقانون الدولي السيبراني من خلال شن هجمات سيبرانية تستهدف المدنيين أو البنية التحتية الحيوية في جنوب لبنان، وأن هذه الأعمال قابلة لتأهيلها كجرائم دولية تخضع لاختصاص المحكمة الجنائية الدولية في حال توفر عناصر النية والمعرفة والمسؤولية الفردية.

كما يُفترض أن هناك احتمالًا حقيقيًا لمعاودة الكيان الصهيوني أو كيانات أخرى مماثلة ارتكاب مثل هذه الانتهاكات في المستقبل، خاصةً في ظل غياب آليات ردع فعَّالة وغياب تطبيق صارم للمسؤولية الجنائية الدولية على مرتكبي الجرائم السيبرانية.

وإلى جانب ذلك، يُفترض أن الهجمات السيبرانية لا تقتصر على لبنان فقط، بل تمتد لتهدد دولاً أخرى مثل العراق، حيث تتعرض المنشآت الحيوية فيها إلى اعتداءات رقمية تُرجَّح ضلوع أطراف أجنبية في تنفيذها، مما يستدعي تطوير استراتيجيات وطنية وتعاونية إقليمية ودولية لمواجهة هذا النوع من التهديدات الأمنية والقانونية.

وأخيرًا، يُفترض أن القانون الدولي يحتاج إلى تعزيز وتطوير في مجال الهجمات السيبرانية، سواء من خلال تبنّي بروتوكولات إضافية للاتفاقيات الدولية الحالية أو عبر إصدار توجيهات وتوصيات من الجمعية العامة للأمم المتحدة أو هيئات فنية متخصصة، بهدف وضع حدٍّ فاصل بين العمل العسكري المشروع والجريمة الإلكترونية غير المشروعة، وضمان حماية المدنيين والأعيان المدنية في الفضاء الرقمي.

ثالثا – أهمية البحث

تتجلى أهمية اختيار هذا الموضوع في الزيادة الملحوظة في الهجمات السيبرانية على المؤسسات المدنية والبنية التحتية، مما يستدعي ضرورة تحليل هذه الأفعال من منظور قانوني منظم، ويسعى البحث إلى تسليط الضوء على أهمية تحديث القانون الدولي العام ليواكب التطورات التكنولوجية المتغيرة، ولضمان تحقيق التوازن بين حماية حقوق الدول وسيادتها وبين ضرورة تبني استراتيجيات دولية مشتركة لمكافحة التهديدات السيبرانية.

رابعا – هدف البحث

يهدف هذا البحث إلى دراسة الهجوم السيبراني على جنوب لبنان من منظور القانون الدولي العام، من خلال تحليل مفهوم الهجوم السيبراني في القانون الدولي، واستعراض الجهود الدولية الرامية إلى وضع تعريف واضح لهذا المصطلح. ويتطرق البحث إلى تقييم مدى توافق الهجمات السيبرانية التي استهدفت جنوب لبنان مع مبادئ القانون الدولي، بما في ذلك مبدأ السيادة، مبدأ عدم التدخل، ومبدأ حظر استخدام القوة. والآثار القانونية لهذه الهجمات، سواء على المستوى الوطني أو الدولي.

خامسا – منهجية البحث

منهج البحث سيكون تحليليًا، حيث سيتم دراسة النصوص القانونية ذات الصلة. يتمثل المنهج في دراسة النصوص القانونية الدولية ذات الصلة بتقييم هذه الهجمات وتحديد إذا كانت تشكل جرائم دولية وما هي الآليات القانونية لمحاسبة مرتكبيها.

سادسا – هيكلية البحث

سيتم تقسيم البحث الى فصلين رئيسين: يتناول الفصل الأول بيان ماهية الهجمات السيبرانية وتصنيفات الهجمات السيبرانية وأنواعها، مع ايراد الإطار القانوني الدولي ذات الصلة، وسيتم تخصيص الفصل الثاني لأثار الهجمات السيبرانية على جنوب لبنان، واليات المحاسبة القانونية قبل أن تختتم الدراسة بالمقترحات والخاتمة التي تلخص النتائج والأفكار الأساسية التي تم التوصل إليها.

1. الفصل الأول: ماهية الهجمات السيبرانية

في ظل التوجه العالمي نحو الحوكمة الالكترونية، واندماج الكيانات الدولية في بودقة النظام الموحد، تمثل الهجمات السيبرانية تهديدًا متزايدًا ومعقدًا يواجه الحكومات والشركات والمجتمعات على حد سواء. هذه الهجمات التي تستهدف الأنظمة المعلوماتية عبر شبكة الإنترنت، قد تحمل في طياتها مخاطر جسيمة على الأمن الوطني والدولي، بالإضافة إلى الأبعاد السياسية والاقتصادية.

من هذا المنطلق، تتزايد الحاجة إلى دراسة ماهية هذه الهجمات وكيفية تعريفها بشكل دقيق، بهدف توجيه السياسات والتشريعات المناسبة لمكافحتها، مما يمثل تحديات كبيرة في إيجاد تعريف موحد وواضح للهجوم السيبراني، يعود ذلك إلى تعدد الجوانب التقنية والقانونية والسياسية التي تدخل في تكوين هذه الهجمات.

ولابد من الاشارة الى عدد من المحاولات الدولية للتعاون من أجل تحديد أسس واضحة لتعريف الهجمات السيبرانية، وذلك لتسهيل التعاون بين الدول والمنظمات الدولية في مواجهة هذه التهديدات. فقد سعت بعض المنظمات، مثل الأمم المتحدة والاتحاد الأوروبي، إلى تطوير إطارات قانونية تدعم التعاون في مكافحة الهجمات السيبرانية.

لذلك، سيتم تقسيم هذا الفصل على مبحثين: الأول منهما لبيان مفهوم الهجمات السيبرانية من خلال استعراض مختلف التعريفات المتبناة في الأدبيات القانونية والتقنية، بينما سيتناول المبحث الثاني تصنيفات الهجمات السيبرانية، بهدف الوصول الى فهم كامل لهذه الهجمات وكيفية التعامل معها ضمن الإطار الدولي.

1.1. المبحث الأول: مفهوم الهجمات السيبرانية

على الرغم من حداثة التداول لمفردة السيبرانية *Cyber (Merriam-Webster*، 2025) على المستوى العربي والعالمي، إلا أن للمفردة جذوراً في اللغة اليونانية حيث يرجعها بعض الباحثين إلى مصطلح *Kubernetes. (Vocabulary.com*، *n.d)* الذي يعني التحكم عن بعد (عزالدين، 2024، ص2)،

Print ISSN: 2791-2248
Online ISSN: 2791-2256
مَجلّةُ تَسْنِيمِ الدَوليّة
للعُلومِ الإنسانيّةِ والاجتمَاعيّةِ والقانونيّةِ

وكان أول استخدام للفظة من قبل عالم الرياضيات نوربرت وينر في مجال التحكم والاتصال عام 1948 (*Dawkins*، 2022)، ولا يوجد ما يقابلها في اللغة العربية، لذلك يصار إلى اعتماد مفردة إلكتروني في ترجمة النصوص ذات العلاقة، بينما يفضل أغلب المختصين استخدام مفردة السيبرانية عند تناولهم لموضوع البحث (الفتلاوي، 2016، ص615).

أما فيما يتعلق بمفهوم الهجوم السيبراني، فأغلب المصادر تشير إلى أنها تتمثل بأي نشاط عدائي يُنفذ عبر الإنترنت أو الشبكات الرقمية بهدف التسبب في أضرار أو تعطيل أنظمة المعلومات، أو سرقة بيانات حساسة. ويشمل التعريف كل أنواع الهجمات السيبرانية التي تهدف إلى تعطيل خدمات الإنترنت (*Microsoft*، 2022، *p*).

لما تقدم، سيتم تقديم تعريف الهجمات السيبرانية الوارد في المصادر الدولية المختلفة، السياسية، القانونية والمتخصصة منها، مع بيان أحدث التصنيفات لهذا النوع من الوسائل بحسب الدراسات المتخصصة.

1.1.1. المطلب الأول: تعريف الهجمات السيبرانية

لا يتوفر تعريف جامع مانع في النصوص القانونية الدولية أو في المصادر التشريعية الوطنية، ولكن يمكن القول بأنها أعمال عدائية تتم عبر الفضاء السيبراني بهدف إلحاق الضرر بالأنظمة الحاسوبية، أو سرقة المعلومات، أو تعطيل الخدمات، وتتضمن هذه الهجمات استخدام تقنيات متقدمة لاستغلال الثغرات الأمنية في الشبكات والأنظمة، مما يؤدي إلى تدهور الثقة في الأمان السيبراني. وقد سعت بعض الجهات الحكومية والمنظمات الدولية إلى وضع تعريف بهدف بيان هذا النوع من النشاطات من أجل تكييفها قانونياً (صبحي، 2020، ص 14). وبالتالي، أمكن للنزاع المسلح أن ينشأ بأي صورة تقليدية أو متطورة (التميمي، 2022، ص11).

أولا – على المستوى الدولي

لا يتوفر تعريف جامع مانع في النصوص القانونية الدولية أو في المصادر التشريعية الوطنية، ولكن يمكن القول بأنها أعمال عدائية تتم عبر الفضاء السيبراني بهدف إلحاق الضرر بالأنظمة الحاسوبية، أو سرقة المعلومات، أو تعطيل الخدمات. وتتضمن هذه الهجمات استخدام تقنيات متقدمة لاستغلال الثغرات الأمنية في الشبكات والأنظمة، مما يؤدي إلى تدهور الثقة في الأمان السيبراني، وقد سعت بعض الجهات الحكومية والمنظمات الدولية إلى وضع تعريف بهدف بيان هذا النوع من النشاطات من أجل تكييفها قانونياً (*OSCE*، 2017). أما المكتب الفيدرالي للتحقيقات *FBI* فإنه يُعرف الهجوم السيبراني بأنه "أي نشاط إجرامي يتم تنفيذه عبر الإنترنت، بما في ذلك اختراق الأنظمة، وسرقة الهوية، والتجسس" (*FBI*، 2020).

Print ISSN: 2791-2248
Online ISSN: 2791-2256

فيما يشير الاتحاد الدولي للاتصالات *ITU* إلى الهجمات السيبرانية على أنها "أعمال تهدف إلى إلحاق الضرر أو إعاقة أو تدمير أنظمة الكمبيوتر والمعلومات، التي قد تؤثر على الأفراد أو الحكومات أو المؤسسات" (القاضي وآخرون، 2024، ص128).

كما أن وكالة الأمن القومي *NSA* تُعرّف الهجوم السيبراني بأنه "أي نشاط موجه ضد أنظمة المعلومات بغرض الإضرار بها أو الوصول إليها دون إذن، بما في ذلك استخدام البرمجيات الخبيثة والتصيد الاحتيالي". ويركز هذا التعريف على الأدوات والأساليب المستخدمة (*NSA*،2020). أما الاتحاد الدولي للاتصالات *ITU* فيصف الهجوم السيبراني بأنه "أعمال تهدف إلى إلحاق الأذى بأنظمة المعلومات أو تعطيل العمليات التجارية عبر استغلال الثغرات". ويُبرز هذا التعريف أهمية الأثر الاقتصادي للهجمات، وقد أولى الاتحاد اهتماماً كبيراً بالهجمات السيبرانية ونظم لها مؤشراً عالمياً وهو ما يعرف بـ *GCI (ITU*،2020*)*.

ثانيا – على المستوى الفقهي

يُعرف الهجوم السيبراني في الأدبيات الأكاديمية (المركز العربي الديمقراطي، 2020) بأنه "أي نشاط عدائي يُنفذ عبر الفضاء الرقمي بهدف إلحاق الضرر بالأنظمة المعلوماتية أو سرقة البيانات أو إحداث انقطاع في الخدمات." ويركز هذا التعريف على الأبعاد التقنية والمقاصد وراء هذه الهجمات، مما يعكس طبيعتها المعقدة (*Snider et al.*، 2021). كما يصف بعض الباحثين الهجمات السيبرانية "بأنها قيام دولة أو فواعل من غير الدول لشن هجوم إلكتروني، يمثل أعمالاً عدائية إلكترونية تستهدف البنية التحتية المعلوماتية للدول لتحقيق أغراض متداخلة سياسية، واقتصادية، وإجرامية، وغيرها" (منيب، 2022، ص121).

من جهة أخرى، فإن العديد من الشركات المتخصصة في الأمن السيبراني، مثل كاسبر سكاي ومكافي، تصف الهجمات السيبرانية بأنها "محاولات إلكترونية تستهدف الأفراد أو المؤسسات، وقد تتضمن استخدام البرمجيات الضارة، هجمات ((*DDoS (Fortinet*،2020)، أو استغلال الثغرات في الشبكات." ويشير تقرير كاسبر سكاي (*Kaspersky*،2020) إلى أن الهجمات السيبرانية تتضمن "كل شكل من أشكال الهجوم الإلكتروني، بما في ذلك البرمجيات الخبيثة، والتصيد الاحتيالي، وهجمات *DDoS*، التي تهدف إلى الاستفادة من نقاط الضعف في الأنظمة".

1.1.2. المطلب الثاني: تصنيفات الهجمات السيبرانية

Print ISSN: 2791-2248
Online ISSN: 2791-2256

تتعدد تصنيفات الهجمات السيبرانية، ويعتمد تصنيفها على عدة عوامل مثل الأهداف، الأساليب المستخدمة، ونوع الأنظمة المستهدفة. تُعتبر هذه التصنيفات ضرورية لفهم طبيعة التهديدات المتزايدة في الفضاء السيبراني، مما يسهم في تطوير استراتيجيات فعالة للتصدي لها.

ولعل أبرز تصنيف نراه متفقا مع هدف البحث هو الاتي:

أولا– الهجمات على البنية التحتية

تُعتبر الهجمات على البنية التحتية الحيوية من أخطر أنواع الهجمات السيبرانية، نظرًا لتأثيرها المباشر على الخدمات الأساسية التي يعتمد عليها المجتمع. وهذه الهجمات تهدف إلى إحداث تعطيل كبير أو تدمير جزئي للأنظمة التي تدعم هذه القطاعات (*Stallings*، 2019، *p.155*).

ومن أبرز الأساليب المستخدمة في هذه الهجمات هو الهجوم الإلكتروني الذي يستهدف أنظمة التحكم الصناعي، مثل أنظمة *SCADA* (أنظمة التحكم الإشرافي وتحصيل البيانات). ويتيح هذا النوع من الأنظمة التحكم في العمليات الصناعية الحيوية، مثل توليد الكهرباء أو معالجة المياه. ويمكن أن يؤدي ذلك إلى انقطاع الخدمة أو حتى الكوارث البيئية. مثل هجوم "ستكسنت" الذي استهدف البرنامج النووي الإيراني، والذي أظهر كيف يمكن استخدام البرمجيات الخبيثة للتلاعب بأنظمة التحكم الحيوية (*Goudarzi et al.*، 2022).

كذلك يتمثل في شل قدرة الطرف المستهدف على الاستفادة من تقنيات المراقبة والإنذار، ففي عام 2007، نفذ الكيان الصهيوني هجومًا سيبرانيًا ضد سوريا، أدى إلى تعطيل عمل أجهزة الرادار ومنظومات الاتصال في المرافق العسكرية والمدنية. وجاء هذا الهجوم أثناء غارة جوية شنتها القوات الجوية الصهيونية على مواقع سورية، والتي زعم الكيان الصهيوني أنها تضم منشآت تتعلق بمفاعل نووي (الاكيابي، 2023، ص1290–1294).

كما تُستخدم هجمات *DDoS* بشكل متزايد ضد البنية التحتية، حيث يُغمر النظام بحركة مرور ضخمة من الطلبات، مما يؤدي إلى تعطيل الخدمات (الرشيدي، 2021، ص42). وفي عام 2016، تعرضت شركة "*Dyn*"، المسؤولة عن خدمات *DNS*، لهجوم *DDoS* أدى إلى انقطاع خدمات العديد من المواقع الكبرى، مما يعكس مدى ضعف الأنظمة البنية التحتية أمام هذه الأنواع من الهجمات (ديفيز وآخرون، 2017، ص8).

ثانيا – الهجمات على الأفراد

تستهدف الهجمات السيبرانية الأفراد بشكل رئيسي بهدف انتهاك خصوصيتهم وأمانهم الشخصي، حيث تعتمد هذه الهجمات على مجموعة متنوعة من الأساليب والتقنيات المتطورة التي تُستخدم لسرقة المعلومات الشخصية الحساسة. وتشمل هذه المعلومات كلمات المرور، وأرقام الحسابات البنكية، ومعلومات الهوية الشخصية، وحتى بيانات البطاقات الائتمانية. وتُعتبر هذه البيانات هدفًا مثاليًا للمهاجمين نظرًا لإمكانية استغلالها في أنشطة احتيالية أو للابتزاز المالي، مما يؤدي إلى آثار مدمرة على الضحايا من الناحية المالية والنفسية (*Reindl*، 2021، *p.79*).

في هذا السياق، يُشير تقرير صادر عن المنظمة الدولية للشرطة الجنائية (*INTERPOL*) بعنوان "*Cybercrime Threat Landscape 2023*" إلى أن الهجمات السيبرانية أصبحت أكثر تطورًا واستهدافًا للأفراد كجزء من استراتيجيات الجرائم الإلكترونية الحديثة. ووفقًا للتقرير، فإن الاستيلاء على البيانات الشخصية يُعد أحد الأهداف الرئيسية لهذه الهجمات، حيث يتم بيع هذه البيانات في السوق السوداء الرقمية (*Dark Web*) أو استخدامها مباشرة في تنفيذ عمليات احتيال أو ابتزاز. كما يلفت التقرير الانتباه إلى أهمية تعزيز التوعية العامة حول ممارسات الأمن السيبراني، مثل استخدام كلمات مرور قوية وتجنب النقر على الروابط المشبوهة، لحماية الأفراد من الوقوع ضحية لهذه الهجمات (*INTERPOL*، 2023).

تُعد الهجمات باستخدام البرمجيات الخبيثة (*Malware*) واحدة من أكثر الأساليب شيوعًا وخطورة في عالم الجرائم السيبرانية. ويتم تثبيت هذه البرمجيات على أجهزة المستخدمين دون علمهم، مما يتيح للمهاجمين الوصول غير المصرح به إلى المعلومات المخزنة على تلك الأجهزة واستغلالها بطرق ضارة (*INTERPOL*، 2023). وتتنوع أنواع البرمجيات الخبيثة لتشمل الفيروسات (*Viruses*)، والبرمجيات التجسسية (*Spyware*)، وبرمجيات الفدية (*Ransomware*)، وكل منها يحمل تهديدات مميزة تؤثر بشكل مباشر على أمان البيانات الشخصية والأمن السيبراني (*McCaffrey*، 2020، *pp.45-47*).

على سبيل المثال، تعمل البرمجيات التجسسية (*Spyware*) على جمع المعلومات الحساسة مثل كلمات المرور وأرقام البطاقات الائتمانية وبيانات التصفح، ثم إرسالها إلى المهاجمين الذين يستخدمونها لأغراض احتيالية أو للتجسس (*Morgan*، 2023). أما برمجيات الفدية (*Ransomware*)، فهي تعتمد على تشفير بيانات الضحية بحيث تصبح غير قابلة للاستخدام، ويطلب المهاجمون فدية مالية مقابل فك التشفير وإعادة الوصول إلى البيانات. وقد أصبحت هجمات برمجيات الفدية واحدة من أكثر التهديدات السيبرانية انتشارًا في السنوات الأخيرة، حيث تستهدف الأفراد والشركات وحتى المؤسسات الحكومية، مما يؤدي إلى خسائر مالية كبيرة وتعطيل للعمليات اليومية (رمضان، 2025، ص1758).

Print ISSN: 2791-2248
Online ISSN: 2791-2256

في هذا السياق، يشير تقرير صادر عن شركة "سايبرسيكيوريتي فينتشرز" (*Cybersecurity Ventures*) حول مستقبل الجرائم السيبرانية إلى أن تكلفة الأضرار الناجمة عن برمجيات الفدية وحدها ستصل إلى حوالي 265 مليار دولار سنويًا بحلول عام 2031، مع تنفيذ هجوم جديد كل ثانيتين تقريبًا (*Morgan*، 2023). كما يوضح التقرير أن المهاجمين أصبحوا أكثر احترافية في تصميم برمجياتهم الخبيثة، مما يجعل من الصعب على الأفراد والمؤسسات اكتشافها أو التصدي لها باستخدام الوسائل التقليدية. لذا يعد الابتزاز الإلكتروني أيضًا شكلًا من أشكال الهجمات على الأفراد، مما يعرّض المستخدمين لمخاطر جديدة (الزهراني، 2021، ص75).

بالإضافة إلى ما تقدم، يمكن تصنيف الهجمات السيبرانية إلى خمس فئات رئيسية:

1. الهجمات على البنية التحتية الحيوية: تستهدف بعض الهجمات السيبرانية الحديثة الأنظمة الحيوية التي تدعم الخدمات الأساسية مثل الماء والكهرباء والنقل والصحة، وهي الأنظمة التي تمثل ركيزة أساسية لحياة المدنيين واستمرار عمل المؤسسات العامة، ويترتب على تعطيلها آثار كارثية تشمل انقطاع التيار الكهربائي، توقف شبكات المياه، وتدهور قطاع النقل والخدمات الطبية، مما يؤدي إلى زعزعة الاستقرار الوطني وتهديد سلامة السكان. ومن أبرز الأمثلة على ذلك الهجمات السيبرانية التي تستهدف محطات توليد الطاقة أو الشبكات الذكية لإدارة الكهرباء، والتي قد تُحدث انهيارًا جزئيًا أو كليًا في البنية التحتية الطاقية، ما يندرج في إطار الاعتداء غير المشروع على المنشآت المدنية وفقًا لمبادئ القانون الدولي الإنساني (*Lewis*، 2006، *p.89*).
2. الهجمات المالية: تُعد الهجمات المالية نوعًا من الجرائم السيبرانية تتركز أهدافها على اختراق الأنظمة المالية واستهداف البيانات الحساسة الخاصة بالمؤسسات أو الأفراد، مثل أرقام الحسابات البنكية، بطاقات الائتمان، وكلمات المرور، وذلك باستخدام أساليب متعددة منها الاحتيال الإلكتروني، والتصيد الاحتيالي (*phishing*)، وبرامج الفدية (*ransomware*)، بهدف تحقيق مكاسب مالية غير مشروعة. وتُشكل هذه الهجمات تهديدًا مباشرًا للاقتصاد الوطني والأمن المالي للمجتمع، كما أنها قد ترقى إلى جريمة دولية إذا تم تنفيذها عبر حدود وطنية أو بدعم من دولة أو جهة معادية، مما يستدعي النظر إليها بمنظار قانوني أوسع يتصل بمسؤولية الدولة والجريمة الإلكترونية الدولية (*Akhgar & Staniforth*، 2014، *p.132*).
3. الهجمات على الأفراد: تستهدف الهجمات السيبرانية على الأفراد خصوصيتهم وأمنهم الشخصي من خلال وسائل مثل التجسس الإلكتروني، وسرقة الهوية الرقمية، والدخول غير المصرح به إلى

حساباتهم الشخصية، وقد تُستخدم هذه الاعتداءات كوسيلة للابتزاز أو الإضرار بالسمعة أو حتى التضييق على الحريات الأساسية. وتُعد هذه الهجمات انتهاكًا جسيمًا لحقوق الإنسان، خصوصًا الحق في الخصوصية والأمان الشخصي، كما قد ترقى إلى جرائم إلكترونية دولية إذا كانت منظمة ومدعومة من قبل جهات أجنبية أو تُنفذ في سياق نزاع مسلح أو عمليات استخبارية معادية، مما يستدعي مساءلة مرتكبيها بموجب القانون الدولي الجنائي (*Reindl*، 2019، *p.78*).

4. الهجمات السياسية: تُنفذ العديد من الهجمات السيبرانية كجزء من صراعات سياسية أو دولية، وتستهدف زعزعة استقرار الدول من خلال التأثير على الانتخابات، تعطيل الأنشطة الحكومية، أو سرقة المعلومات الحساسة والاستخبارية، بهدف تحقيق مكاسب استراتيجية أو إضعاف الخصم دون اللجوء إلى القوة العسكرية التقليدية. وتُعد هذه العمليات تهديدًا جديًا للأمن القومي والسيادة الوطنية، وقد ترقى إلى جرائم حرب أو جرائم ضد الإنسانية إذا أدت إلى انتهاكات جسيمة للقانون الدولي الإنساني، مثل الاعتداء غير المشروع على المنشآت العامة أو التدخل في حقوق الشعوب السياسية، مما يستدعي مساءلة مرتكبيها على المستوى الدولي (*Mazanec*، 2015، *p.215*).
5. الهجمات الموزعة: تُعد الهجمات الموزعة، مثل هجمات الحرمان من الخدمة الموزعة (*DDoS*)، من الأدوات السيبرانية الشائعة التي تُستخدم لإحداث اضطراب في الخدمات الإلكترونية عبر إغراق الأنظمة بكم هائل من الطلبات غير الشرعية، بهدف تعطيل عمل المواقع أو المنصات الرقمية لفترات تتراوح بين القصيرة والطويلة. ويتم تنفيذ هذه الهجمات غالبًا عبر شبكات من الأجهزة المخترقة والمتحكم بها عن بعد (*Botnets*)، مما يجعل من تتبع مصدر الهجوم وتحديد هوية مرتكبيه أمرًا بالغ الصعوبة. ويمكن أن ترقى هذه الهجمات إلى جرائم إلكترونية دولية إذا كانت موجهة ضد مؤسسات حيوية أو جزءًا من عمليات عدائية منظمة تهدد الأمن القومي أو استقرار الدولة، ما يستدعي تعاونًا دوليًا لتعقبها ومعاقبة الجهات المسؤولة عنها (*Shankar*، 2017، *p.30*).

كما ان هناك تصنيفات تتخذ من مضمون الهجوم السيبراني معيارا للتصنيف نوجزها كما يلي:

1. هجمات البرمجيات الخبيثة (*Malware Attacks*):

تُعد هجمات البرمجيات الخبيثة واحدة من أكثر أنواع الهجمات السيبرانية انتشارًا واستخدامًا في النزاعات الرقمية الحديثة. وتشير هذه الهجمات إلى استخدام برامج حاسوبية تم تصميمها بشكل متعمد لأغراض ضارة، بهدف اختراق الأنظمة الرقمية، وتدمير البيانات، أو سرقتها، أو تعطيل العمل الطبيعي للمنشآت الحيوية والبنية التحتية الحساسة.

ويشمل مصطلح "*Malware*" مجموعة واسعة من البرمجيات الضارة، مثل الفيروسات (*Viruses*)، والدودة الحاسوبية (*Worms*)، وحصان طروادة (*Trojan Horse*)، وبرامج الفدية (*Ransomware*)، وأدوات التجسس (*Spyware*)، وغيرها. وكل نوع منها يختلف عن الآخر من حيث طريقة الانتشار، والهدف المُراد تحقيقه، ومدى التعقيد التقني المُستخدم في تصميمه.

وتُعتبر هذه الهجمات أداة فعَّالة في أيدي الجهات التي تسعى إلى تنفيذ عمليات استخبارية، أو تخريبية، أو حتى عسكرية، خصوصًا عندما تستهدف منشآت حيوية مثل شبكات الطاقة، والبنية التحتية للمياه، والأنظمة الصحية، أو المؤسسات الحكومية والأمنية. وفي سياق النزاعات المسلحة، يمكن اعتبار استخدام البرمجيات الخبيثة وسيلة من وسائل القتال غير التقليدية، خاصةً إذا كان الهدف منها هو إحداث ضرر مادي أو معنوي كبير لدى الطرف الآخر، أو تعطيل الخدمات الأساسية التي يحتاجها المدنيون (*Cisco Networking Academy*، 2020، *p.45*).

ومن الناحية القانونية، فإن استخدام البرمجيات الخبيثة ضد أهداف مدنية أو منشآت تحتضن سكانًا مدنيين قد يُشكل انتهاكًا جسيمًا للقانون الدولي الإنساني، خصوصًا إذا أدى إلى إلحاق الضرر العشوائي بالمدنيين أو تدمير الأعيان المدنية دون تمييز. كما أن تنفيذ هذا النوع من الهجمات بقصد الإضرار المتعمد بالمنشآت الحيوية قد يرقى إلى جريمة حرب أو حتى جريمة ضد الإنسانية، وفقًا لنظام روما الأساسي والاتفاقيات الدولية ذات الصلة (*Wang*، 2021، *p.12*).

وعلى الرغم من عدم وجود نص صريح في القانون الدولي يعالج الهجمات السيبرانية بشكل مباشر، إلا أن هناك توجهًا فقهيًا ودوليًا متزايدًا نحو توسيع تفسير مواد القانون الدولي الإنساني لتضم العمليات السيبرانية التي تُشبه من حيث التأثير والنية العمليات العسكرية التقليدية. ومن ثمَّ، فإن هجمات البرمجيات الخبيثة لا تخرج بالضرورة عن نطاق القانون الدولي، بل يمكن تأهيلها كأفعال مجرمة إذا توفرت فيها شروط الانتهاك الجسيم للقانون الدولي الإنساني. وتشير إلى استخدام برامج ضارة تهدف إلى إلحاق الضرر أو الاستيلاء على بيانات الأنظمة الحاسوبية. وهناك أنواع متعددة من البرمجيات الخبيثة، منها: *Worms*، *Trojan Horse*، *Ransomware*، *Spyware*.

2. هجمات التصيد (*Phishing Attacks*):

تُعد هجمات التصيد من أنواع الهجمات السيبرانية التي تعتمد على الخداع الإلكتروني كوسيلة للحصول على معلومات حساسة أو شخصية من الضحايا، مثل كلمات المرور، وبيانات الحسابات البنكية، أو الهويات الرقمية، وذلك تحت ستار التعامل مع جهة موثوقة أو مؤسسة رسمية. وتُعتبر هذه الهجمات شكلًا من

أشكال الاعتداء غير المشروع على الخصوصية والأمن المعلوماتي، وقد ترقى إلى جريمة إلكترونية دولية إذا استهدفت منشآت استراتيجية أو أفرادًا في إطار نزاع مسلح أو عمليات تجسس (*Pfleeger & Pfleeger*، 2015، *p.233*).

وتتخذ هجمات التصيد عدة أشكال رئيسية، منها:

أ. التصيد التقليدي (*General Phishing*): وهو النوع الأكثر شيوعًا، حيث يتم فيه إرسال رسائل إلكترونية جماعية أو إنشاء صفحات ويب مزيفة تُحاكي مواقع إلكترونية حقيقية (مثل المصارف أو خدمات البريد الإلكتروني)، بهدف تضليل المستخدمين من خلال إدخال بياناتهم الشخصية دون علمهم.

ب. التصيد المستهدف (*Spear Phishing*): وهذا النوع أكثر خطورة من حيث الغرض والتنفيذ، إذ يستهدف فردًا محددًا أو مجموعة صغيرة، غالبًا ما تكون من الموظفين المسؤولين عن ملفات حساسة أو مناصب حيوية داخل المؤسسة المستهدفة. ويتميز هذا النوع بدقة التخطيط واعتماده على جمع معلومات مسبقة عن الضحية لزيادة فرص النجاح.

ت. التصيد عبر الرسائل النصية (*Smishing*): ويشير إلى استخدام الرسائل القصيرة (*SMS*) كوسيلة لخداع الضحية، عادةً عبر إرسال روابط أو تعليمات تدفعه إلى الإفصاح عن معلوماته الشخصية أو تنزيل برمجيات خبيثة.

ث. التصيد الصوتي (*Vishing*): وهو نوع من الهجمات التي تستخدم الاتصالات الهاتفية كوسيلة للخداع، حيث يقوم المهاجم بتقمص دور موظف في جهة موثوقة (مثل البنك أو دائرة حكومية) لإرغام الضحية على إعطاء معلوماته السرية شفهيًا.

البعد القانوني لهجمات التصيد:

على الرغم من أن معظم التشريعات الوطنية تصنف التصيد باعتباره جريمة إلكترونية تخضع للقانون الجنائي الداخلي، فإن الإطار القانوني الدولي لا يزال يفتقر إلى نصوص واضحة تتعامل مع هذا النوع من الجرائم بشكل مباشر. ومع ذلك، يمكن اعتبار بعض أنواع التصيد، خاصة تلك التي تُنفذ في سياق نزاع مسلح أو بأهداف استخبارية أو عسكرية، انتهاكًا للقانون الدولي الإنساني إذا كانت تُستخدم كوسيلة للتجسس أو تعطيل البنية التحتية الحيوية أو المساعدة في تنفيذ عمليات عدائية ضد المدنيين (*Gisel & Olejnik*، 2019). وتتضمن هذه الهجمات عادةً تقنيات خداعية تجعل الضحية تعتقد أنها تتعامل مع جهة موثوقة. ومنها: التصيد التقليدي، التصيد المستهدف، التصيد بالرسائل النصية، والتصيد الصوتي.

3. هجمات الحرمان من الخدمة (*Denial of Service Attacks*):

تشير هجمات الحرمان من الخدمة إلى نوع من الهجمات السيبرانية التي تهدف إلى تعطيل عمل الأنظمة أو الشبكات الحاسوبية عن طريق إغراقها بكم هائل من الطلبات أو البيانات غير المشروعة، مما يؤدي إلى إسقاط الخوادم (*Servers*) أو جعل الخدمات غير متاحة للمستخدمين المشروعين لفترات زمنية تتراوح بين الدقائق والأسابيع. وعندما يتم تنفيذ هذه الهجمات باستخدام شبكة واسعة من الأجهزة المصابة والمُحكَمة التحكم (*Botnet*)، فإنها تُعرف باسم هجمات الحرمان من الخدمة الموزعة (*Distributed Denial of Service – DDoS*) (الاتفاقية العربية، 2010).

وتُعد هذه الهجمات واحدة من أكثر أنواع الاعتداءات الرقمية انتشارًا، خصوصًا ضد المؤسسات الحكومية، والبنوك، ووسائل الإعلام، ومنصات الخدمات العامة. وغالبًا ما تُستخدم كأداة للضغط السياسي أو الاقتصادي، أو كجزء من حملة أوسع تستهدف زعزعة استقرار الدولة أو الإضرار بمصالحها الاستراتيجية.

الآثار الناتجة عن هجمات *DoS*:

4. خسائر اقتصادية كبيرة: نتيجة تعطل العمليات التجارية الإلكترونية أو خدمات البنوك والمؤسسات المالية.
5. تدهور الثقة بالخدمات الرقمية: خاصةً إذا كانت المنصة المستهدفة تابعة للدولة أو لمؤسسة عمومية.
6. إعاقة تقديم الخدمات الأساسية: مثل الخدمات الصحية أو التعليمية التي تعتمد على البنية التحتية الرقمية.
7. التأثير على السمعة: حيث يمكن أن تؤثر هذه الهجمات سلبًا على صورة المؤسسة أو الدولة المعنية، وتُعتبر مؤشرًا على ضعف البنية الأمنية.

البعد القانوني لهجمات الحرمان من الخدمة:

رغم أن معظم التشريعات الوطنية تصنف هجمات *DoS* باعتبارها جرائم إلكترونية تخضع للقانون الجنائي المحلي، مع ذلك، يمكن النظر إليها من زاوية قانونية أوسع ضمن إطار القانون الدولي الإنساني والقانون الدولي الجنائي إذا توفرت شروط معينة، منها:

1. أن يكون الهجوم جزءًا من عملية عدائية منظمة تُشن في سياق نزاع مسلح.
2. أن تستهدف منشآت مدنية ذات طبيعة حيوية (مثل البنية التحتية للطاقة أو الصحة).

3. أن تترتب عليها آثار مادية أو معنوية جسيمة تطال المدنيين أو تعرّض حياتهم أو سلامتهم للخطر.
4. أن تكون مرتبطة بنية عدوانية وأن تُنفذ بأمر من جهة قيادية أو جهة سياسية أو عسكرية.

وفي حال توفر هذه الشروط، يمكن اعتبار هجوم *DoS* أو *DDoS* شكلاً من أشكال الهجمات السيبرانية غير المشروعة التي قد ترقى إلى جريمة حرب أو حتى جريمة ضد الإنسانية، وفقًا لأحكام نظام روما الأساسي والاتفاقيات الدولية ذات الصلة. وهذه الهجمات يمكن أن تتسبب في تعطيل الخدمات لفترات زمنية متفاوتة، مما يؤدي إلى خسائر اقتصادية أو تضرر للسمعة (نعمة وآخرون، 2023، ص29).

1.2. المبحث الثاني: الهجوم السيبراني في إطار القوانين الدولية

على الرغم من حداثة موضوع الأمن السيبراني قياسًا بالتطور القانوني للتشريعات المماثلة، ومع تزايد الاعتماد على التكنولوجيا الرقمية في مختلف جوانب الحياة، أصبح الأمن السيبراني أحد أهم القضايا التي تواجه المجتمع الدولي والتي تتطلب الحراك الدولي للتعامل معه (نعمة وآخرون، 2023، ص29). بالاستناد إلى الإرث القانوني للاتفاقات والقوانين المنظمة للنزاعات المسلحة وبسط الأمن والسلام، وكذلك الاتفاقيات الدولية والإقليمية (نعمة وآخرون، 2023، ص91) التي سعت لتقنين استخدام الوسائل السيبرانية في مجال الحرب.

في هذا المبحث، سنستعرض أبرز القوانين والاتفاقيات الدولية التي تنظم مجال الأمن السيبراني، ودور المنظمات الدولية في تعزيز هذه التشريعات، وتأثيرها على الجرائم السيبرانية والتحديات التي تواجه تطبيقها على المستوى العالمي.

1.2.1. المطلب الأول: الاتفاقيات الدولية وتأثيرها على الجرائم السيبرانية

على الرغم من حداثة موضوع الأمن السيبراني قياسًا بالتطور القانوني للتشريعات المماثلة، ومع تزايد الاعتماد على التكنولوجيا الرقمية في مختلف جوانب الحياة، أصبح الأمن السيبراني أحد أهم القضايا التي تواجه المجتمع الدولي والتي تتطلب الحراك الدولي للتعامل معه (نعمة وآخرون، 2023، ص29). بالاستناد إلى الإرث القانوني للاتفاقات والقوانين المنظمة للنزاعات المسلحة وبسط الأمن والسلام، وكذلك الاتفاقيات الدولية والإقليمية (نعمة وآخرون، 2023، ص91) التي سعت لتقنين استخدام الوسائل السيبرانية في مجال الحرب.

أولاً – اتفاقية جنيف لعام 1949 وبروتوكولاتها الملحقة

Print ISSN: 2791-2248
Online ISSN: 2791-2256
مَجلّةُ تَسْنِيمِ الدَوليّة
للعُلومِ الإنسانيّةِ والاجتمَاعيّةِ والقانونيّةِ

تُعرف اتفاقيات جنيف بأنها مجموعة من المعاهدات الدولية التي تم التوصل إليها خلال القرنين التاسع عشر والعشرين، والتي تهدف إلى تنظيم قوانين الحرب وحماية الأفراد أثناء النزاعات المسلحة. أول اتفاقية جنيف وُضعت في عام 1864 (اللجنة الدولية للصليب الأحمر، 1977، م35)، ومن ثم تم تحديثها وتوسيعها عبر عدة بروتوكولات إضافية، وأهمها اتفاقيات جنيف الأربع لعام 1949. وتشمل هذه الاتفاقيات حماية الجنود الجرحى، والأسرى، والمدنيين، والمرضى خلال النزاعات المسلحة (فياض، 2020).

وعلى الرغم من أنها تُركز أساسًا على حماية المدنيين في النزاعات المسلحة، إلا أن بعض مبادئ اتفاقيات جنيف يمكن تطبيقها على الهجمات السيبرانية، خصوصًا تلك التي تستهدف البنية التحتية الحيوية. فقد ورد في نصوصها أن: "يلتزم أي طرف سامٍ متعاقد، عند دراسة سلاح جديد أو تطويره أو اقتنائه أو أداة حرب أو اتّباع أسلوب للحرب، بأن يتحقق مما إذا كان ذلك محظورًا في جميع الأحوال أو في بعضها ....." (اتفاقية جنيف، البروتوكول الإضافي الأول، 1977، م3/ب). وتُشدد هذه الاتفاقيات على أهمية حماية المدنيين والممتلكات خلال النزاعات، مما يتطلب من الدول وضع تدابير لضمان عدم استخدام الهجمات السيبرانية ضد الأهداف المدنية (عبد الجواد، 2023، ص885).

فيما يتعلق بالجرائم السيبرانية مثل الهجمات الإلكترونية ضد الأنظمة الحاسوبية، سرقة البيانات، أو تعطيل البنية التحتية الرقمية، لم تغطي اتفاقيات جنيف بشكل محدد هذا النوع من الجرائم، لأنها تم توقيعها قبل ظهور الإنترنت والتكنولوجيا الحديثة. ومع ذلك، فإن هناك بعض النقاط التي يمكن أن تكون ذات صلة وتأثير على الجرائم السيبرانية في السياق الدولي:

تتعلق اتفاقيات جنيف بحماية المدنيين والبنية التحتية المدنية من الهجمات في النزاعات المسلحة. مما يمكن أن يشمل استخدام الهجمات السيبرانية لتدمير البنية التحتية الحيوية مثل شبكات الكهرباء والمستشفيات أثناء الحرب، وقد تُعتبر انتهاكًا للقانون الدولي الإنساني وحقوق المدنيين. كما يمكن اعتبار الهجمات السيبرانية على الأهداف المدنية جرائم حرب، خاصة إذا استهدفت تعطيل الخدمات الأساسية أو إذا وقعت الهجمات في الأراضي المحتلة، حيث يستمر نفاذ الاتفاقيات طوال فترة الاحتلال (القاموس العملي للقانون الإنساني، 2020).

تنص المادة 36 من البروتوكول الإضافي الأول لاتفاقيات جنيف لعام 1977 على وجوب تقييم الأسلحة الجديدة، بما يشمل الهجمات السيبرانية كأداة حرب حديثة. وعلى الرغم من عدم ذكرها صراحةً، يمكن اعتبار هذه الهجمات ضمن "الأسلحة الجديدة" التي تخضع لتقييم قانوني وفق مبادئ القانون الدولي الإنساني (نعمة وآخرون، 2023، ص53).

يوفر مبدأ شرط مارتنز إطارًا قانونيًا لمعالجة القضايا المستجدة غير المنظمة بوضوح في القانون الدولي، مؤكداً أن المدنيين والمقاتلين يظلون تحت حماية المبادئ الإنسانية والضمير العام. وبالتالي، يجب أن تخضع الهجمات السيبرانية للقواعد الدولية، بما يضمن التزامها بمبادئ التناسب والتمييز وتجنب الإضرار بالبنية التحتية المدنية (*Burgess*، 2019).

على الرغم من أن الهجمات السيبرانية قد تكون فعالة في تعطيل المعدات العسكرية أو البنى التحتية، إلا أن استخدامها يجب أن يلتزم بالقواعد التي تضمن أن الهجوم لا يضر بالمدنيين أو يؤدي إلى آثار جانبية غير مبررة في أي نزاع مسلح (مجلة جامعة الإمارات، 2024، ص395). فيعد استهداف العسكريين أو الأهداف العسكرية من خلال الهجمات السيبرانية جزءًا من العمليات الحربية، طالما أن ذلك يتماشى مع مبادئ التناسب والتمييز في القانون الدولي الإنساني (نعمة وآخرون، 2023، ص222).

على الرغم من أن القانون الدولي لم يعترف بشكل صريح بالهجمات السيبرانية كنوع من الجرائم في سياق اتفاقيات جنيف لاختلاف الأسلوب والأدوات والنتائج عن تلك المميزة للأعمال العسكرية (مجلس أوروبا، 2020)، إلا أنه يمكن أن يُستند إليها لمحاكمة الأفراد أو الدول التي ارتكبت هذه الجرائم إذا كانت تشكل انتهاكًا للقانون الدولي الإنساني (منصة *ASJP*، 2020).

ثانيا – اتفاقية بودابست حول الجرائم السيبرانية

تُعتبر اتفاقية بودابست لمكافحة الجرائم السيبرانية *Budapest Convention on Cybercrime* (المطيري، 2020، ص45)، التي تم تبنيها في عام 2001، واحدة من أبرز الأطر القانونية الدولية. وتهدف هذه الاتفاقية إلى تعزيز التعاون بين الدول لمكافحة الجرائم الإلكترونية، وتحديد الإطار القانوني للجرائم المرتبطة بالتكنولوجيا. وتتناول الاتفاقية مجموعة من الجرائم مثل الوصول غير المصرح به إلى الأنظمة المعلوماتية، والتلاعب بالبيانات، والجرائم المتعلقة بالمحتوى (*Cybercrime Convention Committee*، 2020، *p.5*). كما توفر الاتفاقية أيضًا آليات للتعاون الدولي في التحقيقات والملاحقات القضائية (المصدر نفسه، ص6).

فمن متطلبات الانضمام للاتفاقية من الدول "ضمان تجريم الجرائم المرتكبة ضد أجهزة الكمبيوتر أو باستخدامها في قوانينها المحلية، وتمتع سلطات العدالة الجنائية فيها بالصلاحيات المنصوص عليها في قانونها الإجرائي ليس فقط للتحقيق في الجرائم الإلكترونية بل وفي أي جريمة يكون الدليل فيها في شكل إلكتروني" (اتفاقية بودابست، 2001، م7–8)، بالإضافة إلى العمل على تيسير التعاون الدولي حسب

متطلبات الجريمة المزدوجة، وتشريع قوانين وطنية تتفق مع ما جاء في بنود الاتفاقية (اتفاقية بودابست، 2001، م9). وتغطي اتفاقية بودابست مجموعة من الجرائم، مثل:

الجرائم المرتبطة بالكومبيوتر: تلتزم الدول الأطراف باتخاذ التدابير اللازمة لتجريم الأفعال المتعلقة بالكومبيوتر التي تتم عمدًا ودون وجه حق، مثل إدخال أو تعديل أو حذف أو إتلاف البيانات بشكل يضلل أو يجعل البيانات غير الأصلية تبدو أصلية. كما تلتزم الدول الأطراف بتجريم الأفعال التي تضر بملكية الآخرين عن طريق إدخال أو تعديل أو حذف أو إتلاف بيانات الكومبيوتر. كذلك التدخل في وظائف أنظمة الكومبيوتر بقصد الاحتيال أو للحصول على منفعة اقتصادية غير مشروعة (اتفاقية بودابست، 2001، م12).

الجرائم المتعلقة بالمحتوى: تلتزم الدول الأطراف باتخاذ التدابير اللازمة لتجريم الأفعال المتعلقة بإنتاج وتوزيع وعرض مواد إباحية عن الأطفال عبر أنظمة الكومبيوتر، ويشمل ذلك إنتاج مواد إباحية عن الأطفال بهدف توزيعها، وعرضها أو إتاحتها عبر الكومبيوتر، وتوزيعها أو نقلها من خلاله. كما يتم تجريم الحصول على مواد إباحية عن الأطفال عبر الكومبيوتر لصالح الشخص نفسه أو للآخرين، كما يحق للدول الأطراف الاحتفاظ بحق استثناء تطبيق بعض البنود جزئيًا أو كليًا (اتفاقية بودابست، 2001، م13-15، 22).

كما ألزمت الاتفاقية كل دولة طرف باتخاذ التدابير اللازمة لضمان أن الجرائم تعاقب بعقوبات فعالة ومتناسبة، تشمل العقوبات السالبة للحرية، كما تضمن مساءلة الأشخاص الاعتباريين وتطبيق عقوبات رادعة ومناسبة عليهم. وأن تتخذ كل دولة طرف التدابير اللازمة لتطبيق الإجراءات المقررة في هذا القسم بهدف التحقيق في الجرائم المحددة في الاتفاقية (وحدة التفتيش المشتركة، 2021، ص94). كما بينت الاتفاقية المبادئ العامة المتعلقة بالولاية القضائية، وتسليم المجرمين، والمساعدة المتبادلة في حال عدم وجود اتفاقات دولية، وتشمل تدابير مؤقتة، وسلطات التحقيق، وضمان توفير المساعدة الفورية على مدار الساعة لأغراض التحقيقات والإجراءات المتعلقة بالجرائم الإلكترونية وجمع الأدلة الإلكترونية (الأمين العام للأمم المتحدة، 2024).

ثالثاً – جهود الأمم المتحدة

تركز المنظمة على توفير الحماية اللازمة للصمود أمام الهجمات السيبرانية (عزالدين، 2020، ص5)، على الرغم من عدم إلزامية هذه القرارات، إلا أنها تُعكس التوجهات الدولية نحو تعزيز الأمن السيبراني. وهو ما أكد عليه أنطونيو غوتيريش، الأمين العام بقوله: أن "التكاليف التي يتحملها سلامنا وأمننا واستقرارنا

المشترك – سواء داخل البلدان أو فيما بينها. فالأنشطة الضارة التي تقوض المؤسسات العامة والعمليات الانتخابية والنزاهة عبر الإنترنت تؤدي إلى تآكل الثقة وتأجيج التوترات، بل وتزرع بذور العنف والصراع" (كاستيليك، 2021، ص15–19).

1.2.2. *المطلب الثاني: مساهمات المنظمات الدولية*

تلعب المنظمات الدولية دورًا محوريًا في تعزيز الأمن السيبراني على المستوى العالمي، من خلال تطوير الأطر القانونية الدولية، والتنسيق بين الدول لمكافحة التهديدات السيبرانية، وتقديم الدعم الفني. وتأتي هذه المنظمات لتوحيد الجهود الدولية وضمان بيئة رقمية آمنة.

أولاً: تعمل المنظمات الدولية على وضع الأطر القانونية التي تنظّم المجال السيبراني، من ضمن هذه المعايير أن تتعهد الدول بمنع استخدام شبكات الإنترنت في الأعمال التي تهدد أو تضر بالسلم والأمن الدوليين، وعدم السماح عن قصد باستخدام أراضيها في أفعال غير مشروعة (ليبتون، 2020). إلى جانب ذلك، تقدم منظمة الأمن والتعاون الاقتصادي (*OECD*) إرشادات بشأن كيفية تعزيز الأمن السيبراني، وتشجع الدول على تبني أفضل الممارسات في هذا المجال (مجلس الأمن، 2023، ص36/8). كما أن الاتحاد الدولي للاتصالات (*ITU*) يُعتبر أحد اللاعبين الرئيسيين في تطوير معايير دولية تتعلق بالاتصالات والأمن السيبراني من خلال إرساء سياسات تهدف إلى تأمين نظم المعلومات الالكترونية (*NSfocus*، 2020).

ثانياً: تسهم المنظمات الدولية في تعزيز التعاون بين الدول لمكافحة الجرائم السيبرانية. وأحد أبرز الأمثلة على ذلك هو اتفاقية بودابست التي وضعتها مجلس أوروبا، والتي تهدف إلى تسهيل التعاون بين الدول في مجال مكافحة الجرائم الإلكترونية. وتعمل هذه الاتفاقية على تحسين تنسيق التحقيقات والملاحقات القانونية عبر الحدود، وتبادل المعلومات بين السلطات المختلفة (*CNN*، 2024).

2. الفصل الثاني: آثار الهجمات السيبرانية على جنوب لبنان

تشكل الهجمات السيبرانية في عصرنا الحالي أداة جديدة من أدوات النزاعات الدولية، حيث تتجاوز تأثيراتها الجانب التقني لتطال مختلف الجوانب الإنسانية والاجتماعية والاقتصادية وحتى القانونية. وفي حالة جنوب لبنان، الذي يمثل منطقة ذات حساسية سياسية وأمنية كبيرة، برزت هذه الهجمات كتهديد غير مسبوق نظراً لطبيعة الأهداف التي تم استهدافها وحجم التداعيات التي نتجت عنها.

Print ISSN: 2791-2248
Online ISSN: 2791-2256

يهدف هذا الفصل إلى دراسة الآثار المترتبة على الهجمات السيبرانية التي استهدفت جنوب لبنان، سواء على المستوى الفردي أو المجتمعي أو الوطني. وينقسم هذا الفصل إلى ثلاثة محاور رئيسية. أولًا، سيتم تسليط الضوء على الآثار الإنسانية لهذه الهجمات، بما في ذلك الخسائر البشرية والمآسي التي تعرض لها المدنيون نتيجة الاستهداف المتعمد للأجهزة الشخصية والتكنولوجيا التي بحوزتهم. ثانيًا، سيتم تحليل التداعيات الاجتماعية والاقتصادية التي خلفتها هذه الهجمات، والتي شملت تعطيل الحياة اليومية وتدمير البنية التحتية الرقمية وتأثيرها السلبي على الاقتصاد المحلي. ثالثًا، سيتم استعراض الآثار القانونية والسياسية لهذه الهجمات، بما في ذلك ما يتعلق بخرق مبادئ القانون الدولي الإنساني، ومسألة تحديد المسؤولية الدولية عن مثل هذه الأعمال.

من خلال هذا الفصل، نسعى إلى تقديم قراءة متعمقة لهذه الآثار وكيفية التعامل مع الهجمات السيبرانية ضمن إطار قانوني وسياسي متوازن. للتحديات التي فرضتها هذه الهجمات على جنوب لبنان، مع بيان الاليات القانونية الدولية لمكافحة هذه الظاهرة الخطيرة.

2.1. المبحث الأول: الأثر الأمني والسياسي

تُعَد الهجمات السيبرانية من التهديدات المتزايدة التي تواجه العديد من الدول حول العالم، بما في ذلك لبنان، وخاصة جنوبه الذي يشهد تعقيدات سياسية وأمنية. وفي السنوات الأخيرة، زادت التقارير حول الهجمات السيبرانية التي تستهدف البنية التحتية الحيوية، والمؤسسات الحكومية، والشركات الخاصة في المنطقة، مما يُلقي الضوء على الآثار السلبية لهذه الهجمات.

تشير التقارير الدولية والمحلية عن مصادر تقنية وإخبارية (الجبهة الديمقراطية، 2024) إلى أن الهجمات السيبرانية في جنوب لبنان لم تكن موجهة إلى أهداف محددة بحيث يمكن اعتبارها عملاً عسكرياً صرفاً، حيث أكدت تلك التقارير سقوط عدد من المدنيين ومن ضمنهم أطفال في سلسلة انفجار أجهزة النداء البيجر، وبالتالي، فإن هذه الهجمات لا تؤثر فقط على الأمن الاجتماعي، بل أيضًا على الاستقرار الاقتصادي، مما يؤدي إلى تفاقم الأزمات القائمة (*IISF*، 2017، 4 *p*.).

وقد نتج عن هذا الهجوم السيبراني انفجارات متزامنة وقعت خلال دقائق معدودة، ما أسفر عن سقوط أكثر من ثلاثة آلاف ضحية من المواطنين اللبنانيين، بينهم عدد كبير من المدنيين. وعلى الرغم من أن الكيان الصهيوني لم يعلن رسمياً مسؤوليته عن هذه العملية السيبرانية، إلا أنه لم يَنفِ علاقته بها حتى الآن، مما عزز القناعة لدى العديد من الأطراف بأنها الطرف المسؤول عن تنفيذ الهجوم (وكالة أنباء الإمارات، 2025).

وكان حزب الله قد انتقل مؤخرًا إلى استخدام أجهزة الاستدعاء بعد مخاوف بشأن أمن تكنولوجيا الهاتف المحمول وشبكات الهاتف الخلوي. وكان الهدف من هذا التحول هو التخفيف من خطر الاختراق والمراقبة الإلكترونية الصهيونية. وتتمتع أجهزة الاستدعاء بمزايا معينة للخصوصية مقارنة بالهواتف الخلوية، حيث أن جهاز الاستدعاء أحادي الاتجاه هو جهاز استقبال سلبي فقط لا يرسل أي معلومات إلى محطة قاعدية، ولا يمكن تتبع موقعه. وقد تم استيراد أجهزة الاستدعاء، التي تم تحديدها على أنها من طراز "جولد أبولو *AR-924*"، إلى لبنان في وقت سابق من العام الجاري (يوسف، 2013، ص53).

إن الهجوم السيبراني على لبنان هو ناقوس خطر يدق في وجه التشريع الدولي بكل ملامحه، معلناً عن طور جديد من أطوار الأعمال العسكرية التي تستوجب اهتماماً بالغ التركيز للوقوف على مدى جدية الحاجة إلى تناول هذه الأفعال بالدراسة للوصول إلى قناعة لإصدار القرارات الكفيلة بتقييد قدرات الحكومات التقنية في المجال السيبراني.

ويمكن القول إن الهجمات السيبرانية تمثل تهديدًا متزايدًا للأمن القومي للدول في العصر الحديث، حيث تمتد آثارها لتشمل الجوانب العسكرية والاقتصادية والاجتماعية والسياسية. فمن الناحية العسكرية، تستهدف هذه الهجمات أنظمة الدفاع الوطني، بما في ذلك شبكات الاتصالات العسكرية، وأنظمة التحكم في الأسلحة، وقواعد البيانات الاستخباراتية، مما قد يؤدي إلى تعطيل العمليات العسكرية أو كشف المعلومات السرية.

أما فيما يتعلق بالأبعاد السياسية للنزاع واستخدام الهجمات السيبرانية كأداة في الصراعات السياسية، فقد أصبحت هذه الهجمات وسيلة فعالة لتحقيق أهداف سياسية مختلفة. ويتم استخدامها كوسيلة ضغط سياسي لفرض عقوبات غير مباشرة على الخصوم السياسيين، حيث يمكن استهداف البنية التحتية الاقتصادية أو المالية لدولة ما بهدف إجبارها على تغيير سياساتها أو تقديم تنازلات.

2.1.1. المطلب الأول: تأثير الهجمات السيبرانية على الأمن القومي

تعتبر الهجمات السيبرانية تهديدًا خطيرًا للأمن القومي، حيث تؤثر بشكل مباشر على الاستقرار في مناطق مثل جنوب لبنان. ويتمثل تأثير هذه الهجمات في عدة جوانب رئيسية، منها:

زعزعة الاستقرار الأمني: تسهم الهجمات السيبرانية في زعزعة الاستقرار الأمني في جنوب لبنان من خلال استهداف البنية التحتية الحيوية. وعندما تُستهدف أنظمة الكهرباء أو المياه أو الاتصالات، يمكن أن يؤدي ذلك إلى انقطاع الخدمات الأساسية، مما يخلق حالة من الفوضى وعدم اليقين بين المواطنين (آدمز، 2025). وهذه الظروف يمكن أن تُستغل من قبل الجماعات المتطرفة أو الفاعلين غير الحكوميين لتعزيز نفوذهم وزيادة الفوضى (كريم، 2018، ص 25). كما أصبحت الهجمات السيبرانية جزءًا من الحروب

الحديثة، حيث تُستخدم لتعطيل أنظمة العدو دون الحاجة إلى نشر القوات العسكرية، وهو ما يتجلى في الهجمات الروسية على أوكرانيا التي استهدفت الشبكات الكهربائية والنظام المصرفي (المهيري، 2025). بالإضافة إلى ذلك، يتم استخدام الهجمات السيبرانية لنشر المعلومات المضللة أو الدعاية السياسية بهدف التأثير على الرأي العام المحلي أو الدولي، كما هو الحال في استخدام وسائل التواصل الاجتماعي لنشر الأخبار الزائفة أو التلاعب بالانتخابات (مركز دبي لبحوث السياسات العامة، 2020).

التأثير على الثقة العامة: تؤثر الهجمات السيبرانية سلبًا على الثقة العامة في المؤسسات الحكومية عندما تتعرض هذه المؤسسات لهجمات متكررة (الأشعري وصدقي، 2025)، مما يدفع المواطنين للتساؤل عن قدرتها على حماية المعلومات والبيانات الحساسة (المطيري، 2025). ويُعد نشر المعلومات الزائفة عبر مواقع التواصل الاجتماعي نوعًا من الهجمات السيبرانية المنظمة، ويؤثر بشكل كبير على الأمن القومي والاجتماعي والسياسي. ويتمثل في نشر محتوى مضلل بهدف التلاعب بالرأي العام أو زعزعة الاستقرار الداخلي أو التأثير على العمليات الديمقراطية مثل الانتخابات (منظمة الصحة العالمية، 2024).

وتعد هذه الهجمات أداة فعالة للتأثير بتكلفة منخفضة، حيث تستخدم الجهات الفاعلة الروبوتات الرقمية والحسابات الوهمية لنشر الشائعات وإثارة الانقسامات. كما تمتد آثارها إلى الساحة الدولية لتشويه صور الدول أو التدخل في شؤونها. ومع صعوبة تتبع مصدرها أو احتوائها، ينعكس ذلك سلبًا على الروح المعنوية والثقة في القيادة المحلية، مما قد يؤدي إلى تدهور الوضع الاجتماعي والسياسي (دائرة الصحة بأبو ظبي، 2020، ص7).

وعلى المستوى الاجتماعي، قد تطال الهجمات السيبرانية المؤسسات الصحية والتعليمية والإعلامية، مما يؤدي إلى تعطيل الخدمات الأساسية وزعزعة استقرار المجتمع. فاستهداف المؤسسات الصحية يمكن أن يعرقل تقديم الرعاية الطبية الطارئة، بينما اختراق الأنظمة التعليمية يؤثر على سير العملية التعليمية ويهدد البيانات الشخصية للطلاب (اللجنة الدولية للصليب الأحمر، 2020).

أما على صعيد المؤسسات الإعلامية، فيمكن للهجمات أن تؤدي إلى بث معلومات مضللة أو تعطيل وسائل النشر، مما يسهم في إرباك الرأي العام وإضعاف الثقة في المصادر الإعلامية، الأمر الذي يؤدي إلى إثارة الفوضى وزعزعة ثقة المواطنين في الحكومة وقدرتها على حمايتهم. وبالتالي، أصبحت الحماية السيبرانية جزءًا لا يتجزأ من استراتيجيات الأمن القومي للدول الحديثة (الشرقاوي، 2021، ص49–50).

2.1.2. المطلب الثاني : الأبعاد السياسية للنزاع

تُعد الهجمات السيبرانية واحدة من أدوات الحرب الحديثة، حيث تُستخدم في النزاعات السياسية لأغراض متعددة تشمل التخريب، والتجسس، وزعزعة الاستقرار. وفي سياق جنوب لبنان، يتضح أن هذه الهجمات تُعكس الأبعاد السياسية المعقدة للنزاع، وتُستخدم كوسيلة لتعزيز الأهداف السياسية للفاعلين المحليين والإقليميين.

التخريب والتأثير على المؤسسات الحكومية: تُستخدم الهجمات السيبرانية لتخريب عمل المؤسسات الحكومية، مما يؤدي إلى ضعف الثقة في السلطة القائمة. وعلى سبيل المثال، إذا تعرضت وزارة أو هيئة حكومية لهجوم سيبراني، يمكن أن تتعطل خدماتها الأساسية، مما يؤثر على قدرتها على تنفيذ سياساتها وإدارة الأزمات. ويُستخدم هذا النوع من الهجمات كوسيلة لإظهار ضعف الحكومة وإضعاف قدرتها على السيطرة (المركز الأوروبي لدراسات مكافحة الإرهاب، 2020).

التجسس والاستهداف: تُعتبر الهجمات السيبرانية أداة فعالة للتجسس واستهداف الخصوم (*US Army Training & Doctrine Command*، 2006، *p.VII–2*). وفي الهجوم على لبنان، استخدمت التقنيات السيبرانية لضرب عدد من الأهداف من قيادات المقاومة في سبيل شل التنظيم الإداري والميداني للمقاومة اللبنانية. وبحسب الجانب اللبناني، قامت أجهزة الاستخبارات الصهيونية بتنفيذ عملية معقدة تمثلت في زرع متفجرات داخل حوالي 5000 جهاز اتصال من صنع أوروبي، وذلك قبل أشهر من الهجوم الذي استهدف أجهزة اتصال حزب الله. وأن الانفجارات التي وقعت كانت نتيجة رسالة نصية مشفرة تم إرسالها لتلك الأجهزة. وتُعد هذه المواد المتفجرة شديدة التعقيد ولا يمكن اكتشافها بسهولة باستخدام الأجهزة التقليدية أو الماسحات الضوئية. كما ذُكر أن حزب الله طلب تلك الأجهزة من شركة تايوانية تدعى "*Gold Apollo*"، لكن المسؤولين التنفيذيين في الشركة أكدوا أن تصنيع الأجهزة تم بموجب ترخيص من شركة "*BAC Consulting*" ومقرها بودابست، المجر. وعلّق "إيليا جيه ماجنييه"، محلل المخاطر السياسية المقيم في بروكسل، بعد حديثه مع أعضاء من حزب الله الذين فحصوا بعض الأجهزة التي لم تنفجر. وأشار إلى أن تلك الأجهزة تلقت رسالة مشفرة خاطئة، مما أدى إلى اهتزازها وإصدارها أصوات إنذار لمدة عشر ثوانٍ تقريبًا. ويُظهر هذا الجانب من العملية مدى تعقيد التكنولوجيا المستخدمة وتأثيرها الكبير على الأهداف المحددة (المجلة الدولية للصليب الأحمر، 2020).

وبات استخدام العمليات السيبرانية خلال النزاعات المسلحة سمة بارزة وواقعية ضمن تطورات الحروب الحديثة، ويحظى هذا النوع من العمليات باهتمام أكبر في المستقبل. وقد أعلنت بعض الدول بشكل رسمي

عن تنفيذها عمليات سيبرانية في إطار نزاعات مسلحة قائمة (وكالة أنباء الإمارات، 2020). ومنها الولايات المتحدة والمملكة المتحدة وأستراليا كجزء من جهودها في محاربة تنظيم داعش (*Gill*، 2021، *p.265*).

زعزعة الاستقرار الاجتماعي والسياسي: يمكن أن تؤدي الهجمات السيبرانية إلى زعزعة الاستقرار الاجتماعي والسياسي من خلال خلق حالة من الخوف وعدم اليقين. وعند تعرض المواطنين لهجمات تُعطل حياتهم اليومية، قد تنشأ مشاعر الإحباط والغضب (فاضل، 2020). ويمكن أن يُستغل هذا الإحباط من قبل الجماعات السياسية أو الفاعلين غير الحكوميين لتعزيز موقفهم أو استقطاب الدعم الشعبي (إسماعيل، 2022، ص10).

تصعيد الصراعات الإقليمية: تُستخدم الهجمات السيبرانية أيضًا كوسيلة لتصعيد الصراعات الإقليمية. وفي السياقات التي تشهد توترات بين الدول، دون الحاجة إلى تصعيد النزاع إلى مستويات عسكرية، يمكن أن تُعزز هذه الهجمات من التوترات وتُعقِّد جهود الوساطة والسلام (السعيدي وجفال، 2024).

القدرة على الإنكار: تُتيح الهجمات السيبرانية للدول والجماعات إمكانية الإنكار. فمن الصعب أحيانًا تحديد الجهة المسؤولة عن الهجوم، مما يعزز من القدرة على استخدام الهجمات كجزء من استراتيجيات الصراع السياسي دون مواجهة تبعات مباشرة (الفتلاوي، 2016، ص616).

2.2. المبحث الثاني: الأثر في نطاق القانون الدولي الإنساني واليات المحاسبة

تمثل الهجمات السيبرانية التي استهدفت جنوب لبنان نموذجًا حيًا للتحديات المتزايدة التي تفرضها التكنولوجيا على القوانين الدولية والإنسانية. فبينما يسعى القانون الدولي لتنظيم استخدام القوة وحماية المدنيين في النزاعات المسلحة، تظهر الهجمات السيبرانية كأداة جديدة تتجاوز الأطر التقليدية وتثير تساؤلات حول كيفية تصنيفها وتحديد مسؤولية مرتكبيها.

في هذا المبحث، سيتم التركيز على الآثار القانونية والإنسانية لهذه الهجمات على مستوى انتهاك حقوق الإنسان من خلال دراسة مدى توافقها مع قواعد القانون الدولي الإنساني وميثاق الأمم المتحدة، خاصة فيما يتعلق بحماية المدنيين ومنع الاستهداف العشوائي. كما سيتم تسليط الضوء على آليات المحاسبة القانونية.

2.2.1. المطلب الأول: انتهاك حقوق الإنسان

تُعتبر الهجمات السيبرانية، خاصة تلك التي تستهدف البنية التحتية الحيوية أو المعلومات الشخصية، انتهاكًا لحقوق الإنسان الأساسية، مما يسلط الضوء على الأبعاد القانونية والإنسانية لهذه الظاهرة. وتمتد آثار الهجمات السيبرانية إلى مجموعة من الحقوق، بما في ذلك الحق في الخصوصية، والأمان الشخصي، والوصول إلى المعلومات، والحق في الحياة الكريمة (عبد الصادق، 2017، ص31-32).

تُشكل الهجمات السيبرانية تهديدًا مباشرًا للحق في الخصوصية، حيث تتضمن سرقة المعلومات الشخصية أو الكشف عنها بشكل غير قانوني. وعندما تتعرض بيانات الأفراد للاختراق، يفقد الأفراد السيطرة على معلوماتهم الشخصية، مما يؤدي إلى انتهاك خصوصيتهم. وفي حالات مثل تسريب البيانات الحساسة، قد يتعرض الأفراد لمخاطر مثل الابتزاز أو التمييز (عبد الجواد، 2020، ص394).

تؤدي الهجمات السيبرانية إلى خلق بيئة غير آمنة، حيث يُصبح الأفراد عرضة لمخاطر مختلفة نتيجة عدم الأمان الرقمي. ويمكن أن تؤدي الهجمات على الأنظمة الأمنية إلى تعريض حياة الأفراد للخطر، خاصة في الحالات التي تتعلق بالبنية التحتية الحيوية مثل الرعاية الصحية أو خدمات الطوارئ. وتمثل هذه المخاطر انتهاكًا لحق الأفراد في الأمن الشخصي والسلامة (عرفان، 2024، ص3003).

وتُستخدم الهجمات السيبرانية أحيانًا لتقويض الحق في الوصول إلى المعلومات. وعندما تتعرض مواقع الأخبار أو المنصات الإلكترونية لهجمات، قد تُحرم المجتمعات من المعلومات الضرورية حول الأحداث السياسية أو الاجتماعية. ويُعد هذا الانتهاك خطيرًا، حيث يؤثر على قدرة الأفراد على اتخاذ قرارات مستنيرة ويعزز من الرقابة والتضليل (جبور، 2012، ص9).

كذلك تؤدي الهجمات السيبرانية أيضًا إلى تقييد حرية التعبير. ويمكن أن تُستخدم الهجمات كوسيلة لإسكات الأصوات المعارضة أو تهديد النشطاء الحقوقيين، مما يعزز من ثقافة الخوف ويعيق الحوار المفتوح. وعندما يشعر الأفراد بأنهم مهددون بسبب آرائهم، قد يتراجع البعض عن التعبير عن أفكارهم أو المشاركة في النقاشات العامة (حكومة الإمارات، 2020).

2.2.2. *المطلب الثاني: آليات المحاسبة القانونية*

تُعتبر محاسبة مرتكبي الهجمات السيبرانية أمرًا حيويًا للحفاظ على الأمن السيبراني وضمان حماية حقوق الأفراد. وتتضمن الإجراءات القانونية التي يمكن اتخاذها لمحاسبة الجناة عدة جوانب، تشمل التحقيقات، والتشريعات، والتعاون الدولي.

على المستوى الدولي، أكدت الجمعية العامة للأمم المتحدة اهتمامها في العمل على الحد من انتشار الجرائم السيبرانية، من خلال المؤتمرات التي تعقدها وتشرف عليها، كذلك بإصدار القرارات والتوصيات في هذا الشأن (عسكر، 2021، ص268).

تُعد التشريعات الوطنية الأداة الأولى لمحاسبة مرتكبي الجرائم السيبرانية. ويجب أن تتضمن هذه التشريعات تعريفًا للجرائم السيبرانية، إذ يجب تحديد الجرائم السيبرانية بشكل واضح في القوانين المحلية، مثل الاختراق، وسرقة البيانات، ونشر البرمجيات الخبيثة، والجرائم المتعلقة بالمحتوى. كما يجب أن تتضمن

القوانين عقوبات صارمة تتناسب مع خطورة الجرائم، مما يضمن ردع المحتملين عن ارتكابها. ويجب أن تتضمن القوانين آليات واضحة لإجراء الملاحقات القضائية، بما في ذلك جمع الأدلة والتحقيقات (الاكيابي، 2023، ص1290-1294).

في الإمارات العربية المتحدة تحديدًا، بدأ تطبيق قانون مكافحة الشائعات والجرائم الإلكترونية بموجب المرسوم بقانون اتحادي رقم 34 لسنة 2021 اعتباراً من 2 كانون الثاني 2022. ويهدف هذا القانون إلى وضع إطار قانوني متكامل لتعزيز حماية المجتمع من الجرائم الإلكترونية التي تُرتكب عبر شبكة الإنترنت والتقنيات الرقمية. كما يسعى إلى حماية المواقع الإلكترونية وقواعد البيانات الحكومية في الدولة، والتصدي لانتشار الشائعات والأخبار المضللة، ومكافحة الاحتيال الإلكتروني، إلى جانب الحفاظ على الخصوصية وحماية الحقوق الشخصية (بلقاسم ومحمد، 2017، ص194).

كما تتطلب محاسبة مرتكبي الهجمات السيبرانية إجراء تحقيقات جنائية دقيقة. وتشمل هذه الإجراءات جمع الأدلة الرقمية، إذ يجب على الأجهزة الأمنية استخدام تقنيات متقدمة لجمع الأدلة من الأنظمة المصابة، مثل سجلات الدخول والبيانات المسروقة. كما يمكن أن يتطلب التحقيق الاستعانة بخبراء في الأمن السيبراني لتحديد كيفية وقوع الهجوم وتحليل الأدلة. ومن الضروري استخدام تقنيات التتبع الإلكتروني لتحديد هوية الجناة، سواء كانوا أفرادًا أو جماعات (عرفان، 2024، ص3000).

نظرًا للطبيعة العالمية للهجمات السيبرانية، فإن التعاون الدولي يُعتبر ضروريًا لمحاسبة الجناة. وتشمل آليات التعاون إنشاء اتفاقيات دولية مثل اتفاقية بودابست التي تُعزز من التعاون بين الدول لمكافحة الجرائم السيبرانية وتبادل المعلومات. ويمكن للدول تشكيل فرق عمل مشتركة للتحقيق في الهجمات التي تعبر الحدود، مما يُعزز من فعالية الردود. مما يقتضي أن تقوم الدول بتبادل المعلومات حول الهجمات السيبرانية، بما في ذلك بيانات الجناة وأساليب الهجوم (عسكر، 2021، ص268).

تُعتبر آليات تعويض الضحايا جزءًا مهمًا من المحاسبة القانونية. ويجب أن تشمل الإجراءات تقديم المطالبات، فيجب أن تكون هناك آليات واضحة للضحايا لتقديم المطالبات للحصول على تعويض عن الأضرار التي لحقت بهم. ومن الضروري تقديم الدعم النفسي والقانوني للضحايا لمساعدتهم على التعافي من آثار الهجمات (الاكيابي، 2023، ص1290-1294).

تتطلب محاسبة مرتكبي الهجمات السيبرانية إجراءات قانونية شاملة وتعاونًا دوليًا فعالًا. ويجب أن تتضمن الاستراتيجيات الوطنية تطوير التشريعات اللازمة، وتعزيز التحقيقات، وضمان العدالة للضحايا.

ومن خلال تنفيذ هذه الإجراءات، يمكن تحسين الأمان السيبراني وحماية حقوق الأفراد والمجتمعات من التهديدات المتزايدة (بلقاسم ومحمد، 2017، ص194).

الخاتمــة

تُعد الهجمات السيبرانية ظاهرة متزايدة ومعقدة تتجاوز حدود الجرائم التقليدية لتُشكل تهديدًا استراتيجيًا للأمن القومي والسيادة الوطنية، كما تؤثر بشكل عميق على الأبعاد السياسية والإنسانية في مختلف البلدان، بما في ذلك جنوب لبنان، حيث أصبحت ساحة حقيقية للصراعات الحديثة التي تتخذ الفضاء الرقمي ميدانًا لها.

وقد بيّن هذا البحث أن هذه الهجمات ليست مجرد اختراقات تقنية، بل أدوات سياسية وأمنية تُستخدم لتحقيق أهداف استخبارية، عسكرية، أو حتى اقتصادية، وقد ترقى بعضها إلى جرائم دولية إذا استهدفت المدنيين أو المنشآت الحيوية. وتكشف الآثار الأمنية لهذه الهجمات عن خطر حقيقي يهدد البنية التحتية الرقمية والاستقرار المجتمعي، بينما تبرز أبعادها السياسية كوسيلة فاعلة في تنفيذ الحملات التخريبية أو التأثير على القرار الوطني، خاصةً في حالات النزاعات الإقليمية.

أما من الناحية الإنسانية، فقد سلط البحث الضوء على الانتهاكات الجسيمة التي تطال حقوق الإنسان نتيجة هذه الهجمات، بدءًا من خرق الخصوصية، وصولًا إلى سرقة الهوية، والتجسس الإلكتروني، والابتزاز الرقمي، ما يؤدي إلى زعزعة الشعور بالأمن الشخصي وتقويض الثقة في المؤسسات العامة. ولا يمكن تجاهل التداعيات النفسية والاجتماعية العميقة التي قد تُفاقم من حالة القلق المجتمعي، وتُضعف تماسك النسيج الاجتماعي، خصوصًا في المناطق المتأثرة بالنزاعات.

وقد أكدت نتائج البحث على الحاجة الملحة إلى استجابة شاملة وفعالة من قبل الحكومات والمجتمع الدولي، تعتمد على تعزيز الأطر القانونية الوطنية والدولية لضمان مساءلة مرتكبي هذه الجرائم، وتوفير الحماية اللازمة للمدنيين. ومن هنا تظهر أهمية تطوير آليات المحاسبة الجنائية التي تشمل إجراء تحقيقات دقيقة، وضع تشريعات وطنية رادعة، وتعزيز التعاون الدولي في مجال الأمن السيبراني. كما يجب العمل على تقديم الدعم والتعويضات للضحايا، باعتبارهم محور الانتهاك، وذلك بهدف استعادة ثقتهم في الدولة وفي النظام القانوني الدولي.

وفي هذا السياق، لا يُمكن للحكومات وحدها تحمل عبء مواجهة هذا النوع من التهديدات، بل يتطلب الأمر مشاركة مجتمعية شاملة تشمل مؤسسات التعليم، وشركات التكنولوجيا، والمجتمع المدني، والمراكز

البحثية. فبناء ثقافة وطنية في مجال الأمن السيبراني، وتوعية الجمهور بالمخاطر، وتدريب الكوادر المتخصصة، يُعد خطوة أساسية في مواجهة التحديات المستقبلية.

ومن المتوقع أن تستمر هذه الظاهرة في النمو والتطور مع التقدم التكنولوجي، مما يستدعي من المجتمع الدولي الاستجابة بسرعة وفعالية، عبر تبني سياسات استباقية وتشريعات مرنة تواكب طبيعة التهديدات السيبرانية الجديدة. كما تحتاج الأبحاث المستقبلية إلى التركيز على تطوير استراتيجيات دفاعية وهجومية، وتعزيز التعاون بين الدول في مجال تبادل المعلومات ومواجهة التهديدات المشتركة.

من خلال التحليل المعمق في البحث، تم الوصول إلى عدة نقاط رئيسية:

أولاً: النتائج

أظهرت نتائج هذا البحث أن الهجمات السيبرانية لم تعد مجرد تهديد تقني محدود التأثير، بل تحولت إلى وسيلة استراتيجية في الصراعات الحديثة، خاصة في مناطق النزاع مثل جنوب لبنان. وقد تم التأكيد على أن هذه الهجمات تستهدف البنية التحتية الحيوية والمنشآت المدنية، وتُعد انتهاكًا محتملاً للقانون الدولي الإنساني إذا أدت إلى إلحاق الضرر العشوائي بالمدنيين أو تعطيل الخدمات الأساسية.

وقد تبين أن الإطار القانوني الدولي لا يزال يفتقر إلى النصوص الواضحة التي تنظم استخدام الفضاء السيبراني في النزاعات المسلحة، مما يولّد فجوة تشريعية تُعيق مساءلة مرتكبي هذه الجرائم. ومع ذلك، هناك توجه فقهي ودولي متزايد نحو توسيع تفسير مواد القانون الدولي الإنساني لتشمل العمليات السيبرانية التي تشبه من حيث التأثير والنية الأعمال الحربية التقليدية.

كما أظهرت الدراسة أن الكيان الصهيوني يُعد من الأطراف المشتبه بضلوعها في تنفيذ هجمات سيبرانية متكررة ضد جنوب لبنان، وهو ما يستدعي اهتمام الجهات الدولية المعنية، خصوصًا المحكمة الجنائية الدولية، لتحديد مدى توفر الشروط القانونية التي ترقّي هذه الأعمال إلى جرائم دولية.

وأخيرًا، بيّن البحث أن التعاون الإقليمي والدولي يُعد عنصرًا حاسمًا في مواجهة التهديد السيبراني المتزايد، وأن بناء القدرات الوطنية في مجال الأمن السيبراني يُساهم بشكل مباشر في حماية المدنيين وتعزيز سيادة الدولة.

ثانيًا: التوصيات

1. تقوية الإطار التشريعي الوطني:

دعوة السلطات اللبنانية إلى سن قوانين وطنية شاملة تجرّم الهجمات السيبرانية على المدنيين والبنية التحتية الحيوية، وتُحدد آليات للمحاسبة المحلية.

2. تعزيز التعاون الدولي:

تشجيع لبنان على الانضمام إلى الاتفاقيات الدولية المتعلقة بالأمن السيبراني، مثل اتفاقية بودابست للجريمة الإلكترونية، والعمل على تطوير شراكات إقليمية لتبادل المعلومات والاستخبارات الرقمية.

3. توسيع اختصاص المحكمة الجنائية الدولية:

دعوة المحكمة الجنائية الدولية إلى النظر في إدراج بعض أنواع الهجمات السيبرانية ضمن اختصاصها، خاصةً تلك التي تُرتكب في سياق النزاع المسلح وتستهدف المدنيين.

4. بناء القدرات الوطنية في الأمن السيبراني:

الاستثمار في تدريب الكوادر المتخصصة، وإنشاء وحدات سيبرانية متخصصة داخل المؤسسات الحكومية والأمنية لمواجهة التهديدات الرقمية.

5. رفع مستوى الوعي المجتمعي:

إطلاق حملات توعية للجمهور حول المخاطر السيبرانية وكيفية الوقاية منها، خاصةً فيما يتعلق بالتصيد الإلكتروني والهجمات المالية.

6. دعم الضحايا ومساءلة المعتدين:

وضع آليات لتقديم الدعم النفسي والمالي للضحايا المتضررين من الهجمات السيبرانية، وضمان تقديم التعويضات المناسبة لهم.

7. تشجيع البحث العلمي والدراسات المستقبلية:

دعم الأبحاث الأكاديمية المتخصصة في مجال القانون السيبراني والجرائم الإلكترونية، بهدف صياغة استراتيجيات وطنية ودولية أكثر فعالية في مواجهة هذا النوع من التهديدات.

المصادر

القرآن الكريم

[1] الرشيدي، هالة أحمد. (2021). الإرهاب السيبراني: ماهيته وجهود مكافحته في ضوء التشريعات والقوانين الوطنية والدولية. القاهرة: دار النهضة العربية.

[2] الزهراني، أحمد. (2021). الجرائم الإلكترونية: أنواعها وسبل مواجهتها (ط1). دار الفكر للنشر.

[3] نعمة، علي زعلان، وعبد علي، حيدر كاظم، وجعفر، محمود خليل. (2023). القانون الدولي الإنساني. دار المسلة.

[4] التميمي، مريم نبيل عادي. (2022). مشاركة الأطفال في الأعمال العدائية وفق القانون الدولي (رسالة ماجستير غير منشورة). كلية الحقوق، الجامعة الإسلامية في لبنان، لبنان.

[5] الشرقاوي، محمود حسين. (2021). الهجمات الإلكترونية في ضوء أحكام القانون الدولي الإنساني (رسالة دكتوراه غير منشورة). كلية الحقوق، جامعة بني سويف، مصر.

[6] يوسف، صغير. (2013). الجرائم المرتكبة عبر الإنترنت (رسالة ماجستير غير منشورة). كلية الحقوق، جامعة مولود معمري، الجزائر.

[7] رمضان، إبراهيم السيد أحمد. (2025). مواجهة الهجمات السيبرانية في ضوء أحكام القانون الدولي. مجلة العلوم القانونية والاقتصادية، السنة السابعة والستون، العدد الأول.

[8] الفتلاوي، أحمد عبيس نعمة. (2016). الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر. مجلة المحقق الحلي للعلوم القانونية والسياسية، كلية القانون، جامعة بابل، العدد 4، السنة الثامنة.

[9] إسماعيل، إسراء أحمد. (2022). الحروب السيبرانية: تهديد لأمن الدول بدون اشتباكات عسكرية. مجلة السياسة الدولية، المجلد 57(228).

[10] عبد الجواد، أميرة عبد العظيم محمد. (2020). المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام. مجلة البحوث الفقهية والقانونية، الجزء الثالث، العدد الخامس والثلاثون.

[11] صبحي، أنس أكرم محمد. (2020). الأمن الإنساني وأثره في الأمن الوطني العراقي. مجلة المعهد، العدد 2.

[12] بلقاسم، بن صابر، ومحمد حيدرة. (2017). الهجمات السيبرانية ومواجهتها في ضوء القانون الدولي المعاصر. مجلة حقوق الإنسان والحريات العامة، العدد الرابع.

[13] فياض، حسن. (2020). الهجمات السيبرانية من منظور القانون الدولي الإنساني. مجلة الدفاع الوطني، العدد 114.

[14] المطيري، خالد ظاهر السهيل. (2020). مواجهة الجرائم المعلوماتية في ضوء التشريعات الجنائية المعاصرة والاتفاقيات الدولية. بحث منشور.

[15] الأكيابي، سلوى يوسف. (2023). مدى انطباق القانون الدولي الإنساني على الهجمات السيبرانية.

مجلة روح القوانين، المجلد 35(101).

[16] العيسي، طلال ياسين، وعناب، عدي محمد. (2019). المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر. مجلة الزرقاء للبحوث والدراسات الإنسانية، المجلد 19(1).

[17] عبد الصادق، عادل. (2017). أنماط الحرب السيبرانية وتداعياتها على الأمن العالمي. مجلة السياسة الدولية، العدد 208.

[18] السعيدي، عمر أحمد، وجفال، زياد محمد. (2024). مدى اعتبار الهجمات السيبرانية انتهاكًا للحظر المفروض على استخدام القوة أو التهديد بها في ضوء أحكام القانون الدولي للجوء إلى الحرب. مجلة جامعة الإمارات للبحوث القانونية، العدد 99، السنة 39.

[19] كريم، فريحة محمد. (2018). الأخبار المزيفة على وسائل التواصل الاجتماعي: بين التلاعب والانتهاكات. المجلة العربية للمعلوماتية وأمن المعلومات.

[20] عسكر، محمد عادل محمد. (2021). وضع العمليات السيبرانية في القانون الدولي مع التطبيق على ممارسة التجسس وقت السلم: دراسة على ضوء دليل تالين. مجلة البحوث القانونية والاقتصادية، المجلد 33(1).

[21] (2024). مدى اعتبار الهجمات السيبرانية انتهاكًا للحظر المفروض على استخدام القوة أو التهديد بها في ضوء أحكام القانون الدولي للجوء إلى الحرب. مجلة جامعة الإمارات للبحوث القانونية، المجلد 9(99).

[22] جبور، منى الأشقر. (2012). الأمن السيبراني: التحديات ومستلزمات المواجهة. أعمال اللقاء السنوي الأول للمختصين في أمن وسلامة الفضاء السيبراني، المركز العربي للبحوث القانونية والقضائية.

[23] القاضي، هيثم محمد بهاء، لبيب، محمد أحمد، وكمال، مصطفى أحمد. (2024). دور الاتفاقيات الدولية والإقليمية في مجال الأمن السيبراني. مجلة الحوكمة والوقاية من الفساد ومكافحته، العدد الأول.

[24] مصطفى، وسام محمود عرفان. (2024). سبل مكافحة الهجمات السيبرانية دوليًا. مجلة الدراسات القانونية والاقتصادية، المجلد 10(3).

[25] دائرة الصحة الإماراتية. (دون تاريخ). استراتيجيات أمن المعلومات والأمن السيبراني للقطاع الصحي

في أبو ظبي. أبو ظبي، الإمارات العربية المتحدة.

[26] وحدة التفتيش المشتركة للأمم المتحدة. (2021). الأمن السيبراني في مؤسسات منظومة الأمم المتحدة (التقرير رقم *JIU/REP/2021/3*). الأمم المتحدة.

[27] كاستيليك، أندراز. (2021). التعاون الدولي للتخفيف من العمليات الإلكترونية التي تمس البنية التحتية. معهد الأمم المتحدة لبحوث نزع الأسلحة.

[28] عزالدين، جاسم محمد. (دون تاريخ). الطبيعة القانونية للحروب والنزاعات السيبرانية من منظور القانون الدولي. المؤتمر الدولي الثامن للقضايا القانونية (*IICL8*).

[29] ديفيس الثاني، جون إس، بودرو، بنجامين، ويلبورن، جوناثان ويليام، أغيري، جاير، أوغليتري، كورداي، ماكغوفرن، جوفري، وتشايس، مايكل إس. (2107). نحو مساءلة دولية في الفضاء الإلكتروني. مؤسسة مايكروسوفت ومكتبة الكونغرس.

[30] منيب، عبد المنعم. (2022). ما بعد الإنسانية. تقرير سنوي، شركة آفاق المعرفة.

[31] الأمم المتحدة. مجلس الأمن. (2023). وقائع الجلسة رقم 9497 (السنة الثامنة والسبعون، 7 ديسمبر 2023). نيويورك: الأمم المتحدة.

[32] الجامعة العربية. (دون تاريخ). الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

[33] مجلس أوروبا. (2001). اتفاقية بودابست بشأن الجريمة الإلكترونية (الاتفاقية رقم 185).

[34] اللجنة الدولية للصليب الأحمر. (1949). اتفاقيات جنيف لعام 1949.

[35] اللجنة الدولية للصليب الأحمر. (1977). البروتوكول الإضافي الأول لاتفاقيات جنيف لعام 1977.

[36] أخبار الأمم المتحدة. (2024). منظمة الصحة العالمية: الهجمات الإلكترونية يمكن أن تكون مسألة حياة أو موت. https://news.un.org/ar/story/2024/11/1136451

[37] البوابة الرسمية لحكومة دولة الإمارات العربية المتحدة. (دون تاريخ). السلامة السيبرانية والأمن الرقمي. https://u.ae/information-and-services/justice-safety-and-the-law/

[38] الجبهة الديمقراطية لتحرير فلسطين. (دون تاريخ). التوصيف القانوني لتفجير أجهزة الاتصالات في لبنان. https://dflp.org/5296/

[39] ليبتون، ديفيد. (2020). تهديدات الأمن الإلكتروني تدعو إلى تحرك عالمي. مدونة صندوق النقد الدولي. https://www.imf.org/ar/Blogs/Articles/2020/01/13/blog-cybersecurity-threats-call-for-a-global-response

[40] شركة ميكروسوفت. (دون تاريخ). تعريف الهجمات الموزعة لحجب الخدمة DDoS. https://www.microsoft.com/ar/security/business/security-101/what-is-a-ddos-attack

[41] قاموس المفردات. (دون تاريخ). علم التحكم الآلي. https://www.vocabulary.com/dictionary/cybernetics

[42] قاموس ميريام ويبستر. (دون تاريخ). Cyber. https://www.merriam-webster.com/dictionary/cyber

[43] اللجنة الدولية للصليب الأحمر. (دون تاريخ). العمليات السيبرانية أثناء النزاعات المسلحة. https://www.icrc.org/ar/law-and-policy/cyber-and-information-operations

[44] الأشعري، سعيد، وصدقي، عبد العزيز. (دون تاريخ). الأخبار الزائفة في وسائل التواصل الاجتماعي: تأصيل في المفهوم وبحث عن الدوافع والأسباب. مجلة البحث في العلوم الإنسانية والمعرفية. https://crshc.com/3392/

[45] المجلة الدولية للصليب الأحمر. (دون تاريخ). بعد عشرين عامًا: آثار العمليات السيبرانية أثناء النزاعات المسلحة. https://international-review.icrc.org/ar/articles/twenty-years-international-humanitarian-law-and-protection-civilians-against-effects-cyber

[46] المركز الأوروبي لدراسات مكافحة الإرهاب والاستخبارات. (دون تاريخ). تحول قواعد الاشتباك ما بين حزب الله وإسرائيل إلى الحرب الهجينة. https://www.europarabct.com

[47] المركز العربي الديمقراطي. (دون تاريخ). التهديدات السيبرانية والعلاقات الأمريكية الروسية. https://democraticac.de/?p=99583

[48] مركز دبي لبحوث السياسات العامة. (دون تاريخ). اضطراب الأمن السيبراني، سلاسل التوريد، والاقتصاد العالمي. https://bhuth.ae/ar/publication/cybersecurity-disruption-supply-chains-and-the-global-economy

[49] مكتب التحقيق الفيدرالي الأمريكي. (دون تاريخ). Cybersecurity. https://www.fbi.gov/investigate/cyber

[50] منصة ASJP للنشر الإلكتروني للمجلات العلمية الجزائرية. (دون تاريخ). https://asjp.cerist.dz/

[51] كاسبرسكي. (دون تاريخ). الأمن السيبراني. https://me.kaspersky.com/

[52] وكالة الأمن القومي الأمريكية. (دون تاريخ). مركز تعاون الأمن السيبراني.

https://www.nsa.gov/

[53] هيئة الإذاعة البريطانية. (دون تاريخ). بول آدمز، هجوم روسي "ضخم" يتسبب في انقطاع التيار الكهربائي بأوكرانيا. https://www.bbc.com/arabic/articles/c20636npp3eo

[54] هيئة الإذاعة البريطانية. (دون تاريخ). What we know about the Hezbollah pager explosions. https://www.bbc.co.uk/news/articles

[55] هيئة الإذاعة البريطانية. (دون تاريخ). Two children among 12 killed by exploding pagers. https://www.bbc.com/news/live/cwyl9048gx8t?page=4

[56] شبكة سي إن إن الإخبارية. (دون تاريخ). Hezbollah vows retaliation against Israel for deadly pager explosions across Lebanon. https://edition.cnn.com/world/live-news/lebanon-pagers-explode-hezbollah-israel-09-18-24-intl-hnk/index.html

[57] شبكة سي إن إن الإخبارية. (دون تاريخ). Hezbollah vows retaliation against Israel for deadly pager explosions. https://www.cnn.com/world/live-news/lebanon-pagers-attack-hezbollah/index.html

[58] فرونت لاين. (دون تاريخ). Distributed Denial-of-Service (DDoS). https://www.fortinet.com/resources/cyberglossary/ddos-attack

[59] فرونت لاين. (دون تاريخ). Cyber Attack on Hezbollah: Pagers Explode. https://frontline.thehindu.com/news/lebanon-hezbollah-cyber-attack-pager-explosions-warfare-israel-gaza/article68654302.ece

[60] وكالة أنباء الإمارات. (دون تاريخ). مجلس "الأمن السيبراني" يتصدى لهجمات سيبرانية يومية تصدر عن جماعات إرهابية من 14 دولة. https://www.wam.ae/ar/article/bhs9ovr

[61] صحيفة البيان. (دون تاريخ). حسين المهيري، الأمن السيبراني وحماية البيانات. https://www.albayan.ae/opinions/articles/10724

[62] وكالة الأنباء الإماراتية. (دون تاريخ). الأمن السيبراني يتصدى لهجمات سيبرانية يومية تصدر عن جماعات إرهابية من 14 دولة. https://www.wam.ae/ar/article/bhs9ovr

[63] اليوم الثامن. (دون تاريخ). حنين فاضل، تفجير أجهزة البيجر: محاولة صهيونية لإخضاع حزب الله أم خطوة استراتيجية؟ https://www.alyoum8.net/posts/94726

[64] شبكة ليزر. (2025). محمد المطيري، تأثير الهجمات السيبرانية على الثقة العامة. https://lezrweb.com/2025/02/09

[65] NSFocus) .n.d (.Cyber Attacks Behind the Lebanon Explosions. https://nsfocusglobal.com/the-supply-chain-conspiracy-cyber-attacks-

behind-the-lebanon-explosions/
[66] Irish Information Security Forum) .n.d (.World's first weaponized cyber-attacks? https://www.iisf.ie/weaponised-pager-cyber-attack
[67] Dawkins, Jerald. (2022). The origin of cyber. CISO Global. https://www.osce.org/cyber-ict-security
[68] Gisel, Laurent & Olejnik, Lukasz (Eds.). (2019). ICRC expert meeting: The potential human cost of cyber operations. International Committee of the Red Cross. https://www.icrc.org/en/download/file/96008/the-potential-human-cost-of-cyber-operations.pdf
[69] Burgess, Mike. (2019). Offensive cyber and the people who do it. Australian Signals Directorate. https://www.asd.gov.au/news-events-speeches/speeches/director-general-asd-speech-lowy-institute
[70] Council of Europe) .n.d (.Convention on Cybercrime (Budapest Convention, ETS No. 185). https://www.coe.int/en/web/cybercrime/the-budapest-convention
[71] Interpol. (2023). Cybercrime threat landscape. International Criminal Police Organization. https://www.interpol.int/Cybercrime
[72] Interpol. (2023). Cybercrime threat landscape. International Criminal Police Organization. https://www.interpol.int/Cybercrime
[73] Gill, Amandeep Singh. (2021). The changing role of multilateral forums in regulating armed conflict in the digital age. Cambridge University Press on behalf of the International Committee of the Red Cross.
[74] Akhgar, Babak, Staniforth, Andrew, Goudarzi, Arman, Ghayoor, Farzad, Waseem, Muhammad, Fahad, Shah, & Traore, Issa. (2022). A survey on Internet of Things-enabled smart grids: Emerging applications, challenges, and outlook. Energies.
[75] Mazanec, Brian M. (2015). Cyber warfare: Information warfare in a digital age (1st ed.). Praeger.
[76] Pfleeger, Charles P., & Pfleeger, Shari Lawrence. (2015). Introduction to cyber security (3rd ed.). Prentice Hall.
[77] Cisco Networking Academy. (2020). Cybersecurity essentials (2nd ed.). Cisco Press.
[78] Syngress. (2014). Cyber crime and cyber terrorism investigator's handbook (1st ed.). Syngress Publishing.
[79] Cybercrime Convention Committee. (2020). The Budapest Convention on Cybercrime: Benefits and impact in practice.
[80] McCaffrey, John. (2020). Malware: A beginner's guide (1st ed.). O'Reilly Media.

[81] Erickson, Jon. (2008). The art of exploitation (2nd ed.). No Starch Press.
[82] Snider, Keren L. G., et al. (2021). Journal of Cybersecurity, 7.*(1)*
[83] Reindl, N. J. E. H. B. (2019). Digital privacy: Theory, technologies, and practices. Springer.
[84] Wang, S. J. (2021). Phishing and countermeasures: Understanding the risks (1st ed.). Springer.
[85] Shankar, S. Z. (2017). Denial of service attacks in a nutshell (2nd ed.). O'Reilly Media.
[86] Lewis, Ted G. (2006). Critical infrastructure protection in homeland security. Wiley.
[87] United States Army Training and Doctrine Command. (2006). DCSINT handbook No. 1.02: Critical infrastructure threats and terrorism: Cyber operations and cyber terrorism handbook.
[88] Stallings, William. (2019). Network security essentials: Applications and standards (6th ed.). Pearson.