ISSN: 2519 – 6138 (Print)
E-ISSN: 2663 – 8983(On Line)

TUJR
مجلة جامعة تكريت للحقوق
Tikrit University Journal for Rights

IRAQI Academic Scientific Journals
العراقية المجلات الاكاديمية العلمية

Tikrit University Journal for Rights
Journal Homepage : http://tujr.tu.edu.iq/index.php/t

كلية القانون
College of Law

# The Israeli cyber war against Hezbollah and Lebanon and its impact on national security under international law

**Assistant Professor Dr. Abdul samad Raheem Kareem Zangana**

**Department of Law, Al-Aqlam University College, Kirkuk, Iraq**

tujr@tu.edu.iq

**Article info.**

**Article history:**
- Received 10 June 2024
- Accepted 3 August 2024
-Available online 1 March 2025

**Keywords:**

- Israeli cyber war

**Abstract** : Cyber warfare has become an essential part of modern conflicts between states, with some parties relying on cyberattacks to disrupt the critical infrastructure of their adversaries. In this context, Israeli cyberattacks against Hezbollah and Lebanon play a significant role in fueling the conflict between the two sides, raising questions about the legality of these attacks under international law and their impact on Lebanese national security.

With the rapid advancement of technology and the increasing reliance on cyberspace, cyberattacks have come to pose a direct threat to global security.

International law is still adapting to accommodate this type of conflict, presenting a complex challenge to public international law. Although international humanitarian law provides a general framework for armed conflicts, it remains insufficient to address all aspects of cyber warfare. Thus, there is a need for greater international cooperation to establish new legal rules or amend existing ones in line with modern cyber threats, which would help prevent the misuse of cyberspace, maintain stability and peace, enhance global security, and protect national sovereignty.

This research aims to shed light on Israeli cyberattacks against

Hezbollah and Lebanon, analyze the impact of these attacks on Lebanese national security, and examine their compatibility with international legal rules governing the use of force in armed conflicts.



# الحرب السيبرانية الإسرائيلية ضد حزب الله ولبنان وتأثيرها على الأمن الوطني في ظل القانون الدولي

**أ.م. د. عبدالصمد رحيم كريم زنگنه**

**قسم القانون, كلية القلم الجامعة ، كركوك، العراق**

**tujr@tu.edu.iq**

**معلومات البحث :**

**تواريخ البحث:**
- الاستلام : ١٠/ حزيران /٢٠٢٤
- القبول : ٣ /آب/ ٢٠٢٤
- النشر المباشر :١/ أذار/٢٠٢٥

**الكلمات المفتاحية :**

**.الحرب السيبرانية الإسرائيلية**

**الخلاصة:** تعد الحرب السيبرانية جزءًا لا يتجزأ من الصراعات الحديثة بين الدول، حيث تعتمد بعض الأطراف على الهجمات الإلكترونية لتعطيل البنى التحتية الحيوية للخصم. في هذا السياق، تلعب الحرب السيبرانية الإسرائيلية ضد حزب الله ولبنان دورًا رئيسيًا في تصعيد النزاع بين الطرفين، مما يطرح تساؤلات حول مشروعية هذه الهجمات بموجب القانون الدولي وتداعياتها على الأمن الوطني اللبناني.

ومع التطور المتسارع للتكنولوجيا والتوسع في استخدام الفضاء السيبراني، أصبحت الهجمات السيبرانية تشكل تهديدًا مباشرًا للأمن الدولي.

أن القانون الدولي لا يزال في طور التطور لاستيعاب هذه النوعية من النزاعات وتعد تحديًا معقدًا للقانون الدولي العام، على الرغم من أن القانون الدولي الإنساني يوفر إطارًا عامًا للنزاعات المسلحة.

إلا أنه لا يزال غير كافٍ لمعالجة جميع القضايا المتعلقة بالحرب السيبرانية ويتطلب الأمر مزيدًا من التعاون الدولي لوضع قواعد قانونية جديدة أو تعديل القواعد القائمة بما يتناسب مع التهديدات السيبرانية الحديثة من شأنه أن يساهم في منع إساءة استخدام الفضاء السيبراني والحفاظ على الاستقرار والسلام ويعزز الأمن العالمي ويحمي السيادة الوطنية.

ويهدف البحث إلى تسليط الضوء على الهجمات السيبرانية الإسرائيلية ضد حزب الله

ولبنان، وفحص تأثير هذه الهجمات على الأمن القومي اللبناني، ودراسة مدى توافقها مع قواعد القانون الدولي التي تنظم استخدام القوة في النزاعات المسلحة.



المقدمة : تعد الهجمات السيبرانية من أبرز التحديات الأمنية التي تواجه الدول والمنظمات في العصر الرقمي، حيث أصبحت الحرب السيبرانية جزءًا لا يتجزأ من الصراعات الحديثة. في السنوات الأخيرة، شهدت الساحة اللبنانية، وخصوصًا حزب الله، استهدافًا متزايدًا من الهجمات السيبرانية الإسرائيلية.

تهدف هذه الهجمات إلى التأثير على البنية التحتية الرقمية، جمع المعلومات الاستخبارية، وتعطيل القدرات التقنية لحزب الله ولبنان بشكل عام.

يتناول هذا البحث طبيعة الهجمات السيبرانية الإسرائيلية الموجهة ضد حزب الله ولبنان، وأهداف هذه الهجمات وأثرها على الأمن القومي اللبناني. كما يستعرض البحث الطرق التي يمكن من خلالها التصدي لهذه التهديدات، ودور التكنولوجيا المتقدمة في تعزيز الأمن السيبراني في لبنان.

أصبحت الحرب السيبرانية ظاهرة متزايدة في العلاقات الدولية، حيث تسعى الدول إلى تحقيق أهدافها الاستراتيجية من خلال استهداف الأنظمة الرقمية لخصومها.

في هذا السياق، تعرض لبنان، وخاصة حزب الله، لسلسلة من الهجمات السيبرانية الإسرائيلية التي تهدف إلى التأثير على البنية التحتية الحيوية وجمع المعلومات الاستخبارية. تتجاوز هذه الهجمات الصراع التقليدي، لتطرح تحديات قانونية تتعلق بمدى توافقها مع قواعد القانون الدولي العام والقانون الدولي الإنساني.

يركز هذا البحث على تحليل الهجمات السيبرانية الإسرائيلية على حزب الله ولبنان من منظور قانوني، بهدف تقييم مدى شرعيتها وفقًا لأحكام القانون الدولي العام والإنساني.

سيتناول البحث المبادئ التي تحكم استخدام القوة في الفضاء السيبراني، وأثر هذه الهجمات على السكان المدنيين والبنية التحتية الحيوية، إلى جانب تقييم مسؤولية إسرائيل عن هذه الأعمال بموجب القوانين الدولية.

**أهمية البحث:**

تنبع أهمية هذا البحث من كونه يسلط الضوء على أحد أكثر المواضيع الحديثة تعقيدًا في العلاقات الدولية والقانون الدولي، وهو الهجمات السيبرانية وآثارها القانونية.

فمع تصاعد الحرب السيبرانية بين الدول والجهات الفاعلة غير الحكومية، مثل حزب الله، يصبح من الضروري فهم كيفية تأطير هذه الهجمات في ضوء القانون الدولي العام والقانون الدولي الإنساني.

تكمن أهمية البحث في النقاط التالية: –

١. فهم الأبعاد القانونية: يساهم البحث في توضيح مدى شرعية الهجمات السيبرانية الإسرائيلية ضد لبنان وحزب الله وفقًا للقوانين الدولية.

٢. معالجة الفراغ القانوني: يلقي البحث الضوء على التحديات القانونية الناشئة عن عدم وجود إطار قانوني واضح يحكم الحرب السيبرانية، مما قد يساعد على تطوير قوانين دولية جديدة.

٣. تعزيز الأمن السيبراني: يوفر البحث فهماً أفضل لتأثير الهجمات السيبرانية على الأمن الوطني اللبناني، ويطرح حلولاً لتعزيز القدرة على التصدي لتلك التهديدات.

٤. المساهمة في النقاش الأكاديمي: يساهم البحث في إثراء النقاش الأكاديمي حول الحرب السيبرانية ودور القانون الدولي في تنظيمها، مما يساعد في تشكيل مواقف الدول والمنظمات الدولية حيال هذه الظاهرة.

**مشكلة البحث: –**

تعد الحرب السيبرانية جزءًا لا يتجزأ من الصراعات الحديثة بين الدول، حيث تعتمد بعض الأطراف على الهجمات الإلكترونية لتعطيل البنى التحتية الحيوية للخصم.

في هذا السياق، تلعب الحرب السيبرانية الإسرائيلية ضد لبنان دورًا رئيسيًا في تصعيد النزاع بين الطرفين، مما يطرح تساؤلات حول مشروعية هذه الهجمات بموجب القانون الدولي وتداعياتها على الأمن الوطني اللبناني.

تتمثل مشكلة البحث في التحديات القانونية التي تثيرها الهجمات السيبرانية الإسرائيلية على حزب الله ولبنان في ظل غياب إطار قانوني دولي واضح ينظم الحرب السيبرانية.

ويبقى السؤال حول مدى توافق هذه الهجمات مع قواعد القانون الدولي العام والقانون الدولي الإنساني، وتتجسد المشكلة في الأسئلة التالية:

١. هل يمكن اعتبار الهجمات السيبرانية نوعًا من استخدام القوة بموجب ميثاق الأمم المتحدة؟

٢. إلى أي مدى تحترم الهجمات السيبرانية مبادئ القانون الدولي الإنساني، خصوصًا تلك المتعلقة بحماية المدنيين والبنية التحتية الحيوية؟

٣. كيف يمكن تطبيق قواعد المسؤولية الدولية على الهجمات السيبرانية، خصوصًا في حالة عدم وجود أدلة واضحة تثبت الجهات الفاعلة؟

٤. هل يقتضي الواقع الراهن تطوير قوانين دولية جديدة أو تعديل القوانين الحالية لتواكب التهديدات السيبرانية المتزايدة؟

يشكل البحث محاولة للإجابة على هذه الأسئلة وتحديد الأطر القانونية المناسبة لمواجهة التحديات التي تطرحها الحرب السيبرانية على الصعيد الدولي.

**فرضية البحث:**

تنطلق فرضية البحث من أن الهجمات السيبرانية الإسرائيلية على حزب الله ولبنان قد تنتهك قواعد القانون الدولي العام والقانون الدولي الإنساني، خاصة فيما يتعلق باستخدام القوة وحماية المدنيين والبنية التحتية الحيوية.

كما تفترض الفرضية أن الإطار القانوني الدولي الحالي قد لا يكون كافيًا للتعامل بفعالية مع الحرب السيبرانية، مما يستدعي تطوير قواعد جديدة أو تعديل القوانين القائمة لتغطية الفجوات القانونية المتعلقة بهذا النوع من الهجمات، وبناءً على ذلك، تسعى الفرضية إلى اختبار ما إذا كانت الهجمات السيبرانية الإسرائيلية تتعارض مع: –

١. القانون الدولي العام: من حيث اعتبار الهجمات السيبرانية شكلًا من أشكال العدوان أو الاستخدام غير المشروع للقوة.

٢. القانون الدولي الإنساني: من حيث انتهاك مبادئ التمييز والتناسب وحماية المدنيين في النزاعات المسلحة.

٣. مسؤولية الدول: من حيث مدى قابلية تحميل إسرائيل مسؤولية قانونية عن هذه الهجمات في ضوء المعايير الدولية القائمة.

**أهداف البحث:**

١. تحليل الهجمات السيبرانية من منظور قانوني: فهم طبيعة الهجمات السيبرانية الإسرائيلية ضد حزب الله ولبنان وتحليلها وفقًا لمبادئ القانون الدولي العام والقانون الدولي الإنساني.

٢. تقييم شرعية الهجمات السيبرانية: تقييم مدى توافق الهجمات السيبرانية الإسرائيلية مع أحكام ميثاق الأمم المتحدة المتعلقة باستخدام القوة، وكذلك مع قواعد القانون الدولي الإنساني التي تهدف إلى حماية المدنيين والبنية التحتية الحيوية.

٣. تحديد المسؤولية القانونية: دراسة إمكانية تحميل إسرائيل المسؤولية القانونية عن الهجمات السيبرانية على لبنان وحزب الله بموجب قواعد المسؤولية الدولية.

٤. استكشاف الفجوات القانونية: تحديد الفجوات الموجودة في القانون الدولي الحالي فيما يتعلق بتنظيم الحرب السيبرانية، وتقديم توصيات حول كيفية سد هذه الفجوات من خلال تطوير أو تعديل القوانين الدولية.

٥. اقتراح حلول وتوصيات: تقديم حلول قانونية لتعزيز الحماية من الهجمات السيبرانية على المستوى الوطني والدولي، بما يشمل تحسين الأطر القانونية وتعزيز التعاون الدولي في هذا المجال.

**منهجية البحث:**

لتحقيق أهداف البحث، سيتم استخدام منهجية تحليلية وصفية تعتمد على مجموعة من الأدوات والأساليب البحثية:

١. المنهج الوصفي: سيتم استخدام المنهج الوصفي لفهم طبيعة الهجمات السيبرانية الإسرائيلية على حزب الله ولبنان، وتقديم صورة واضحة حول تطور هذه الهجمات وأهدافها وتأثيراتها.

٢. المنهج التحليلي القانوني: سيتم تحليل النصوص القانونية الدولية، مثل ميثاق الأمم المتحدة واتفاقيات جنيف والقوانين ذات الصلة بالقانون الدولي الإنساني، لتقييم مدى توافق الهجمات السيبرانية مع المبادئ والقواعد القانونية الدولية.

**خطة البحث:**

يتكون من مقدمة ومبحثين: –

المبحث الأول: الإطار النظري للحب السيبرانية والذي بدوره ينقسم الى مطلبين:

المطلب الأول: مفهوم الحرب السيبرانية

المطلب الثاني: الهجمات السيبرانية الاسرائيلية ضد لبنان وطبيعة الحرب السيبرانية الاسرائيلية

المبحث الثاني: الحرب السيبرانية في ضوء القانون الدولي العام

المطلب الأول: مشروعية الهجمات السيبرانية الإسرائيلية بموجب المواثيق الدولية

المطلب الثاني– الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني

## المبحث الأول

## الإطار النظري للحرب السيبرانية

تشكل الحرب السيبرانية تحديًا معاصرًا يعيد تعريف مفاهيم النزاع والأمن في العصر الرقمي. يتضمن الإطار النظري للحرب السيبرانية دراسة الجوانب التقنية والقانونية والأخلاقية المرتبطة باستخدام الفضاء السيبراني كبيئة للصراع. يتناول الإطار المفاهيمي جوانب الردع والدفاع السيبراني، ودور القانون الدولي في تنظيم وحظر الأنشطة العدائية السيبرانية. في هذا السياق، يصبح التعاون الدولي وتبادل المعلومات بين الدول أمرًا حيويًا لمواجهة التحديات المتنامية التي تفرضها الحرب السيبرانية على السلم والأمن العالميين.[1]

## المطلب الاول

## مفهوم الحرب السيبرانية

تسعى هذه الدراسة في هذا المطلب إلى تحليل مفهوم الحرب السيبرانية، ودوره في النزاعات المسلحة المعاصرة والفرق بين الحرب السيبرانية والأنواع التقليدية من الحروب تاريخ وتطور الحروب السيبرانية وانواعها.

### أولا- تعريف الحرب السيبرانية:

هناك الغموض في تعريف الحرب السيبرانية ولكن لم يمنع الأوساط الأكاديمية أو العسكرية أو الحكومات من محاولة وضع تعريف. الحرب السيبرانية هي شكل من أشكال النزاع غير التقليدي الذي يعتمد على الهجمات الرقمية لتعطيل أو تدمير أنظمة الحواسيب والشبكات المرتبطة بها، والتي تتحكم في البنية التحتية للدولة، والتي تستخدم التكنولوجيا الرقمية والهجمات الإلكترونية لتحقيق أهداف سياسية أو عسكرية. تعتمد هذه الحرب على استهداف شبكات الكمبيوتر وأنظمة المعلومات للخصوم وأنظمة الطاقة، والاتصالات، والمؤسسات المالية، والخدمات العامة.

---

([1]) د. راجي يوسف محمود البياتي، الإرهاب السيبراني نماذج من الجهود الدولية للحد منه، مجلة تكريت للعلوم السياسية، ع٢٨، ٢٠٢٢، ص٨٨.

وتُعرف الحرب السيبرانية بأنها "النزاع الذي يُستخدم فيه الفضاء الإلكتروني كأداة لتحقيق أهداف عسكرية أو سياسية.

وهناك تعريف آخر للحرب السيبرانية يصفها بأنها "أعمال هجومية ودفاعية، متكافئة أو غير متكافئة، تتم في الشبكات الرقمية بواسطة الدول أو كيانات تشبه الدول (أو ما دون الدول). وتشتمل هذه الأعمال على مخاطر تهدد البنية التحتية الوطنية الحيوية والأنظمة العسكرية.[1]

وعرف كل من ريتشارد أ. كلارك وروبرت كناك الحرب الإلكترونية بأنها "أعمال تقوم بها دولة تهدف إلى اختراق أجهزة الكمبيوتر والشبكات التابعة لدولة أخرى بهدف التسبب في أضرار جسيمة أو تعطيلها.[2]

من كل ما تقدم يتبين لنا ان الحرب السيبرانية هي أنشطة هجومية ودفاعية تحدث في الفضاء الرقمي باستخدام الوسائل الإلكترونية، تستهدف اختراق وتعطيل الشبكات والأجهزة التابعة لدول أو كيانات أخرى. تشمل هذه الأنشطة الاستطلاع، وتعطيل الأنظمة، ومقاومة الاستطلاع المعادي، وحماية الأنظمة الصديقة، ويمكن أن تؤدي الهجمات السيبرانية إلى أضرار كبيرة تشمل تهديد الخدمات الأساسية مثل المياه والرعاية الطبية وأجهزة الاتصالات. يتطلب هذا النوع من الحرب ترابطًا عاليًا بين الشبكات والبنية التحتية من جانب المدافع وتقدمًا تكنولوجيًا من جانب المهاجم، مع ضرورة توخي الحذر لحماية المدنيين وتطبيق قواعد الحرب بشكل مشابه للحروب التقليدية.

وتختلف هذه الحرب عن الحروب التقليدية بكونها لا تتطلب استخدام القوة المسلحة بشكل مباشر، بل تعتمد على التكنولوجيا واختراق الشبكات. تتضمن أساليب الحرب السيبرانية الهجمات الإلكترونية، التجسس السيبراني، تخريب البيانات، والعمليات النفسية.

**ثانيا: خصائص الحرب السيبرانية ومميزاتها**

---

(1) Shane M, Coughlan: "Is there a common understanding of what constitutes cyber warfare master theses, University of Birmingham School of Politics and International Studies,30 September, 2003, p, 2.

(2) انصر سفاح كريم: الحروب الإلكترونية وأثرها على الامن القومي، مقال منشور على موقع مركز النهرين للدراسات الاستراتيجية-رئاسة الوزراء-مستشارية الامن القومي، متاح على الرابط التالي: https://www.alnahrain.iq/post/1031

تعود جذور الحرب السيبرانية إلى نهاية القرن العشرين، مع انتشار التكنولوجيا الرقمية وزيادة الاعتماد على الإنترنت. كانت البداية مع الهجمات البسيطة مثل فيروسات الكمبيوتر والاختراقات الإلكترونية. ومع مرور الوقت، تطورت هذه الهجمات لتصبح أكثر تعقيدًا واستهدفت المؤسسات الحكومية، والشركات الكبرى، والبنية التحتية الحيوية.

والتكنولوجيا الرقمية والإنترنت غيرت طبيعة النزاعات العسكرية، حيث أصبح بإمكان الدول والجماعات غير الحكومية شن هجمات من مسافات بعيدة وبكلفة منخفضة نسبيًا.

أدت هذه التغييرات إلى تصعيد النزاعات من خلال تمكين الأطراف من اختراق أنظمة الخصوم وتعطيل عملياتهم دون الحاجة إلى اشتباكات عسكرية تقليدية، وتجعل هذه النزاعات السكان المدنيين في حالة من الاستضعاف وتعرض، حقوقهم للانتهاك والاستغلال.[1]

ولعل من نتائج التطور التقني وظهور الفضاء السيبراني ان أصبح لدينا ما يعرف بالحروب السيبرانية.

تتميز الحروب السيبرانية بعدد من الخصائص التي تجعلها جذابة للفاعلين الدوليين، سواء كانوا دولًا أو جهات غير حكومية:

١- تعتبر الحرب الرقمية حربًا تقنية متطورة، حيث تركز على شبكة الإنترنت التي تتميز بالتطور المستمر والتنوع والابتكار في تقنياتها. ترتبط هذه الحرب بالمصالح الحيوية للدول، وتتميز بسرعة التنفيذ وإمكانية المراوغة، مما يمنح المهاجم ميزة واضحة على المدافع.

٢- كما أن أهداف الحرب السيبرانية وتأثيراتها غير محددة، وقد تتجاوز مخاطرها ميادين القتال التقليدية لتطال أكثر المواقع السيادية والحساسة، بعيدًا عن دائرة المعارك المباشرة.[2]

٣- من أبرز خصائص الحروب السيبرانية انخفاض تكلفتها مقارنة بأدوات الحرب التقليدية. إذ لا يتطلب انخراط طرف غير دولتي في هذا النوع من الصراعات تصنيع أسلحة مكلفة مثل حاملات الطائرات أو

---

([1]) نهى عبد الخالق احمد و د. سلوى احمد ميدان: المسؤولية الدولية عن استغلال الأطفال في القانون الدولي الإنساني، مجلة كلية القانون للعلوم القانونية والسياسية، مج١١، ٢٠٢٢، ص٢٠٨.

([2]) وفاء بوكابوس، تحول القوة في العلاقات الدولية "دراسة في انتقال القوة من التقليدية الى الحديثة"، ط١، المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية، المانيا، ٢٠١٩، ص٦٩.

المقاتلات المتطورة لتهديد الأطراف الأخرى بشكل جدي. يكفي بدلاً من ذلك تطوير البرمجيات اللازمة وامتلاك الأجهزة الحاسوبية المناسبة لتحقيق هذا الهدف.

٤- تتمثل إحدى خصائص الحرب السيبرانية في قدرتها على تحقيق نتائج ملموسة ضمن الصراعات والنزاعات المسلحة. كما تختلف العقيدة العسكرية وقواعد الاشتباك في الحروب السيبرانية بشكل كبير عن تلك المطبقة في الحروب التقليدية.

٥- الحرب التقليدية تعتمد على المواجهات العسكرية المباشرة باستخدام الأسلحة التقليدية، مثل الجيوش والدبابات والطائرات. بالمقابل، الحرب السيبرانية تركز على استهداف البنية التحتية الرقمية دون الحاجة إلى مواجهة مادية مباشرة.

٦- كما أن الحرب السيبرانية غالباً ما تكون غير مرئية وذات تأثيرات بعيدة المدى وسريعة، مما يجعلها تختلف من حيث السرعة، والتعقيد، والقدرة على استهداف الأهداف بدقة، فمن الصعب تحديد الجهة المسؤولة عن الهجمات السيبرانية، حيث يمكن إخفاء مصدر الهجمات أو استخدام قراصنة غير تابعين للدولة بشكل مباشر.

وقد أثرت حروب الفضاء السيبراني بشكل كبير على طبيعة المواجهات، إذ أصبح بإمكان أطراف غير دولية أن تشارك، حيث أن الأسلحة المستخدمة في هذه الحروب ليست حكرًا على الدول. وهذا يجعل وصف حروب الفضاء السيبراني بأنها حروب غير متكافئة دقيق. [١]

٧- وتتسم الحرب السيبرانية ايضاً بميزة بارزة وهي فشل مفهوم الردع الذي يُستخدم عادةً بين الدول في الحروب التقليدية. يرجع ذلك إلى أن الهجمات الإلكترونية غالبًا ما تترك آثارًا غير واضحة أو أدلة على وقوعها، كما أن الدمار الناتج عنها قد يشمل التجسس والتسلل والتدمير بدون الحاجة إلى دماء أو أنقاض.

٨- كما أن اتساع الفضاء السيبراني قد يسمح بزيادة عدد المهاجمين وامتداد الصراع في الزمان والمكان [2]وفي الحرب السيبرانية، يكون هذا المفهوم غير فعّال بسبب عدة عوامل، أبرزها صعوبة تحديد الدولة

---

(١) نورة شلوش: القرصنة الالكترونية في الفضاء السيبراني "التهديد المتصاعد من الدول"، مجلة مركز بابل للدراسات الإنسانية، مج٨، ع٢، جامعة بابل، ٢٠١٨، ص٥٧.

أو الجهة التي نفذت الهجوم. إذ يمكن للقوة المهاجمة شن هجوم على دولة لصالح دولة أخرى انطلاقًا من دولة ثالثة عبر استخدام خوادم موجودة هناك، مما يجعل تحديد مصدر الهجمات الإلكترونية شبه مستحيل في كثير من الأحيان.

وتتميز الحروب السيبرانية بعدم وجود حدود جغرافية واضحة، كما لا يوجد مفهوم السيادة بمعناه التقليدي في العالم الواقعي، حيث لا يمكن منع الأطراف الأخرى من الدخول إلى المناطق الخاضعة لسيادة دولة معينة. يمكن وصف الحدود في الفضاء الإلكتروني بأنها حدود مائعة أو غير موجودة، إذ تتداخل الشبكات بين الدول بشكل كبير، حيث تشترك الدول الصغيرة والكبيرة في نفس الشبكات التي قد تكون موجودة في بلدان أخرى. علاوة على ذلك، تشمل الحروب السيبرانية عمليات تدعم العمل العسكري مثل التجسس على الإشارات، أو التشويش على نظام تحديد المواقع العالمي (GPS) وإعاقته لدى العدو، وعرقلة عمليات توجيه الأسلحة العسكرية المعادية. تتنوع البرمجيات المستخدمة في عمليات التسلل والاختراق، ومن أبرزها القنابل المنطقية، وهي قطع من التعليمات البرمجية المضافة عمدًا إلى نظام برمجي، تقوم بإطلاق وظيفة ضارة عند توافر شروط محددة.

كما تشمل البرمجيات الديدان الحاسوبية التي تعتبر أدوات جديدة تتطور بسرعة مستمرة وتحتاج إلى فك شفرتها. جوهر العقيدة العسكرية في الحرب السيبرانية يعتمد على السعي لكسب الحروب من خلال استهداف البنية التحتية الاستراتيجية للهياكل الإلكترونية للخصم. بالتوازي مع ذلك، يستمر تطوير استراتيجيات وقدرات للحماية عبر أنظمة الدفاع السيبراني لضمان التفوق والحماية في هذا المجال المتطور[1] تعتمد القوة السيبرانية في الحروب على استخدام الأجهزة والبرامج. تشمل الأجهزة أنظمة الحاسوب مثل وحدة المعالجة المركزية، ومحرك الأقراص الضوئية، ولوحة المفاتيح، بالإضافة إلى الأقمار الصناعية. أما البرامج، فتتضمن الصياغات البرمجية التي توجه عمليات الحاسوب، بما في ذلك البرمجيات الضارة والفيروسات. على سبيل المثال، تشمل لغة الاستعلام الهيكلية (SQL) مجموعة من التعليمات للتفاعل مع قواعد البيانات، وعمليات الحقن الإلكتروني التي تتضمن إدخال برمجيات ضارة في الأنظمة الحاسوبية المستهدفة. كما تشمل البرمجة النصية للمواقع، التي تُستخدم لتشويه وإتلاف صفحات

---

([2]) د. شويرب جيلالي وفائزة دمراد، مصدر سابق، ص١٦٣.

([1]) د. انعام عبد الرضا سلطان العكابي: توظيف الحروب السيبرانية في تطوير مفهوم القوة للدول الكبرى، ع٧٣، مجلة قضايا سياسية، جامعة النهرين، ٢٠٢٣، ص٤٣١-٤٣٢.

الويب الخاصة بالعدو، كما حدث في الهجوم الإلكتروني الروسي على إستونيا، حيث هاجم القراصنة الروس مواقع تابعة للحكومة الإستونية.[1]

مما سبق نستنتج انه تتميز الحروب السيبرانية بعدد من الخصائص التي تجعلها جذابة للفاعلين الدوليين، بما في ذلك انخفاض تكلفتها مقارنة بالحروب التقليدية. لا تتطلب هذه الحروب استثمارات ضخمة في الأسلحة، بل يمكن أن تتم باستخدام البرمجيات والأجهزة الحاسوبية. كما أنها قادرة على تحقيق نتائج ملموسة في الصراعات المسلحة، تستهدف البنية التحتية الاستراتيجية للخصم، وتفتقر إلى الحدود الجغرافية الواضحة، مما يجعل مفهوم الردع التقليدي غير فعال.[2] اذ تعتمد الحروب السيبرانية على أدوات متطورة مثل الفيروسات والقنابل المنطقية، وتتميز بصعوبة تتبع مصدر الهجمات وعدم وضوح الأطراف المشاركة.

## المطلب الثاني

## الهجمات السيبرانية الاسرائيلية ضد لبنان وطبيعة الحرب السيبرانية الاسرائيلية

الهجمات السيبرانية الإسرائيلية ضد لبنان تُعتبر جزءًا من الصراع المستمر بين البلدين والذي يتخذ أبعادًا متعددة، بما في ذلك الجانب العسكري، الاقتصادي، والسياسي. الهجمات السيبرانية هي شكل من أشكال الحرب الحديثة التي تستهدف البنية التحتية الرقمية لدولة معينة بهدف التسبب في أضرار اقتصادية أو سياسية أو حتى أمنية.

١- وفي حالة إسرائيل ولبنان يُزعم أن إسرائيل شنت عدة هجمات سيبرانية على أهداف لبنانية خلال العقود الماضية، خاصة أثناء وبعد النزاعات المسلحة التقليدية بين البلدين.[3] . وهذه الهجمات تشمل:

- تعطيل مواقع حكومية أو مؤسسات حيوية.

- اختراق شبكات الاتصالات وجمع معلومات استخبارية.

---

([1]) احمد عيسى الفتلاوي، الهجمات السيبرانية "دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر، ط١، منشورات زين الحقوقية، بيروت، ٢٠١٨، ص٦٨.

([2]) عبد الله زهير، الحروب السيبرانية في القانون الدولي العام، دار النشر العلمي، ٢٠١٩، ص١١٢.

([3]) علي مصطفى، حروب الفضاء السيبراني: التهديدات الإسرائيلية لحزب الله ولبنان، دار النشر الحديثة، ٢٠٢٠، ص ١٤٣.

– التأثير على وسائل الإعلام الإلكترونية اللبنانية.

٢– استهداف البنى التحتية الحيوية مثل شبكات الكهرباء.[1]

**أولا– سياق الهجمات السيبرانية الإسرائيلية ضد لبنان:**

١–التوترات السياسية والعسكرية: العلاقة المتوترة بين إسرائيل ولبنان تاريخيًا، وخاصة مع وجود حزب الله كأحد الفاعلين الرئيسيين في الساحة اللبنانية، جعلت من الهجمات السيبرانية أحد الأدوات المستخدمة في هذا الصراع.

٢– استهداف البنية التحتية: إسرائيل تستخدم الهجمات السيبرانية لتعطيل البنية التحتية الحيوية في لبنان، مثل شبكات الاتصالات، القطاعات المالية، أو حتى الأنظمة الحكومية.

٣–الردع والاستطلاع: الهجمات السيبرانية لا تُستخدم فقط للتدمير أو التعطيل، بل أحيانًا بهدف جمع المعلومات الاستخباراتية واستطلاع نقاط الضعف في النظام السيبراني اللبناني. قد يكون الهدف هنا هو التحضير لهجمات مستقبلية أو التأثير على القرارات السياسية.

٤–الحرب النفسية: الهجمات السيبرانية يمكن أن تُستخدم أيضًا كجزء من الحرب النفسية، حيث يمكنها خلق حالة من الذعر أو الارتباك بين السكان أو المؤسسات.[2]

ومن أمثلة للهجمات السيبرانية هجمات ٢٠١٨ و٢٠٢٠ اذ تعرضت لبنان خلال هذه السنوات لعدة هجمات سيبرانية يعتقد أن إسرائيل وراءها، حيث استهدفت مواقع حكومية ومؤسسات مالية. هذه الهجمات شملت اختراقات وتسريب بيانات، إلى جانب تعطيل بعض الخدمات الأساسية.

٥– الهجمات على وسائل الإعلام: في بعض الأحيان، تُستهدف وسائل الإعلام اللبنانية في هجمات سيبرانية بهدف بث أخبار أو معلومات مضللة، مما يؤدي إلى زعزعة الثقة بين المواطنين والحكومة.[3]

---

([1]) نضال أحمد، إسرائيل والتكنولوجيا السيبرانية: تهديدات إلكترونية لحزب الله، مركز الدراسات العربية، ٢٠٢١، ص٢٥٤.

([2]) د. سامر الشامي، إسرائيل وحزب الله: الصراع الإلكتروني، دار الشروق للنشر، ٢٠١٨، ص٧٥.

([3]) مازن كنعان، حرب الشبكات الإلكترونية، حزب الله وإسرائيل، دار الأمة، ٢٠٢٠، ص ١٧٣.

**ثانيا- التحديات اللبنانية في مواجهة الهجمات السيبرانية:**

ان دولة لبنان تعاني من ضعف في البنية التحتية السيبرانية وضعف التنسيق بين المؤسسات الحكومية والخاصة في التعامل مع مثل هذه التهديدات. وبالتالي، فإن القدرة على الرد أو الدفاع ضد هذه الهجمات محدودة، مما يجعله هدفًا سهلاً للهجمات السيبرانية.

ان الهجمات السيبرانية الإسرائيلية ضد لبنان تعكس ديناميكية جديدة في الصراع بين البلدين، حيث تتجاوز الأسلحة التقليدية لتشمل الحرب الرقمية مما يعزز الحاجة إلى تطوير قدرات الدفاع السيبراني اللبناني.

وان السياق الجيوسياسي للنزاع بين إسرائيل ولبنان معقد ومتعدد الأبعاد، ويتداخل فيه التاريخ والدين والجغرافيا السياسية.[1]

ويمكن تقسيم هذا النزاع إلى مراحل زمنية مختلفة، تتأثر بعوامل إقليمية ودولية، فضلاً عن الديناميات الداخلية لكل من إسرائيل ولبنان.

**١- العوامل التاريخية:**

الصراع الإسرائيلي اللبناني هو جزء من الصراع العربي الإسرائيلي الأوسع، ويتميز بتداخل أبعاد جغرافية وسياسية معقدة. بدأ هذا الصراع منذ تأسيس دولة إسرائيل عام ١٩٤٨ وازداد تعقيدًا مع مرور الوقت. [2]

أ- الأبعاد الجغرافية والحدود المشتركة: تشترك إسرائيل ولبنان في حدود تمتد على طول (خط الأزرق) الذي رسمته الأمم المتحدة بعد انسحاب إسرائيل من جنوب لبنان عام ٢٠٠٠، ومع ذلك، لا يزال هناك نزاع حول منطقة (مزارع شبعا).[3]

---

([1]) د. بن تغري موسى: الحرب السيبرانية والقانون الدولي الإنساني، مجلة الاجتهاد القضائي، مج١٢، عدد خاص- العدد التسلسلي (٢٢)، جامعة محمد خيضر بسكرة، الجزائر، ٢٠٢٠، ص٢٠٦.

([2]) مازن كنعان، حرب الشبكات الإلكترونية، مصدر سابق، ص ٤٢.

([3]) جاد صبحي، الحرب الإلكترونية في الشرق الأوسط: دور إسرائيل وحزب الله، دار الهلال، ٢٠٢١، ص١٣٤.

وكان الجنوب اللبناني منطقة نزاع رئيسية، حيث كانت (منظمة التحرير الفلسطينية) نشطة هناك في السبعينيات، ولاحقًا أصبح معقلًا لـ (حزب الله)، الذي قاد مقاومة مسلحة ضد إسرائيل.

ب-الأبعاد السياسية: نشأ حزب الله كحركة مقاومة مسلحة في الثمانينيات بدعم إيراني وسوري، ويعد الفاعل الرئيسي في الصراع ضد إسرائيل، ودخل في عدة مواجهات مع الجيش الإسرائيلي، أبرزها حرب عام ٢٠٠٦.

ت-الدور الإقليمي: تلعب إيران وسوريا دورًا حاسمًا في دعم حزب الله، بينما تعتبر الولايات المتحدة وإسرائيل حزب الله تهديدًا أمنيًا خطيرًا.

ث-التوترات الداخلية في لبنان: وجود حزب الله كقوة سياسية وعسكرية مؤثرة في لبنان يزيد من تعقيد المشهد السياسي اللبناني، خاصة مع الفصائل الداخلية التي تتبنى مواقف مختلفة تجاه إسرائيل. (1)

ج- ان الصراع الإسرائيلي اللبناني مرتبط بالصراعات الإقليمية الأوسع بين إسرائيل وإيران وسوريا، ويتأثر بالجغرافيا المتوترة للحدود الجنوبية للبنان، والدور المتزايد لحزب الله كقوة سياسية وعسكرية في المنطقة.

**أولا- تأثير الهجمات السيبرانية على الامن الوطني اللبناني**

الهجمات السيبرانية لها تأثير كبير على الأمن الوطني اللبناني، حيث تؤدي إلى زعزعة الاستقرار وتعريض البنية التحتية الحيوية والمعلومات الحساسة للخطر.[2]

في حالة لبنان، الذي يعاني بالفعل من أزمات اقتصادية وسياسية، تزيد الهجمات السيبرانية من التحديات التي تواجه الأمن الوطني. فيما يلي بعض التأثيرات الرئيسية لهذه الهجمات: -

١- إضعاف البنية التحتية الحيوية.

٢- تعريض الأمن الاقتصادي للخطر.

٣- التجسس وجمع المعلومات الاستخباراتية.

---

([1]) د. بن تغري موسى، مصدر سابق، ص٢٠٦ وما بعدها.

([2]) د. سامر الشامي، مصدر سابق، ص ١٥٣.

٤- تعطيل الاتصالات والتنسيق العسكري.

٥- الحرب النفسية وزعزعة الثقة في الحكومة.

٦- الاعتماد على الدعم الخارجي لمواجهة هذه التهديدات.

٧- إضعاف القدرات العسكرية والدفاعية.[1]

ان الهجمات السيبرانية لها تأثيرات مدمرة على الأمن الوطني اللبناني، حيث تؤدي إلى إضعاف البنية التحتية الحيوية، تعريض الأمن الاقتصادي للخطر، وتعطيل قدرة الحكومة والجيش على حماية البلاد. وهذه الهجمات في نفس الوقت تشكل جزءًا من الحرب الحديثة التي تعتمد على الفضاء السيبراني كوسيلة لتحقيق أهداف سياسية وعسكرية، مما يستدعي تطوير استراتيجيات دفاع سيبراني قوية لحماية لبنان من هذه التهديدات.

**ثانيا – تأثير الهجمات على البنية التحتية الحيوية كالاتصالات والطاقة وغيرها**

الهجمات السيبرانية على البنية التحتية الحيوية في لبنان، مثل الاتصالات والطاقة، لها تأثيرات خطيرة ومباشرة على الأمن القومي والاقتصادي، ويمكن أن تؤدي إلى حالة من الفوضى والعجز عن تقديم الخدمات الأساسية للمواطنين. فيما يلي أبرز تأثيرات هذه الهجمات[2] : –

١- تعطيل خدمات الاتصالات وشل التواصل الحكومي والشعبي وقطع التواصل الداخلي والخارجي.

٢- تعطيل قطاع الطاقة والا زمة في إمدادات الكهرباء والتأثير على الاقتصاد والتأثير على البنية التحتية الأخرى.

٣- تهديد الأمن الغذائي والصحي وتعطيل سلاسل الإمداد وتعطيل المستشفيات والخدمات الطبية.[3]

٤- تعزيز حالة عدم الاستقرار السياسي والاجتماعي وزيادة التوتر الاجتماعي وانعدام الثقة في الحكومة

٥- التأثير على الأمن الاقتصادي واستهداف المؤسسات المالية وتراجع الاستثمارات.

---

([1]) علي مصطفى، حروب الفضاء السيبراني، مصدر سابق، ص٢٣٠

([2]) د. بن تغري موسى، مصدر سابق، ص٢٠٨.

([3]) فادي عبد الله، إسرائيل والحروب الإلكترونية، منظور قانوني، دار الفكر المعاصر،٢٠١٧، ص ١٨٧.

٦- إضعاف الدفاع الوطني والأمن الداخلي والتأثير على التنسيق العسكري وكذلك تعطيل أنظمة المراقبة والسيطرة.

٧- تفاقم الأزمات الإنسانية والضغط على الخدمات الأساسية وزيادة العبء على المساعدات الدولية، اذ ان الهجمات السيبرانية على البنية التحتية الحيوية في لبنان، وخاصة في مجالات الاتصالات والطاقة، تؤثر بشكل كبير على الأمن القومي والاقتصاد والخدمات الأساسية. [1]فتعطل هذه البنية يزيد من التوترات الداخلية، ويضعف قدرة الحكومة على الاستجابة للأزمات، كما يعرض لبنان لمزيد من الاضطرابات السياسية والاجتماعية، مما يزيد من هشاشة الوضع الداخلي.

**ثالثا – التأثيرات الاقتصادية والسياسية والاجتماعية للهجمات**

الهجمات السيبرانية على لبنان، وخاصة تلك التي تستهدف البنية التحتية الحيوية مثل الاتصالات والطاقة، تؤثر بشكل عميق على مختلف جوانب الحياة الاقتصادية، السياسية، والاجتماعية. فيما يلي استعراض للتأثيرات الرئيسية في كل من هذه المجالات:

١- التأثيرات الاقتصادية وتعطيل الإنتاج والخدمات والتأثير على النظام المالي كذلك فقدان الثقة الاستثمارية وزيادة التكلفة على الدولة. [2]

٢- التأثيرات السياسية وإضعاف ثقة المواطنين في الحكومة وتعطيل قدرة الحكومة على الإدارة وتأجيج الانقسامات الداخلية.

٣- التأثيرات الاجتماعية وانقطاع الخدمات الأساسية وزيادة الفقر وزيادة الهجرة ونزوح العقول وتعزيز الانقسامات الطائفية وتزايد الفوضى وانتشار الجرائم.[3]

ان الهجمات السيبرانية على لبنان تؤدي إلى تأثيرات واسعة على الاقتصاد، السياسة، والمجتمع. على الصعيد الاقتصادي، تؤدي إلى خسائر مالية، تراجع الاستثمارات، وزيادة الفقر. سياسيًا، تضعف ثقة المواطنين في الحكومة وتؤدي إلى تفاقم الانقسامات الداخلية. أما اجتماعيًا، فهي تزيد من حدة الفقر

---

([1]) د. بن تغري موسى، مصدر سابق، ص٢٠٩.

([2]) نضال أحمد، إسرائيل والتكنولوجيا السيبرانية، مصدر سابق، ص ٢٤٢.

([3]) د. بن تغري موسى، مصدر سابق، ص٢٠٨.

والهجرة وتؤجج التوترات الطائفية. كل هذه العوامل تزيد من هشاشة لبنان وتجعله أكثر عرضة للصراعات الداخلية والخارجية.

## المبحث الثاني

## الحرب السيبرانية في ضوء القانون الدولي العام

شهد العالم تطورًا سريعًا في التكنولوجيا والاتصالات الرقمية خلال العقود الأخيرة، مما أدى إلى ظهور نوع جديد من النزاعات الدولية، وهو (الحرب السيبرانية) تتمثل الحرب السيبرانية في استخدام الهجمات الإلكترونية ضد الدول أو المنظمات بهدف تحقيق أهداف سياسية أو اقتصادية أو عسكرية.

ومع تزايد هذه الهجمات ظهرت تساؤلات حول كيفية تنظيمها في إطار القانون الدولي العام ومدى توافقها مع القواعد الدولية التي تحكم النزاعات المسلحة التقليدية.[1]

ان ميثاق الأمم المتحدة يوفر إطارًا عامًا يمكن من خلاله التعامل مع الحروب السيبرانية من خلال المبادئ الأساسية مثل حظر استخدام القوة، السيادة، وحق الدفاع عن النفس. ورغم أن الميثاق لم يُكتب خصيصًا للتعامل مع التهديدات السيبرانية، فإن تطور التكنولوجيا يتطلب تطبيق هذه المبادئ التقليدية على الفضاء السيبراني، مع الاعتراف بالحاجة إلى قواعد إضافية أو تفصيلية لمواجهة التحديات الفريدة التي تطرحها الحروب السيبرانية.[2]

القانون الدولي الإنساني الذي يُعرف أيضًا ب" قانون النزاعات المسلحة"، يهدف إلى تقليل آثار النزاعات المسلحة على المدنيين والمقاتلين من خلال تنظيم أساليب ووسائل الحرب. فمن أهم المبادئ الأساسية في هذا القانون مبدآ التمييز والتناسب. هذان المبدآن يلعبان دورًا رئيسيًا في ضمان عدم انتهاك حقوق الإنسان الأساسية أثناء النزاعات المسلحة.[3]

---

([1]) عبد الرؤوف سعيد، الهجمات السيبرانية: الأطر القانونية الدولية، دار الثقافة، ٢٠١٨، ص ٤١.

([2]) كوردولا دوريجي: لا تقترب من حدود فضائي الإلكتروني، الحرب الإلكترونية والقانون الدولي الإنساني وحماية المدنيين، مجلة اللجنة الدولية للصليب الأحمر، مج٩٤، ع٨٨٦، ٢٠١٢، ص٥٤٢.

([3]) حسن الشمري، القانون الدولي الإنساني والحروب السيبرانية، دار النهضة العربية، ٢٠١٨، ص٤٨.

فتسعى هذه الدراسة في هذا الفصل الى تحليل وتحديد القواعد الدولية التي قد تنطبق عليها، كما نناقش الإشكاليات القانونية الناشئة عن هذا النوع من الحروب ومدى استعداد القانون الدولي للتعامل مع هذه التحديات الجديدة. وفيما يلي شرح مفصل لكل منهما.

## المطلب الأول

## مشروعية الهجمات السيبرانية وفقا للمواثيق الدولية

تعتبر مشروعية الهجمات السيبرانية، بما في ذلك تلك التي تقوم بها إسرائيل، موضوعًا معقدًا يرتبط بالمواثيق الدولية والقانون الدولي وقانون النزاعات المسلحة.

وتعتبر جزءًا من النزاعات الحديثة التي تتضمن استخدام التكنولوجيا والفضاء السيبراني كأداة للصراع ويمكن مناقشة هذا الموضوع في إطار القانون الدولي من عدة زوايا تتعلق بمفاهيم سيادة الدول واستخدام القوة وحماية المدنيين.[1]

ان الحرب السيبرانية تُعتبر مجالًا جديدًا نسبيًا في القانون الدولي، وما زال المجتمع الدولي يعمل على تطوير قواعد واضحة لتنظيم هذا النوع من النزاع، ومع ذلك هناك عدة مبادئ عامة في القانون الدولي يمكن تطبيقها على الهجمات السيبرانية.

١- **حظر استخدام القوة – المادة (٢-٤)** تنص هذه المادة من ميثاق الأمم المتحدة على أنه (يمتنع جميع الأعضاء في علاقاتهم الدولية عن التهديد باستخدام القوة أو استخدامها ضد السلامة الإقليمية أو الاستقلال السياسي لأي دولة، أو بأي طريقة أخرى تتنافى مع أهداف الأمم المتحدة). المادة ٢ف٤، ميثاق الامم المتحدة. [2] والهجمات السيبرانية قد ترتقي إلى مستوى (استخدام القوة) إذا تسببت في أضرار جسيمة للبنية التحتية الحيوية لدولة أخرى أو تسببت في خسائر بشرية، وفي هذه الحالة تُعتبر الهجمات السيبرانية انتهاكًا لميثاق الأمم المتحدة، فوفقًا للمادة (٢-٤) من ميثاق الأمم المتحدة، يُحظر على الدول استخدام القوة أو التهديد باستخدامها

---

([1]) أمير فرج يوسف، جريمة مكافحة الإرهاب الالكتروني –الإرهاب الرقمي– في ظل اتفاقية دول مجلس التعاون لمكافحة الارهاب، ط١، دار الكتب والدراسات العربية، الإسكندرية، ٢٠١٦، ص ٢٥٣.

([2]) د. عيسى دباح، موسوعة القانون الدولي، دار الشروق المجلد الثالث، ٢٠٠٣، ص١٠٠.

في العلاقات الدولية، إلا في حالات الدفاع عن النفس أو بناءً على تفويض من مجلس الأمن.[1] ولكن يبقى السؤال حول ما إذا كانت الهجمات السيبرانية تُعد "استخدامًا للقوة" بالمعنى المنصوص عليه في ميثاق الأمم المتحدة.

هناك بعض الحالات التي قد تُعتبر فيها الهجمات السيبرانية استخدامًا للقوة إذا تسببت في أضرار كبيرة، مثل تعطيل شبكات الكهرباء أو الأنظمة المالية، أو إذا أسفرت عن خسائر بشرية.

وتطبيق هذه المادة على الحرب السيبرانية فهناك تساؤلات حول ما إذا كانت الهجمات السيبرانية تُعتبر (استخدامًا للقوة)، إذا تسببت الهجمات السيبرانية في أضرار مادية جسيمة.[2] كتعطيل البنية التحتية الحيوية مثل (شبكات الكهرباء والأنظمة المالية أو المستشفيات) أو الإضرار بالمواطنين، فقد تُعتبر هذه الهجمات استخدامًا غير مشروع للقوة بموجب المادة (٢-٤).

وإذا هددت دولة ما باستخدام هجمات سيبرانية لتعطيل أنظمة حيوية لدولة أخرى. فقد يُعتبر ذلك أيضًا تهديدًا باستخدام القوة، فيمكن اعتبار الهجمات السيبرانية بمثابة استخدام للقوة إذا كانت تُلحق أضرارًا تُعادل في تأثيرها استخدام الأسلحة التقليدية.

٢- **الدفاع عن النفس - المادة (٥١)** تنص هذه المادة من ميثاق الأمم المتحدة على حق الدول في الدفاع عن نفسها إذا تعرضت (لهجوم مسلح) إلى أن يتخذ مجلس الأمن التدابير اللازمة للحفاظ على السلام والأمن الدوليين وفقاً للمادة (٥١)، من ميثاق الأمم المتحدة.[3]

فإذا تسببت الهجمات السيبرانية في أضرار جسيمة أو هددت حياة السكان أو استقرار الدولة، فإن الدولة المتضررة (مثل لبنان) قد يكون لها الحق في الدفاع عن نفسها بما في ذلك الرد على الهجمات الإلكترونية بطريقة تتناسب مع حجم التهديد.

لذلك يمكن اعتبار الهجوم السيبراني الذي يُحدث أضرارًا مادية كبيرة مثل تدمير البنية التحتية والتسبب في خسائر بشرية بمثابة (هجوم مسلح) يسمح للدولة المتضررة بالدفاع عن نفسها ولكن تحديد متى يُعتبر الهجوم السيبراني (هجومًا مسلحًا) يظل محل نقاش، وفي حالة تعرض دولة لهجوم سيبراني

---

([1]) سعاد إبراهيم، الحروب السيبرانية والقانون الدولي الإنساني، دار الشرق، ٢٠٢٠، ص ١٨٤.

([2]) أمير فرج يوسف: جريمة مكافحة الإرهاب الالكتروني، مصدر سابق، ص ٢٥٣.

([3]) د. عيسى دباح، مصدر سابق، ص١١٠.

خطير يُمكنها أن ترد بهجوم سيبراني دفاعي أو باستخدام وسائل تقليدية طالما أن الرد يكون متناسبًا مع حجم الهجوم وفي إطار القانون الدولي.

٣-**مبدأ السيادة – المادة (١/٢)** تنص هذه المادة من ميثاق الأمم المتحدة على مبدأ السيادة واحترام سيادة كل دولة وتعتبر جميع الدول متساوية في السيادة، المادة (١/٢) ميثاق الأمم المتحدة. [1]

ويتمثل مبدأ السيادة في أنه لا يجوز لدولة أن تنتهك سيادة دولة أخرى من خلال شن هجمات سيبرانية، وتُعتبر البنية التحتية السيبرانية (مثل شبكات الاتصالات والأنظمة الحكومية والخدمات الرقمية) جزءًا من سيادة الدولة، وبالتالي فإن اختراق أنظمة دولة أخرى أو تعطيلها يُعد انتهاكًا لمبدأ السيادة. الذي يعد أحد المبادئ الأساسية في القانون الدولي، ويُعتبر كل من الفضاء السيبراني جزءًا من سيادة الدولة إذا كان يتضمن بنيتها التحتية الرقمية.[2]

مثل شبكات الإنترنت والأنظمة الحكومية، وفقًا لهذا المبدأ لا يجوز لدولة أن تنتهك سيادة دولة أخرى من خلال هجمات سيبرانية تستهدف شبكاتها أو أنظمتها. ويُعد اختراق البنية التحتية لدولة أخرى دون إذن انتهاكًا لمبدأ السيادة، والقانون الدولي يعترف بسيادة الدول على بنيتها التحتية السيبرانية، الهجمات الإلكترونية التي تنفذها دولة ضد دولة أخرى بدون موافقة مثال ذلك الهجمات الإسرائيلية على لبنان والذي تُعتبر انتهاكًا للسيادة.

ولكل دولة الحق في حماية بنيتها التحتية الإلكترونية، والحصول على مساعدة دولية في حالة تعرضها لهجمات سيبرانية تهدد أمنها واستقرارها. وكذلك مبدأ عدم التدخل هو جزء من مبدأ السيادة الذي يحظر على الدول التدخل في الشؤون الداخلية لدول أخرى [3]، بما في ذلك التدخل السيبراني الذي قد يؤثر على العمليات السياسية أو الاقتصادية أو الاجتماعية في دولة أخرى. وهذا يشمل الهجمات السيبرانية التي تستهدف الانتخابات، المؤسسات الحكومية، أو البنية التحتية الاقتصادية لدولة أخرى.

---

([1]) د. عيسى دباح، مصدر سابق، ص١٠٠.

([2]) كوردولا دوريجي، مصدر سابق، ص٥٤٢.

([3]) د. عصام العطية، القانون الدولي العام، دار السنهوري، بيروت، ٢٠١٥، ص٢٢٣ وما بعدها.

ان أي تدخل سيبراني في الشؤون الداخلية لدولة أخرى مثل التلاعب في الانتخابات أو شن هجمات على أنظمتها الحكومية، يُعد انتهاكًا لمبدأ السيادة، وتعتبر السيادة السيبرانية امتدادًا لسيادة الدولة على أراضيها ومجالها الجوي ومياهها الإقليمية.

٤- **تسوية المنازعات – المادة (١/٣٣):** تنص هذه المادة من ميثاق الأمم المتحدة على أنه (يجب على أطراف أي نزاع يهدد حفظ السلم والأمن الدوليين أن يسعوا أولاً إلى حله بالتفاوض أو التحكيم أو التسوية القضائية) المادة (١/٣٣)، ميثاق الأمم المتحدة.[1] وفي حالة نشوب نزاع سيبراني بين دولتين يشجع ميثاق الأمم المتحدة على تسوية النزاع بطرق سلمية مثل المفاوضات أو التحكيم، وقد تكون الهجمات السيبرانية مصدرًا لتصاعد التوتر بين الدول ومن ثم يصبح التعاون الدولي والتسوية السلمية أمرًا ضروريًا لتجنب التصعيد.

٥- **مسؤولية الدول عن الهجمات السيبرانية:** بينما لا يحتوي ميثاق الأمم المتحدة على أحكام صريحة تتعلق بالمسؤولية عن الهجمات السيبرانية فإن القانون الدولي يفرض على الدول عدم استخدام أراضيها لشن هجمات على دول أخرى، هذا المبدأ ينطبق أيضًا على الفضاء السيبراني. وإذا سمحت دولة باستخدام بنيتها التحتية أو تقاعست عن منع الهجمات التي تنطلق من أراضيها ضد دول أخرى، فقد تُعتبر مسؤولة عن تلك الهجمات[2] لذلك تتحمل الدول المسؤولية القانونية عن الأفعال غير القانونية التي تنفذها عبر الفضاء السيبراني، سواء بشكل مباشر أو غير مباشر عبر وكلاء أو جهات غير حكومية. وإذا قامت دولة بتنفيذ أو دعم هجوم سيبراني على دولة أخرى، يمكن تحميلها المسؤولية بموجب القانون الدولي، وتتحمل التبعات القانونية مثل العقوبات أو المطالبة بالتعويض.[3]

٦- **دور مجلس الأمن – الفصل السابع** يمكن لمجلس الأمن وفقًا للفصل السابع من ميثاق الأمم المتحدة، أن يتخذ تدابير لحفظ أو إعادة السلم والأمن الدوليين بما في ذلك التصرف ضد الدول التي تشن هجمات سيبرانية تهدد السلام العالمي. المادتان ٣٩و٤٤، ميثاق الأمم المتحدة[4] فإذا اعتبر مجلس الأمن أن هجومًا سيبرانيًا يمثل تهديدًا للسلم والأمن الدوليين فإنه يمكنه اتخاذ

---

([1]) د. عيسى دباح، مصدر سابق، ص١٠٦.

(2) د. احمد ابو الوفا، النظرية العامة للقانون الدولي الإنساني، دار النهضة العربية، القاهرة ،٢٠٠٩، ص٨٤.

(3) د. احمد ابو الوفا، النظرية العامة للقانون الدولي الإنساني، مصدر سابق، ص٨٥.

(4) د. عيسى دباح، موسوعة القانون الدولي، مصدر سابق، ص١٠٨.

تدابير ضد الدولة المهاجمة، هذه التدابير قد تشمل العقوبات والقرارات، أو حتى استخدام القوة لحماية الأمن الدولي.

٧- **مبدأ المساءلة والشفافية:** من المهم في الحروب السيبرانية أن تتحمل الدول والمنظمات الدولية المسؤولية عن أفعالها، وأن تكون شفافة في أعمالها السيبرانية التي قد تؤثر على دول أخرى. اذ يجب أن تلتزم الدول بالإبلاغ عن الهجمات السيبرانية وتقديم الأدلة التي تدعم مزاعمها إذا تعرضت لهجمات، وذلك لتعزيز التعاون الدولي والحد من النزاعات.[1]

## المطلب الثاني

## الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني

ان تفجيرات أجهزة اتصال حزب الله اللبناني تتعلق بالصراع بين إسرائيل وحزب الله، حيث استهدفت إسرائيل أنظمة الاتصالات الخاصة بحزب الله أو منشآته المتعلقة بالاتصالات. وفي هذا السياق، يمكن تحليل تلك التفجيرات ضمن إطار (القانون الدولي الإنساني) الذي يضع قواعد صارمة لحماية المدنيين والبنية التحتية المدنية أثناء النزاعات المسلحة.[2]

ينظم القانون الدولي الإنساني النزاعات المسلحة ويهدف إلى حماية الأشخاص غير المشاركين في الأعمال القتالية، والقانون الدولي الإنساني الذي يُعرف أيضًا بقانون النزاعات المسلحة، وضع قواعد لتنظيم النزاعات المسلحة التقليدية[3] ولكنه لا يزال غامضًا فيما يتعلق بالنزاعات السيبرانية، على الرغم من أن اتفاقيات جنيف والبروتوكولات الإضافية لا تنص صراحة على الحرب السيبرانية، فإن بعض المبادئ العامة يمكن أن تطبق على هذا النوع من الحروب يجب أن تتماشى أي هجمات سيبرانية مع مبادئ التمييز والتناسب والضرورة العسكرية. [4] وفي حالة وجود نزاع مسلح ينطبق القانون الدولي الإنساني (قوانين الحرب) الذي يتطلب تجنب استهداف المدنيين أو البنية التحتية المدنية بشكل مباشر.

---

(1) عبد الرؤوف سعيد، الهجمات السيبرانية، مصدر سابق، ص ١٦٣.

(١) Jeffrey T. G Kelsey, Hacking in to international humanitarian law: The principles of distinction and neutrality in the age of cyber warfare, Michigan law review ,Vol2008, Issue7,106 P. 1437.

([3]) حسن الشمري، مصدر سابق، ص ١٥١.

(4) مايكل ن. شميت: الحرب بواسطة شبكات الاتصال الهجوم على شبكات الكمبيوتر (الحاسوب) والقانون في الحرب، المجلة الدولية للصليب الأحمر، مختارات من أعداد ٢٠٠٢، ص٩٠.

اما الهجمات السيبرانية التي تستهدف البنية التحتية المدنية مثل أنظمة المياه أو المستشفيات يمكن أن تُعتبر انتهاكًا لقوانين الحرب.

١- **مبدأ التمييز (Distinction)** مبدأ التمييز هو حجر الزاوية في القانون الدولي الإنساني، وينص على ضرورة التمييز في جميع الأوقات بين المقاتلين والمدنيين، وبين الأهداف العسكرية والأعيان المدنية. الهدف من هذا المبدأ هو حماية المدنيين والأعيان المدنية (مثل المدارس، المستشفيات، البنية التحتية المدنية) من الهجمات غير المبررة خلال النزاعات المسلحة.[1]

ويتعين على الأطراف المتحاربة توجيه هجماتهم فقط نحو الأهداف العسكرية التي تشمل المقاتلين والمرافق أو الأسلحة التي يستخدمها العدو، يجب أن تكون الهجمات موجهة فقط ضد من يشاركون مباشرة في الأعمال العدائية.[2] ويحظر الهجوم على الأعيان المدنية ما لم تُستخدم لأغراض عسكرية. يجب أن تكون الأهداف العسكرية واضحة، ويجب تجنب الهجمات على الأعيان المدنية التي لا تُستخدم في العمليات العسكرية.

وينص هذا المبدأ على ضرورة التمييز بين المقاتلين والمدنيين في سياق الحرب السيبرانية، قد يكون من الصعب تطبيق هذا المبدأ وخاصة إذا كانت الهجمات السيبرانية تستهدف البنية التحتية التي يستخدمها المدنيون.

ففي الحروب السيبرانية، قد يكون من الصعب تطبيق مبدأ التمييز بوضوح، لأن العديد من الأنظمة والبنية التحتية التي تستهدفها الهجمات السيبرانية تُستخدم لكل من الأغراض العسكرية والمدنية.[3]

على سبيل المثال، شبكات الاتصالات أو البنوك قد تُستخدم من قبل المدنيين والعسكريين على حد سواء، مما يعقد التمييز بين الأهداف المشروعة وغير المشروعة، اما إذا كانت أنظمة الاتصالات الخاصة بحزب الله تُستخدم لأغراض عسكرية، فقد تعتبر هدفًا عسكريًا مشروعًا بموجب القانون الدولي.

٢- **مبدأ التناسب (Proportionality)** مبدأ التناسب ينص على أنه حتى عندما يتم استهداف هدف عسكري مشروع، يجب أن تكون الخسائر في أرواح المدنيين أو الأضرار التي تلحق

---

(1) مايكل شميت، مصدر سابق، ص١٠٥.

(2) د. علي زعلان نعمة واخرون، القانون الدولي الإنساني، دار المسلة للنشر والتوزيع، ط٥ ،٢٠٢٣، ص١٢٧.

(3) علاء الدين بو مرعي: دراسات وتقارير: مبدأ التمييز، والأساليب والوسائل الحربية الحديثة دراسة على ضوء مبادئ القانون الدولي الإنسان– آذار ٢٠٢٣، المركز الاستشاري للدراسات والوثائق، لبنان، ص١٥.

بالأعيان المدنية متناسبة مع الميزة العسكرية المتوقعة من الهجوم. بمعنى آخر، يُحظر شن هجمات عسكرية إذا كانت الأضرار الجانبية على المدنيين غير متناسبة مع الفائدة العسكرية المرجوة.[1] لذلك يتعين على المخططين العسكريين إجراء تقييم دقيق قبل تنفيذ أي هجوم لتقدير الخسائر المحتملة بين المدنيين والتأكد من أن هذه الخسائر ليست مفرطة مقارنة بالأهمية العسكرية للهجوم. وإذا كان من الممكن تحقيق نفس الهدف العسكري بأقل خسائر بين المدنيين، يجب على الدولة المهاجمة اختيار البديل الذي يُقلل من الضرر على المدنيين والبنية التحتية المدنية. [2] ففي النزاعات السيبرانية، قد يكون تقدير "التناسب" صعبًا نظرًا لأن الهجمات السيبرانية قد تتسبب في تعطيل خدمات ضرورية للسكان المدنيين، مثل أنظمة المياه أو الكهرباء، دون التسبب مباشرة في إصابات أو خسائر في الأرواح.[3]

ولكن إذا أدى الهجوم السيبراني إلى تعطيل الخدمات الحيوية مما يتسبب في معاناة كبيرة للمدنيين، قد يُعتبر هذا انتهاكًا لمبدأ التناسب. وان مبدأ ا لتناسب يستوجب على الأطراف المتحاربة تجنب استخدام القوة بشكل يؤدي إلى إلحاق أضرار غير متناسبة بالأهداف العسكرية المرجوة في الحرب السيبرانية، يعني هذا المبدأ أن أي هجوم سيبراني يجب أن يتجنب التسبب في أضرار واسعة على المدنيين أو البنية التحتية المدنية إذا كانت تلك الأضرار غير متناسبة مع الفائدة العسكرية المتوقعة.[4]

ويجب ألا تؤدي الهجمات السيبرانية إلى أضرار جانبية مفرطة للمدنيين، فيحظر القانون الدولي الهجمات التي تسبب أضرارًا مفرطة مقارنة بالفائدة العسكرية المرجوة. ولكن في الحرب السيبرانية، من الصعب تقدير حجم الضرر مسبقًا، مما يثير تساؤلات حول كيفية تطبيق هذا المبدأ، والقانون الدولي يتطلب أن يكون الرد على الهجوم متناسبًا مع حجم الضرر ولكن في الهجمات السيبرانية، يمكن أن يكون من الصعب تحديد حجم الضرر الفعلي وتأثير الهجوم على المدى الطويل.

---

([1]) د. احمد ابو الوفا، النظرية العامة للقانون الدولي الإنساني، مصدر سابق، ص٨٢.

([2]) مايكل شميت، مصدر سابق، ص١٢١.

([3]) د. احمد عبيس نعمة الفتلاوي، الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية والسياسية جامعة بابل – كلية القانون، العدد الرابع، السنة الثامنة، ٢٠١٦، ص٦٣٨.

([4]) جودي ر. وستبي: دعوة إلى الاستقرار الجيو سيبراني، مقال منشور ضمن العمل الجماعي لدكتور حمدون إ. تورية: البحث عن السلام السيبراني، الاتحاد الدولي للاتصالات، يناير ٢٠١١، ص ٦.

٣- **مبدأ الضرورة العسكرية:** يجب أن تكون الهجمات السيبرانية ضرورية لتحقيق أهداف عسكرية مشروعة ومعينة وعدم استهداف المدنيين أو البنية التحتية الحيوية ما لم تكن هناك حاجة ملحة. ويزداد المبدأ تعقيداً عندما يكون الحدود بين الأهداف العسكرية وغير العسكرية غامضاً.[1] فهذا المبدأ ينص على أنه لا يجوز تنفيذ هجمات إلا إذا كانت ضرورية لتحقيق هدف عسكري مشروع. في الحروب السيبرانية، قد يشمل هذا المبدأ هجمات تستهدف تعطيل الأنظمة العسكرية للعدو أو الإضرار بقدرته على شن هجمات، بشرط أن تكون هذه الهجمات محددة وموجهة نحو تحقيق أهداف مشروعة.[2]

٤- **مبدأ الإنسانية:** يُلزم هذا المبدأ المتحاربين بالتصرف بطريقة إنسانية، وتجنب إلحاق الأذى بالمدنيين والأشخاص المحميين.[3]

في الحرب السيبرانية، قد يشمل هذا المبدأ تجنب شن هجمات تؤدي إلى تعطيل الخدمات الأساسية التي يحتاجها المدنيون، مثل المياه أو الكهرباء أو الرعاية الصحية.[4] وخلاصة القول ان مبدأ التمييز والتناسب هما أساسيات في القانون الدولي الإنساني لضمان أن العمليات العسكرية تلتزم بأخلاقيات الحرب وتُقلل من المعاناة المدنية، في حين أنه من الأسهل تطبيق هذه المبادئ في الحروب التقليدية التي تتضمن مقاتلين وأهدافًا مادية واضحة، تبرز تحديات كبيرة في تطبيقها على الحروب السيبرانية نظرًا للطبيعة المشتركة للبنية التحتية المدنية والعسكرية.

---

([1]) اياد محمد أبو مصطفى: مبدأ الضرورة العسكرية وانتهاكات قواعد القانون الدولي الإنساني "دراسة تطبيقية على مخالفة إسرائيل لمبدأ الضرورة العسكرية خلال حرب مايو ٢٠١٢"، مجلة جامعة الازهر-غزة، سلسلة العلوم الإنسانية، مج٢٣، ع٢، ٢٠٢١، ص٣٣٥.

([2]) د. علي زعلان نعمة واخرون، مصدر سابق، ص١١٧.

([3]) د. علي زعلان نعمة واخرون، القانون الدولي الإنساني، مصدر سابق، ص١٢٣.

([4]) مايكل شميت: الحرب بواسطة شبكات الاتصال الهجوم على شبكات الكومبيوتر (الحاسوب) والقانون في الحرب، مصدر سابق، ص ١٣٥.

## المطلب الثالث

## الهجمة السيبرانية الإسرائيلية ضد حزب الله ولبنان الاخيرة ومدى شرعيتها

بخصوص الهجمة السيبرانية الأخيرة على أجهزة اتصال حزب اللبناني ففي بيان له، حمل حزب الله إسرائيل المسؤولية الكاملة عن الهجوم، قائلا في بيان "نحمل العدو الإسرائيلي المسؤولية كاملة عن العدوان الذي طال المدنيين أيضا"

١- في سياق النزاع بين إسرائيل وحزب الله، غالبًا ما تتعرض لبنان والبنية التحتية المعلوماتية الخاصة بها لعمليات سيبرانية. تعتبر إسرائيل حزب الله تهديدًا أمنيًا رئيسيًا، وبالتالي، فإنها تعتبر الهجمات السيبرانية وسيلة لتعطيل القدرات العسكرية لحزب الله.

٢- إذا كانت الهجمات السيبرانية الإسرائيلية تستهدف فقط الأهداف العسكرية لحزب الله وتلتزم بمبادئ القانون الدولي الإنساني، فقد تكون مشروعة. ومع ذلك، يجب أن تتجنب استهداف المدنيين أو البنية التحتية الحيوية والمدنية أو أدت إلى أضرار جانبية كبيرة للمدنيين، فإنها قد تُعتبر انتهاكًا للقانون الدولي، مما قد يؤدي إلى محاسبة قانونية.[1] ويعد النزاع بين إسرائيل وحزب الله سياقًا معقدًا، حيث يختلف تقييم المجتمع الدولي لمشروعية الهجمات حسب الظروف والتداعيات.

وبشكل عام، فإن مشروعية الهجمات السيبرانية تعتمد على السياق والأهداف، ويستمر النقاش حول كيفية تطبيق القانون الدولي في هذا المجال المتطور، ولا تزال الهجمات السيبرانية تحتاج إلى مزيد من التنظيم القانوني الدولي.[2] وهي – المشروعية – تعتمد على الالتزام بالقوانين الدولية المعمول بها، ويجب أن تكون أي هجمات متناسبة مع الأهداف العسكرية المحددة. وتعد مسألة المسؤولية عن الهجمات السيبرانية تحديًا كبيرًا في القانون الدولي، ان إحدى المشاكل الرئيسية هي تحديد الجهة المسؤولة عن الهجوم، حيث يمكن للمهاجمين السيبرانيين استخدام تقنيات التمويه وتوجيه الهجمات من خلال دول أو أنظمة مختلفة، مما يصعب عملية التحديد الدقيق للمسؤولين.[3]

---

([1]) كورديولا درويغ: الحرب السيبرانية والقانون الدولي الإنساني: كيف نحمي المدنيين من الآثار العرضية لهجوم إلكتروني؟ مجلة الإنساني، ع٥٢، مارس ٢٠١١، متاح على الرابط التالي: https://blogs.icrc.org/alinsani/2011/03/20/5043 (٢٠٢٤/٧/١٩).

([2]) د. سامر الشامي، إسرائيل وحزب الله، مصدر سابق، ص ١٥٧.

([3]) مايكل شميت، مصدر سابق، ص١٣٠.

ووفقًا لمبادئ القانون الدولي، يمكن للدولة التي تتعرض لهجوم سيبراني أن تطالب الدولة المسؤولة بالتعويض عن الأضرار الناتجة عن هذا الهجوم، ولكن يتطلب ذلك تقديم أدلة قاطعة على مسؤولية الدولة المعتدية.

في هذا السياق، يُطرح تساؤل حول مدى إمكانية اعتبار الهجمات السيبرانية بمثابة "هجمات مسلحة" بالمعنى الوارد في ميثاق الأمم المتحدة، والذي يسمح للدول بالدفاع عن نفسها في حالة وقوع هجوم مسلح[1] فبالرغم من أن القانون الدولي لم يُصمم في الأصل للتعامل مع التهديدات السيبرانية، إلا أن المبادئ التقليدية للقانون الدولي، مثل السيادة، عدم التدخل، استخدام القوة، والدفاع عن النفس، يمكن أن تنطبق على النزاعات السيبرانية.

ومع ذلك، تبقى هناك حاجة إلى تطوير إطار قانوني واضح ومنسق لمعالجة التحديات الفريدة التي تطرحها الحرب السيبرانية، وخاصة فيما يتعلق بتحديد المسؤولية وتطبيق مبادئ القانون الإنساني الدولي [2]اذ ان القانون الدولي قد وُضع في الأصل لتنظيم النزاعات المسلحة التقليدية، إلا أنه يحتوي على مبادئ يمكن تطبيقها على الحروب السيبرانية. ومع ازدياد الهجمات السيبرانية والتأثير المتنامي لها على البنية التحتية والأمن الدولي، أصبح من الضروري دراسة كيفية تطبيق هذه المبادئ على هذا النوع من النزاعات.[3]

ويبقى ميثاق الأمم المتحدة هو الأساس الذي يُنظم العلاقات بين الدول في إطار القانون الدولي، وقد تم وضعه في عام ١٩٤٥، بالرغم رغم أن الميثاق لا يتناول صراحةً الحرب السيبرانية، فإن المبادئ الأساسية للميثاق، مثل حظر استخدام القوة واحترام السيادة، يمكن أن تُطبق على النزاعات السيبرانية. فيما يلي توضيح لكيفية تطبيق هذه المبادئ في سياق الحرب السيبرانية.

يمكن أن نبدأ بالتساؤل حول إمكانية اعتبار الهجمات السيبرانية استخدامًا للقوة، اذ ليس هناك اتفاق واضح بين الدول على أن الهجمات السيبرانية تُعتبر دائمًا (استخدامًا للقوة) بموجب المادة (٤/٢) من

(1) سعاد إبراهيم، الحروب السيبرانية والقانون الدولي الإنساني، مصدر سابق، ص ٧٦.

(2) عبد الله زهير، الحروب السيبرانية في القانون الدولي العام، مصدر سابق، ص ٥٣.

(3) د. عصام العطية، القانون الدولي العام، مصدر سابق، ص١٢٩.

ميثاق الأمم المتحدة[1] ولكن هناك عدة عوامل يمكن أن تجعل الهجمات السيبرانية تُعتبر استخدامًا للقوة: –

**الأثر المادي:** إذا أدت الهجمات السيبرانية إلى أضرار مادية كبيرة، مثل تدمير بنية تحتية حساسة، تعطيل المرافق الحيوية أو تهديد حياة المدنيين، فقد تُعتبر استخدامًا للقوة.

على سبيل المثال، تعطيل شبكة الكهرباء أو أنظمة الاتصالات بشكل يؤدي إلى أضرار اقتصادية هائلة أو تهديد مباشر للأمن الوطني قد يرقى إلى مستوى استخدام القوة.

**التهديد العسكري أو الأمني:** إذا كانت الهجمات السيبرانية جزءًا من عمل عسكري أكبر أو إذا شكلت تهديدًا للأمن الوطني بشكل مباشر، فقد تكون مشابهة للهجمات العسكرية التقليدية.[2]

ونتساءل هل الهجمات الإسرائيلية تُعد استخدامًا غير مشروع للقوة؟ لتحديد ما إذا كانت الهجمات الإسرائيلية تُعتبر استخدامًا غير مشروع للقوة بموجب ميثاق الأمم المتحدة، يجب النظر فيما إذا كانت هذه الهجمات تفي بشروط الدفاع عن النفس بموجب المادة (٥١) من ميثاق الأمم المتحدة.[3]

فإذا زعمت إسرائيل أن الهجمات السيبرانية تأتي في إطار الدفاع عن النفس ضد هجمات سيبرانية أو تقليدية من حزب الله أو من لبنان فقد تحاول تبريرها، مع ذلك يجب أن يكون هذا الدفاع مشروعًا وفقًا للشروط التي تتطلب وجود هجوم مسلح وأن تكون الهجمات الإسرائيلية متناسبة مع التهديد. وإذا لم تستطع إسرائيل إثبات أن الهجمات كانت دفاعية أو أنها كانت ردًا على تهديد وشيك، فقد تُعتبر هذه الهجمات استخدامًا غير مشروع للقوة بموجب المادة (٤/٢) من ميثاق الأمم المتحدة.[4]

والخلاصة الهجمات السيبرانية الإسرائيلية ضد لبنان قد تُعتبر انتهاكًا للسيادة اللبنانية، خاصة إذا استهدفت البنية التحتية الحيوية دون مبرر قانوني، فالهجمات السيبرانية يمكن اعتبارها استخدامًا غير مشروع للقوة إذا كانت ذات تأثير كبير على البنية التحتية أو الأمن اللبناني، خاصةً إذا لم تستطع إسرائيل إثبات أنها تمثل دفاعًا مشروعًا وفقًا للمادة (٥١) من ميثاق الأمم المتحدة.

---

(1) د. عيسى دباح، موسوعة القانون الدولي، مصدر سابق، ص١٠٠.

(2) عبد الرؤوف سعيد، الهجمات السيبرانية، مصدر سابق، ص ١٤٧.

(3) عبد الله زهير، الحروب السيبرانية في القانون الدولي العام، مصدر سابق، ص٧٩.

(4) د. عيسى دباح، مصدر سابق، ص١٠٠.

١- **دور المنظمات الدولية:** فالأمم المتحدة وحلف شمال الأطلسي (الناتو)، قد تلعب دورًا في تنظيم الردود الدفاعية على الهجمات السيبرانية، ويمكن أن تتدخل هذه المنظمات للمساعدة في تنسيق الردود، وتحديد المسؤوليات، وتقديم المساعدة التقنية، وفرض العقوبات على الدول التي تقوم بشن هجمات سيبرانية. [1]

ان دور المنظمات الدولية قد يكون حاسمًا في حل النزاعات المتعلقة بالهجمات السيبرانية، يمكن للبنان أن يلجأ إلى المجتمع الدولي للضغط على إسرائيل لوقف الهجمات السيبرانية أو لطلب تحقيق دولي في الانتهاكات المحتملة من جهة أخرى، قد تستفيد إسرائيل من دعم حلفائها لتبرير دفاعها السيبراني ضد التهديدات التي تشعر بها.

فمن منظور القانون الدولي ان الهجمات السيبرانية الإسرائيلية ضد لبنان وحزب الله قد تواجه تحديات قانونية كبيرة. يجب أن تلتزم إسرائيل بمبادئ السيادة وحق الدفاع عن النفس وكذلك القانون الدولي الإنساني. في حين أن إسرائيل قد تبرر هذه الهجمات كدفاع عن النفس ضد التهديدات المباشرة أو الوشيكة.[2]

إلا أن مدى احترامها للضرورات القانونية مثل التناسب والتمييز بين الأهداف العسكرية والمدنية، يظل موضع تساؤل. وان مبدأ الدفاع عن النفس في الهجمات السيبرانية يخضع لتفسير مبادئ القانون الدولي التقليدي، مع الأخذ في الاعتبار الخصائص الفريدة للهجمات السيبرانية[3] فالهجمات السيبرانية التي تُلحق أضرارًا جسيمة بالبنية التحتية أو تُهدد الأمن القومي يمكن أن تُبرر الدفاع عن النفس وفقًا للمادة (٥١) من ميثاق الأمم المتحدة، بشرط أن تتوافر شروط الضرورة والتناسب.

---

(1) عبد الرؤوف سعيد، الهجمات السيبرانية، مصدر سابق، ص ١٣٢.

(2) د. حسين علي، حزب الله في العصر الرقمي، الأمن الإلكتروني والتهديدات الإسرائيلية، دار المعارف، ٢٠١٩، ص٨٤.

(3) سعاد إبراهيم، الحروب السيبرانية والقانون الدولي الإنساني، مصدر سابق، ص ٩٧.

## الخاتمة

في نهاية بحثنا هذ توصلنا الى النتائج والتوصيات الاتية:

### أولا: النتائج

١. السيبرانية انتهاك للسيادة: تُظهر الهجمات السيبرانية الإسرائيلية ضد لبنان احتمالية انتهاك السيادة اللبنانية. حيث تُعتبر البنية التحتية السيبرانية جزءًا لا يتجزأ من سيادة الدولة، وبالتالي فإن أي تدخل خارجي دون موافقة يُعد انتهاكًا لهذه السيادة.

٢.استخدام غير مشروع للقوة: في حالة عدم إثبات إسرائيل أن هجماتها كانت دفاعية ومبررة بموجب المادة (٥١) من ميثاق الأمم المتحدة، فإنها قد تُعتبر استخدامًا غير مشروع للقوة، خصوصًا إذا كانت هذه الهجمات تُلحق أضرارًا جسيمة بالبنية التحتية المدنية أو تهدد أمن المدنيين.

٣.التحديات القانونية في تحديد الهجوم السيبراني" كهجوم مسلح": تحديد ما إذا كان الهجوم السيبراني يمكن أن يُصنف كـ"هجوم مسلح" بموجب القانون الدولي يمثل تحديًا، حيث يعتمد ذلك على حجم الأضرار وتأثيرها. الهجمات السيبرانية التي تُسبب أضرارًا مادية كبيرة أو تهديدًا للأرواح قد تُعتبر هجومًا مسلحًا، بينما الهجمات الأقل تأثيرًا قد لا تبرر الرد العسكري.

٤.غموض المعايير القانونية: رغم محاولات تطوير المعايير الدولية المتعلقة بالهجمات السيبرانية، لا يزال هناك غموض حول كيفية تطبيق مبادئ القانون الدولي التقليدي على الفضاء السيبراني. ما يؤدي إلى احتمالية إساءة استخدام هذا الفضاء بشكل يتعارض مع القانون الدولي.

### ثانيا: المقترحات

١.تطوير إطار قانوني دولي واضح للهجمات السيبرانية: هناك حاجة ملحة لتطوير إطار قانوني دولي محدد يحكم الهجمات السيبرانية. يجب أن يتضمن هذا الإطار تعريفًا واضحًا لما يُعد "هجومًا سيبرانيًا" وما إذا كان يمكن تصنيفه كـ"استخدام للقوة" أو "هجوم مسلح". إضافةً إلى ذلك، ينبغي أن يشمل توجيهات حول كيفية تقييم التناسب والتمييز في النزاعات السيبرانية.

٢-تعزيز التعاون الدولي في مجال الدفاع السيبراني: يُنصح الدول بتعزيز التعاون فيما بينها من خلال اتفاقيات دفاعية تُعنى بالهجمات السيبرانية. هذا يشمل التعاون في تبادل المعلومات الاستخبارية وتنسيق الردود السيبرانية، بما يضمن الدفاع عن الدول بشكل مشروع دون انتهاك للقوانين الدولية.

٣.إدخال الفضاء السيبراني ضمن القوانين الدولية الإنسانية: يجب تحديث قوانين النزاعات المسلحة لتشمل صراحةً الهجمات السيبرانية. يجب أن تضمن هذه القوانين حماية المدنيين والبنية التحتية المدنية، مع التمييز بين الأهداف العسكرية والمدنية في الفضاء السيبراني.

٤.تشجيع التحقيقات الدولية في الهجمات السيبرانية: يُفضل تعزيز دور المنظمات الدولية مثل الأمم المتحدة والمحكمة الجنائية الدولية في التحقيق في الهجمات السيبرانية ذات التأثير الكبير على السيادة والسلامة الإقليمية للدول. هذا سيساهم في وضع سوابق قانونية ويشجع الالتزام بالقوانين الدولية.

٥.الاستثمار في الدفاع السيبراني: على الدول أن تستثمر في تقنيات وأنظمة دفاعية قوية لحماية بنيتها التحتية السيبرانية من الهجمات الخارجية. تعزيز القدرات الدفاعية السيبرانية الوطنية سيساهم في تقليل الحاجة إلى الردود العسكرية ويعزز السيادة الرقمية.

**أولا: المصادر باللغة العربية**

- **الكتب والمواثيق الدولية: -**

١- د. احمد ابو الوفا، النظرية العامة للقانون الدولي الإنساني، دار النهضة العربية، القاهرة، ٢٠٠٩.

٢- احمد عيسى الفتلاوي: الهجمات السيبرانية "دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر، ط١، منشورات زين الحقوقية، بيروت، ٢٠١٨.

٣- أمير فرج يوسف: جريمة مكافحة الإرهاب الالكتروني -الإرهاب الرقمي- في ظل اتفاقية دول مجلس التعاون لمكافحة الارهاب، ط١، دار الكتب والدراسات العربية، الإسكندرية، ٢٠١٦.

٤- د. علي زعلان نعمة واخرون، القانون الدولي الإنساني، دار المسلة للنشر والتوزيع، ط٥، بغداد،٢٠٢٣.

٥- د. عصام العطية، القانون الدولي العام، دار السنهوري، بيروت، ٢٠١٥.

٦- د. عيسى دباح، موسوعة القانون الدولي، دار الشروق المجلد الثالث، ٢٠٠٣

٧- د. سامر الشامي، إسرائيل وحزب الله: الصراع الإلكتروني، دار الشروق للنشر، ٢٠١٨.

٨- د. حسين علي، حزب الله في العصر الرقمي، الأمن الإلكتروني والتهديدات الإسرائيلية، دار المعارف، ٢٠١٩.

٩- فادي عبد الله، إسرائيل والحروب الإلكترونية، منظور قانوني، دار الفكر المعاصر، ٢٠١٧.

١٠- مازن كنعان، حرب الشبكات الإلكترونية، حزب الله وإسرائيل، دار الأمة، ٢٠٢٠.

١١- حسن الشمري، القانون الدولي الإنساني والحروب السيبرانية، دار النهضة العربية، ٢٠١٨.

١٢- جاد صبحي، الحرب الإلكترونية في الشرق الأوسط: دور إسرائيل وحزب الله، دار الهلال، ٢٠٢١.

١٣- علي مصطفى، حروب الفضاء السيبراني: التهديدات الإسرائيلية لحزب الله ولبنان، دار النشر الحديثة، ٢٠٢٠.

١٤- عبد الرؤوف سعيد، الهجمات السيبرانية: الأطر القانونية الدولية، دار الثقافة، ٢٠١٨.

١٥- نضال أحمد، إسرائيل والتكنولوجيا السيبرانية: تهديدات إلكترونية لحزب الله، مركز الدراسات العربية، ٢٠٢١.

١٦- سعاد إبراهيم، الحروب السيبرانية والقانون الدولي الإنساني، دار الشرق، ٢٠٢٠.

١٧- عبد الله زهير، الحروب السيبرانية في القانون الدولي العام، دار النشر العلمي، ٢٠١٩.
١٨- ميثاق الامم المتحدة.

**البحوث المنشورة: -**

١- د. احمد عبيس نعمة الفتلاوي، الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية والسياسية جامعة بابل – كلية القانون، العدد الرابع، السنة الثامنة، ٢٠١٦.
٢- د. انعام عبد الرضا سلطان العكابي: توظيف الحروب السيبرانية في تطوير مفهوم القوة للدول الكبرى، ع٧٣، مجلة قضايا سياسية، جامعة النهرين، ٢٠٢٣.
٣- اياد محمد أبو مصطفى: مبدأ الضرورة العسكرية وانتهاكات قواعد القانون الدولي الإنساني "دراسة تطبيقية على مخالفة إسرائيل لمبدأ الضرورة العسكرية خلال حرب مايو ٢٠١٢"، مجلة جامعة الازهر–غزة، سلسلة العلوم الإنسانية، مج٢٣، ع٢، ٢٠٢١.
٤- د. بن تغري موسى: الحرب السيبرانية والقانون الدولي الإنساني، مجلة الاجتهاد القضائي، مج١٢، عدد خاص (العدد التسلسلي ٢٢)، جامعة محمد خيضر بسكرة، الجزائر، ٢٠٢٠.
٥- جودي ر. وستبي: دعوة إلى الاستقرار الجيو سيبراني، مقال منشور ضمن العمل الجماعي لدكتور حمدون إ. تورية: البحث عن السلام السيبراني، الاتحاد الدولي للاتصالات، يناير ٢٠١١.
٦- د. شويرب جيلالي وفائزة دمراد: مفهوم الحروب السيبرانية والامن السيبراني، مج١١، ع١، مجلة الحقوق والحريات، جامعة محمد خيدر بسكرة، الجزائر، ٢٠٢٣.
٧- علاء الدين بو مرعي: دراسات وتقارير: مبدأ التمييز، والأساليب والوسائل الحربية الحديثة دراسة على ضوء مبادئ القانون الدولي الإنسان–آذار٢٠٢٣، المركز الاستشاري للدراسات والوثائق، لبنان.
٨- كوردولا دوريجي: لا تقترب من حدود فضائي الإلكتروني، الحرب الإلكترونية والقانون الدولي الإنساني وحماية المدنيين، مجلة اللجنة الدولية للصليب الأحمر، مج٩٤، ع٨٨٦، ٢٠١٢.
٩- كورديولا درويغ: الحرب السيبرانية والقانون الدولي الإنساني: كيف نحمي المدنيين من الآثار العرضية لهجوم إلكتروني؟ مجلة الإنساني، ع٥٢، مارس ٢٠١١، متاح على الرابط

التالي: https://blogs.icrc.org/alinsani/2011/03/20/5043 تاريخ الاطلاع (٢٠٢٤/٧/١٩).

١٠-مايكل ن. شميت: الحرب بواسطة شبكات الاتصال الهجوم على شبكات الكمبيوتر (الحاسوب) والقانون في الحرب، المجلة الدولية للصليب الأحمر، مختارات من أعداد ٢٠٠٢.

١١-نهى عبد الخالق احمد و د. سلوى احمد ميدان: المسؤولية الدولية عن استغلال الأطفال في القانون الدولي الإنساني، مجلة كلية القانون للعلوم القانونية والسياسية، مج١١، ٢٠٢٢.

١٢-نورة شلوش: القرصنة الالكترونية في الفضاء السيبراني "التهديد المتصاعد من الدول"، مجلة مركز بابل للدراسات الإنسانية، مج٨، ع٢، جامعة بابل، ٢٠١٨.

١٣-د. راجي يوسف محمود البياتي: الإرهاب السيبراني نماذج من الجهود الدولية للحد منه، مجلة تكريت للعلوم السياسية، ع٢٨، ٢٠٢٢.

١٤-وفاء بوكابوس: تحول القوة في العلاقات الدولية "دراسة في انتقال القوة من التقليدية الى الحديثة"، ط١، المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية، المانيا، ٢٠١٩.

**ثانياً: المصادر باللغة الإنكليزية: -**

1- law: The Jeffrey T. G Kelsey, Hacking in to international humanitarian principles of distinction and neutrality in the age of cyber warfare, .Michigan law review, Vol.106Issue ,7 ,2008.
2- Shane M, Coughlan: “Is there a common understanding of what constitutes cyber warfare?, master theses, University of Birmingham ,School of Politics and International Studies30 September 2003 .