ISSN: 2663-5798 || Arab Journal for Scientific Publishing

الإصدار الثامن – العدد السادس والثمانون
تاريخ الإصدار: 2 – كانون الأول – 2025م
www.ajsp.net

"تحديات القانون الدولي في مواجهة التهديدات السيبرانية"

إعداد الباحثان:

د. جيهان حمية

أستاذ باحث في القانون الجنائي الدولي

موسى البزال

باحث في القانون الدولي العام

1446هـ-2025 م

https://doi.org/10.36571/ajsp861

ISSN: 2663-5798 || Arab Journal for Scientific Publishing

الإصدار الثامن – العدد السادس والثمانون
تاريخ الإصدار: 2 – كانون الأول – 2025م
www.ajsp.net

الملخّص:

يتناول هذا البحث التحديات المتصاعدة التي يفرضها الفضاء السيبراني على القانون الدولي، ولا سيما مع تطوّر الهجمات الرقمية المدعومة بالذكاء الاصطناعي. فقد أدّت الطبيعة غير المادية لهذه الهجمات وصعوبة إسنادها إلى دولة محددة إلى خلق فراغ قانوني واضح، الأمر الذي أضعف فعالية قواعد المسؤولية الدولية وحدّ من قدرة المنظومة الدولية على مواجهة التهديدات السيبرانية بكفاءة. ويستعرض البحث الإطار النظري للتهديدات الرقمية، والجهود الأممية والإقليمية في تنظيم السلوك السيبراني، إضافةً إلى دراسة حالات تطبيقية أبرزت هشاشة البنى الرقمية. ويخلص إلى ضرورة وضع منظومة قانونية عالمية أكثر تطورًا، وإلى أهمية بناء تعاون دولي فعّال يواكب سرعة الابتكار التقني.

الكلمات المفتاحية: الأمن السيبراني – الهجمات السيبرانية – الذكاء الاصطناعي –المسؤولية الدولية –القانون الدولي – الحرب السيبرانية.

المقدمة:

يشهد العالم في العقود الأخيرة تحوّلًا جذريًا بفعل الثورة الرقمية والتطور المتسارع في تقنيات الإتصال والمعلومات، الأمر الذي أفرز فضاءً جديدًا للنشاط الإنساني يُعرف بـ الفضاء السيبراني، والذي أصبح ميدانًا حيويًا تتقاطع فيه المصالح السياسية والإقتصادية والعسكرية للدول. غير أنَّ هذا الفضاء لم يخلُ من التهديدات والمخاطر التي تجاوزت الحدود الجغرافية التقليدية، فأضحت الهجمات السيبرانية من أبرز مظاهر النزاعات الحديثة التي تهدد الأمن والسلم الدوليين، وتطرح تساؤلات قانونية عميقة حول مدى قدرة القانون الدولي على مواكبة هذه التحولات.

ومع تصاعد الإعتماد على الذكاء الإصطناعي في تطوير وتنفيذ الهجمات السيبرانية، ازدادت خطورة هذه التهديدات وتعقيدها، إذ أصبح من الصعب تحديد الفاعل المسؤول عنها أو إسنادها إلى دولة بعينها، مما أوجد فراغًا قانونيًا واضحًا في ميدان المسؤولية الدولية. وقد تبيّن أنَّ الإطار القانوني الدولي القائم بما في ذلك ميثاق الأمم المتَّحدة والإتفاقيات الدولية ذات الصلة لم يعد كافيًا لتنظيم هذا الفضاء الجديد وضبط السلوك السيبراني بين الدول.

أهمية البحث:

تكمن أهمية هذا البحث في تسليطه الضوء على التهديدات السيبرانية المعززة بالذكاء الاصطناعي، التي تشكل خطرًا متناميًا على أمن الدول وسيادتها الرقمية وبنيتها التحتية الحيوية، مع إبراز الإشكاليات القانونية الناجمة عن غياب إطار دولي ملزم ينظّم الفضاء السيبراني، والحاجة الملحّة لتطوير قواعد قانونية تتوافق مع سرعة التطور التقني وتحافظ على التوازن بين الأمن السيبراني وحقوق الإنسان الرقمية.

أسباب اختيار الموضوع

يُعزى اختيار هذا الموضوع إلى عدة اعتبارات، من أهمها:

1. تعقيد التهديدات السيبرانية، تهديدات متطورة تشكل خطرًا على الأمن الدولي، خاصة مع استخدام الذكاء الاصطناعي.
2. غياب إطار قانوني دولي واضح، نقص في تحديد المفهوم السيبراني ومسؤولية الدول عن الأفعال الضارة.
3. ضعف التعاون الدولي والإقليمي، تحديات في التنسيق والكشف عن الفاعلين وإثبات الإسناد السيبراني.
4. تأثير الفضاء السيبراني على النظام الدولي، تغير موازين القوة والحاجة لربط التطورات التقنية بالإطار القانوني.
5. الرغبة في المساهمة العلمية في إثراء النقاش القانوني حول هذا المجال الناشئ، وربط التطورات التقنية بالإطار القانوني الدولي.

أهداف البحث

يهدف هذا البحث إلى تحقيق مجموعة من الأهداف، أبرزها:

1. توضيح المفهوم وحدوده في القانون الدولي مع دراسة التهديدات السيبرانية وأسباب تناميها ومخاطرها على الأمن الدولي.
2. تحليل المبادرات المبذولة لمواجهة التهديدات وتقييم فعاليتها القانونية، مع كشف أوجه القصور في الإتفاقيات الدولية.
3. تسليط الضوء على التحديات العملية للهجمات السيبرانية المعززة بالذكاء الاصطناعي، ودراسة تأثيرها على النظام القانوني الدولي والممارسات القائمة.
4. تعزيز الأمن السيبراني وتحقيق التوازن بين الحماية والأمن من جهة، واحترام الحقوق والحريات الرقمية من جهة أخرى.

فرضيات البحث

ينطلق هذا البحث من الفرضيات التالية:

1. أن الإطار القانوني الدولي الحالي غير كافٍ لمواجهة التهديدات السيبرانية المعقّدة، ولا سيما تلك المدعومة بالذكاء الإصطناعي .
2. أنَّ غموض الطبيعة القانونية للهجمات السيبرانية يعيق مساءلة الدول والفاعلين عن أفعالهم في الفضاء الرقمي.
3. أنَّ جهود المؤسسات الدولية رغم أهميتها، ما زالت محدودة وتعاني من غياب التنسيق والإلتزام الملزم بين الدول.
4. أنَّ تحقيق الأمن السيبراني الدولي الفعّال يتطلب تطوير آليات قانونية مشتركة تراعي مسألة الإستفادة من تقنياتالذكاء الإصطناعي.

إشكالية البحث

تتمحور الإشكالية الرئيسة لهذا البحث حول التساؤل الآتي:

"إلى أي مدى يستطيع القانون الدولي مواكبة التهديدات السيبرانية المستقبلية المعزّزة بالذكاء الاصطناعي؟"

الأسئلة المتفرعة عن الإشكالية، لأجل مقاربتها، تُطرح الأسئلة الفرعية التالية:

1. ما الأساس القانوني للأمن السيبراني؟
2. ما طبيعة التهديدات السيبرانية الراهنة؟
3. ما مدى فعالية الجهود الدولية في التصدي لها؟
4. كيف أثّر الذكاء الاصطناعي في تعقيدها؟

منهجية البحث

سيتّبع هذا البحث المنهج الوصفي والتحليلي:

1. المنهج الوصفي: لتوصيف ظاهرة التهديدات السيبرانية ومكوناتها، وبيان المفاهيم القانونية ذات الصلة، واستعراض الجهود الدولية في هذا المجال.
2. المنهج التحليلي: لتحليل النصوص القانونية الدولية ذات الصلة (كميثاق الأمم المتحدة، واتفاقية بودابست، وقواعد تالين)، وتقييم مدى كفايتها لمواجهة التهديدات السيبرانية المعززة بالذكاء الاصطناعي، مع تحليل حالات واقعية ودراسة آثارها القانونية والسياسية.

هيكلية البحث

جاء البحث في فصلين رئيسيين على النحو الآتي:

- **الفصل الأول: الإطار النظري والقانوني للتهديدات السيبرانية**
  - المبحث الأول: مفهوم الأمن والتهديد السيبراني
  - المبحث الثاني: الجهود الدولية في مكافحة التهديدات السيبرانية
- **الفصل الثاني: تحديات الهجمات السيبرانية المعزّزة بالذكاء الاصطناعي**
  - المبحث الأول: التحديات التي تواجه الجهود الدولية لضبط السلوك السيبراني الدولي
  - المبحث الثاني: الأثر العملي للتهديدات السيبرانية الذكية
- **الخاتمة: تضمنت أهم النتائج التي توصلنا إليها، والمقترحات.**
- **المراجع.**

الفصل الأول: الإطار النظري والقانوني للتهديدات السيبرانية

يشهد العالم توسعًا متسارعًا في الاعتماد على الفضاء الرقمي، الأمر الذي جعل الأمن السيبراني عنصرًا أساسيًا لحماية المعلومات وضمان استقرار الدول والمؤسسات. وقد أدّى تنامي الهجمات الإلكترونية وتطوّر أساليبها إلى بروز حاجة ملحّة لفهم طبيعة التهديدات الرقمية وآثارها القانونية والأمنية.

ونظرًا للطابع العابر للحدود للفضاء السيبراني، أصبحت التهديدات الإلكترونية تتجاوز القدرات الوطنية، مما استدعى تعزيز التعاون الدولي[1] . وقد أكدت القمة العالمية لمجتمع المعلومات (2003 و2005) على ضرورة وضع أطر قانونية ومؤسسية مشتركة لتعزيز حماية الفضاء السيبراني والحد من الجرائم المعلوماتية. كما أسهمت الأمم المتحدة والمنظمات الدولية والإقليمية في تطوير منظومة معيارية وتقنية تنظّم هذا المجال.

وبناءً على ذلك، يتناول هذا الفصل محورين رئيسين:
المبحث الأول :مفهوم الأمن السيبراني والتهديدات الرقمية.
المبحث الثاني :الجهود الدولية في مكافحة التهديدات السيبرانية.

المبحث الأول: مفهوم الأمن والتهديد السيبراني

بدأ مفهوم الأمن السيبراني يكتسب اهتمامًا واسعًا منذ أن استخدمه الرئيس الأمريكي السابق باراك أوباما عام 2009، باعتباره عنصرًا أساسيًا في تعزيز الأمن القومي الأمريكي . ومع التطور السريع لتكنولوجيا المعلومات وانتشار الإنترنت، بات الفضاء السيبراني يشكل تحديًا أمنيًا واقتصاديًا عالميًا، خاصة مع تزايد اعتماد الدول على الأنظمة الرقمية في المجالات الحيوية والعسكرية، مما أدى إلى ظهور تهديدات سيبرانية معقدة يصعب إدراكها حتى من قبل المختصين.

وعليه تم تقسيم هذا المبحث إلى مطلبين، تناول المطلب الأول ماهية الأمن السيبراني، أمّا الثاني تمحور حول تصنيف ومخاطر التهديدات السيبرانية.

[1]– تامر أحمد، **الهجمات على شبكات الحاسوب في القانون الدولي الإنساني**، رسالة دكتوراه، كلية الحقوق، جامعة النهرين، العراق، 2015، ص 64.

المطلب الأول: ماهية الأمن السيبراني

الأمن السيبراني (Cyber security): هو مجموعة الممارسات والتقنيات والعمليات المصممة لحماية الشبكات والأجهزة والبرامج والبيانات من الهجوم أو التلف أو الوصول غير المصرح به. بعبارة أخرى، هو فن وعلم حماية الفضاء السيبراني بكل مكوناته من التهديدات الرقمية. لا يقتصر مفهومه على الحلول التقنية مثل برامج مكافحة الفيروسات أو جدران الحماية، بل يمتد ليشمل أطرًا سياسية وتشريعية، وعمليات إدارية، وممارسات فردية تهدف جميعها إلى تحقيق بيئة رقمية آمنة وموثوق[2].

ينقسم هذا المطلب إلى فرعين، الأول يتناول أنواع الأمن السيبراني، والثاني يركز على أسباب تنامي التهديدات السيبرانية

الفرع الأول: أنواع الأمن السيبراني

يتكوّن الأمن السيبراني من مجالات فرعية متكاملة تهدف إلى حماية الفضاء الرقمي من التهديدات والهجمات الإلكترونية، ولكل مجالٍ منها بُعدٌ قانوني وتقني يحدّد مسؤوليات الفاعلين والتزاماتهم في البيئة الرقمية[3]:

أ- **أمن الشبكات**(Network Security): يُعنى هذا النوع بحماية البنية التحتية للشبكات من الاختراقات، أو الوصول غير المصرّح به، أو التعطيل المتعمّد. ويشمل ذلك حماية مكوّنات الشبكة من أجهزة التوجيه والمبدّلات وأنظمة التشغيل. وتُعدّ القواعد القانونية الدولية التي تنظّم استخدام الفضاء السيبراني في هذا السياق (مثل مبادئ حظر التدخل في الشؤون الداخلية للدول) إطارًا مرجعيًا لحماية سيادة الدول الرقمية وضمان أمن شبكاتها الوطنية[4] .

ب- **جدران الحماية**(Firewalls): تمثّل جدران الحماية خط الدفاع الأول بين الشبكات الداخلية الموثوقة والشبكات الخارجية غير الموثوقة، كالإنترنت. وهي تُطبّق سياسات أمنية تحدّد ما يُسمح بمروره أو يُحظر من حركة البيانات. وتُعتبر من متطلبات "العناية الواجبة" التي تفرضها التشريعات الوطنية لحماية الأنظمة الحيوية من الاختراقات، كما هو منصوص عليه في قوانين حماية البنى التحتية المعلوماتية[5].

ج- **أنظمة كشف ومنع التسلل**(Intrusion Detection and Prevention Systems – IDS/IPS) : تعمل هذه الأنظمة على مراقبة حركة المرور داخل الشبكة لرصد الأنشطة المشبوهة أو غير المصرّح بها. وعند اكتشاف تهديد محتمل، تُصدر تنبيهًا أو

---

[2]– سمير باي، التهديدات الأمنية السيبرانية: دراسة في انعكاسات الحرب الإلكترونية على الأمن القومي للدول واستراتيجيات المقاومة، **مجلة الرسالة للدراسات والبحوث الإنسانية**، المجلد 8، العدد 2، 2023، ص 190.

[3] – ماهو الأمن السيبراني وأنواعه ولماذا هو ضروري؟، على الموقع التالي: **https: //elmarefa.com**، تاريخ الزيارة: 2025/10/26، الساعة: 3. عصراً.

[4] – **أشهر تهديدات الأمن الإلكتروني وطرق التصدي لمواجهتها**، على الموقع التالي:https://teknokeys.com ، تاريخ الزيارة: 2025/11/13، الساعة: 5 مساء.

[5]- Léopold & Lhotse, S., La securité informatique. 3éme éditions. Éditions Puff. , 2007, p. 85.

تتخذ إجراءات وقائية فورية. وتُعدّ هذه الإجراءات جزءًا من الالتزامات القانونية الواقعة على المؤسسات بموجب قوانين الأمن المعلوماتي، مثل الالتزام بالإخطار المبكر عند وقوع حوادث سيبرانية تهدّد سلامة البيانات العامة أو الخاصة.

د- **أمن التطبيقات**(Application Security): يركّز على حماية البرمجيات والتطبيقات من الاستغلال عبر الثغرات التقنية أو البرمجية، بدءًا من مرحلة التطوير والتصميم .(DevSecOps) ويُعتبر فحص التعليمات البرمجية الثابتة والديناميكية من أهم أدواته على الصعيد القانوني، يُدرج هذا الجانب ضمن المسؤولية المهنية لمطوّري البرمجيات، إذ تلزمهم بعض القوانين، كالقانون الأوروبي لحماية البيانات(GDPR) ، بضمان أمن الأنظمة والتطبيقات التي تعالج البيانات الشخصية[6].

هـ- **أمن المعلومات**(Information Security – InfoSec): يهدف إلى حماية البيانات من التعديل أو السرقة أو الضياع، سواء أثناء تخزينها أو نقلها أو معالجتها. ويستند إلى ثلاث ركائز أساسية :السرية، والسلامة، والتوافر (Confidentiality, Integrity, Availability).ويُعتبر التشفير من الأدوات القانونية والتقنية المعتمدة بموجب الاتفاقيات الدولية[7]، مثل اتفاقية بودابست لمكافحة الجريمة السيبرانية(2001)، التي تُلزم الدول بتجريم الدخول غير المشروع إلى الأنظمة المؤمنة بالوسائل التشفيرية.

و- **أمن التشغيل**(Operational Security – OPSEC): يركّز على الإجراءات اليومية التي تتخذها المؤسسات لحماية المعلومات الحساسة أثناء تنفيذ العمليات التشغيلية[8]، بما في ذلك إدارة صلاحيات الوصول، ومراقبة الأنشطة، وتحديث الأنظمة بشكل دوري، وأخذ نسخ احتياطية للبيانات. ويُعتبر هذا الجانب تنفيذًا عمليًا لالتزامات الوقاية والرقابة المنصوص عليها في التشريعات الوطنية لحماية الأنظمة المعلوماتية من المخاطر التشغيلية.

ز- **الأمن السحابي** (Cloud Security): مع التحول المتزايد نحو الخدمات السحابية، برزت الحاجة إلى وضع ضوابط قانونية وتقنية تحكم حماية البيانات في البيئات السحابية. ويقوم هذا المجال على نموذج المسؤولية المشتركة بين مزود الخدمة والمستخدم. وتشمل الإجراءات القانونية هنا تحديد شروط استخدام الخدمة، وضمان الامتثال لمعايير الخصوصية، وتحديد نطاق المسؤولية في حال اختراق البيانات أو فقدانها.

ح- **أمن إنترنت الأشياء**(IoT Security): يركّز على حماية الأجهزة الذكية المتصلة بالإنترنت، مثل الكاميرات والمستشعرات والأجهزة الطبية. فكل جهاز متصل يُعدّ نقطة ضعف محتملة يمكن استغلالها لأغراض التجسس أو التخريب. ويستلزم هذا المجال وضع أطر قانونية تُلزم الشركات المصنّعة بتحديث الأنظمة، وتأمين واجهات الاتصال، وضمان سلامة البيانات المنقولة عبرها، تماشيًا مع مبادئ الحق في الأمان الرقمي وحماية المستهلك الإلكتروني[9] .

---

[6] – فهم تهديدات الأمن السيبراني والحماية منها، 27/ مارس 2025، على الموقع التالي: https://almithaqinstitute.com/ar/blog/، تاريخ الزيارة الزيارة: 2025/11/12، الساعة: 1 ظهراً.

[7] – فيلالي أسماء و شليل عبد اللطيف، تهديدات أمن المعلومات وسبل التصدي لها، **مجلة البشائر الإقتصادية**، المجلد 4، العدد 3، 2019، ص 170.

[8] – فريال خوري موسى، **تحديات الأمن السيبراني وكيفية مواجهتها**، على الموقع التالي: https: //www.lebarmy.gov.lb، تاريخ الزيارة: 2025/10/26، الساعة: 5.35 مساء.

[9] - Mozzaquatro, B., Agostinho, C., Gonçalves, D., Martins, J., Jardim-Gonçalves, R. "An Ontology-Based Cybersecurity Framework for the Internet of Things". *Sensors (Basel). 2018 Sep 12; 18(9):3053.

ISSN: 2663-5798 || Arab Journal for Scientific Publishing

الفرع الثاني: أسباب تنامي التهديدات السيبرانية

أضحى الفضاء السيبراني ميدانًا جديدًا للصراع والتنافس بين الدول والجماعات والأفراد، نتيجة جملة من العوامل التقنية والقانونية والاجتماعية التي ساهمت في تصاعد حجم وخطورة التهديدات الإلكترونية[10].

أ- **التطور العلمي والتكنولوجي:** أدى التقدم السريع في مجالات التكنولوجيا والمعلومات إلى ظهور بيئة خصبة لجرائم جديدة، إذ استفاد المجرمون والمنظمات من أدوات التكنولوجيا الحديثة لتنفيذ جرائم الحاسوب والإنترنت، مما جعل التطور التقني سلاحًا ذا حدين: وسيلة للبناء ووسيلة للهدم في آن واحد[11].

ب- **ضعف الرقابة على الشبكات المعلوماتية:** ساهم الانفتاح الواسع للشبكات وضعف الرقابة الأمنية في جعلها عرضة للاختراق، حيث تستغل الجماعات الإرهابية هذا الانفتاح لاختراق الأنظمة وسرقة المعلومات الحساسة باستخدام أدوات كالفيروسات والديدان وحصان طروادة، ما يهدد الأمن القومي للدول.

ج- **صعوبة اكتشاف وإثبات الجريمة الإلكترونية:** تُنفذ الجرائم الإلكترونية غالبًا عن بُعد ودون أثر مادي، مما يصعّب اكتشافها أو إثباتها، ويمكّن المجرمين من التحرك بحرية لفترات طويلة دون مساءلة، وهو ما يشجع على تكرارها وتطورها[12].

د- **سهولة الاستخدام وقلة التكلفة:** تتميز الهجمات السيبرانية بسهولة تنفيذها وتدني تكلفتها مقارنة بالحروب التقليدية، إذ يمكن شن هجمات واسعة باستخدام أدوات وبرامج بسيطة عبر الإنترنت، ما يجعلها وسيلة مغرية لتحقيق أهداف سياسية أو عسكرية بتكلفة محدودة[13].

هـ- **قصور التشريعات والتنظيمات الدولية:** تُعاني المنظومة القانونية الدولية من فراغ واضح في مجال مكافحة الجرائم المعلوماتية، مما يتيح للمجرمين استغلال التفاوت بين القوانين الوطنية وغياب جهة رقابية موحدة للفضاء السيبراني العالمي[14].

---

[10] – حسن هاني حسن محمود وآخرون، أثر التهديدات السيبرانية علي الأمن القومي: دراسة حالة ماليزيا 2015 –2022 م، **المركز الديمقراطي العربي**، على الموقع التالي: https://democratic.de تاريخ الزيارة: 2025/10/10، الساعة: 8.45 مساء.

[11] – مراد عبد الفتاح، **شرح جرائم الكمبيوتر والإنترنت**، دار الكتب والوثائق المصرية، مركز الإمارات للدراسات والبحوث الإستراتيجية، 2014، ص33-36.

[12] – حسن هاني حسن محمود وآخرون، أثر التهديدات السيبرانية علي الأمن القومي: دراسة حالة ماليزيا 2015 –2022 م، مرجع سابق.

[13] – صباح عبد الصبور عبد الحي، إستخدام القوة الإلكترونية في التفاعلات الدولية: تنظيم القاعدة نموذجاً، **المعهد المصري للدراسات السياسية، تركيا**، 2016 ، ص55-50.

– ورقاء محمد رحيم، الإرهاب الإلكتروني وأثره على الأمن الوطني، مركز الدراسات الإستراتيجية والدولي، جامعة بغداد، ص 10، على الموقع التالي: https://www.researchgate.net ، تاريخ الزيارة: 2025/11/18، الساعة: 5 عصراً .

[14] – عادل عبد الصادق، الإرهاب الإلكتروني: القوة في العلاقات الدولية نمط جديد وتحديات مختلفة، **مركز الدراسات السياسية والإستراتيجية بالأهرام**، القاهرة، 2009، ص35.

و- **استهداف الأنظمة العسكرية والبنية التحتية:** باتت الأنظمة العسكرية والبنى التحتية الحيوية من أبرز أهداف الهجمات السيبرانية، إذ يمكن عبرها تعطيل منظومات القيادة والدفاع والطاقة والاتصالات، ما يؤدي إلى شلل في مرافق الدولة وإرباك وظائفها الحيوية.

ز- **تهديد الأمن القومي واستهداف المعلومات:** أصبحت الهجمات السيبرانية وسيلة للتجسس والإرهاب الإلكتروني، ووسيلة للحصول على البيانات الحساسة أو تدميرها لتحقيق مكاسب سياسية أو اقتصادية، بما يشكل تهديدًا مباشرًا لسيادة الدول وأمنها القومي[15].

ح- **غياب الحدود الجغرافية وتدني المخاطرة:** غياب الحدود المكانية في الفضاء الرقمي يمنح المهاجمين حرية مطلقة للتحرك بهويات مجهولة ومن دون مخاطرة مادية، ما يسهم في انتشار الجرائم الإلكترونية عالميًا.

ط- **الدوافع الاجتماعية والنفسية:** تؤدي البطالة والتهميش الاجتماعي، إلى جانب الدوافع الانتقامية، إلى دفع بعض الأفراد، خاصة الشباب، نحو الانخراط في الجرائم الإلكترونية أو الانضمام إلى جماعات متطرفة تستخدم الفضاء السيبراني لأغراض عدائية.

المطلب الثاني: تصنيف ومخاطر التهديدات السيبرانية

تشكل التهديدات السيبرانية، بأشكالها وأنواعها المتعددة، تحديًا متصاعدًا للأمن الرقمي، إذ تمتد مخاطرها لتشمل استقرار الدول، وأمن المؤسسات، وسلامة بيانات الأفراد، كما تؤثر على استمرارية العمليات الحيوية واعتماد المجتمعات على التكنولوجيا. لذلك أصبح الأمن السيبراني ضرورة استراتيجية لا غنى عنها لحماية المعلومات الحيوية وضمان الاستقرار في العصر الرقمي.
وسيُبحث هذا المطلب في فرعين: الفرع الأول يختص بأنواع التهديدات السيبرانية، والفرع الثاني يستعرض مخاطرها وآثارها.

الفرع الأول: أنواع التهديدات السيبرانية

تتعدد أشكال الهجمات السيبرانية وتتطور باستمرار، فهم هذه التهديدات هو الخطوة الأولى نحو بناء دفاع فعال[16].

أ- **البرامج الضارة وأنواعها (Malware):** التعريف القانوني، برنامج أو جزء منه مُصمَّم للقيام بأفعال ضارة على نظم معالجة المعلومات دون موافقة المالك أو المستخدم المصرَّح له، تشمل أنواعها:

1. برامج الفدية (Ransom ware): تقوم بتشفير ملفات الضحية وتطلب فدية مالية مقابل مفتاح فك التشفير أو القفل.
2. برامج التجسس (Spyware): تتسلل إلى جهاز الضحية سراً لجمع المعلومات دون علمه، مثل عادات التصفح أو بيانات تسجيل الدخول، أو نقل بيانات شخصية. كما يمكن استخدام برنامج في جهاز الشخص المعتدى عليه من خلال الإطلاع والإستماع إلى جميع مراسلاته التي تصدر عنه[17].

---

[15]- حسن هاني حسن محمود وآخرون، أثر التهديدات السيبرانية علي الأمن القومي: دراسة حالة ماليزيا 2015 –2022 م، مرجع سابق.

[16]- هيلة عبد المجيد عبد الحافظ العودى، التحديات التي تواجه الأمن السيبراني، **مجلة العلوم الإنسانية والطبيعية**، المجلد 6، العدد 7، 2025 ، ص 725.

[17]- صالح بن على بن عبد الرحمن الربيعة، **الأمن الرقمي وحماية المستخدم من مخاطر الإنترنت**، مركز هيئة الاتصالات وتقنية المعلومات، المملكة العربية السعودية، 2018، ص 53.

3. الفيروسات (Viruses): برامج خبيثة تربط نفسها ببرامج أو ملفات مشروعة (نظيفة) وتنتشر من جهاز إلى آخر بغرض الإتلاف أو الإعاقة.
4. أحصنة طروادة (Trojans): تتنكر في شكل برامج شرعية لخداع المستخدمين لتثبيتها، ثم تقوم لاحقاً بأنشطة ضارة وخبيثة في الخلفية[18].

ب- **هجمات الهندسة الاجتماعية:** تعتمد الهندسة الاجتماعية (Social Engineering) على التلاعب النفسي بالأفراد بغرض الكشف عن معلومات سرية أو إقناعهم بالقيام بأفعال تفضي إلى اختراق أمني يتعلق بهم.

ج- **التصيد الاحتيالي (Phishing):** هو الشكل الأكثر انتشاراً، حيث يتم إرسال رسائل بريد إلكتروني أو رسائل نصية تبدو وكأنها من مصادر موثوقة تهدف إلى خداع الضحايا للنقر على روابط ضارة أو تقديم معلومات هامة ترتبط بالأمور الشخصية[19].

د- **هجمات رفض الخدمة:** تهدف هجمات رفض الخدمة (Denial of Service – DoS) إلى القيام بعمليات توليد حركة مرور زائدة أو استنفاد موارد نظام أو شبكة عن قصد، بحيث تصبح الخدمة غير متاحة للمستخدمين الشرعيين. إذا كانت الهجمة مُنَفَّذة من مصادر متعددة أو بواسطة شبكة من الأجهزة المخترقة يُشار إليها بـ.(DDoS)، يتم استخدام شبكة واسعة من الأجهزة المخترقة (Botnet) لشن الهجوم من مصادر متعددة.

هـ- **التهديدات المتقدمة المستمرة (APTs):** التهديد المتقدم المستمر (Advanced Persistent Threat – APT) سلسلة من الأفعال المخطَّط لها بعناية والتي تستهدف شبكات أو بيانات جهات محددة، وتُنفَّذ على مدى زمني طويل بواسطة فاعلين مزوَّدين بموارد متقدمة (قد تكون متصلة بدول أو جهات منظمة)، تتميز هجمات APT بأنها مستهدفة وممنهجة وذات موارد جيدة.

و- **الهجمات الإلكترونية:** الهجمات الإلكترونية، بما في ذلك الاختراقات (Hacking)، تستهدف سرقة المعلومات أو تعطيل الخدمات. يعتمد المهاجمون على تقنيات متقدمة لاختراق الأنظمة والوصول إلى البيانات الحساسة. تتنوع أهداف هذه الهجمات من الشركات الكبيرة إلى الأفراد، ويتم استغلال الثغرات الأمنية لأغراض مختلفة، بما في ذلك الابتزاز أو المنافسة غير الشريفة[20].

ز- **التهديدات الداخلية:** لا تقتصر التهديدات السيبرانية على الهجمات من الخارج إذ يمكن أن تأتي التهديدات أيضًا من داخل المؤسسة نفسها. بعض الموظفين، سواء عن قصد أو عن غير قصد، قد يسرّبون بيانات حساسة أو يسهّلون الوصول إلى المعلومات غير المصرّح بها. يمكن أن تشمل هذه التهديدات سوء استخدام الوصول أو حتى إهمال إجراءات الأمان.

ح- **الهجمات على البنية التحتية الحيوية:** تشمل هذه الهجمات استهداف الأنظمة التي تدير البنية التحتية الحيوية، مثل خدمات المياه والكهرباء والنقل. وأي تعطيل لهذه الأنظمة يمكن أن يؤدي إلى عواقب وخيمة على المجتمعات بأكملها، ويشكل تهديدًا للأمن القومي[21].

---

[18]– اسماعيل صبري مقلد، ثورة المعلومات وحروب المستقبل، **مجلة آفاق المستقبل**، العدد15، القاهرة، أيلول 2012، ص 4.

[19]– صغير يوسف، **الجريمة المرتكبة عبر الأنترنت**، مذكرة لنيل شهادة الماجستير في القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2013، ص 45.

[20]– فريال خوري موسى، **تحديات الأمن السيبراني وكيفية مواجهتها**، مرجع السابق.

[21]– حمدون تورية، دليل الأمن السيبراني للبلدان النامية، الاتحاد الدولي للإتصالات، جنيف، 2006.

ط- **الأبواب الخلفية BAKDOORS:** هي ثغرة تترك عن قصد من قبل مصممي النظام، بغية التسلل إليه عند الحاجة.

ي- **الرقائق CHIPPING:** يمكن أن تحتوي الرقائق على وظائف إضافية أثناء تصنيعها، حيث لا تعمل في الظروف العادية، إلاّ أنَّها تعمل في توقيت معين وذلك بعد تشغيلها عن بعد، فتحدث شللاً في بيئة إجتماعية أو داخل دولة ما[22].

ك- **الإختناق المروري الإلكتروني:** هي عملية سد قنوات الإتصال وخنقها لمنع تبادل المعلومات بين المستقبل والمرسل.

ل- مدافع HERF، وقنابل EMP: مدافع HERF تطلق موجات راديوية مركّزة عالية الطاقة قادرة على تعطيل أو إتلاف الأجهزة والشبكات (من تعطيل مؤقت إلى تلف دائم). قنابل EMP تعمل بنبضات كهرومغناطيسية تُخترق المواقع الإلكترونية الحساسة وتدمر الحواسب والبنى التحتية داخل نطاق انفجارها[23].

لا بد من الإشارة إلى أنَّ التهديدات السيبرانية تعد من أبرز الجرائم الإلكترونية التي تتميز بسمات عدّة، أهمُّها: استعمال الأسلحة الناعمة، وهي جريمة عابرة لحدود أي دولة، ويصعب اكتشافها، كما تشكِّل صعوبة لناحية اكتشافها وإثباتها، وسهلة الإستعمال والكلفة[24].

الفرع الثاني: مخاطر التهديدات السيبرانية

يمكن توضيح مخاطر التهديدات السيبرانية في الآتي[25]:

أ- **مخاطر التهديدات السيبرانية على الدول:** أضحت التهديدات السيبرانية تمثل أحد أخطر التحديات الأمنية التي تواجه الدول في العصر الرقمي، إذ تحولت الحروب التقليدية إلى حروب رقمية تستخدم الفضاء السيبراني كساحة صراع رئيسية. وتتمثل خطورة هذه التهديدات فيما تُحدثه من أضرار جسيمة تمسّ الأمن القومي والبنى التحتية الحيوية، كالطاقة والمياه والاتصالات والمواصلات والقطاعين المالي والصحي[26].

فالأسلحة السيبرانية، كالقنابل الإلكترونية ومدافع الموجات عالية التردد، تُمكّن الفاعلين من تعطيل شبكات التحكم والتشغيل وإحداث شلل تام في المرافق العامة دون اللجوء إلى القوة المسلحة التقليدية، وهو ما يضع هذه الهجمات ضمن نطاق **التهديدات للأمن والسلم الدوليين** وفق مقاصد ميثاق الأمم المتحدة.

وقد صنّفت تقارير برلمانية بريطانية الهجمات السيبرانية بأنها "أكثر تدميراً من التفجير الذري"، لما تحدثه من انهيار شامل في الأنظمة الإلكترونية والمالية. وقد أثبتت الوقائع العملية خطورة هذه الهجمات، بدءاً من فيروس **Love You** عام 2000 الذي سبب خسائر

---

[22]- حمدون تورية، البحث عن السلام السيبراني، الإتحاد الدولي للإتصالات- جنيف، 2011.

[23]- HERF: HIGH ENERGY RADIO FREQUENCY, EMP: ELCTROMAGNETIC PULSE.

[24]- غلاف كريمة و جرلان زوهرة، **جريمة الإرهاب الإلكتروني**، رسالة ماجستير، كلية الحقوق والعلوم السياسية قسم القانون الخاص تخصص قانون جنائي وعلوم جنائية، جامعة عبد الرحمان ميرة، 2018/2019، ص16-17.

[25]- حسن هاني حسن محمود وآخرون، **أثر التهديدات السيبرانية علي الأمن القومي : دراسة حالة ماليزيا 2015 -2022 م**، مرجع سابق.

[26]- Rid, Thomas, "Cyber War Will Not Take Place." , **Journal of Strategic Studies**, (2012) , 35(1), 5–32, DOI: 10.1080/01402390.2011.608939.

- هيله عبد المجيد عبد الحافظ.، «التحديات التي تواجه الأمن السيبراني»، مرجع سابق.

تجاوزت 10 مليارات دولار، مروراً بفيروس **Blaster** عام 2003، وصولاً إلى استغلال التكنولوجيا في **هجمات 11 سبتمبر 2001**، وهو ما دفع المجتمع الدولي إلى اعتماد **اتفاقية بودابست لمكافحة الإجرام المعلوماتي (2001)**، كأول إطار قانوني دولي لمواجهة الجرائم السيبرانية[27].

وبذلك، أصبحت التهديدات السيبرانية تشكل تهديداً مباشراً لسيادة الدول وأمنها الداخلي، وتستدعي تطوير قواعد القانون الدولي لمواكبة طبيعتها غير التقليدية والعابرة للحدود.

ب- **مخاطر التهديدات السيبرانية على المؤسسات:** تُعدّ التهديدات السيبرانية من أبرز المخاطر التي تواجه المؤسسات المعاصرة، إذ تستهدف شبكاتها وقواعد بياناتها الحيوية، بما يؤدي إلى تعطيل أنشطتها وإلحاق خسائر مالية جسيمة. وتشمل هذه التهديدات عمليات اختراق الأنظمة وسرقة البيانات التجارية والمالية، أو شنّ هجمات لحجب الخدمة وإسقاط المواقع الإلكترونية بما يعرقل المعاملات الإلكترونية للمؤسسة. كما تُعدّ سرقة الملكية الفكرية واختراق نظم التشفير من أخطر صور الاعتداءات الرقمية التي تمس المصالح الاقتصادية للمؤسسات، وتُنشئ في المقابل مسؤوليات قانونية تتعلق بالإهمال في حماية البيانات أو الإخلال بالتزامات الإخطار عن الحوادث الأمنية وفقاً للتشريعات الوطنية والدولية[28].

ج- **مخاطر التهديدات السيبرانية على الأفراد:** لم تقتصر التهديدات السيبرانية على المؤسسات، بل امتدت إلى الأفراد مهدِّدة خصوصيتهم وسلامتهم الرقمية. فاختراق البريد الإلكتروني أو الحسابات الشخصية يؤدي إلى تسريب المعلومات الخاصة واستغلالها في الابتزاز أو التشهير، كما تتنامى جرائم انتحال الهوية الإلكترونية واستخدامها لأغراض احتيالية أو سياسية وتبرز كذلك خطورة استقطاب وتجنيد الشباب عبر الإنترنت من قبل جماعات متطرفة تستغل المنصات الرقمية لبث أفكارها والتأثير في الفئات الهشّة اجتماعياً ونفسياً[29].

1. **التهديد والابتزاز المعلوماتي** :يتم باختراق الحسابات أو التجسس لنشر معلومات أو صور خاصة بغرض الابتزاز أو التشهير، خاصة ضد الشخصيات العامة[30].
2. **استقطاب وتجنيد الشباب** :تستغل الجماعات المتطرفة الإنترنت لنشر أفكارها واستقطاب الشباب عبر تحويل الفضاء الرقمي إلى ساحة للتجنيد والتحريض، وعن طريق مواقع التواصل الإجتماعي: الفيسبوك وتويتر ومنتديات وغرف الدردشة ورسائل الدعاية والإعلام.

---

[27]- أسامة مهمل، **الإجرام السيبراني**، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، 2018/2017، ص 88.

[28]- وفاء بوكابوس، تحول القوة في العلاقات الدولية دراسة في انتقال القوة من التقليدية إلى الحديثة، **المركز الديمقراطي العربي للدراسات الإستراتيجية والسياسية والاقتصادية، ألمانيا**، 2019، ص 56.

- المخاطر السيبرانية: الكشف عن مخاطر الأحداث، التهديد المتزايد للهجمات السيبرانية، على الموقع التالي: HTTPS://FASTER CAPITAL.COM، تاريخ الزيارة: 2025/11/16، الساعة: 2 ظهراً.

[29]- توفيق شريخي، **الإرهاب الإلكتروني وتأثيره على أمن الدولة**، رسالة ماجستير تخصص إستراتيجية وعلاقات دولية، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، الجزائر، 2018/2017، ص 60.

[30]- محمود عمر محمود، **الجرائم المعلوماتية والإلكترونية**، خوارزم العلمية، الطبعة الأولى، ٢٠١٥، ص 63.

المبحث الثاني: الجهود الدولية في مكافحة التهديدات السيبرانية

أدّى الطابع **العابر للحدود** للهجمات السيبرانية إلى بروز حاجةٍ مُلحّة لتعزيز **التعاون الدولي المنظَّم** في هذا المجال[31]، باعتبار أنَّ التهديدات الرقمية لا تعترف بالسيادة الإقليمية ولا تخضع لحدودٍ جغرافية. وقد أقرّت **القمة العالمية لمجتمع المعلومات (WSIS)** المنعقدة عامي 2003 و**2005** بضرورة وضع **آليات وأدوات قانونية ومؤسسية فاعلة** على المستويين الدولي والوطني، بغية **ضمان الأمن السيبراني** وتعزيز **القدرات الوطنية** في مجال مكافحة **الجرائم المعلوماتية**[32] .

وقد امتدت هذه الجهود لتشمل **منظومة الأمم المتحدة** وعددًا من **المنظمات الدولية والإقليمية**، إضافةً إلى **المنظمات غير الحكومية** التي أسهمت بدورٍ مكمل في بناء الإطار المعياري والتقني للأمن السيبراني.
وانطلاقًا من ذلك، جرى تقسيم هذا المبحث إلى المطلبين الآتيين:

المطلب الأول: جهود المنظمات الإقليمية في تعزيز الأمن السيبراني

المطلب الثاني: جهود المنظمات غير الحكومية مع مراعاة القانون الإنساني.

المطلب الأول: جهود المنظمات الحكومية

تزايدت أهمية الدور الذي تضطلع به المنظمات الحكومية في مواجهة التهديدات السيبرانية، نظراً لما تمثله من خطر متنامٍ يهدد الأمن والسلم الدوليين. وقد برزت جهود هذه المنظمات من خلال وضع الأطر القانونية والتنسيقية لمكافحة الجرائم الإلكترونية وتعزيز الأمن الرقمي المشترك. وفي هذا الإطار، يمكن التمييز بين الجهود المبذولة على المستوى الدولي من قبل منظمة الأمم المتحدة وبعض الأجهزة التابعة لها، وعلى المستوى الإقليمي من خلال المنظمات الإقليمية التي سعت إلى بلورة استراتيجيات خاصة تتلاءم مع خصوصياتها القانونية والسياسية.

وعليه، يُقسم هذا المطلب إلى فرعين: يتناول الفرع الأول دور الأمم المتحدة، بينما يتناول الفرع الثاني دور المنظمات الإقليمية.

الفرع الأول: دور الأمم المتَّحدة

تبذل منظمة الأمم المتحدة جهوداً مستمرة لمواجهة التهديدات السيبرانية وحماية الدول والأفراد من الاعتداءات الإلكترونية، من خلال تطوير الأطر التشريعية وتنظيم مؤتمرات دولية لتعزيز التعاون بين الدول.

[31] - Syed Qandil Abbas, Hareem Fatima, Cyber Security Threats to Iran and its Countermeasures: Defensive and Offensive Cyber Strategies, **Journal of Research in Social Sciences (JRSS)** , Vol 12, No 2, July 2024, p. 10.

[32] – تامر أحمد، **الهجمات على شبكات الحاسوب في القانون الدولي الإنساني**، مرجع سابق، ص 64.

ومن أبرز هذه الجهود[33]:

أ- **المؤتمرات الدولية:** عقدت الأمم المتحدة مؤتمرات لمنع الجريمة، مثل المؤتمر السابع بميلانو (1980) الذي شدد على الاستفادة من التطورات العلمية لمكافحة جرائم الحاسوب، والمؤتمر التاسع بالقاهرة (1995) الذي ركز على حماية التكنولوجيا وتعزيز التعاون الدولي، والمؤتمر العاشر في بودابست الذي اعتبر جرائم الحاسوب نمطاً جديداً من الجرائم المستحدثة.

ب- **القرارات الدولية:** أقرت الجمعية العامة القرار (56/285) عام 2002 لتشجيع استخدام تكنولوجيا المعلومات لأغراض التنمية وتنبيه المجتمع الدولي لمخاطر الجرائم السيبرانية[34].

ت- **الاتفاقيات الدولية:** وقعت الأمم المتحدة في 12 أبريل 2000 اتفاقية لمكافحة إساءة استخدام تكنولوجيا المعلومات لأغراض إجرامية، مؤكدة على أهمية التنسيق والتعاون بين الدول.

ث- **مبادرات مجلس الأمن:** أصدر مجلس الأمن القرار رقم (1963) عام 2010، والقرار رقم (2255) عام 2015، للتحذير من استخدام الإرهابيين للإنترنت والتكنولوجيا في التجنيد والتحريض وتمويل الإرهاب. كما أصدر القرار رقم S/RES/2370(2017)، الصادر في 2/اب/2017 والذي يدعو الأعضاء إلى العمل بصورة تعاونية لمنع الإرهابيين والمتطرفين من حيازة الأسلحة، من خلال تكنولوجيا المعلومات والإتصالات ...[35].

ج- **المؤتمرات المتخصصة:** مثل المؤتمر الثاني عشر لمنع الجريمة والعدالة الجنائية (سلفادور، 2010) الذي تناول جرائم الإنترنت والتعاون الدولي لمكافحتها.

ح- **بعض جهود اللجان والهيئات والأجهزة التابعة للامم المتحدة:** أولت الأمم المتحدة اهتماماً متزايداً بمسألة الأمن السيبراني من خلال أجهزتها وهيئاتها المتخصصة، إدراكاً منها لخطورة التهديدات الرقمية المتنامية على السلم والأمن الدوليين. ففي أبريل من عام 2010، قامت لجنة الأمم المتحدة لمنع الجريمة والعدالة الجنائية، خلال دورتها الثانية عشرة، بصياغة مجموعة من الإعلانات الهامة التي تضمنت إنشاء فريق خبراء حكومي دولي يُعنى بدراسة ظاهرة الجريمة السيبرانية وسبل الاستجابة الدولية لها[36].

كما شهد عام 2010 مبادرة أخرى تمثلت في قيام المجلس الاقتصادي والاجتماعي التابع للأمم المتحدة بعقد جلسة إعلامية خُصصت لبحث التحديات التي يطرحها الأمن السيبراني، إلى جانب ما يوفره التوسع المتسارع في استخدام الإنترنت من فرص وتحديات. وقد شدّد المشاركون في تلك الجلسة على ضرورة تنسيق الجهود الأممية وتوحيد أداء أجهزة الأمم المتحدة لمواجهة الأخطار السيبرانية بفعالية

---

[33]- حسن هاني حسن محمود وآخرون، **أثر التهديدات السيبرانية علي الأمن القومي:** دراسة حالة ماليزيا 2015 -2022 م، مرجع سابق.

[34]- غازي عبد الرحمن رشيد، **الحماية القانونية من الجرائم المعلوماتية**، رسالة دكتورة، كلية الحقوق، الجامعة الإسلامية، لبنان، 2004 ، ص11-14.

[35] - إبراهيم السيد أحمد رمضان، مواجهة الهجمات السيبرانية في ضوء أحكام القانون الدولي، **مجلة العلوم القانونية والإقتصادية**، العدد 1، السنة 67، 2025، ص 1828.

[36]- مراد مشوس، الجهود الدولية لمكافحة الإجرام السيبراني، **مجلة الواحات للبحوث والدراسات**، العدد 2، 2019، المجلد رقم 12، على الموقع التالي: https://www.asjp.cerist.dz/en/PresentationRevue/2، تاريخ الزيارة: 2025/11/1، الساعة: 7 مساء.

أكبر، محذرين من أن أي حرب سيبرانية واسعة النطاق قد تخلّف عواقب وخيمة تتطلب استجابة دولية منسقة، تتجاوز الحلول التقنية الجزئية أو الدفاعات المنعزلة[37].

وفي سياق تعزيز البنية المؤسسية للأمن السيبراني، أنشأت الأمم المتحدة في عام 2009 الشراكة التعددية ضد التهديدات السيبرانية (IMPACT)، وهي أول منظمة دولية تدعمها الأمم المتحدة لتنسيق الجهود العالمية الرامية إلى تعزيز القدرات في مجال الأمن السيبراني، وتطوير آليات التعاون والتصدي للهجمات الإلكترونية على المستويين الإقليمي والدولي[38].

على الرغم من غياب نص صريح في ميثاق الأمم المتحدة بشأن تجريم الإرهاب الإلكتروني، إلا أن الممارسة الدولية تتفق مع اعتبار استخدام المعلومات لأغراض إرهابية انتهاكاً للسيادة الوطنية والسلامة الإقليمية، ويُعد ضمن أعمال العدوان التي تهدد العلاقات الدولية.

يمكن القول أنَّ دور الأمم المتَّحدة في إطار مواجهة التهديدات السيبرانية والجرائم الإلكترونية والفضاء الرقمي، أخذت بثلاثة محاور وهي[39]:

1. نشر الوعي الدولي والتنبيه من مخاطر التهديدات السيبرانية عبر سلسلة من الجهود الهادفة.
2. ضمان حرية التعبير والوصول الحر للمعلومات مع مراقبة الإنترنت للحفاظ على الأمن والسلم الدوليين.
3. وضع استراتيجيات علمية شاملة لمكافحة التهديدات السيبرانية على أرض الواقع.

الفرع الثاني: دور المنظمات الإقليمية

يُلاحظ أنّ المنظمات الإقليمية قد أبدت قدراً أكبر من الجرأة والفعالية في تناول موضوع الهجمات السيبرانية مقارنة بالمستوى الدولي العام، إذ بادرت العديد منها إلى تبنّي مبادرات واستراتيجيات تهدف إلى تعزيز التعاون الإقليمي في مجال مكافحة الجريمة المعلوماتية وتنظيم الفضاء السيبراني. وبالنظر إلى تنوّع هذه الأطر المؤسسية وتعدد مقارباتها القانونية، سنكتفي في هذا السياق بدراسة النماذج الأوروبي والعربي والأفريقي، لما تمثّله من تجارب متمايزة ومتكاملة في بناء قواعد قانونية لمواجهة التهديدات السيبرانية وتعزيز الأمن الرقمي الجماعي[40].

---

[37]– هبة جمال الدين، الأمن السيبراني والتحول في النظام الدولي، **مجلة كلية الاقتصاد والعلوم السياسية**، على الموقع التالي: https: jpsa.journals.ekb.eg، تاريخ الزيارة: 2025/10/12، الساعة: 11.35 مساء.

[38]– مراد مشوس، الجهود الدولية لمكافحة الإجرام السيبراني، مرجع سابق.

[39]– نعيم سعداني، **أليات البحث والتحرى عن الجريمة المعلوماتية في القانون الجزائري**، رسالة ماجستير، كلية الحقوق، جامعة حاج لخضر باتنة، 2013، ص 21.

[40]– بوفليح محمد السعيد، أطر التعاون الدولي للتصدي للتهديدات السيبرانية، **مجلة الدراسات القانونية والتطبيقية**، العدد2020، 2024، ص 10-12.

أ- **المنظمات الأوروبية:** أنشأ **اليوروبول (Europol)** في عام **2013** المركز الأوروبي للجرائم الإلكترونية، وذلك بهدف **تعزيز قدرات أجهزة إنفاذ القانون في دول الاتحاد الأوروبي على مواجهة الجريمة المعلوماتية** والتصدي لظواهر الإجرام السيبراني المنظّم[41].

كما تم تأسيس **الهيئة الأوروبية للتعاون القضائي يوروجست (Euro just –** في **فبراير 2002** وافتُتحت رسميًا في **أبريل 2003**، بهدف **تعزيز التنسيق والتعاون القضائي بين سلطات الدول الأعضاء في الاتحاد الأوروبي** في مجال مكافحة الجريمة عبر الحدود، بما في ذلك الجرائم الإلكترونية.

وعلى الصعيد الدولي، تم في **بودابست سنة 2001** إبرام **اتفاقية مكافحة الجريمة المعلوماتية** بمشاركة **26 دولة** إضافة إلى **كندا واليابان وجنوب إفريقيا والولايات المتحدة الأمريكية** .وتُعد هذه الاتفاقية **أول معاهدة دولية مخصّصة لمكافحة الأفعال الإجرامية المرتكبة ضد نظم وشبكات الحاسوب أو بواسطة استخدامها**، وهي **مفتوحة لانضمام جميع الدول الراغبة** في الالتزام بأحكامها[42].

أما **المجلس الأوروبي** وعلى غرار **منظمة الإنتربول**، فقد أنشأ في **لوكسمبورغ سنة 1991** جهازًا للشرطة الأوروبية يُعدّ **حلقة وصل بين أجهزة الشرطة في الدول الأعضاء**، بهدف **تعزيز التعاون الأمني في ملاحقة مرتكبي الجرائم العابرة للحدود، بما في ذلك الجرائم المعلوماتية**[43].

ب- **المنظمات الإفريقية:** أُبرِمت اتفاقية الاتحاد الأفريقي للأمن السيبراني وحماية البيانات الشخصية خلال القمة الثالثة والعشرين للاتحاد الأفريقي المنعقدة في ملابو (غينيا الاستوائية) بتاريخ 27جوان 2014[44]، وكان هدفها الأساس يتمثل في تعزيز التشريعات الوطنية وتنمية الأنظمة القانونية والتنظيمية المتعلقة بتكنولوجيات المعلومات والاتصال في الدول الأعضاء، ولا سيّما وضع قواعد أمنية فعّالة لإنشاء فضاء رقمي موثوق للمعاملات الإلكترونية، إضافةً إلى حماية البيانات ذات الطابع الشخصي ومكافحة الجريمة الإلكترونية[45].

وقد قسّم المشرّع الأفريقي هذه الاتفاقية إلى أربع مجموعات رئيسية، هي:

1. المجموعة الأولى: تعنى بالهجمات الموجهة ضد أنظمة الحاسوب وكل ما يتصل بها.
2. المجموعة الثانية: تتعلق بالجرائم التي تستهدف البيانات ذات الطابع الشخصي.
3. **المجموعة الثالثة: تُعنى بالجرائم المرتبطة بالمحتوى الإلكتروني.**

---

[41]- بن مكي، **السياسة الجنائية لمكافحة جرائم المعلوماتية**، دار الخلدونية، الجزائر، 2017، ص 149.

[42]- نورهان محمد الربيعي، الجريمة السيبرانية وآليات مكافحتها، **مجلة الفارابي للعلوم الإنسانية**، العدد 1، المجلد 3، 2024، ص 83-84.

[43]- بن مكي، **السياسة الجنائية لمكافحة جرائم المعلوماتية**، مرجع سابق، ص 150.

[44]- محمد العيداني، التهديدات السيبرانية وجرتئم المعلومات، **مجلة الإجتهاد للدراسات القانونية والإقتصادية**، المجلد 12، العدد 1، 2024 ، ص 24.

[45]- مناصرة يوسف، **جرائم المساس بأنظمة المعالجة الآلية للمعطيات (ماهيتها، صورها، الجهود الدولية لمكافحتها- دراسة مقارنة)**، دار الخلونية، الجزائر، 2018، ص 283.

4. المجموعة الرابعة: تتناول الجرائم المتعلقة بتأمين الرسائل الإلكترونية، وتحدد الأجهزة المختصة العاملة في هذا المجال.

كما تجسدت فكرة إنشاء "أفريبول" (الشرطة الأفريقية) خلال مؤتمر وهران سنة 2013، حيث أُنيطت به مهام متعددة من بينها تعزيز القدرات التحليلية لتقييم التهديدات الإجرامية وتطوير الاستجابات المناسبة في إطار دعم عمليات حفظ السلام، إضافةً إلى تقديم المساعدة التقنية في مجال مكافحة الجرائم المعلوماتية[46].

ج- منظمة جامعة الدول العربية: أقرّ مجلس وزراء العدل العرب سنة 1996 القانون الجزائي العربي الموحّد، الذي خُصصت فيه المواد من 461 إلى 464 لمعالجة الأفعال الماسة بحقوق الأشخاص الناشئة عن المعالجة المعلوماتية للبيانات، حيث أكّد المشرّع العربي من خلالها على وجوب حماية البيانات ذات الطابع الشخصي، ونصّ على جزاءات جنائية تتمثل في عقوبات سالبة للحرية وغرامات مالية بحق كل من يرتكب أفعالاً تمسّ الخصوصية المعلوماتية للأفراد. كما شدّد القانون على أهمية التعاون العربي المشترك في هذا المجال من خلال تفعيل آليات المساعدة القضائية المتبادلة والإنابات القضائية في ملاحقة مرتكبي الجرائم المعلوماتية[47].

وفي السياق ذاته، بادر مجلس وزراء الداخلية العرب سنة 1965 إلى إنشاء المكتب العربي للشرطة الجنائية، يتولى تنسيق الجهود الأمنية بين الدول العربية، ويعاونه في ذلك المكتب العربي لمكافحة الجريمة، بهدف صون الأمن الاجتماعي ومكافحة مختلف صور الجريمة، بما فيها الجريمة المعلوماتية[48].

كما صدر عن جامعة الدول العربية قانوناً استرشادياً لمكافحة جرائم تقنية الفضاء السيبراني، حيث عملت الدول العربية على تجريم الأعمال الغير مشروعة والتي ترتكب عبر الفضاء السيبراني، وذلك من خلال التوقيع على الإتفاقية العربية لمكافحة جرائم تقنية المعلومات بهدف تعزيز روابط التعاون بين الدول العربية كافة لمكافحة الجرائم السيبرانية لعام 2010 حفظاً لأمنها وسلامتها[49].

المطلب الثاني: جهود المنظمات غير الحكومية مع مراعاة مبادئ القانون الإنساني

على الرغم من حداثة ظاهرة الهجمات السيبرانية على الصعيد الدولي، فقد بادرت بعض المنظمات غير الحكومية إلى اتخاذ خطوات عملية للتعامل مع هذا الواقع المستجد، إذ إنَّ التردد الذي تبديه الدول في إبرام معاهدات دولية للحد من تصاعد التهديدات السيبرانية، لم يمنع تلك المنظمات من إبداء مواقفها والمساهمة في صياغة المبادرات الرامية إلى الحد من تسارع وتيرة هذه الهجمات،

[46]– مناصرة يوسف، المرجع السابق، ص 284.

[47]– خراشي عادل عبد العال إبراهيم، **إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها**، دار الجامعة الجديدة للنشر، مصر، 2015، ص 310.

[48] – خراشي عادل عبد العال إبراهيم، **إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها**، المرجع السابق، ص 285.

[49]- مجة حفصة، **جرائم إختراق الأمن السيبراني في التشريع الجنائي المقارن**، ماستر في الحقوق، كلية الحقوق والعلوم السياسية، جامعة بجاية، 2022/2021، ص 57.

كما برزت تحديات كبيرة مع تطور التكنولوجيا في وسائل القتال وأساليبه على صعيد القانون الدولي الإنساني لكونه ينظم وسائل القتال وأساليبه خلال النزاعات.

بناءً على ذلك، يُقسَّم هذا المطلب إلى فرعين رئيسيين: يتناول الفرع الأول دور حلف الشمال الأطلسي، بينما يخصص الفرع الثاني التوازن بين الأمن السيبراني وحقوق الإنسان.

الفرع الأول: حلف الشمال الأطلسي (قواعد تالين)

أنشأ حلف شمال الأطلسي (الناتو) إطاراً مؤسسياً متقدّماً لتنظيم وتعزيز جهوده في مجال الدفاع السيبراني، وذلك من خلال استحداث هيئة مختصة بإدارة الدفاع السيبراني تُعنى بوضع السياسات والتدابير اللازمة لحماية البنية التحتية الرقمية للدول الأعضاء.

أ- **حلف الناتو والأمن السيبراني:** تُظهر التجربة الدولية المعاصرة أن حلف شمال الأطلسي (الناتو) يعد أحد أبرز الفاعلين الذين تعاملوا مع التهديدات السيبرانية على أنها جزء لا يتجزأ من الأمن الجماعي، فمع تصاعد الهجمات الإلكترونية العابرة للحدود واستهدافها للبنى التحتية الحيوية للدول الأعضاء، اضطر الحلف إلى تطوير استراتيجية دفاعية رقمية شاملة[50].

في قمة وارسو2016 ، أقر الناتو رسميًا أن الفضاء السيبراني أصبح مجالًا للعمليات العسكرية مثل البر والبحر والجو[51]، وهو ما يعني أن أي هجوم سيبراني واسع النطاق على دولة عضو يمكن اعتباره هجومًا مسلحًا يبرر تفعيل المادة الخامسة من معاهدة واشنطن [52]، وقد شكّل هذا الإعلان تحولًا نوعيًا في مفهوم الدفاع الجماعي، إذ انتقل ليشمل البعد الرقمي والتكنولوجي.

1. **مركز التميز للدفاع السيبراني التعاوني CCDCOE:** استجابةً للهجمات السيبرانية على إستونيا عام2007 ، أنشأ الناتو سنة 2008مركز التعاون للدفاع السيبراني التعاوني (CCDCOE) في تالين[53]. يهدف هذا المركز إلى:
   - تطوير القدرات الوطنية والإقليمية للدفاع السيبراني
   - صياغة سياسات واستراتيجيات قانونية للتعامل مع الهجمات الإلكترونية.
   - دراسة الإطار القانوني لتطبيق قواعد القانون الدولي الإنساني على النزاعات السيبرانية.

---

[50]- عبد الرحمن بن ناصر الشمري، الحرب السيبرانية في القانون الدولي الإنساني :دراسة تحليلية لقواعد تالين، **مجلة جامعة نايف للأمن الوطني**، العدد19 ، الرياض، 2020 ، ص17 .

[51]- عبد السلام المريني، الناتو والأمن السيبراني من الدفاع الجماعي إلى الردع الرقمي، **مجلة المستقبل العربي**، مركز دراسات الوحدة العربية، بيروت،2021 ، ص 44 .

[52]- خالد يوسف العتوم، التهديدات السيبرانية وتحديات الأمن الجماعي في ضوء ميثاق الأمم المتحدة، **مجلة دراسات القانون الدولي**، جامعة اليرموك،2022 ، ص61 .

[53]- **مركز التميز في الدفاع السيبراني التعاوني**، على الموقع التالي: https: //ar.hisour.com، تاريخ الزيارة: 2025/11/18، الساعة: 4 عصراً.

وقد كانت تجربة إستونيا علامة فارقة، حيث أظهرت هشاشة البنى التحتية الرقمية للدول أمام الهجمات المنسقة عبر الإنترنت، ما دفع الناتو لاعتماد التدريب، والتمارين، والمحاكاة العملية لتعزيز جاهزية الأعضاء.

2. **قواعد تالين(Tallinn Manual)**: أهم مخرجات مركز CCDCOE كانت قواعد تالين، وهي مجموعة مبادئ قانونية تهدف إلى تطبيق القانون الدولي على الفضاء السيبراني[54] .

- Tallinn Manual 1.0 (2013) ، ركز على النزاعات السيبرانية المسلحة[55].
- Tallinn Manual 2.0 (2017) ، توسع ليشمل العمليات السيبرانية في زمن السلم والنزاع.

أبرز المبادئ الأساسية لقواعد تالين التالية:

- السيادة وعدم التدخل: لكل دولة سيادة رقمية على بنيتها التحتية، وأي اختراق يُعد انتهاكًا للقانون الدولي[56].
- التمييز: لا يجوز استهداف المدنيين أو البنية التحتية المدنية.
- التناسب والضرورة العسكرية: يُقيد استخدام القوة السيبرانية بحيث تكون متناسبة مع الهدف العسكري.
- المسؤولية الدولية: الدولة مسؤولة عن عملياتها السيبرانية المباشرة أو المدعومة[57].

فيما يتعلق بحق الدفاع أثناء الهجوم السيبراني، فقد حددت القواعد أن الهجوم السيبراني يمكن أن يُصنّف كهجوم مسلح إذا كانت آثاره تعادل استخدام القوة التقليدية، مثل تدمير منشآت حيوية أو إحداث خسائر بشرية كبيرة، مما يجيز للدولة الدفاع عن نفسها وفق المادة (51)من ميثاق الأمم المتحدة[58].

ب- **التحليل القانوني لشرعية الدفاع الجماعي السيبراني:** يثير تطبيق الناتو لقواعد تالين إشكالية تتعلق بتوافق هذا التطبيق مع مبادئ ميثاق الأمم المتحدة، وخصوصًا المادة[59]2/4 ، التي تحظر استخدام القوة أو التهديد بها. فاعتبار بعض الهجمات الإلكترونية هجومًا مسلحًا يمنح الناتو سلطة تقدير نوع العدوان دون الرجوع إلى مجلس الأمن، وهو ما قد يوسع نطاق الدفاع الجماعي السيبراني خارج الإطار الأممي[60].

من هنا لا بدّ من التوازن بين الدفاع وميثاق الأمم المتحدة، بحيث يجب أن تبقى شرعية الدفاع الجماعي السيبراني مقيدة بـ:

---

[54] - Schmitt, Tallinn Manual 2.0, 2017, p. 12.

[55] - Michael N. Schmitt (ed.), **Tallinn Manual 1.0 on the International Law Applicable to Cyber Warfare**, Cambridge University Press, 2013, p. 11.

[56]– محمد جلال حمزة، القانون الدولي الإنساني والفضاء السيبراني :قراءة في قواعد تالين، **المجلة القانونية الدولية**، جامعة القاهرة،2021 ، ص 35.

[57]– مازوني كوثر، **الجريمة المعلوماتية**، دار الخلدونية، الجزائر، ط1، 2022 ، ص 177.

[58]– عبد الرحمن بن ناصر الشمري، الحرب السيبرانية في القانون الدولي الإنساني :دراسة تحليلية لقواعد تالين، مرجع السابق، ص 39 .

[59]– خالد يوسف العتوم، التهديدات السيبرانية وتحديات الأمن الجماعي في ضوء ميثاق الأمم المتحدة، مرجع السابق، ص 66 .

[60]– عبد السلام المريني، الناتو والأمن السيبراني من الدفاع الجماعي إلى الردع الرقمي، مرجع السابق، ص 51–50 .

1. الالتزام بالضوابط القانونية الدولية، وعدم اللجوء إلى الرد الاستباقي دون هجوم فعلي.
2. احترام مبدأ حظر استخدام القوة وحق الدول في الدفاع المشروع عن النفس.
3. البحث عن إطار دولي ملزم لتقنين الرد السيبراني ضمن هيئة الأمم المتحدة[61].

رغم عدم إلزاميتها قانونيًا، توفر قواعد تالين إطارًا لتفسير القانون الدولي في الفضاء السيبراني، وتوضح:

- متى يمكن أن يعتبر الهجوم السيبراني مسلحًا.
- كيف توازن الدولة بين الدفاع وحقوق المدنيين.
- حدود المسؤولية الدولية للدول عن أعمالها السيبرانية[62].

يتضح أن قواعد تالين تمثل محاولة جادة لربط القانون الدولي بالفضاء السيبراني، وأن الناتو اعتمدها لتطوير استراتيجيته الدفاعية الرقمية .ومع ذلك، يبقى تطبيق هذه القواعد مرتبطًا بالامتثال لمبادئ ميثاق الأمم المتحدة، لضمان شرعية الدفاع الجماعي السيبراني، ومنع توسع استخدام القوة خارج نطاق مجلس الأمن، ومن ثم، فإن الطريق الأمثل هو اعتماد إطار دولي ملزم ينظم الحرب السيبرانية، ويحافظ على توازن الأمن الرقمي بين حق الدفاع وواجب احترام السلم والأمن الدوليين[63].

الفرع الثاني: التوازن بين الأمن السيبراني وحقوق الإنسان

رغم التردد الذي يكتنف الدول في الدخول في معاهدات للحد من انتشار التهديد السيبراني، فإنَّ بعض المنظمات غير الحكومية سارعت إلى احتواء تداعيات الهجمات السيبرانية من خلال إبداء رأيها في هذا الشأن. كما تطرح مسألة وجوب مراعاة مبادئ القانون الدولي الإنساني أثناء الحروب السيبرانية.

أ- **رأي اللجنة في نظرية الفراغ التشريعي:** جاء في رأي لجنة الصليب والهلال الأحمر الدولي بمناسبة إبداء رأيهما لناحية انطباق القانون الدولي الإنساني على التهديدات أو الهجمات السيبرانية كما يلي: " ليس للجنة الهلال والصليب الأحمر الدولي أدنى شك أنَّ القانون الدولي الإنساني ينطبق على العمليات السيبرانية خلال النزاعات، وبالتالي يحد من استخدامها تماماً مثلما ينظم استخدام الأسلحة والوسائل والأساليب الأخرى للقتال في أي نزاع مسلح، جديدة كانت أو قديمة وهذا أمر صحيح سواء كان الفضاء السيبراني يعتبر مجالاً مختلفاً، لأنَّه مجال جديد للحرب يشبه الفضاء الجوي والبري والبحري والفضاء الخارجي أو إذا كان مجالاً مختلفاً لأنَّه من صنع الإنسان في حين أنَّ المجالات السابقة طبيعية أم أنَّه ليس مجالاً في حد ذاته[64].

ب- **ضرورة تطبيق قواعد الإشتباك في الفضاء السيبراني:** حسب اللجنة، فإنَّ مبادئ القانون الدولي الإنساني تنطبق على العمليات السيبرانية خلال النزاعات المسلحة دون شك، وذلك تجنباً لخسائر عرضية قد تصيب المدنيين أو أضرار تلحق بالأعيان المدنية،

---

[61]- خالد يوسف العتوم، التهديدات السيبرانية وتحديات الأمن الجماعي في ضوء ميثاق الأمم المتحدة، مرجع السابق، ص.68 .

[62]- Schmitt, Tallinn Manual 2.0 ص 15-16.

[63]- عبد الرحمن بن ناصر الشمري، الحرب السيبرانية في القانون الدولي الإنساني: دراسة لقواعد تالين، مرجع السابق، ص 45-46.

[64]- **ورقة موقف اللجنة الدولية للهلال والصليب الأحمر الدولي المقدمة لفريق العمل: القانون الدولي الإنساني والعمليات السيبرانية خلال النزاعات المسلحة، 2019**، على الموقع التالي: https: //www.icr.org، تاريخ الزيارة: 2025/11/22، الساعة: 9.20 مساءًا.

ISSN: 2663-5798 || Arab Journal for Scientific Publishing

كما تلزم الأطراف باتخاذ كافة الإحتياطات الممكنة عند تنفيذ الهجمات، كما يجب العمل على حماية الوحدات الطبية بكل أشكالها وأنواعها واحترامها مع ضرورة استثناء المراكز الصحية والمستشفيات. كما طالبت لجنة الصليب الأحمر الدولي بالإشارة البيضاء في الفضاء السيبراني لتتمكن من القيام بمهامها بعيداً عن الصراع السيبراني بين الدول المتحاربة. كما شارك خبراء اللجنة الدولية في نقاشات متقدمة حول مستقبل الدبلوماسية السيبرانية، مؤكِّدين على مواكبة القانون الدولي الإنساني والدبلوماسية للتطور السريع في التهديدات الرقمية من أجل حماية المدنيين من أي أذى في هذا السياق، جرى ذلك في الحوار الذي تشكل في المنتدى العالمي للأمن السيبراني 2025 الذي عقد في الرياض، وقد سعت اللجنة الدولية إلى التعاون مع الجهات والهيئات الإقليمية لتطوير حلول تضمن الإمتثال للقانون الدولي الإنساني بموازاة تعزيز الأمن السيبراني العالمي[65].

ج- **مدى انطباق مبادئ القانون الدولي الإنساني على الهجمات السيبرانية:** أصبحت الهجمات السيبرانية تشكّل أداة جديدة في النزاعات المسلحة المعاصرة، مما يفرض إعادة النظر في مدى انطباق قواعد ومبادئ القانون الدولي الإنساني عليها. وعلى الرغم من عدم وجود نصوص صريحة تتناول الهجمات السيبرانية، إلاَّ أنَّ المبادئ الأساسية لهذا القانون تبقى مرجعية ملزمة لكل سلوك عدائي، سواء تقليدي أو حديث، وعليه يقوم القانون الدولي الإنساني على المبادئ التي تحكم سير العمليات العدائية وهي[66]:

1. **مبدأ التمييز** (Principe de distinction): ينص القانون الدولي الإنساني على وجوب التمييز الدائم بين المدنيين والمقاتلين، وبين الأعيان المدنية والأهداف العسكرية[67]، ويُمنع استهداف المدنيين أو البنى التحتية المدنية كالمستشفيات، محطات الكهرباء، وشبكات المياه. تطبيقه سيبرانياً: يُعد استهداف نظام معلوماتي مدني أو شبكة خدمات عامة بهجوم إلكتروني يشلها أو يدمرها خرقاً لهذا المبدأ، حتى إن لم يكن الضرر مادياً مباشراً[68].

---

[65]- **إبراز الصوت الإنساني في قلب الأمن السيبراني- اللجنة الدولية للصليب الأحمر في المنتدى العالمي للأمن السيبراني**، 2025/10/14، على الموقع التالي: https: //www.icr.org-ar-law-and-policy-cyber-an، تاريخ الزيارة: 2025/11/22، الساعة: 9.20 مساءا.

[66]- حسن فياض، **الهجمات السيبرانية من منظور القانون الدولي الإنساني**، العدد 114 – تشرين الأول 2020، على الموقع الرسمي للجيش اللبناني، تاريخ الزيارة/ 2025/10/12، الساعة: 9.30 مساء.

[67]- اللجنة الدولية للصليب الأحمر، **دليل تفسيري لمفهوم المشاركة المباشرة بالأعمال العدائية**، الطبعة الأولى، المركز الإقليمي للإعلام، القاهرة، آذار 2010، ص 20.

[68]- نسيب نجيب، الحرب السيبرانية من منظور القانون الدولي الإنساني، **المجلة النقدية للقانون والعلوم السياسية**، المجلد 16، العدد 4، 2021، ص 232-233.

2. **مبدأ التناسب** (Principe de proportionality): يمنع هذا المبدأ تنفيذ هجوم إذا كان الضرر العرضي المتوقع على المدنيين أو الأعيان المدنية مفرطًا بالنسبة للميزة العسكرية المتوقعة[69]، تطبيقه سيبرانياً: أي هجوم إلكتروني قد يؤدي إلى تعطيل بنية تحتية تؤثر على حياة المدنيين – كأنظمة النقل أو الصحة يعتبر غير متناسب إن تجاوز الضرر الحد المعقول عسكريًا [70].
3. **مبدأ الضرورة العسكرية** (Principe de necessity militaries): لا يجوز استخدام القوة أو الوسائل الهجومية إلا لتحقيق هدف عسكري مشروع وضروري، ولا يُبرر استخدام القوة لمجرد التفوق أو الانتقام، تطبيقه سيبرانياً: اختراق نظام دولة معادية يجب أن يكون لتحقيق غاية عسكرية مشروعة[71]، لا لمجرد التخريب أو استعراض القدرات التقنية، وأن يحقق الهدف أقل خطر على المدنيين والأعيان المدنية[72].
4. **مبدأ الإنسانية** (Principe d'humanité): يحظر استخدام أساليب ووسائل تسبب معاناة مفرطة أو غير ضرورية، تطبيقه سيبرانياً: تعطيل أنظمة المستشفيات أو قطع الاتصالات عن المدنيين خلال فترة حرجة يمكن اعتباره مساسًا بكرامة الإنسان ومعاناة غير مبررة.
5. **مبدأ الحياد** (Principe de neutrality): يمنع القانون الدولي الإنساني أطراف النزاع من استخدام أراضي أو أنظمة معلوماتية تابعة لدول محايدة لأغراض عسكرية [73] ، تطبيقه سيبرانياً: إطلاق هجوم إلكتروني عبر خوادم موجودة في دولة محايدة أو استخدامها دون علمها يُعد انتهاكًا لمبدأ الحياد.
6. **مبدأ الحماية الخاصة لبعض الفئات والبنى**(Principe de protection special): يوفر القانون حماية خاصة للمستشفيات، ووحدات الإغاثة، الإعلاميين، والبيئة الطبيعية[74]، تطبيقه سيبرانياً: أي هجوم إلكتروني يستهدف أنظمة معلومات المستشفيات أو يعطل إيصال المساعدات الإنسانية يُعد خرقًا لهذه الحماية الخاصة.
7. **مبدأ المسؤولية القانونية**(Principe de responsibility): تقع المسؤولية القانونية على الدولة أو الفاعل غير الحكومي عن أي انتهاك للقانون الإنساني، وتبعاً لذلك تكللت الجهود الفقهية والدولية بإنشاء المحكمة الجنائية الدولية ومهمتها النظر في

---

[69]– سلوي يوسف الأكيابي، مدى انطباق القانون الدولي الإنساني على الهجمات السيبرانية، **مجلة روح القوانين**، المجلد 35، العدد 101، 2023، ص 1401.

[70]– هبة جمال الدين، الأمن السيبراني والتحول في النظام الدولي، مرجع سابق.

[71]– يحي ياسين سعود، الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني، **المجلة القانونية**، المجلد 4، العدد 4، 2018، ص 94.

[72]– مايكل شميدت، الحرب بواسطة شبكات الاتصال: الهجوم على شبكات الكمبيوتر والقانون في الحرب، **المجلة الدولية للصليب الأحمر**، 2002، ص 130.

[73]– اللجنة الدولية للصليب الأحمر، البروتوكول الإضافي الأول لاتفاقيات جنيف لعام 1949 المتعلق بحماية ضحايا النزاعات المسلحة الدولية، (1977)، جنيف، **اللجنة الدولية للصليب الأحمر**، https://ihl-databases.icrc.org .

المادة 12–15: حماية الوحدات الطبية والمستشفيات.

المادة 70: حماية عمليات الإغاثة.

المادة 79: حماية الصحفيين.

المادة 35 و55: حماية البيئة الطبيعية.

[74]– اللجنة الدولية للصليب الأحمر، البروتوكول الإضافي الأول لاتفاقيات جنيف لعام 1949، (1977)، المرجع السابق.

الجرائم التي يرتكبها الأشخاص الطبيعيون[75]، تطبيقه سيبرانياً: حتى في الهجمات السيبرانية، تقع المسؤولية على الدولة التي انطلق منها الهجوم أو لم تمنعه، وفقًا لمبدأ "السيطرة الفعلية."

خلاصة القول: رغم الطابع المعقد للهجمات السيبرانية وصعوبة إسنادها المباشر، إلاَّ أنَّ جميع المبادئ الأساسية للقانون الدولي الإنساني قابلة للتطبيق عليها. وتُعد تلك المبادئ أداةً أساسية لضمان حماية المدنيين في النزاعات المعاصرة ذات الطابع الرقمي، وتفرض التزامات قانونية صارمة على أطراف النزاع لضبط استخدامهم للوسائل السيبرانية.

الفصل الثاني: تحديات الهجمات السيبرانية المعزّزة بالذكاء الإصطناعي

يشهد الفضاء السيبراني تطورًا سريعًا ومعقدًا في طبيعة الهجمات الرقمية، ولا سيما الهجمات المعزّزة بالذكاء الاصطناعي، التي توظف تقنيات متقدمة لتجاوز نظم الحماية التقليدية وإحداث تأثيرات ملموسة على البنى التحتية الحيوية. وتشكل هذه الهجمات تحديًا مزدوجًا للمجتمع الدولي، إذ تتقاطع الاعتبارات التقنية مع الأبعاد القانونية والسياسية، ما يستدعي وضع أطر قانونية وتنظيمية لضبط السلوك السيبراني وحماية الأمن الدولي.

ويرتبط هذا التحدي بصعوبات تطوير التعاون والتنسيق الدولي بسبب العقبات القانونية في تحديد الفاعلين وإثبات المسؤولية، إضافةً إلى تأثير القدرات السيبرانية على موازين القوى التقليدية، ما يعيد ترتيب العلاقات الدولية ويضاعف التعقيدات الأمنية.

وبناءً عليه، يركّز هذا الفصل على محورين متكاملين:

المبحث الأول: التحديات التي تواجه الجهود الدولية لضبط السلوك السيبراني

المبحث الثاني: الأثر العملي للتهديدات السيبرانية الذكية .

المبحث الأول: التحديات التي تواجه الجهود الدولية لضبط السلوك السيبراني

يمثّل ضبط السلوك السيبراني أحد أبرز التحديات التي يواجهها المجتمع الدولي، نظرًا لطبيعة الهجمات الرقمية المتسارعة والمعقّدة وتأثيرها المباشر على الأمن الدولي والاستقرار الإقليمي. فرغم تعدّد المبادرات الدولية وتنامي الوعي بأهمية حماية الفضاء السيبراني، تواجه الجهود الجماعية عقبات قانونية وتنظيمية، أبرزها ضعف التنسيق والتعاون بين الدول، والإشكاليات المتعلقة بتحديد الفاعلين السيبرانيين وإسناد المسؤولية إليهم.

كما يفرض الفضاء السيبراني إشكاليات على هيكل النظام الدولي، نتيجة سرية القدرات السيبرانية، وعدم وضوح توزيع الموارد الاقتصادية والعسكرية، وتأثير هذه القدرات على موازين القوة التقليدية، مما يعيد ترتيب القوى العالمية ويحفز سلوك الهجمات الإلكترونية بين الدول.

[75]– أشرف عبد العزيز الزيات، **المسؤولية الدولية لرؤساء الدول**، دار النهضة العربية: القاهرة، ط1، 2011، ص 2.

وبناءً عليه، يتناول هذا المبحث هذين المحورين الرئيسيين:

المطلب الأول: الصعوبات التي تواجه الجهود الدولية في التصدي للهجمات السيبرانية

المطلب الثاني: أبرز الإشكالات التي فرضها الفضاء السيبراني على بنيان النظام الدولي.

المطلب الأول: الصعوبات التي تواجه الجهود الدولية في التصدي للهجمات السيبرانية

يمثّل التصدي للهجمات السيبرانية أحد أبرز التحديات التي تواجه المجتمع الدولي في ظل الطبيعة المتسارعة والمعقّدة للتهديدات الرقمية. فرغم تعدّد المبادرات الدولية وتنامي الوعي بأهمية حماية الفضاء السيبراني، ما تزال الجهود الجماعية تعترضها مجموعة من العوائق البنيوية والقانونية التي تحدّ من فاعليتها. وتبرز هذه الصعوبات بصورة خاصة في جانبين أساسيين: الأول مرتبط بضعف التنسيق والتعاون الدولي، والثاني متصل بالإشكاليات القانونية التي تواجه الإتفاقيات الدولية في تحديد الفاعلين السيبرانيين وإثبات المسؤولية عن الهجمات.

ويهدف هذا المطلب إلى تحليل هذه الإشكاليات من خلال فرعين رئيسين:
الفرع الأول: معوّقات التعاون الدولي لمواجهة الهجمات السيبرانية
الفرع الثاني: عوائق التحديد والإسناد السيبراني

الفرع الأول: معوّقات التعاون الدولي لمواجهة الهجمات السيبرانية

نادى العديد من الفقهاء والمتخصصين بضرورة إنشاء وحدات متخصصة لمكافحة الجريمة المعلوماتية على غرار أجهزة البحث الجنائي الوطنية والدولية، كمنظمة الشرطة الجنائية الدولية (الإنتربول)، وذلك بهدف إثبات الجريمة عند وقوعها، وتحديد أدلتها ومرتكبيها، بما يتيح إيجاد آلية فعّالة للتعاون الدولي في مكافحة جرائم الاعتداء على المعلومات الخاصة، وتبادل الخبرات والمعلومات بشأن مرتكبيها ووسائل مكافحتها.
ورغم ما أُثير من دعوات إلى تعزيز هذا التعاون، إلاَّ أنّ ثمة عوائق جوهرية تحول دون تحقيقه، وتجعل من التعاون الدولي في هذا المجال مهمّة معقدة، ويمكن إجمال أبرز هذه العوائق فيما يلي[76]:

أ- **غياب نموذج قانوني موحد للنشاط الإجرامي المعلوماتي:** يُعد اختلاف الأنظمة القانونية في تحديد صور الجريمة المعلوماتية من أبرز العقبات التي تواجه التعاون الدولي، إذ لم تتفق التشريعات الوطنية على تعريف محدد لما يُعد «إساءة استخدام نظم

[76]- قطاف سليمان، مواجهة الجرائم السيبرانية في ضوء الإتفاقيات الدولية، **مجلة البحوث القانونية والإقتصادية**، المجلد 5، العدد 2، 2022، ص 81-83.

المعلومات»، ولا على الأفعال الواجب تجريمها ضمن هذا الإطار. ويرجع ذلك إلى قصور التشريعات الوطنية عن مواكبة التطور التقني المتسارع، مما أفرز تبايناً في المفاهيم والمصطلحات ذات الصلة[77].

ب- **عدم وجود تشريعات خاصة بالجريمة المعلوماتية:** سواء تلك المرتكبة عبر الحاسب الآلي أو شبكة الإنترنت، ولا يزال الجدل قائماً حول أنسب الطرق لمعالجة هذه الظاهرة، بين من يدعو إلى تعديل التشريعات العقابية القائمة لتشمل النماذج الجديدة من الجرائم المعلوماتية، ومن يرى بضرورة تعديل قوانين حماية الملكية الفكرية، وبين من يفضل إصدار تشريعات مستقلة تعالج هذه الجرائم بصورة شاملة.

ويُفضي هذا التباين إلى صعوبة التكييف القانوني للسلوك الإجرامي المعلوماتي، الأمر الذي يُشجع القراصنة على استغلال الثغرات التشريعية وارتكاب أفعالهم عبر الحدود الجغرافية دون رادع فعال، مما يؤكد الحاجة الملحّة إلى تعاون دولي منظم لمواجهة هذا النوع من الجرائم.

ج- **ضعف الإطار الإتفاقي للتعاون الدولي:** تفتقر معظم الدول إلى وجود اتفاقيات ثنائية أو جماعية فعالة في مجال مكافحة الجريمة المعلوماتية. وحتى في الحالات التي وُجدت فيها مثل هذه الاتفاقيات، فإنها غالباً ما تكون قاصرة عن مواكبة التطورات التقنية المتسارعة لأنظمة المعلومات وشبكات الإنترنت، وهو ما يؤدي إلى إرباك المشرّعين والسلطات الأمنية، ويُضعف القدرة على مواجهة التحديات المستجدة.

وقد أولت الأمم المتحدة وبعض الدول الأوروبية هذا الموضوع اهتماماً خاصاً، إلاَّ أنَّ الجهود المبذولة لا تزال محدودة الأثر في تحقيق التعاون المنشود[78].

د- **غياب التنسيق في الإجراءات الجنائية الدولية:** يُعد غياب التنسيق بين الدول فيما يتعلق بإجراءات التحقيق وجمع الأدلة في الجرائم المعلوماتية من أبرز المعوقات العملية للتعاون الدولي. إذ إن الحصول على الأدلة في هذا النوع من الجرائم، ولا سيما تلك الموجودة خارج حدود الدولة، يمثل تحدياً قانونياً وتقنياً بالغ الصعوبة، سواء تعلق الأمر بعمليات الضبط أو التفتيش الإلكتروني لأنظمة معلوماتية أجنبية، أو بالحصول على الأدلة الرقمية ذاتها[79] .

هـ- **إشكالية الاختصاص القضائي في الجرائم المعلوماتية:** تُعتبر مسألة تحديد الاختصاص القضائي الدولي من أكثر الإشكاليات تعقيداً في مجال الجرائم الإلكترونية، نظراً للطبيعة العابرة للحدود لهذه الجرائم، إذ قد تُرتكب في دولة وتُحدث آثارها في دولة أخرى[80].

وتقوم معظم التشريعات الجنائية المعمول بها في العالم على مبدأ الإقليمية في تطبيق القواعد الإجرائية، مما يحدّ من قدرة السلطات الوطنية على ملاحقة المجرمين عبر الحدود. ولهذا، تبرز الحاجة إلى اتفاقيات دولية مرنة تُنظم التعاون القضائي، وتُسهّل إجراءات التحقيق وتبادل الأدلة وتسليم المجرمين.

77- **التعاون الدولي في مكافحة الجرائم السيبرانية: التحديات والفرص، على الموقع التالي:** freetech.tech/information-security-essentials/%D8%A7%D9%84%D8%AA%D8%B9، تاريخ الزيارة: 2025/11/11، الساعة 7 مساء.

78- ليندا شرابسة، السياسة الدولية والإقليمية في مجال مكافحة الجريمة الإلكترونية، **مجلة دراسات وأبحاث**، المجلد 1، العدد 1، 24101-253، 2009 ، ص 250.

79- قطفان سليمان، مواجهة الجرائم السيبرانية في ضوء الإتفاقيات الدولية، مرجع سابق، ص 83.

80- عراب مريم، الإختصاص القضائي في الجرائم المعلوماتية، **حوليات كلية الحقوق**، المجلد 7، العدد 3، 2015، وعلى الموقع التالي، https://www.scribd.comK، ص 231-283.

وعلى الرغم من إبرام عدد من الاتفاقيات الدولية في هذا الشأن، إلا أنها لم تفِ بالغرض المنشود، إذ لا تزال المشكلات المتعلقة بالاختصاص وتبادل الأدلة قائمة، الأمر الذي يفرض ضرورة صياغة تشريعات جنائية أكثر ديناميكية وملاءمة للتطور التكنولوجي.

وفي هذا السياق، نصّت توصية المجلس الأوروبي رقم (13/95) على وجوب تمكين سلطات التحقيق من التدخل السريع لمدّ إجراءاتها إلى أنظمة كمبيوتر موجودة خارج الدولة، شريطة أن يتم ذلك وفق قاعدة قانونية صريحة تضمن عدم المساس بسيادة الدول أو مخالفة أحكام القانون الدولي[81].

الفرع الثاني: عوائق التحديد والإسناد السيبراني

تُعدّ الهجمات السيبرانية من أبرز التهديدات المستحدثة التي تواجه النظام القانوني الدولي المعاصر، إذ تمثل تحديًا حقيقيًا للسيادة الوطنية والأمن الجماعي، وقد دفعت هذه التهديدات المجتمع الدولي إلى إبرام اتفاقيات متعدِّدة، أبرزها اتفاقية بودابست لعام 2001 الخاصّة بمكافحة الجريمة المعلوماتية، واتفاقيات التعاون الثنائي والإقليمي في المجال الرقمي[82].

إلاَّ أنَّ هذه الإتفاقيات تواجه عوائق بنيوية متعدِّدة تحد من فعاليتها في تحديد الفاعلين أو إسناد المسؤولية القانونية عن الأفعال السيبرانية، وتتوزّع هذه العوائق بين ما هو قانوني وتنظيمي واقتصادي وثقافي، مما يجعل من الأمن السيبراني ميدانًا تتشابك فيه الإعتبارات التقنية والسياسية والقانونية على نحو غير مسبوق.

أ- **العوائق القانونية:** تُعدّ العوائق القانونية من أكثر الجوانب تأثيرًا في إضعاف فعالية الإتفاقيات الدولية المتعلقة بالأمن السيبراني، وذلك بسبب الطبيعة المجهولة للفضاء الإلكتروني، وغياب قواعد قانونية دقيقة تحدد المسؤولية الدولية عن الأفعال السيبرانية، تشمل[83]:

1. **صعوبة الإسناد وتحديد الفاعلين:** تُعتبر مشكلة الإسناد من أعقد المسائل القانونية في الفضاء السيبراني، إذ إنّ تحديد هوية مرتكب الهجوم يتطلب قدرات تقنية متقدمة تتجاوز إمكانات كثير من الدول[84].

وغالبًا ما يلجأ الفاعلون إلى استخدام الشبكات الافتراضية الخاصة (VPNs) أو الخوادم الوسيطة (Proxy Servers) لإخفاء مواقعهم الجغرافية، مما يعقد عملية التتبع القانوني والتقني[85]. كما يعمد الفاعلون إلى تطوير تقنيات الهجمات السيبرانية المعتمدة

---

[81]- ليندا شرابسة، السياسة الدولية والإقليمية في مجال مكافحة الجريمة الإلكترونية، مرجع سابق، ص 251.

[82]- إبراهيم السيد أحمد رمضان، مواجهة الهجمات السيبرانية في ضوء أحكام القانون الدولي، **مجلة العلوم القانونية والإقتصادية**، العدد الأول، السنة السابعة والستون، 2025، ص 1808- 1809.

[83]- روان بنت عطية الله الصحفي، **المجلة الإلكترونية الشاملة متعددة التخصصات**، العدد الرابع والعشرون، المجلد 5، 2020، ص 12.

[84]- Michael Schmitt, **Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations**, Cambridge University Press, 2017, p. 45.

[85]- Schmitt, M. N. (Ed.), Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press, (2013), p. 81-96

على الذكاء الإصطناعي مما يزيد من تعقيد قضايا الفضاء السيبراني[86].

وقد أكد تقرير قواعد تالين الصادر عن مركز الدفاع السيبراني التعاوني التابع لحلف الناتو أنّ الإسناد في المجال السيبراني يظلّ مسألة تقديرية، ولا توجد معايير دولية قاطعة لتحديده[87].

2. **غياب المعايير الدولية الموحدة:** لا توجد حتى اليوم معايير قانونية دولية متفق عليها لتحديد المسؤولية عن الأفعال السيبرانية، فكل دولة تتعامل مع الهجمات السيبرانية وفقًا لمصالحها وأولوياتها الوطنية، ما يؤدي إلى تضارب في الممارسات الدولية[88].

وهذا التباين ينعكس على عدم وجود إطار قانوني يحدِّد متى يمكن اعتبار الهجوم السيبراني عدوانًا بالمعنى المقصود في ميثاق الأمم المتَّحدة، مما يجعل تطبيق القواعد المتعلقة بالدفاع الشرعي أو المسؤولية الدولية أمرًا محل خلاف دائم[89].

ب- **العوائق التنظيمية:** تُعدّ الهياكل التنظيمية الوطنية والدولية عاملاً حاسمًا في مدى قدرة الدول على تنفيذ التزاماتها بموجب الإتفاقيات السيبرانية، إلاَّ أنَّ الواقع يكشف عن ضعف واضح في هذا الجانب، يتجلى بـ:

1. **نقص الآليات الفعّالة للتنفيذ:** تفتقر العديد من الدول، خاصّة النامية، إلى مؤسسات وطنية متخصِّصة لمراقبة تنفيذ الإتفاقيات الدولية، أو لهيئات مستقلّة تُعنى بالتحقيق في الجرائم السيبرانية العابرة للحدود[90]. كما أنَّ غياب التنسيق بين الأجهزة الأمنية والقضائية في الدولة الواحدة يؤدي إلى ازدواجية الجهود، ويجعل من عملية تطبيق الإتفاقيات أمرًا صعبًا[91].
2. **المقاومة السياسية:** تُعدّ الإعتبارات السياسية والسيادية من أبرز المعوقات أمام الإلتزام بالإتفاقيات السيبرانية، إذ تخشى بعض الحكومات أن يؤدي التعاون الدولي في هذا المجال إلى كشف بنيتها التحتية التقنية أو تقويض سيادتها الرقمية[92].

---

[86] - jaling Liu, Artificial Intelligence and International Law: The Impact of Emerging Technologies on the Global Legal System, **Economics, Law and Policy**, Vol. 7, No. 2, 2024 , p. 75.

[87] - Schmitt, op. cit, p. 48.

[88] – عبد الفتاح بيومي حجازي، **الدليل الجنائي والتزوير في جرائم الكمبيوتر والأنترنت**، دار الكتب القانونية: مصر، 2008، ص 102.

– **الأمن السيبراني: تحديات الحاضر وحلول المستقبل**، 19/نوفمبر/2024، عالم القانون، على الموقع التالي: https://alamalkanoun.com، تاريخ الزيارة: 2025/11/19، الساعة: 12 ظهراً.

[89] – حسن البنا، **القانون الدولي والأمن السيبراني**، القاهرة: دار النهضة العربية، 2021، ص 25–27.

[90] – حسن البنا، **القانون الدولي والأمن السيبراني، مرجع سابق**، ص 42.

[91] – **التعاون الدولي في مكافحة الجرائم السيبرانية: التحديات والفرص**، 2025/4/9، على الموقع التالي: https://fretch.tech، تاريخ الزيارة: 2025/11/17، الساعة: 11.45 صباحاً.

[92] – عزيزة لرقط، التعاون الدولي في مكافحة الجرائم المعلوماتية (إشكالاتها وآليات التغلب عليها)، **مجلة التواصل في الإقتصاد وإدارة القانون**، المجلد 25، العدد 4، 2019، ص 5–6.

وتتخذ بعض الدول مواقف متحفظة تجاه الإلتزامات الدولية المتعلقة بمشاركة البيانات أو تسليم المتهمين في الجرائم المعلوماتية، خاصة عندما ترتبط هذه الإلتزامات بمصالح استخباراتية أو أمنية[93].

ج- **العوائق المتعلقة بالموارد:** يشمل ذلك:

1. **نقص الموارد البشرية والتقنية:** تواجه الدول النامية تحديًا يتمثّل في قلة الكوادر المؤهلة في مجال أمن المعلومات[94]، علاوةً نقص الكفاءات والخبرات التقنية اللازمة لتنفيذ متطلبات الإتفاقيات الدولية، سواء في مجالات التحليل الجنائي الرقمي أو التحقيقات العابرة للحدود، كما ينعكس هذا النقص على قدرة الدول على بناء أنظمة حماية فعّالة ضدّ الهجمات السيبرانية، مما يجعلها أكثر عرضة للاستهداف[95].
2. **التوزيع غير المتكافئ للموارد:** حتى في الدول التي تملك موارد مالية وتقنية متقدِّمة، غالبًا ما يُلاحظ عدم التوازن في توزيع تلك الموارد بين المؤسّسات المختلفة، أو بين المناطق الجغرافية داخل الدولة الواحدة، مما يؤدِّي إلى ضعف شامل في منظومة الحماية السيبرانية.

د- **العوائق الثقافية والإجتماعية:** تعود إلى الأمور التالية[96]:

1. **التفاوت في الوعي السيبراني:** تختلف الدول في مستوى إدراكها لطبيعة التهديدات السيبرانية، مما يؤثّر على مدى جدية التزامها بالإتفاقيات الدولية ذات الصلة[97].
2. **غياب الثقافة القانونية الرقمية:** تعاني الكثير من الدول العربية من ضعف في الثقافة القانونية الرقمية، حيث لم تُدمج بعد المفاهيم السيبرانية في التعليم القانوني، مما يُضعف تطبيق الإتفاقيات الدولية.
3. **تضارب القيم الإجتماعية والسياسية:** تتباين الدول بين من يركز على حماية الخصوصية ومن يعطي الأولوية للأمن الوطني، وهو ما يخلق توترات في تنفيذ الإتفاقيات السيبراني.

---

[93]- الأمم المتحدة، **تقرير مجموعة الخبراء الحكوميين في الأمن السيبراني الدولي**، نيويورك، 2022، ص. 15.

[94]- **الأمن السيبراني في العالم العربي: التحديات والحلول في عصر التحول الرقمي**، 6/ يونيو 2025، على الموقع التالي: https://zainoonai.com، تاريخ الزيارة: 2025/11/18، الساعة: 7.30 صباحاً.

[95]- European Union Agency for Cyber security (ENISA), **cyber security Skills Gap Report**, 2023, p. 27.

[96]- عبد الإله حمدي، **التحول الرقمي والمسؤولية القانونية في الفضاء الإلكتروني**، دار الفكر العربي، بيروت، 2021، ص. 119.

[97]- **أهم التحيات التي تواجه الأمن السيبراني**، على الموقع التالي: https: //tanqib4tech.com، تاريخ الزيارة: 2025/11/17، الساعة: 10.20 صباحاً.

المطلب الثاني: أبرز الإشكالات التي فرضها الفضاء السيبراني على بنيان النظام الدولي

يُظهر الأمن السيبراني تأثيراً جوهرياً على هيكل النسق الدولي، إذ أفرز عدداً من الإشكاليات تتمثل في سرية القدرات السيبرانية لدى الدول، وعدم وضوح توزيع المقدرات الاقتصادية، فضلاً عن تأثير الفضاء السيبراني على القوة العسكرية التقليدية، مما أدى إلى غموض في موازين القوى وتحفيز سلوك الهجمات السيبرانية بين الفاعلين الدوليين. كما أسهمت القدرات السيبرانية، في إعادة ترتيب القوى العالمية للنظام الدولي.

وعليه، تم تقسيم هذا المطلب إلى فرعين:

يتناول الأول، الإشكاليات المرافقة للتغير في هيكل النظام الدولي، والثاني يستعرض تأثير الأمن السيبراني على ترتيب الدول: منظور قانوني واستراتيجي.

الفرع الأول: الإشكاليات المرافقة للتغير في هيكل النظام الدولي

يشكل الفضاء السيبراني أحد أبرز العوامل التي أسهمت في إحداث تغيرات جوهرية في بنية النظام الدولي، إذ خلق هذا الفضاء حالة من الجدل حول توزيع المقدرات بين الوحدات الدولية الفاعلة، وأعاد النظر في ترتيب القوى داخل النسق الدولي. ويمكن تصنيف أبرز هذه الإشكاليات في ثلاثة محاور رئيسية:

أ- **مقدرات القوى السيبرانية وإشكالية نقص المعلومات:** تكتنف القوى السيبرانية حالة من السرية الشديدة ونقص المعلومات المتاحة للجمهور، نظراً لارتباطها الوثيق بالأمن القومي للدول. وتشمل هذه الإشكالية:

1. غياب البيانات الدقيقة حول عدد العسكريين العاملين في الفضاء السيبراني أو المختصين بالاستخبارات الإلكترونية[98].
2. نقص المعلومات الأقل حساسية، مثل عدد العمالة الماهرة في مجال التكنولوجيا، نتيجة ضعف قواعد البيانات أو تعمد بعض الدول إخفاء هذه المعلومات لأسباب تتعلق بالحرب السيبرانية، مثل ضمان عنصر المفاجأة أو التهرب من المسؤولية القانونية[99].
3. الطبيعة الخفية للمعاملات الاقتصادية المرتبطة بالعملات المشفرة، مما يزيد من صعوبة تقدير القوة السيبرانية الواقعية لكل دولة أو فاعل دولي، ويحد من القدرة على فهم كيفية استباق التهديدات وإدارة المشاريع الرقمية بفعالية[100].

ب- **الأمن السيبراني وإشكالية توزيع المقدرات الاقتصادية:** ترتبط المقدرات الاقتصادية في الفضاء السيبراني بتدفقات البيانات التي أصبحت أساس الإقتصاد العالمي. ومع الإنتشار السريع للتقنيات الرقمية، مثل الحوسبة السحابية وتحليلات البيانات، اكتسبت

98 - Voo Julia and others, National Cyber Power Index 2020 Methodology and Analytical Considerations, China Cyber Policy Initiative, Belfer Center for science and International Affairs, Harvard Kennedy School, Sept 2020, https://www.belfercenter.org/sites/default/files/2020-09/NCPI_2020.pdf, accessed on 4/11/2025.

99- هبة جمال الدين، الأمن السيبراني والتحول في النظام الدولي، **مجلة كلية الاقتصاد والعلوم السياسية**، مرجع سابق.

100- عيسي المسعودي، **احذروا الاستثمار في العملات الرقمية**، الشبيبة، 25 فبراير 2021، على الموقع التالي: https://shabiba.com/article/id/153333، تاريخ الزيارة: 2025/11/5.

البيانات أهمية كبيرة في التنمية الإقتصادية، ليس فقط لصناعات المعلومات، بل أيضًا للصناعات التقليدية والتحويلية.

ويترتب على ذلك:

1. **وجود علاقة مباشرة بين شبكة المعلومات الدولية والتنمية الاقتصادية**[101]، حيث يشكل الإقتصاد الرقمي منصة لتعزيز قدرات الدول، والشركات متعددة الجنسيات، والمنظمات الدولية، على النمو الإقتصادي، وتمكين الفاعلين من سد الفجوات الاقتصادية. في المقابل، يمثل الفضاء السيبراني ساحة لاستغلال القدرات الإقتصادية من قبل وسطاء الظل والجماعات الإرهابية، مما يجعل توزيع الموارد الإقتصادية بين الوحدات الفاعلة غير متكافئ ويصعب رصده.
2. **استخدام العملات المشفرة**، رغم ما توفره من أمان وموثوقية للمعاملات، يحمل مخاطر اقتصادية للدول غير القادرة على الرقابة التكنولوجية، ويتيح خروج ودخول الأموال دون مراقبة البنوك المركزية، مع آثار سلبية محتملة على الأمن الإقتصادي[102].
3. **الهجمات السيبرانية المستمرة على المؤسسات المالية والخدمات الرقمية تزيد من اضطراب النظام المالي العالمي**، وتعرض مصالح الدول والفاعلين الدوليين لتهديدات مباشرة، بما في ذلك سرقة الأصول الفكرية، والغش، وغسيل الأموال والإرهاب[103]، والقرصنة الإلكترونية، وقدرت هذه الجرائم على تحويل الثروات بمليارات الدولارات سنوياً[104].

ج- **تأثير الفضاء السيبراني على القوى العسكرية وزيادة الهجمات السيبرانية:** يسهم الفضاء السيبراني في إعادة تشكيل توزيع القوى العسكرية التقليدية، حيث أصبحت الولايات المتَّحدة الأمريكية، على الرغم من قدرتها العسكرية الهائلة، تواجه تحديات كبيرة في حماية أمنها السيبراني. وتشير الحوادث المسجلة، مثل الهجمات الإلكترونية على الوكالات الحكومية الأمريكية عامي 1998 و 2020، إلى[105]:

1. **صعوبة تحديد المسؤولية المباشرة للدول في الهجمات السيبرانية**، نتيجة الطبيعة المعقدة والمجهولة للمصدر، مما يزيد من حالة عدم الثقة بين الدول.

---

[101] - Kristen Eichenseh, **Order Today's Revolution: Cyber security and the International** , Law fare, February 8, 2018, https://www.lawfareblog.com/todays-revolution-cybersecurity-and-international-order. Accessed on 5/11/2025.

[102]– عيسي المسعودي، **احذروا الاستثمار في العملات الرقمية**، مرجع سابق.

[103]– مستشارية الأمن الوطني: **أمانة سر اللجنة الفنية العليا لأمن الاتصالات والمعلومات**، استراتيجية الأمن السيبراني العراقي، على الموقع التالي: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/00056_06_iraqi-cybersecurity-strategy.pdf، تاريخ الزيارة: 2025/11/06، الساعة: 5 عصراً.

[104]- المؤسسات المالية أمام تهديدات سيبرانية معقدة، **المركز العربي لأبحاث الفضاء الإلكتروني**، 8/يناير 2024، على الموقع التالي: https://accronline.com، تاريخ الزيارة: 2025/11/16، الساعة: 1 ظهراً.

[105] - TIM MAURE, HANNES EBERT & **International Relations and Cyber Security: Carnegie Contribution to Oxford Bibliographies**, OXFORD UNIVERSITY PRESS, Carnegie Endowment for International Peace, JANUARY 11, 2017, https://carnegieendowment.org/2017/01/11/international-relations-and-cyber-security-carnegie-contribution-to-oxford-bibliographies-pub-67672, accessed on 3/11/2025.

– سلمى حامد سليمان، **القوة السيبرانية كساحة للنزاعات الدولية..تحديات متجددة**، 2025/6/3، على موقع مجلة السياسة الدولية التالي: https://www.siyassa.org.eg، تاريخ الزيارة: 2025/11/21، الساعة: 3.30 عصراً.

2. **احتمال تمكن الدول المنافسة من تطوير أسلحة إلكترونية تمنحها ميزة غير متكافئة**، دون اللجوء إلى النزاع العسكري التقليدي، ما يضعف من فاعلية الردع العسكري التقليدي.

كما أفرزت جائحة فيروس كورونا "COVID-19 " تأثيراً إضافياً على الأمن السيبراني، إذ أدّى التحوُّل السريع إلى العمل عن بُعد وزيادة الاعتماد على الإنترنت، بما في ذلك الإنترنت الصناعي وإنترنت الأشياء، إلى زيادة معدلات الهجمات السيبرانية، مستغلة ضعف ثقافة الأمن الرقمي لدى المستخدمين، وانتشار البرمجيات غير الأصلية أو غير المحدثة، واستغلال المخاوف الصحية للمتعاملين على الإنترنت[106].

يمكن القول إن الفضاء السيبراني ساهم في إعادة تشكيل النظام الدولي، سواء على صعيد توزيع المقدرات الإقتصادية أو العسكرية أو التكنولوجية، وهو ما يستدعي مزيداً من البحث القانوني والسياسي لفهم تأثيره على العلاقات الدولية، وفاعلية أسلحة الردع السيبراني، وآليات ضبط النفس بين الدول الفاعلة في ظل المنافسة الرقمية.

الفرع الثاني: تأثير الأمن السيبراني على ترتيب الدول: منظور قانوني واستراتيجي

مع تطوّر الحضارات الإنسانية، ظهرت الحاجة إلى الأمن كآلية أساسية للتحرّر من الخوف وتحقيق الإستقرار والأمان، وقد ارتبط مفهوم الأمن بالقومي ليعبّر عن حماية الدولة ومصالحها الحيوية، باعتبارها كيانًا قانونيًا وسياسيًا يسعى للبقاء ويضمن سيادته على أراضيه وشعبه، فالدولة القومية تمثل الإطار القانوني والسياسي الذي ينظم الأمن القومي ويحدّد أدوات حمايته، سواء عبر القوة العسكرية أو السياسات الإقتصادية والسياسية، بما يحقق حماية مصالحها الحيوية ويدعم قدرتها على الردع في النظام الدولي[107]. كما ساعد التقدم العلمي الحديث على اتساع حجم العلاقات السياسية والفكرية والإقتصادية للدولة التي أصبحت بحاجة ماسة إلى دوام التفاهم واستتباب الأمن واستمرار الإستقرار[108].

ويرتبط الأمن القومي بالبعد الوظيفي الاستراتيجي للدولة، حيث تلعب القوات المسلحة دورًا محوريًا في حماية الدولة من الأخطار الخارجية، سواء من خلال عمليات الردع أو مشاركة الدولة في مسارح العمليات العسكرية. ويُعتبر الردع العسكري أداة رئيسية لضمان استقرار الدولة وتعزيز مكانتها في النسق الدولي، بما يعكس الموقف التقليدي للنظرية الواقعية في العلاقات الدولية.

مع ظهور الفضاء السيبراني وارتفاع مستوى التهديدات الرقمية، أصبح الأمن السيبراني عنصرًا جوهريًا في تقييم القوة الدولية، إذ يفرض على الدول حماية بنيتها التحتية الرقمية الحيوية، بما يشمل شبكات الاتصالات، والقطاع المالي، والطاقة، والبيانات الحكومية الحساسة،

[106]-Faintish News, the 2020 Cyber security stats you need to know, August 20, 2020, https://www.fintechnews.org/the-2020-cybersecurity-stats-you-need -to-know, accessed on 9/11/2025.

[107]– حسن نافعة (وآخرون)، **مقدمة في علم السياسة: الأيديولوجيات والأفكار والنظم السياسية "الجزء الأول "**، الجيزة: دار الجامعة للطباعة والنشر، 2001–2002، ص 41.

[108]– محمد المجذوب، **القانون الدولي العام**، ط الخامسة، بيروت، منشورات الحلبي الحقوقية، 2004، ص 45.

من الهجمات السيبرانية المحتملة. ويترتب على ذلك إعادة النظر في موازين القوى التقليدية، إذ لم يعد امتلاك القوة العسكرية وحده مؤشرًا كافيًا على التأثير الدولي، بل أصبح امتلاك القدرات السيبرانية معيارًا إضافيًا لتحديد النفوذ الدولي[109].

من الناحية القانونية الدولية، يرتبط الأمن السيبراني بمبادئ السيادة وعدم التدخل ومسؤولية الدولة عن الأفعال السيبرانية التي تنطلق من أراضيها[110]. فالدولة ملزمة وفق القانون الدولي بالحفاظ على أمن الفضاء السيبراني ومنع استخدام بنيتها التحتية أو مواردها لتنفيذ هجمات سيبرانية ضد دول أخرى، كما تلتزم بمسؤولية تصحيح الأضرار الناتجة عن أي نشاط سيبراني ينسب إليها، بما ينسجم مع مبادئ المسؤولية الدولية للدول عن الأفعال الضارة.

وقد أظهرت التجارب الدولية أن القدرات السيبرانية قد تمنح الدول التقليدية الأقل قوة إمكانية تحدّي القوى الكبرى، لا سيما نظرًا لانخفاض تكلفة دخول الحرب السيبرانية مقارنة بالحروب التقليدية. ومن الأمثلة البارزة على ذلك: تدريب كوريا الشمالية لآلاف القراصنة الإلكترونيين، وأنشطة الوحدة 61398 الصينية في التجسس السيبراني ضد الولايات المتحدة، والتطور المستمر في تكتيكات الحرب الإلكترونية الإيرانية. كما أن الدول الأكثر تقدّمًا تكنولوجيًا، بقدر ما تمتلك قدرات هجومية متطورة، هي الأكثر اعتمادًا على البنية التحتية الرقمية، مما يجعلها عرضة لهجمات سيبرانية معوِّقة، وهو ما يقوّض أحيانًا الديناميكيات التقليدية للقوة. وعلى النقيض، يرى الباحث Lindsay أن القوى التكنولوجية العظمى وحدها تمتلك القدرة على تطوير أسلحة سيبرانية متقدمة، ما يدل على أن الطابع غير المتكافئ للفضاء السيبراني قد يكون مبالغًا فيه، وأنه سيظل بشكل أساسي تحت سيطرة الدول الكبرى[111].

وفي سياق البحث الأكاديمي، ركّزت مراكز الدراسات والجامعات الكبرى، مثل مركز بلفر للعلوم والشؤون الدولية بجامعة كينيدي هارفارد، على وضع مقاييس تقييم القدرات السيبرانية للدول. وتشمل هذه المقاييس مؤشرات كمية ونوعية، مثل عدد براءات الاختراع التقنية، وعدد الشركات الرائدة في مجال الأمن السيبراني، والكفاءات التقنية الوطنية، إضافة إلى مستوى التخطيط والاستراتيجيات الوطنية للأمن السيبراني وخطط إدارة الأزمات والسياسات الحكومية المتعلقة بالأمن الرقمي[112].

ويخلص التحليل القانوني والاستراتيجي إلى أن الأمن السيبراني أصبح معيارًا أساسيًا لتحديد القوة والنفوذ الدولي، إذ إنه يمثل أداة قانونية واستراتيجية لحماية مصالح الدولة الحيوية، وتعزيز مكانتها الدولية، وإعادة ترتيب مراكز القوة في النسق الدولي وفقًا لما تمتلكه من قدرات رقمية وتقنية، وما تنتهجه من سياسات دفاعية وهجومية مسؤولة قانونيًا، بما يتوافق مع مبادئ القانون الدولي.

المبحث الثاني: الأثر العملي للتهديدات السيبرانية الذكية

---

[109]– حسن نافعة (وآخرون)، **مقدمة في علم السياسة: الأيديولوجيات والأفكار والنظم السياسية "الجزء الأول "**، المرجع السابق، ص 44.

[110]– محمد صلاح عبد اللاه ربيع، الهجمات السيبرانية بين مشروعيتها كوسيلة للدفاع الشرعي وادانتها كاعتداء غير مشروع: دراسة تحليلية في ضوء القانون الدولي، **مجلة الدراسات القانونية والإقتصادية**، المجلد 10، العدد1، 2024، ص 4208–4209.

[111] - Anthony Craig and Brandon Valeriano, Realism and Cyber Conflict: Security in the Digital Age, Feb 3, 2018, https://www.e-ir.info/2018/02/03/realism-and-cyber-conflict-security-in-the-digital-age/, accessed on 9/11/2025.

[112] - Julia Voo & Others, op cit.

يشهد المجتمع الدولي تطوّرًا نوعيًّا في طبيعة التهديدات الرقمية مع بروز ما يُعرف بالتهديدات السيبرانية الذكية، التي توظّف تقنيات الذكاء الاصطناعي والتعلّم الآلي لتجاوز أدوات الحماية التقليدية وإحداث تأثيرات مادية ملموسة. وقد أصبحت هذه التهديدات تمثّل ميدانًا جديدًا للصراع بين الدول، تتقاطع فيه الاعتبارات التقنية مع الأبعاد القانونية والسيادية. ويشكّل محاولة لتأصيل الإطار القانوني المنظّم لهذه الظاهرة المعقّدة، بما يوازن بين متطلبات الابتكار التقني وصون الأمن الدولي وسيادة الدول في الفضاء الإلكتروني.

يتناول هذا المبحث في المطلب الأول، النماذج الحديثة للاختراقات السيبرانية المدعومة بالذكاء الاصطناعي، من خلال دراسات حالة تعبّر عن التداخل بين المجالين الرقمي والمادي، في حين يُعنى **المطلب الثاني**، بتحليل دور الذكاء الاصطناعي في تعزيز منظومات الدفاع السيبراني واستشراف مستقبلها في ظل التطور التقني المتسارع.

المطلب الأول: النماذج الحديثة للإختراقات السيبرانية المعززة بالذكاء الاصطناعي (لبنان – إيران)

شهدت المنطقة نماذج حديثة من الهجمات السيبرانية المدعومة بتقنيات الذكاء الاصطناعي، حيث تمازجت العمليات الرقمية مع تأثيرات مادية ملموسة. يهدف هذا المطلب إلى بيان الكيفية التي غير بها الذكاء الاصطناعي تكتيكات الهجوم وأساليب المواجهة وإطار المساءلة القانونية[113]، وذلك من خلال تحليله في الفرعين العمليين التاليين:

الفرع الأول، يدرس حادثة «البيجر واللاسلكي» في لبنان كنموذج لهجوم مختلط استهدف شبكات اتصال مدنية وبنى بسيطة؛ والثاني، يعرض «حرب الظل» بين إسرائيل وإيران كصراع سيبراني إقليمي استُخدمت فيه أدوات تعطيل واستهداف متقدمة على مدار اثني عشر يوماً.

الفرع الأول: حالة "البيجر واللاسلكي" – لبنان (حرب الـ66 يوم 2024)

[113] - Jialing Liu, "Artificial Intelligence and International Law: The Impact of Emerging Technologies on the Global Legal System", **Economics, Law and Policy**, ISSN 2576-2060 (Print) ISSN 2576-2052 (Online), Vol. 7, No. 2, 2024, www.scholink.org/ojs/index.php/elp.

شهد لبنان يومي 17 و 18 أيلول/سبتمبر عام 2024 موجة من التفجيرات[114]، إستهدفت أجهزة إتصال محمولة شملت أجهزة النداء الآلي "البيجر وأجهزة لاسلكية "icom"، يستخدمها عناصر وقادة من حزب الله اللبناني، على نطاق واسع بغية التواصل بينهم[115]. أدَّت هذه العملية الواسعة إلى مقتل ما لا يقل عن 39 شخصاً وإصابة آلاف آخرين. وقد أقرَّت إسرائيل بهذه العملية [116].

في السياق ذاته، أدان خبراء حقوق الإنسان الأممين التلاعب الخبيث بأجهزة البيجر واللاسلكي التي انفجرت في لبنان وسوريا بصورة متزامنة ووصفوا ذلك بأنَّه إنتهاك مرعب للقانون الدولي، كما تشكِّل هذه الهجمات جرائم حرب من القتل ومهاجمة المدنيين وشن هجمات عشوائية، بالإضافة إلى انتهاك الحق في الحياة[117].

أ- **أسباب تفجيرات البيجر واللاسلكي في لبنان**[118]: نظراً لعدم وجود معلومات دقيقة عن هذه العملية بسبب حداثتها وأيضاً لقدم هذه التقنية، وكذلك لعدم وجود حوادث سابقة لانفجار هذا النوع من هذه الأجهزة، تمَّ الإستعانة بالذكاء الإصطناعي في تحليل هذه الحوادث ووضع سيناريوهات تقنية لعملية الإختراق التي حصلت، وقد اعتمد على برنامج "شات جي بي تي" وهو "4 ". وحول ما إذا كان التفجير ناتجاً عن هجوم سيبراني فكان الرد، أنَّه من الناحية التقنية من الممكن أن تنفجر مثل هذه الأجهزة نتيجة محاولة اختراق سيبراني، ويتطلَّب ذلك شروطاً محدّدة جداً، إذ يمكن للمخترق أن يعدِّل البرمجيات الثابتة أو البرامج المتعلِّقة بالتحكم في استهلاك الطاقة، ممّا يؤدِّي إلى ارتفاع درجة حرارة البطارية وانفجارها، لكنَّ هذا السيناريو معقّد وغير محتمل ما لم تكن هناك ثغرات كبيرة في نظام الأمان أو إدارة الطاقة للجهاز.

كما سيتطلَّب الإختراق استهداف الأجهزة المادية مباشرة، وهو أمر في غاية الخطورة، قد يساعد التحقيق في سجلات الجهاز والبرمجيات في تحديد ما إذا كان هناك اختراق سيبراني واضح[119]. وهذا الأمر لا يمنع من عدم استبعاد احتمالات أخرى، (مثل عيوب البطارية أو الأعطال الكهربائية..).

---

[114]– **مجزرة تفجير شبكة إتصالات حزب الله: الدلالات والتداعيات**، المركز العربي للأبحاث ودراسات السياسات، 2023/9/22، على الموقع التالي: https: www.dohainstitude.org ، تاريخ الزيارة: 2025/11/11، الساعة: 8 صباحاً.

– زيد المحبشي، جبهة الإسناد اللبنانية، **وكالة الأنباء اليمنية: مركز البحوث والمعلومات**، صنعاء 2024، ص 32.

[115]– إلياس فرحات، **حرب السبع جبهات إسرائيلياً..ماذا بعد والغلبة لمن؟**، المركز الإستشاري للدراسات والتوثيق، 2025/8/25.

[116]– محمد شادي و مصطفى أحمد، **استعادة الردع المفقود: انفجارات البيجر في لبنان**، 2024/9/18، على الموقع التالي: https://www.habtoorresearch.com، تاريخ الزيارة: 2024/11/14، الساعة: 4 عصراً.

[117]– **مقرِرون أمميون: إنفجار أجهزة البيجر واللاسلكي إنتهاك مرعب للقانون الدولي، 2024/9/19**، على الموقع التالي: صحيفة الرأي: https://alrai.com، 2024/9/19، تاريخ الزيارى: 2025/11/14، الساعة: 11.30 صباحاً.

[118]– **ماذا قال الذكاء الاصطناعي عن فرضية اختراق وتفجير "البيجر" في لبنان؟**، على الموقع التالي: https: //www.aljazwwra.net 2024/9/17، تاريخ الزيارة:/ 2025/11/9، الساعة 8 صباحاً.

[119]– هاجر أيمن، **تكتيكات الحرب النفسية الإسرائيلية في الحرب على قطاع غزة ولبنان**، 2024/10/22، المركز المصري للفكر والدراسات الإستراتيجية.

كما أجاب البرنامج عن سيناريو يرتبط بإمكانية انفجار هذه الأجهزة "البيجر أو الاسلكي" نتيجة الإختراق في البيانات، حيث أكَّد أنَّ المهاجم يحتاج للوصول إلى الأنظمة الداخلية، وذلك عبر ثغرات في البرمجيات الثابتة أو البرمجيات الأخرى التي تتم من خلال الدخول والتلاعب بدورات شحن البطارية، يقوم المحترفون المخترقين استغلال بعض الثغرات في نظام الجهاز كالأخطاء البرمجية وحالات الطاقة المنخفضة مما يتسبّب في سحب مستمر للطاقة ما يؤدّي إلى إجهاد البطارية، كل ذلك يحصل عند اتصال الجهاز بشبكة خارجية، عندها يمكن للمخترق إرسال أوامر متكرّرة تجهد العمليات الداخلية.

يتطلّب تنفيذ مثل هذا الإختراق معرفة متخصِّصة جداً بهيكل الجهاز وبرمجياته الثابتة، ما يجعل هذا السيناريو معقّداً ونادراً، كما تحدث الإنفجارات في الأجهزة نتيجة لعيوب البطارية أو أخطاء التصنيع أو الظروف البيئية.

إنَّ نظرية الهجوم السيبراني ممكنة التحقُّق، لكنها تتطلّب خبرة فنية عالية واستغلالات دقيقة للبرمجيات الثابتة أو نظام إدارة البطارية أو بروتوكولات الشبكة. كما أنَّ تحليلات الذكاء الإصطناعي تبقى محدودة وتستدعي تحقيقاً رسمياً، ولا يُستبعد سيناريو بديل يتمثّل في تفخيخ الأجهزة يدوياً مع استخدام الرسائل المبهمة[120]، علاوةً على دور تقنية زرّ تشغيل الجهاز.

ب- **التكييف القانوني وحدود المسؤولية الجنائية لحادثة التفجير:** وفقاً للقانون الإنساني الدولي، يحظَّر في جميع الظروف استخدام أي لغم أو فخ أو جهاز آخر مُصَمّم للتسبّب في إصابة زائدة أو مُعاناة غير ضرورية. إنَّ العدوان الإسرائيلي الذي اشتمل على تفخيخ وتفجير أجهزة البيجر واللاسلكي في لبنان يُثير انتهاكات كبيرة للقانون الدولي، حيث يُعَدّ هذا الهجوم عدواناً على الدولة اللبنانية وخرقاً لسيادتها. إذ تخطّت إسرائيل كلّ القواعد المُحَرّمة في الحروب الأمنيّة، ومنها انتهاك مبدأ حماية المدنيين، ومبدأ عدم المشاركة المباشرة في الأعمال العدائية[121].

1. **المسؤولية الجنائية الدولية:** إنّ استهداف المدنيين والتسبّب بقتلهم أو إلحاق الأذى بهم، وعدم التمييز بينهم وبين المقاتلين، يشكّل انتهاكاً جسيماً لقواعد القانون الدولي الإنساني. وإذا تمّ ارتكاب هذه الأفعال بصورة منهجية أو واسعة النطاق، فإنَّها قد ترقى إلى مستوى الجريمة ضدّ الإنسانية. وبالنظر إلى أن القانون الدولي يقرّر مسؤولية الدولة عن الإنتهاكات التي ترتكبها قواتها المسلحة أو وكلاؤها، ويؤكِّد في الوقت نفسه على الطابع الفردي للمسؤولية الجنائية، فإنّ القادة والفاعلين الإسرائيليين الذين أمروا بهذا العدوان أو ساهموا في تنفيذه يتحمّلون المسؤولية الجنائية الدولية عن هذه الأفعال وما ترتّب عليها من نتائج. يمكن للبنان اللجوء إلى المحكمة الجنائية الدولية في حال منحها الإختصاص للنظر في جرائم قتل الصحافيين وتفجيرات البيجر واللاسلكي[122].

---

[120]– صبري عفيف العلوي، الحرب السيبرانية بيم إيران وإسرائيل (2010–2025).. قراءة تحليلية في الأهداف الأدوات والإنعكاسات الإقليمية، **مجلة بريم**، يونيو 2025، ص 7.

[121]– **جديد تفجيرات البيجر.. ماذا يقول القانون عنها؟**، على الموقع التالي: https://ibmirror.com ,lebanonmirror ، 2025/3/26، تاريخ الزيارة: 2025/11/13، الساعة : 2.30 ظهراً.

[122]– ليلى نقولا، **تفجير "البيجر": ماذا يقول القانون الدولي؟**، 2024/9/18، أستاذة العلاقات الدولية في الجامعة اللبنانية، على الموقع التالي: https://www.almayadeen.net/ ، تاريخ الزيارة: 2025/11/14، الساعة: 2 ظهراً.

2. **إنتهاك مبدأ حماية المدنيين:** يفرض القانون الإنساني الدولي حماية المدنيين وحظر استهدافهم. التفجيرات الناتجة عن أجهزة البيجر واللاسلكي التي أدّت إلى قتل مدنيين تشكل انتهاكاً صارخاً وجسيماً لاتفاقيات جنيف الأربع إضافةً إلى البروتوكولات الإضافية[123].
3. **مبدأ عدم المشاركة المباشرة في الأعمال العدائية:** النزاع بين "حزب الله وإسرائيل" يُعدّ نزاعاً مسلّحاً غير دولي يخضع للمادة الثالثة المشتركة التي تحمي المدنيين والمقاتلين الذين لا يشاركون في الأعمال العدائية[124]. استهداف المنتسبين إلى حزب الله الذين كانوا خارج القتال يشكّل انتهاكاً لهذه الحماية، ويضرب أهم مبادئ القانون الدولي الإنساني (التمييز –التناسب– الضرورة)[125]

الفرع الثاني: صراع "الظل"– بين إسرائيل وإيران (حرب الـ يوم 2025)

يشهد النظام الدولي تحولًا نوعيًا في طبيعة النزاعات المسلحة، إذ أصبح الفضاء السيبراني ساحةً رئيسة للمواجهة بين الدول إلى جانب الحروب التقليدية. وتُعدّ الحرب السيبرانية بين إسرائيل وإيران نموذجًا بارزًا لهذا التحول[126]، بعدما تجاوز الصراع بينهما الحدود الجغرافية ليتمدّد إلى المجال الرقمي مستهدفًا البنى التحتية والأنظمة الاقتصادية والعسكرية. أمام هذا المشهد لا بدّ من دراسة تطوُّر ذلك الصراع بين الطرفين وأبعاده القانونية، مع التركيز على دور الذكاء الاصطناعي في تدعيم الهجمات السيبرانية التي حصلت خلال **حرب الاثني عشر يومًا (2025)** بوصفها محطة مفصلية في تطور هذه المواجهة[127].

أ– **تطوّر الصراع السيبراني بين إسرائيل وإيران:** يشهد الصراع السيبراني بين إسرائيل وإيران تصاعدًا نوعيًا، ما أضفى على المواجهة طابعًا إستراتيجيًا معقّدًا.

1. **من المواجهة غير المباشرة إلى الحرب المفتوحة:** شكّل هجوم "ستاكسنت" عام 2010 نقطة التحوّل في العلاقات السيبرانية بين الطرفين، إذ استُخدم الفيروس في تعطيل منشأة "نطنز" النووية الإيرانية، ليؤسس لمرحلة جديدة من "حرب الظل الرقمية" التي تواصلت لعقد كامل[128]، عبر عمليات اختراق متبادلة استهدفت أنظمة حكومية ومالية وإعلامية للطرفين.

في حالة الحرب بين إسرائيل وإيران، استهدفت الهجمات الإسرائيلية شبكات الكهرباء والبنوك الإيرانية وبورصة العملات الرقمية الإيرانية نوبيتكس Nobitex، مما أدّى إلى توقُّف خدمات عامّة ووقوع خسائر مالية ضخمة، وهو ما يُقارب معيار الضرر المكافئ للهجوم

123 – دخلافي سفيان، تكييف الهجمات السيبرانية في ضوء أحكام القانون الدولي، **المجلة الأكاديمية للبحث القانوني**، المجلد 13، العدد2، 2022، ص 318–322.

124– المادة الثالثة المشتركة، من اتفاقيات جنيف الأربعة للعام 1949.

125– شويرب جيلالي ومراد فائزة، مفهوم الحروب السيبرانية والأمن السيبراني، **مجلة الحقوق والحريات**، المجلد 11، العدد 1، 2023، ص 175.

126– ماركو مسعد، حرب سيبرانية بين إسرائيل وإيران... ما أهدافها وأسلحتها؟، **المجلة**، 2025/6/21، على الموقع التالي: majalla.com، تاريخ الزيارة: 2025/11/12، الساعة: 1.30 صباحاً.

127 – شربل صفير، "**صدام عقول " بين إسرائيل وإيران... من ينتصر؟**، المركز الإستشاري للدراسات والتوثيق، 2025/6/20.

128-Syed Qandil Abbas, Hareem Fatima, op. Cit, p. 9-10.

المسلح[129]. بالمقابل، استخدمت إيران هجمات سيبرانية لتعطيل أنظمة الملاحة الإسرائيلية، دون أضرار بشرية مباشرة، مما يثير مسألة التناسب والتمييز في القانون الدولي الإنساني.

2. **تصعيد المواجهة العسكرية والسيبرانية بين الطرفين (2025):** شهد شهر يونيو/حزيران 2025 تحوّل الصراع إلى مواجهة علنية، حيث شنّت إسرائيل هجمات إلكترونية منسّقة مع عمليات عسكرية محدودة ضد أهداف إيرانية. وردّت طهران بإطلاق صواريخ وطائرات مسيّرة نحو منشآت إسرائيلية، مع قطع الاتصال بالإنترنت الوطني يوم 18 يونيو 2025 للحد من آثار الهجوم السيبراني الإسرائيلي الذي عطّل قطاعات حكومية ومصرفية. وقد أعلنت مجموعة "Predatory Sparrow" المقرّبة من إسرائيل مسؤوليتها عن اختراق بنك "سِبَه" الإيراني الحكومي، ما أدى إلى شلل مالي مؤقت وخسارة بيانات حساسة[130].
3. **القدرات الإيرانية وأذرع الحرب الرقمية:** طوّرت إيران قدراتها في مجال الحرب السيبرانية ضمن استراتيجية الردّ غير المتماثل، عبر مجموعات قرصنة تابعة للحرس الثوري مثل APT33 و APT34 و APT39 و APT42 ، تركّز هذه المجموعات على الإختراق طويل المدى وجمع المعلومات، بهدف إضعاف البنية التحتية الرقمية الإسرائيلية دون اللجوء إلى المواجهة التقليدية المباشرة[131].
4. **القدرات الإسرائيلية والوحدة 8200:** تمتلك إسرائيل واحدة من أقوى المنظومات السيبرانية عالميًا، تقودها الوحدة 8200 التابعة للاستخبارات العسكرية. وتُعدّ هذه الوحدة مسؤولة عن تطوير برمجيات التجسس والتحليل الاستخباراتي وتنفيذ الهجمات السيبرانية ضدَّ خصوم إسرائيل وفي مقدمتهم إيران، مستفيدة من تعاون وثيق مع شركات التكنولوجيا الكبرى وخوارزميات الذكاء الاصطناعي التي تتيح تحليلًا لحظيًا للاتصالات والبيانات الإيرانية[132]. كما تعمل إسرائيل على استشراف التهديد المحدق ببناها التحتية نتيجة التهديدات السيبرانية، من خلال تركيزها على إنشاء منظومة دفاع متطورة باستمرار تقوم على توظيف القوة السيبرانية في إجمالي قوتها الصلبة والناعمة في آنٍ واحد[133].

ب– **الذكاء الاصطناعي والحرب السيبرانية – الإطار القانوني والتحديات الإستراتيجية:** يطرح هذا الواقع تحديات تستدعي البحث في الأمور التالية:

---

[129]– صالح حسن، **إسرائيل وإيران بعد حرب الـ12 يوما.. هجمات سيبرانية بلا هدنة، 11/8/2025** ، على الموقع التالي: العين الإخبارية، https: //al-ain.com-Iran- Israel-attak، تاريخ الزيارة: 2025/11/11، الساعة: 2.30 ظهراً.

[130]– إسراء الردايدة، **حرب الظل بين إسرائيل وإيران: التجسُّس والتخريب السيبراني في المواجهة**، 2025/6/18، على الموقع التالي: جريدة الغد، https://alghad.com، تاريخ الزيارة: 2025/11/15، الساعة: 1 صباحاً.

[131]– تقرير معهدRAND ، Iran's Asymmetric Cyber Strategy, 2024، ص 61 .

Cyber Security Threats to Iran and its Countermeasures: Defensive and Offensive Cyber Strategies Journal of Research – in Social Sciences (JRSS), Vol.12, No 02, July 2024 , p. 15-16.

Syed Qandil Abbas , op. Cit, .p. 16. -

[132]– Davies, H. & Abraham, Y. (2025, September 25). Microsoft blocks Israel's use of its technology in mass surveillance of Palestinians. The Guardian : www.theguardian.com/world/2025/sep/25/microsoft-blocks-israels-use-of-its-technology-in-mass-surveillance-of-palestinians

[133]– رندة حيدر، **كيف تحضر إسرائيل حروبها المستقبلية**، مراجعة كتاب السلاح السيبراني في حروب إسرائيل المستقبلية– دراسات لباحثين إسرائيليين كبار، مؤسسة الدراسات الفلسطينية، 2019 ، ص 267.

1. **توظيف الذكاء الاصطناعي كأداة في إدارة العمليات العسكرية:** أصبح الذكاء الإصطناعي عنصرًا مركزيًا في إدارة الصراعات الحديثة، خلال حرب الـ 12 يوماً من العام 2025، وقد استخدمه الطرفان في تحليل أنماط الهجمات السيبرانية والتنبؤ بمصادرها، كما اعتمدت إسرائيل على أنظمة ذكاء إصطناعي متقدّمة لدمج المعلومات الميدانية والإستخباراتية ما أتاح سرعة اتخاذ القرار وتخفيض هامش الخطأ العملياتي[134]، في حين طوّرت إيران مشروع "فجر السيبراني" عام 2024 لتطوير أدوات هجومية تعتمد على تحليل السلوك السيبراني للخصم[135].
2. **الطائرات المسيّرة واستخداماتها في النزاعات الحديثة:** استخدمت إيران طائرات "شاهد–136" لضرب أهداف إسرائيلية خلال الحرب، بينما استعملت إسرائيل طائرات "هيرون" و"هاروب" المزوّدة بأنظمة ذكاء اصطناعي لرصد الإتصالات الإيرانية واستهداف مراكز القيادة[136]. وأثار ذلك جدلاً قانونيًا حول مدى مسؤولية الدولة عن أفعال الأنظمة المستقلة ذات القرار الذاتي في العمليات العسكرية[137].
3. **الإطار القانوني للهجمات السيبرانية بين إسرائيل وإيران خلال حرب الـ12 يومًا:** تُعدّ الهجمات السيبرانية خلال حرب 2025 مثالًا معاصرًا على التحدي القانوني في توصيف الأعمال الرقمية كـ «أعمال عدوان» في ضوء ميثاق الأمم المتَّحدة والقانون الدولي الإنساني.

   إذ يُطرح التساؤل: هل تُعدّ هذه الهجمات استخدامًا للقوة بمفهوم المادة (4/2) من الميثاق؟

   يُشير تقرير مجموعة الخبراء الحكوميين للأمم المتَّحدة (UN GGE) إلى أنَّ الهجمات السيبرانية التي تُحدث آثارًا مادية جسيمة، كتعطيل البنى التحتية أو تعريض حياة المدنيين للخطر، قد تُعامل كاستخدامٍ للقوة يستوجب تطبيق قواعد النزاع المسلح[138].

كما يُبرز النزاع مسألة المسؤولية الدولية، إذ يصعب إثبات مصدر الهجوم أو إسناده بدقّة، بسبب طبيعة الفضاء السيبراني. ويجعل ذلك تطبيق قواعد الردّ المشروع عن النفس وفقاً (للمادة 51 من الميثاق) أمرًا إشكاليًا في غياب دليل قاطع على إسناد ونسبة الهجوم إلى دولة

---

[134]– تقرير وزارة الدفاع الإسرائيلية، AI Integration in National Security Operations, 2024، ص 22.

– كيف استغلت إسرائيل الذكاء الإصطناعي في الهجوم على إيران؟، موقع 24، التالي: https: //24.ae، تاريخ الزيارة: 2025/11/19، الساعة: 1.30 صباحاً.

[135]– وكالة فارس، تقرير حول مشروع "فجر السيبراني"، 15 يناير 2024، ص 3.

[136]– عبد الله الأشعل، **القانون الدولي والنزاعات المسلحة غير التقليدية**، دار النهضة العربية، القاهرة، 2022، ص 119.

– محمد إبراهيم حسن فرج، أثر الحرب الإسرائيلية– الإيرانية على الأمن الإقليمي في الشرق الأوسط، **مجلة السياسة الدولية**، 2025/7/21، على الموقع التالي: https://www.siyassa.org.eg ، تاريخ الزيارة: 2025/11/21، الساعة: 1.30 مساء.

[137]– اللجنة الدولية للصليب الأحمر, **Autonomous Weapon Systems and International Humanitarian Law**, Geneva, 2025/10/13، على الموقع التالي: https:///www.icr.org، تاريخ الزيارة: 2025/11/21، الساعة: 11.15 صباحاً.

[138] - United Nations Group of Governmental Experts (UN GGE). (2015). **Report of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security**. https://undocs.org/A/70/174, date consultation: 17/11/2025, heure: 18.30.

معينة[139].

تُظهر الحرب السيبرانية بين إسرائيل وإيران عام 2025 أنَّ الصراعات الحديثة تجاوزت الميدان العسكري إلى فضاءٍ رقمي مفتوح[140]، اللافت في الأمر إمتزاج الذكاء الإصطناعي بالقدرات التقنية في حرب هجينة عالية الخطورة، أثّرت في الإقتصاد والأمن والبنى التحتية[141].

ويظلّ غياب الإطار القانوني الدولي الملزم أبرز ثغرة في ضبط استخدام القوة السيبرانية، مما يستدعي بلورة اتفاق دولي خاص بالحرب السيبرانية يوازن بين متطلّبات الأمن القومي والإلتزامات الإنسانية، ويضع حدًّا لمسؤولية الدول عن الأفعال المنفّذة عبر الأنظمة الذكية.

المطلب الثاني: واقع الذكاء الإصطناعي في تعزيز الدفاع السيبراني

أصبح الذكاء الاصطناعي عنصرًا محوريًا في تطوير منظومات الأمن السيبراني، بعدما وفّر قدرات متقدمة في التحليل والكشف والإستجابة للتهديدات الرقمية. ويكشف واقع هذا التطوُّر عن بعدين أساسيين، يتمثل الأول في تحليل البيانات الضخمة والتنبؤ بالهجمات ورفع كفاءة حماية الأنظمة، أما البعد الثاني فيتعلق بـ مستقبل الأمن السيبراني، حيث تتوسّع فرص الحماية بقدر ما تتزايد التحديات الناجمة عن تقدم الهجمات وأتمتة أساليب الاختراق. ويبيّن الجمع بين هذين البعدين أن الذكاء الاصطناعي لم يعد مجرد أداة تقنية، بل أصبح ركيزة لإعادة تشكيل الأمن السيبراني حاضرًا ومستقبلاً.

يتناول هذا المطلب الفرعين التالين، الأول يتحدث عن استخدامات الذكاء الاصطناعي في تعزيز الأمن السيبراني، والثاني عن مستقبل الأمن السيبراني في ظل تطور الذكاء الإصطناعي.

الفرع الأول: استخدامات الذكاء الاصطناعي في تعزيز الأمن السيبراني

يمثل الذكاء الاصطناعي ركيزة فاعلة في تطوير وتعزيز آليات الأمن السيبراني المعاصرة، بفضل قدرته على معالجة كميات هائلة من البيانات بسرعة ودقة، يتيح الذكاء الاصطناعي كشف التهديدات المبكرة، أتمتة الاستجابة للحوادث، وتحسين قدرة الأنظمة على التكيُّف مع تهديدات جديدة. ومع ذلك، لا يخلو الأمر من مخاطر؛ إذ إنّ ذات التقنيات يمكن أن تُستخدم لأغراض هجومية أو

---

[139]- United Nations Group of Governmental Experts (UN GGE). (2015). **Report of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security**. https://undocs.org/A/70/174, p 16-18.

[140]– حسن سلمان خليفة البياضاني، الحرب السيبرانية في المواجهة العسكرية الإيرانية (الإسرائيلية)، 30 – يونيو/2025، مركز حمورابي للبحوث والدراسات الإستراتيجية، على الموقع التالي: https://www.hcrsiraq.net، تاريخ الزيارة: 2025/11/20، الساعة: 2 ظهراً.

[141]- Frank G. Hoffman ، مقالته **"Hybrid Threats: Reconceptualizing the Evolving Character of Modern Conflict"** المنشورة في **April 2009** ضمن سلسلة *Strategic Forum No. 240*. digitalcommons.ndu.edu+2ETH Zurich Files+2, date consultation 14/11/2025, الساعة: 11.11 مساء.

- كيف يدير الذكاء الإصطناعي دفّة الحروب الحديثة؟، 20 مايو/2024، **مركز المستقبل للأبحاث والدراسات المتقدمة**، على الموقع التالي: https: //futureuae.com، تاريخ الزيارة: 2025/11/21، الساعة: 11 صباحاً.

تؤدي إلى آثار سلبية أخرى على المجتمع والاقتصاد. يناقش هذا الفرع استخدامات الذكاء الاصطناعي في الأمن السيبراني، وآليات أتمتة الاستجابة، وأنواع التهديدات الناشئة، وكذلك السلبيات والمخاطر المصاحبة [142].

أ- **دور الذكاء الإصطناعي في معالجة البيانات وأتمتة الإستجابة للحوادث الأمنية:** يتجلى ذلك في:

1. **تحليل البيانات الضخمة واكتشاف التهديدات:** يمثل الذكاء الاصطناعي بقدراته الهائلة على معالجة البيانات وتحليلها بسرعة ودقة، سلاحًا قويًا في مكافحة التهديدات السيبرانية[143]. من خلال خوارزميات **التعلم الآلي**، يستطيع الذكاء الاصطناعي تحليل سجلات الأحداث، وحركة الشبكات، وبيانات المستخدمين، للكشف عن أنماط غير عادية قد تشير إلى هجوم سيبراني. يعمل الذكاء الاصطناعي على بناء نموذج لما يبدو عليه السلوك الطبيعي للشبكة. وعندما يتم تقديم بيانات جديدة، يقوم الأخير بمقارنتها بالنموذج الذي تم بناؤه، واكتشاف أي انحرافات عن السلوك الطبيعي، هذه الانحرافات قد تشير إلى وجود تهديد، مثل محاولة اختراق أو هجوم برمجي.
2. **أتمتة الإستجابة للحوادث الأمنية:** عندما يحدث اختراق أمني، فإن كل ثانية تُعد، فكلما تم اكتشاف الهجوم والاستجابة له بشكل أسرع، قلت الخسائر المحتملة. هنا يأتي دور الذكاء الاصطناعي ليلعب دورًا حاسمًا في أتمتة الاستجابة للحوادث الأمنية. من خلال امتلاك نظام أمن سيبراني قادر على اكتشاف الهجوم في لحظته الأولى وتحليل طبيعته، واتخاذ الإجراءات اللازمة لاحتوائه وتقليله من تلقاء نفسه.

ب- **التهديدات التي يشكلها الذكاء الإصطناعي على الأمن السيبراني:** تشمل[144]:

1. **هجمات التصيد الاحتيالي:** هي نوع من الهجمات السيبرانية التي تستهدف الأفراد والشركات من خلال خداعهم للكشف عن معلومات حساسة، مثل كلمات المرور وأرقام بطاقات الائتمان.

تبدأ هجمة التصيد الاحتيالي المتقدمة بجمع المعلومات عن الضحية المحتملة. يمكن للمهاجمين جمع هذه المعلومات من وسائل التواصل الاجتماعي، أو مواقع الويب العامة، أو حتى من قواعد البيانات المسربة. ثم يتم استخدام هذه المعلومات لإنشاء رسالة مصممة خصيصًا للضحية. قد تحتوي الرسالة على روابط تؤدي إلى مواقع ويب مزيفة مصممة لتبدو وكأنها مواقع شرعية. إذا قام الضحية بإدخال معلومات حساسة في هذه المواقع، فإنها تسرق وتستخدم لأغراض ضارة.

2. **الهجمات التي تستهدف أنظمة التعلم الآلي:** تُعتبر أنظمة التعلم الآلي عماد العديد من التقنيات الحديثة، بدءًا من السيارات ذاتية القيادة وحتى تطبيقات التعرف على الوجه. ولكن مع تزايد اعتمادنا على هذه الأنظمة، تزايدت أيضًا المخاطر التي تهددها. فكما يمكن خداع البشر، يمكن أيضًا خداع أنظمة التعلم الآلي، وهذا ما يعرف بهجمات أنظمة التعلم الآلي.

---

[142]– **الأمن السيبراني والذكاء الاصطناعي: تحديات عالم التكنولوجيا الحديثة، على الموقع التالي:** https://www.forsatani.com، تاريخ الزيارة: 2025/10/27، الساعة: 6.15.

[143]– رغدة عتمه، البقاء للأذكى...حين تقاتل التكنولوجيا عن صناعها، independentarabia، **المركز الإستشاري للدراسات والتوثيق**، 2025/6/22.

[144] – **الهجمات السيبرانية بالذكاء الإصطناعي: التحديات والحلول**، 2024/10/24، عبر الموقع التالي: https: //arabi.ai، تاريخ الزيارة: 2025/11/11، الساعة 8.30 صباحاً.

هجمات أنظمة التعلم الآلي هي أي محاولة للتلاعب بنظام التعلم الآلي لجعله يرتكب أخطاء. يمكن أن يكون الهدف من هذه الهجمات هو إلحاق الضرر المادي، أو سرقة البيانات، أو حتى التلاعب بالقرارات التي يتخذها النظام.

3. **تطوير برمجيات ضارة ذكية:** البرمجيات الضارة الذكية هي الجيل الجديد من التهديدات السيبرانية التي تستغل تقنيات الذكاء الاصطناعي والتعلم الآلي لتعزيز قدراتها على الاختراق والتدمير. هذه البرامج ليست مجرد أكواد ضارة بسيطة، بل هي أنظمة معقدة قادرة على التكيف مع البيئة التي تعمل فيها، وتجاوز الدفاعات التقليدية، وحتى إصلاح نفسها.

ج- **مخاطر عامة ناتجة عن الذكاء الاصطناعي في المجال السيبراني:** تتمثل في الآتي:

1. **استخدام الذكاء الاصطناعي في الهجمات** :يمكن للمهاجمين استخدام الذكاء الاصطناعي لشن هجمات أكثر تطورًا.
2. **الاعتماد المفرط على الذكاء الاصطناعي** :قد يؤدي الاعتماد المفرط على الذكاء الاصطناعي إلى تقليل الوعي بالمخاطر وإضعاف الدفاعات البشرية.
3. **الخطأ البشري في تصميم وتطوير أنظمة الذكاء الاصطناعي** :يمكن أن تؤدي الأخطاء في تصميم وتطوير أنظمة الذكاء الاصطناعي إلى ظهور ثغرات أمنية.

د- **سلبيات إضافية لاستخدام الذكاء الاصطناعي**[145]: بالإضافة إلى المخاطر الأمنية، هناك سلبيات تشمل التالي:

1. **فقدان الوظائف** :قد يؤدي انتشار الذكاء الاصطناعي إلى فقدان العديد من الوظائف.
2. **التحيز** :قد تعكس أنظمة الذكاء الاصطناعي التحيزات الموجودة في البيانات التي تم تدريبها عليها.
3. **الخصوصية** :قد يتم استخدام الذكاء الاصطناعي للتجسس على الأفراد وانتهاك خصوصيتهم.

الفرع الثاني: مستقبل الأمن السيبراني في ظل تطور الذكاء الإصطناعي

إن تطور الذكاء الاصطناعي أحدث تحولاً عميقاً في مشهد الأمن السيبراني. هذا التحول يفرض على الدول والمؤسسات إعادة النظر في أدوات الحماية وقدرات الاستجابة، لأن الجمع بين قوة الخوارزميات وهشاشة البنى الرقمية قد يخلق اختباراً وجودياً حقيقياً. يقتضي هذا الاختبار خطوات متدرجة تشمل الجوانب التقنية والقانونية والبشرية، وذلك وفق الآتي: [146]

أ- **التعاون بين الخبراء والمختصين:** يُعدّ التعاون المهني قاعدة الارتكاز في مواجهة التهديدات السيبرانية المتسارعة. فمع تطور التقنيات واتساع الاعتماد على الأنظمة الرقمية، تصبح الهجمات أكثر تعقيداً. لذلك يشكل التنسيق بين الخبراء ضرورة لتعزيز القدرة على التحليل والاستجابة، وتقليل الفجوات التي يستغلها المهاجمون.

---

[145] – عبد الرحمان أنور، **تقاطع الذكاء الإصطناعي والأمن السيبراني– التحديات والحلول**، 2023/4/10، على الموقع التالي: https://jawak.com تاريخ الزيارة: 2025/11/10، الساعة: 5 عصراً.

[146] – **الأمن السيبراني والذكاء الإصطناعي: تحديات عالم التكنولوجيا الحديثة**، 9/ت1/2024، على الموقع التالي: forsatani.com، تاريخ الزيارة: 2025/11/15، الساعة 3.30 عصراً.

ب- **دور التشريعات والقوانين في حماية الأمن السيبراني:** مع تزايد التهديدات السيبرانية وتنوعها، يصبح دور التشريعات والقوانين في حماية الأمن السيبراني أكثر أهمية من أي وقت مضى. هذه التشريعات تعمل كدرع واقٍ يحمي الأفراد والشركات والحكومات من الهجمات الإلكترونية، ويعزز الثقة في الأنظمة الرقمية، كما توفّر قواعد واضحة للمساءلة وتحديد مسؤوليات الجهات الفاعلة.

ج- **الإستثمار في البحث والتطوير في مجال الأمن السيبراني:** تطور التكنولوجيا يفرض سباقاً موازياً في ابتكار حلول الحماية. الاستثمار في البحث والتطوير لم يعد ترفاً بل ضرورة لمواجهة التهديدات المتغيرة. كلما تطورت الهجمات، يجب أن تتطور آليات الدفاع بصورة تواكبها وتتفوق عليها.

د- **التكامل بين الذكاء الاصطناعي والأمن السيبراني:** يُعد الذكاء الاصطناعي محركاً رئيسياً لتعزيز الدفاعات، وفي الوقت نفسه أداة يمكن أن يستغلها المهاجمون. فهو يتيح للأنظمة التعلّم واتخاذ القرار، بينما يعمل الأمن السيبراني على حماية تلك الأنظمة من الاختراق. هذا التكامل يجعل العلاقة بينهما علاقة تكاملية تحتاج إدارة دقيقة.

هـ- **دور الذكاء الاصطناعي في الأمن والدفاع**[147]: الذكاء الإصطناعي له دور كبير في تعزيز الأمن والدفاع، يمكن استخدامه في:

1. **كشف التهديدات** :تحليل كميات هائلة من البيانات للكشف عن أنماط غير طبيعية تشير إلى وجود تهديد.
2. **الاستجابة السريعة** :اتخاذ إجراءات وقائية بشكل أسرع من البشر.
3. **تحليل المخاطر** :تقييم المخاطر المحتملة وتحديد الأولويات.
4. **تطوير تقنيات جديدة** :تطوير تقنيات دفاعية جديدة مثل أنظمة الكشف عن الاختراقات القائمة على الذكاء الاصطناعي.

و- **التحديات العامة للأمن السيبراني**[148]: تواجه الأنظمة الرقمية تحديات مستمرة تتمثل في تطور أساليب الهجمات، ونقص الخبراء المؤهلين، وتعقيد البنى التقنية. هذه التحديات تجعل مهمة التأمين أصعب، وتفرض تطوير استراتيجيات دفاعية أكثر مرونة.

ز- **التحديات المرتبطة باستخدام الذكاء الاصطناعي نفسه:** اعتماد الذكاء الإصطناعي داخل منظومات الأمن السيبراني يرافقه تحديات خاصة، أبرزها[149]:

1. **نقص البيانات** :تحتاج أنظمة الذكاء الاصطناعي إلى كميات كبيرة من البيانات للتدريب، وقد يكون من الصعب الحصول على هذه البيانات في مجال الأمن السيبراني.
2. **ظهور التحيز في النماذج:** قد تعكس أنظمة الذكاء الاصطناعي التحيزات الموجودة في البيانات التي تم تدريبها عليها، مما يؤدي إلى اتخاذ قرارات غير عادلة.
3. **صعوبة تفسير قرارات الأنظمة الذكية:** قد يكون من الصعب فهم كيفية اتخاذ أنظمة الذكاء الاصطناعي لقراراتها، مما يجعل من الصعب تحديد الأخطاء وتصحيحها.

---

[147]– **الأمن السيبراني في عصر الذكاء الإصطناعي.. مخاطر وحلول**، 2023/5/10، على الموقع التالي: https://rowadalaamal.com ، تاريخ الزيارة: 2025/11/8، الساعة: 10 صباحاً.

[148]– أمجد عبد السلام الحميدي، **مستقبل الأمن السيبراني**، على الموقع التالي: https: //eppda.com، تاريخ الزيارة: 2025/11/15، الساعة: 11 صباحاً.

[149]– أميرة محمود حسن إسماعيل، دور الذكاء الإصطناعي في تعزيز الأمن السيبراني دراسة تحليلية للتحديات والحلول المستقبلية، **المجلة المصرية للدراسات المتخصِّصة**، المجلد 13، العدد 46، 2025، مصر، ص 1353– 1354.

ح- **الوظائف المهددة بأتمتة الذكاء الاصطناعي:** انتشار الذكاء الاصطناعي قد يدفع بعض الوظائف إلى الانحسار، مثل[150]:

1. **الوظائف الروتينية** : التي تتطلّب تكرار في المهام البسيطة الروتينية.
2. **وظائف خدمة العملاء** :يمكن للذكاء الاصطناعي التعامل مع العديد من استفسارات العملاء.
3. **الوظائف الإدارية** :يمكن للذكاء الاصطناعي أتمتة العديد من المهام الإدارية وفق هيكلية ادارية مترابطة.

ط- **حماية أنظمة الذكاء الإصطناعي من الناحية الأمنية:** أمن برامج الذكاء الإصطناعي بحد ذاتها لا تقل أهمية عن تأمين البيانات نفسها، يستلزم ذلك القيام بالخطوات التالية[151]:

1. **التشفير** :استخدام تقنيات التشفير لحماية البيانات والاتصالات.
2. **الكشف عن التهديدات** :استخدام أنظمة الكشف عن التهديدات القائمة على الذكاء الاصطناعي.
3. **التدقيق المستمر** :إجراء تدقيق مستمر لأنظمة الذكاء الاصطناعي للكشف عن الثغرات الأمنية.
4. **تدريب الموظفين** :تدريب الموظفين على أفضل الممارسات الأمنية.

ك- **الحلول التقنية لمكافحة الهجمات السيبرانية الذكية**[152]: تطورت الحلول التقنية في مواجهة الهجمات المدعومة بالذكاء الاصطناعي عبر الإعتماد على تقنيات متقدمة للكشف والتحليل الوقائي، ومن أبرزها:

1. **التحليل التنبؤي** :رصد السلوك غير الطبيعي والتنبؤ بالهجمات قبل وقوعها.
2. **التعلم الآلي للكشف التلقائي** :تحسين الاكتشاف الفوري للتهديدات الجديدة عبر التعلم المستمر.
3. **التشفير الذكي** :تقوية حماية البيانات باستخدام خوارزميات تشفير أكثر كفاءة.
4. **الهاكر الأخلاقي والاختبارات الأمنية** :محاكاة الهجمات لاكتشاف الثغرات، مع دعم الذكاء الاصطناعي في سرعة التحليل.

خلاصة القول، لا بدَّ من اتخاذ التدابير الممكنة على المستوى الكلي للأمن السيبراني الفعال في جميع أنحاء العالم[153].

الخاتمة

لقد أظهر هذا البحث أنّ الفضاء السيبراني لم يعد مجرّد امتداد تقني للأنشطة البشرية، بل أصبح مكوّنًا بنيويًا في منظومة العلاقات الدولية المعاصرة، وركيزة أساسية في حسابات الأمن القومي للدول. فمع التحوّل الرقمي العالمي واتّساع استخدام الذكاء

---

[150] – **الأمن السيبراني والذكاء الإصطناعي: تحديات عالم التكنولوجيا الحديثة**، مرجع سابق.

[151] – **الهجمات السيبرانية بالذكاء الإصطناعي: الأسباب وطرق الوقاية منها**، على الموقع التالي: https: // xevensolutions.com/blog/ways-to-p، تاريخ الزيارة: 2025/11/13، الساعة 7.30 صباحاً.

[152] – **الحل للهجمات السيبرانية بالذكاء الاصطناعي: التحديات والحلول**، 24/10/2024/ على الموقع التالي: https://3arabi.ai، تاريخ الزيارة: 2025/11/14، الساعة 7. مساء.

[153] - Ravi Kumar Ramachandran, **Cyber security and its Critical Role in Global Economy** ,ISACA Now Blog, 23 January ,2019 https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2019/cybersecurity-and-its-critical-role-in-global-economy, accessed on 06/11/2025.

الاصطناعي، باتت التهديدات السيبرانية أكثر تعقيدًا وفعالية، الأمر الذي كشف هشاشة الإطار القانوني الدولي التقليدي الذي ما زال يعتمد على قواعد صيغت في زمنٍ لم يكن يتصوّر مثل هذه التحوّلات.

وقد أدّت طبيعة الهجمات السيبرانية، لا سيما تلك المعزّزة بالذكاء الاصطناعي، إلى إضعاف قدرة المجتمع الدولي على تحديد الفاعل المسؤول عنها، وإلى خلق تحدّيات غير مسبوقة في مجالات الإسناد، السيادة، المسؤولية الدولية، وحماية البنى التحتية الحيوية. كما أن الأمثلة العملية من الواقع الميداني مثل تفجيرات أجهزة "البيجر" في لبنان وصراع "الظل" بين إسرائيل وإيران، قد أكّدت أن الذكاء الاصطناعي أصبح أداة مركزية في العمليات الهجينة التي تمزج بين الحرب التقليدية والسيبرانية، وهو ما يفرض إعادة النظر في قواعد اشتباك جديدة تنسجم مع هذه التطورات.

وعليه، فإن مواجهة هذه المخاطر لا تتطلب فقط تطوير منظومة قانونية دولية أكثر تطورًا، بل أيضًا بناء شراكات تقنية واستخباراتية عابرة للحدود، وتأسيس قواعد أخلاقية تنظّم استخدام الذكاء الاصطناعي في النزاعات المسلحة. ولئن كان القانون الدولي لا يزال يراوح مكانه أمام هذه التحديات، فإن الإقرار بالحاجة إلى نظام قانوني سيبراني جديد أصبح مسألة ملحّة لا تحتمل التأجيل.

توصلنا إلى مجموعة من النتائج والتوصيات التالية:

أولًا: النتائج

1. وجود فجوة معيارية واضحة في القانون الدولي تجاه تنظيم الفضاء السيبراني وضبط سلوك الدول فيه.
2. صعوبة الإسناد السيبراني ما تزال العائق الأكبر أمام مساءلة الدول عن الهجمات الرقمية المنسوبة إليها.
3. تباين القدرات السيبرانية للدول أسهم في إضعاف شبكات التعاون الدولي وتبادل المعلومات.
4. تسارع تطوّر الذكاء الاصطناعي أسهم في رفع مستوى التهديدات وتعزيز طابعها الهجومي.
5. قصور الأطر الأممية والإقليمية، بما فيها قواعد تالين، في فرض قواعد إلزامية تنسجم مع طبيعة التهديدات الرقمية.
6. تحوّل القوة السيبرانية إلى عنصر مؤثر في إعادة توزيع القوة داخل النظام الدولي.
7. الهجمات المستجدة كشفت هشاشة البنى التحتية الرقمية وغياب منظومات حماية متكاملة.
8. استمرار الإشكالية المزدوجة بين تعزيز الأمن السيبراني والحفاظ على حقوق الإنسان والخصوصية الرقمية.

ثانيًا: التوصيات

1. الدعوة لصياغة اتفاقية دولية ملزمة تنشئ قواعد عامة للسلوك السيبراني وتحدّد نطاق استخدام القوة في الفضاء الرقمي.
2. تأسيس آلية دولية محايدة للإسناد السيبراني تعتمد على خبرات تقنية وقانونية مشتركة بين الدول.
3. بناء نظام دولي لتبادل البيانات السيبرانية يوفّر إنذارًا مبكرًا للهجمات ويقلّل فجوات الاستجابة.
4. وضع إطار دولي لتنظيم الذكاء الاصطناعي في المجال العسكري والسيبراني للحد من الاستخدامات التي تتجاوز الرقابة البشرية.
5. تعزيز دور الأمم المتحدة من خلال تحويل الوثائق الإرشادية إلى قواعد معيارية قابلة للتنفيذ.
6. إدماج معيار "القوة السيبرانية الوطنية" ضمن مؤشرات تقييم مكانة الدول في النظام الدولي.

7. وضع خطط وطنية وإقليمية لحماية البنى الرقمية الحيوية واختبار جاهزيتها ضمن محاكاة دورية للهجمات.
8. إقرار ميثاق دولي للحقوق الرقمية يحدّد ضوابط حماية البيانات وضمانات عدم إساءة استخدام أدوات الأمن السيبراني.

وبالنظر إلى تسارع التطور التقني مقابل بطء تطوّر القواعد القانونية، يثور تساؤل محوري يمكن أن يشكّل منطلقًا لبحوث لاحقة:

هل سيتمكّن القانون الدولي من ابتكار منظومة تنظيمية قادرة على مواكبة الذكاء الاصطناعي والهجمات السيبرانية قبل أن تتحوّل هذه التقنيات إلى أدوات صراع منفلتة تعجز المنظومة القانونية عن احتوائها؟

المراجع:

أولاً– المراجع العربية

الزيات، أ. ع. ع. (2011). المسؤولية الدولية لرؤساء الدول. القاهرة: دار النهضة العربية.

بن مكي. (2017). السياسة الجنائية لمكافحة جرائم المعلوماتية. الجزائر: دار الخلدونية.

خراشي، ع. ع. إ. (2015). إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها. مصر: دار الجامعة الجديدة للنشر.

الربيعة، ص. ب. ع. ب. ع. الر. (2018). الأمن الرقمي وحماية المستخدم من مخاطر الإنترنت. المملكة العربية السعودية: مركز هيئة الاتصالات وتقنية المعلومات.

عبد الصادق، ع. (2009). الإرهاب الإلكتروني: القوة في العلاقات الدولية – نمط جديد وتحديات مختلفة. القاهرة: مركز الدراسات السياسية والإستراتيجية بالأهرام.

الزرفي، ع. ن. ج. (2019). الجريمة المعلوماتية الماسة بالحياة الخاصة: دراسة مقارنة. المكتب الجامعي الحديث.

اللجنة الدولية للصليب الأحمر. (2010). دليل تفسيري لمفهوم المشاركة المباشرة بالأعمال العدائية (الطبعة الأولى). القاهرة: المركز الإقليمي للإعلام.

مازوني، ك. (2022). الجريمة المعلوماتية. الجزائر: دار الخلدونية.

عبد الفتاح، م. (2014). شرح جرائم الكمبيوتر والإنترنت. القاهرة: دار الكتب والوثائق المصرية، مركز الإمارات للدراسات والبحوث الاستراتيجية.

مناصرة، ي. (2018). جرائم المساس بأنظمة المعالجة الآلية للمعطيات: ماهيتها، صورها، الجهود الدولية لمكافحتها – دراسة مقارنة. الجزائر: دار الخلدونية.

حجازي، ع. ب. (2008). الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت. مصر: دار الكتب القانونية.

البنا، ح. (2021). القانون الدولي والأمن السيبراني. القاهرة: دار النهضة العربية.

حمدي، ع. إ. (2021). التحول الرقمي والمسؤولية القانونية في الفضاء الإلكتروني. بيروت: دار الفكر العربي.

المجذوب، م. (2004). القانون الدولي العام (الطبعة الخامسة). بيروت: منشورات الحلبي الحقوقية.

نافعة، ح.، وآخرون. (2001–2002). مقدمة في علم السياسة: الأيديولوجيات والأفكار والنظم السياسية – الجزء الأول. الجيزة: دار الجامعة للطباعة والنشر.

حيدر، ر. (2019). كيف تحضر إسرائيل حروبها المستقبلية: مراجعة كتاب السلاح السيبراني في حروب إسرائيل المستقبلية – دراسات لباحثين إسرائيليين كبار. مؤسسة الدراسات الفلسطينية.

الأشعل، ع. (2022). القانون الدولي والنزاعات المسلحة غير التقليدية. القاهرة: دار النهضة العربية.

اللجنة الدولية للصليب الأحمر. (2025، 14 أكتوبر). إبراز الصوت الإنساني في قلب الأمن السيبراني: اللجنة الدولية للصليب الأحمر في المنتدى العالمي للأمن السيبراني. تم الاسترجاع في 22 نوفمبر 2025 من https://www.icr.org-ar-law-and-policy-cyber-an

برنامج الأمم المتحدة الإنمائي. (2022). الأمن السيبراني في العالم العربي: التحديات والفرص. نيويورك: برنامج الأمم المتحدة الإنمائي. تم الاسترجاع في 16 نوفمبر 2025 من https://www.arabstates.undp.org

اللجنة الدولية للهلال والصليب الأحمر. (2019). ورقة موقف: القانون الدولي الإنساني والعمليات السيبرانية خلال النزاعات المسلحة. تم الاسترجاع في 22 نوفمبر 2025 من https://www.icr.org

وكالة فارس. (2024، 15 يناير). تقرير حول مشروع "فجر السيبراني".

مهمل، أ. (2018/2017). الإجرام السيبراني (رسالة ماجستير، جامعة محمد بوضياف).

أحمد، ت. (2015). الهجمات على شبكات الحاسوب في القانون الدولي الإنساني (رسالة دكتوراه، جامعة النهرين، العراق).

يوسف، ص. (2013). الجريمة المرتكبة عبر الإنترنت (رسالة ماجستير، جامعة مولود معمري، تيزي وزو).

رشيد، غ. ع. ر. (2004). الحماية القانونية من الجرائم المعلوماتية (رسالة دكتوراه، الجامعة الإسلامية، لبنان).

غلاف، ك.، وجرلان، ز. (2019/2018). جريمة الإرهاب الإلكتروني (رسالة ماجستير، جامعة عبد الرحمان ميرة).

حفصة، م. (2022/2021). جرائم اختراق الأمن السيبراني في التشريع الجنائي المقارن (رسالة ماستر، جامعة بجاية).

سعداني، ن. (2013). آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري (رسالة ماجستير، جامعة حاج لخضر باتنة).

سعداني، ن. (2013). آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري (رسالة ماجستير، جامعة حاج لخضر باتنة).

United Nations. (2022). Report of the Group of Governmental Experts on International Cybersecurity. New York: United Nations.

RAND Corporation. (2024). Iran's Asymmetric Cyber Strategy. RAND.

Israeli Ministry of Defense. (2024). AI Integration in National Security Operations. Ministry of Defense.

تورية، ح. (2011). البحث عن السلام السيبراني. جنيف: الاتحاد الدولي للاتصالات.

تورية، ح. (2006). دليل الأمن السيبراني للبلدان النامية. جنيف: الاتحاد الدولي للاتصالات.

عبد الحي، ص. ع. ع. (2016). استخدام القوة الإلكترونية في التفاعلات الدولية: تنظيم القاعدة نموذجاً. تركيا: المعهد المصري للدراسات السياسية.

رمضان، إ. س. أ. (2025). مواجهة الهجمات السيبرانية في ضوء أحكام القانون الدولي. مجلة العلوم القانونية والاقتصادية، 67(1).

مقلد، إ. ص. (2012). ثورة المعلومات وحروب المستقبل. مجلة آفاق المستقبل، 15.

بوفليح، م. س. (2024). أطر التعاون الدولي للتصدي للتهديدات السيبرانية. مجلة الدراسات القانونية والتطبيقية، 2020.

محمود، ح. هـ. ح. وآخرون. (2025). أثر التهديدات السيبرانية على الأمن القومي: دراسة حالة ماليزيا 2015–2022. المركز الديمقراطي العربي. تم الاسترجاع من https://democratic.de

العتوم، خ. ي. (2022). التهديدات السيبرانية وتحديات الأمن الجماعي في ضوء ميثاق الأمم المتحدة. مجلة دراسات القانون الدولي، جامعة اليرموك.

الصحفي، ر. ب. ع. (2020). [المجلة الإلكترونية الشاملة متعددة التخصصات، العدد الرابع والعشرون، المجلد 5].

الأكيابي، س. ي. (2023). مدى انطباق القانون الدولي الإنساني على الهجمات السيبرانية. مجلة روح القوانين، 35(101).

باي، س. (2023). التهديدات الأمنية السيبرانية: دراسة في انعكاسات الحرب الإلكترونية على الأمن القومي للدول واستراتيجيات المقاومة. مجلة الرسالة للدراسات والبحوث الإنسانية، 8(2).

الشمري، ع. ب. ن. (2020). الحرب السيبرانية في القانون الدولي الإنساني: دراسة تحليلية لقواعد تالين. مجلة جامعة نايف للأمن الوطني، 19.

المريني، ع. س. (2021). الناتو والأمن السيبراني من الدفاع الجماعي إلى الردع الرقمي. مجلة المستقبل العربي، مركز دراسات الوحدة العربية.

عراب، م. (2015). الإختصاص القضائي في الجرائم المعلوماتية. حوليات كلية الحقوق، 7(3). تم الاسترجاع من https://www.scribd.comK

فيلالي، أ. و شليل، ع. ل. (2019). تهديدات أمن المعلومات وسبل التصدي لها. مجلة البشائر الاقتصادية، 4(3).

قطاف، س. (2022). مواجهة الجرائم السيبرانية في ضوء الاتفاقيات الدولية. مجلة البحوث القانونية والاقتصادية، 5(2).

شرابسة، ل. (2009). السياسة الدولية والإقليمية في مجال مكافحة الجريمة الإلكترونية. مجلة دراسات وأبحاث، 1(24101–253).

شميدت، م. (2002). الحرب بواسطة شبكات الاتصال: الهجوم على شبكات الكمبيوتر والقانون في الحرب. المجلة الدولية للصليب الأحمر.

العيداني، م. (2024). التهديدات السيبرانية وجريمة المعلومات. مجلة الاجتهاد للدراسات القانونية والاقتصادية، 12(1).

حمزة، م. ج. (2021). القانون الدولي الإنساني والفضاء السيبراني: قراءة في قواعد تالين. المجلة القانونية الدولية، جامعة القاهرة.

مشوس، م. (2019). الجهود الدولية لمكافحة الإجرام السيبراني. مجلة الواحات للبحوث والدراسات، 12(2). تم الاسترجاع من https://www.asjp.cerist.dz/en/PresentationRevue/2

نجيب، ن. (2021). الحرب السيبرانية من منظور القانون الدولي الإنساني. المجلة النقدية للقانون والعلوم السياسية، 16(4).

الربيعي، ن. م. (2024). الجريمة السيبرانية وآليات مكافحتها. مجلة الفارابي للعلوم الإنسانية، 3(1).

جمال الدين، هـ. (2025). الأمن السيبراني والتحول في النظام الدولي. مجلة كلية الاقتصاد والعلوم السياسية. تم الاسترجاع من https://jpsa.journals.ekb.eg

عبد الحافظ، هـ. ع. م. (2025). التحديات التي تواجه الأمن السيبراني. مجلة العلوم الإنسانية والطبيعية، 6(7)، 720–734. تم الاسترجاع من http://www.hnjournal.net/6-7-46

رحيم، و. م. (2025). الإرهاب الإلكتروني وأثره على الأمن الوطني. مركز الدراسات الإستراتيجية والدولي، جامعة بغداد. تم الاسترجاع من https://www.researchgate.net

بوكابوس، و. (2019). تحول القوة في العلاقات الدولية: دراسة في انتقال القوة من التقليدية إلى الحديثة. المركز الديمقراطي العربي للدراسات الإستراتيجية والسياسية والاقتصادية، ألمانيا.

سعود، ي. ي. (2018). الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني. المجلة القانونية، 4(4).

عبد الحافظ العودي، هـ. ع. م. (2025). التحديات التي تواجه الأمن السيبراني. مجلة العلوم الإنسانية والطبيعية، 6(7).

لرقط، ع. (2019). التعاون الدولي في مكافحة الجرائم المعلوماتية: إشكالاتها وآليات التغلب عليها. مجلة التواصل في الاقتصاد وإدارة القانون، 25(4).

المركز العربي لأبحاث الفضاء الإلكتروني. (2024، 8 يناير). المؤسسات المالية أمام تهديدات سيبرانية معقدة. تم الاسترجاع من https://accronline.com

ربيع، م. ص. ع. ل. (2024). الهجمات السيبرانية بين مشروعيتها كوسيلة للدفاع الشرعي وإدانتها كاعتداء غير مشروع: دراسة تحليلية في ضوء القانون الدولي. مجلة الدراسات القانونية والاقتصادية، 10(1).

المركز العربي للأبحاث ودراسات السياسات. (2023، 22 سبتمبر). مجزرة تفجير شبكة اتصالات حزب الله: الدلالات والتداعيات. تم الاسترجاع من https://www.dohainstitute.org

المحبشي، ز. (2024). جبهة الإسناد اللبنانية. وكالة الأنباء اليمنية: مركز البحوث والمعلومات.

فرحات، إ. (2025، 25 أغسطس). حرب السبع جبهات إسرائيلياً.. ماذا بعد والغلبة لمن؟. المركز الاستشاري للدراسات والتوثيق.

أيمن، هـ. (2024، 22 أكتوبر). تكتيكات الحرب النفسية الإسرائيلية في الحرب على قطاع غزة ولبنان. المركز المصري للفكر والدراسات الاستراتيجية.

العلوي، ص. ع. (2025، يونيو). الحرب السيبرانية بين إيران وإسرائيل (2010–2025): قراءة تحليلية في الأهداف والأدوات والانعكاسات الإقليمية. مجلة بريم.

دخلافي، س. (2022). تكييف الهجمات السيبرانية في ضوء أحكام القانون الدولي. المجلة الأكاديمية للبحث القانوني، 13(2).

الصليب الأحمر الدولي. (1949). المادة الثالثة المشتركة، من اتفاقيات جنيف الأربعة للعام 1949.

جيلالي، ش. و فائزة، م. (2023). مفهوم الحروب السيبرانية والأمن السيبراني. مجلة الحقوق والحريات، 11(1).

صفير، ش. (2025، 20 يونيو). "صدام عقول" بين إسرائيل وإيران... من ينتصر؟. المركز الاستشاري للدراسات والتوثيق.

البياضاني، ح. س. خ. (2025، 30 يونيو). الحرب السيبرانية في المواجهة العسكرية الإيرانية (الإسرائيلية). مركز حمورابي للبحوث والدراسات الإستراتيجية. تم الاسترجاع من https://www.hcrsiraq.net

مركز المستقبل للأبحاث والدراسات المتقدمة. (2024، 20 مايو). كيف يدير الذكاء الاصطناعي دفّة الحروب الحديثة؟ تم الاسترجاع من https://futureuae.com

عتمه، ر. (2025، 22 يونيو). البقاء للأذكى... حين تقاتل التكنولوجيا عن صناعها. independentarabia، المركز الاستشاري للدراسات والتوثيق.

إسماعيل، أ. م. ح. (2025). دور الذكاء الاصطناعي في تعزيز الأمن السيبراني: دراسة تحليلية للتحديات والحلول المستقبلية. المجلة المصرية للدراسات المتخصِّصة، 13(46).

. (2025). ماهو الأمن السيبراني وأنواعه ولماذا هو ضروري؟ تم الاسترجاع في 26 أكتوبر 2025 من elmarefa.com https://elmarefa.com

. (2025، 27 مارس). فهم تهديدات الأمن السيبراني والحماية منها. تم الاسترجاع في 12 نوفمبر 2025 من almithaqinstitute.com https://almithaqinstitute.com/ar/blog/

موسى، ف. خ. (2025). تحديات الأمن السيبراني وكيفية مواجهتها. تم الاسترجاع في 26 أكتوبر 2025 من https://www.lebarmy.gov.lb

. (بدون تاريخ). أشهر تهديدات الأمن الإلكتروني وطرق التصدي لمواجهتها. تم الاسترجاع في 13 نوفمبر 2025 من teknokeys.com https://teknokeys.com

. (بدون تاريخ). المخاطر السيبرانية: الكشف عن مخاطر الأحداث، التهديد المتزايد للهجمات السيبرانية. تم الاسترجاع في 16 نوفمبر 2025 من Faster Capital https://fastercapital.com

مركز التميز في الدفاع السيبراني التعاوني. (بدون تاريخ). تم الاسترجاع في 18 نوفمبر 2025 من https://ar.hisour.com

فياض، ح. (2020، تشرين الأول). الهجمات السيبرانية من منظور القانون الدولي الإنساني، العدد 114. تم الاسترجاع في 12 أكتوبر 2025 من الموقع الرسمي للجيش اللبناني

اللجنة الدولية للصليب الأحمر. (1977). البروتوكول الإضافي الأول لاتفاقيات جنيف لعام 1949 المتعلق بحماية ضحايا النزاعات المسلحة الدولية. جنيف: اللجنة الدولية للصليب الأحمر. تم الاسترجاع من https://ihl-databases.icrc.org

. (بدون تاريخ). التعاون الدولي في مكافحة الجرائم السيبرانية: التحديات والفرص. تم الاسترجاع في 11 نوفمبر 2025 من freetech.tech https://freetech.tech/information-security-essentials/%D8%A7%D9%84%D8%AA%D8%B9

. (بدون تاريخ). أهم التحديات التي تواجه الأمن السيبراني. تم الاسترجاع في 17 نوفمبر 2025 من tanqib4tech.com https://tanqib4tech.com

. (2024، 19 نوفمبر). الأمن السيبراني: تحديات الحاضر وحلول المستقبل. تم الاسترجاع في 19 نوفمبر 2025 من alamalkanoun.com https://alamalkanoun.com

. (2025، 6 يونيو). الأمن السيبراني في العالم العربي: التحديات والحلول في عصر التحول الرقمي. تم الاسترجاع في 18 نوفمبر 2025 من zainoonai.com https://zainoonai.com

المسعودي، ع. (2021، 25 فبراير). احذروا الاستثمار في العملات الرقمية. الشبيبة. تم الاسترجاع من https://shabiba.com/article/id/153333

سليمان، س. ح. (2025، 3 يونيو). القوة السيبرانية كساحة للنزاعات الدولية: تحديات متجددة. تم الاسترجاع في 21 نوفمبر 2025 من https://www.siyassa.org.eg

شادي، م. و أحمد، م. (2024، 18 سبتمبر). استعادة الردع المفقود: انفجارات البيجر في لبنان. تم الاسترجاع في 14 نوفمبر 2024 من https://www.habtoorresearch.com

الرأي. (2024، 19 سبتمبر). مقرّرون أمميون: انفجار أجهزة البيجر واللاسلكي انتهاك مرعب للقانون الدولي. تم الاسترجاع في 14 نوفمبر 2025 من https://alrai.com

ماذا قال الذكاء الاصطناعي عن فرضية اختراق وتفجير "البيجر" في لبنان؟، على الموقع التالي: https: //www.aljazwwra.net 2024/9/17، تاريخ الزيارة:/ 12025/11/9 .. المراجع العربية

إبراهيم السيد أحمد رمضان، مواجهة الهجمات السيبرانية في ضوء أحكام القانون الدولي، مجلة العلوم القانونية والإقتصادية، العدد الأول، السنة السابعة والستون، 2025.

اسماعيل صبري مقلد، ثورة المعلومات وحروب المستقبل، مجلة آفاق المستقبل، العدد15، القاهرة، أيلول 2012.

"جديد تفجيرات البيجر.. ماذا يقول القانون عنها؟"، lebanonmirror، 2025/3/26، تم الاطلاع عليه في 2025/11/13، https://ibmirror.com

ليلى نقولا، تفجير "البيجر": ماذا يقول القانون الدولي؟، 2024/9/18، تم الاطلاع عليه في 2025/11/14، /https://www.almayadeen.net

المراجع الأجنبية:

Léopold, & Lhotse, S. (2007). La securité informatique (3éme éd.). Éditions Puff.

Schmitt, M. N. (Ed.). (2013). Tallinn Manual 1.0 on the International Law Applicable to Cyber Warfare. Cambridge University Press.

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

Rid, T. (2012). Cyber War Will Not Take Place. Journal of Strategic Studies, 35(1), 5–32. https://doi.org/10.1080/01402390.2011.608939

Liu, J. (2024). Artificial Intelligence and International Law: The Impact of Emerging Technologies on the Global Legal System. Economics, Law and Policy, 7(2). www.scholink.org/ojs/index.php/elp

Abbas, S. Q., & Fatima, H. (2024). Cyber Security Threats to Iran and its Countermeasures: Defensive and Offensive Cyber Strategies. Journal of Research in Social Sciences (JRSS), 12(2), July 2024.

Mozzaquatro, M., Agostinho, B., Gonçalves, C., Martins, D., Jardim-Gonçalves, J., & R. (2018). An Ontology-Based Cybersecurity Framework for the Internet of Things. Sensors (Basel), 18(9), 3053.

United Nations Group of Governmental Experts (UN GGE). (2015). Report on Developments in the Field of Information and Telecommunications in the Context of International Security. https://undocs.org/A/70/174

Eichenseh, K. (2018, February 8). Today's Revolution: Cyber security and the International Order. Lawfare. https://www.lawfareblog.com/todays-revolution-cybersecurity-and-international-order

Davies, H., & Abraham, Y. (2025, September 25). Microsoft blocks Israel's use of its technology in mass surveillance of Palestinians. The Guardian. www.theguardian.com/world/2025/sep/25/microsoft-blocks-israels-use-of-its-technology-in-mass-surveillance-of-palestinians

"Challenges of International Law in Confronting Cyber Threats"

Prepared by:

Dr. Jihane Hamieh

Research Professor in International Criminal Law

Moussa Al-Bazzal

Researcher in Public International Law

1446 AH – 2025 AD

Abstract:

This study examines the growing challenges posed by cyberspace to international law, particularly with the evolution of AI-enhanced cyberattacks. The intangible nature of such attacks and the difficulty of attributing them to specific states have created a significant legal gap, limited the effectiveness of state responsibility mechanisms and weakened the international system's ability to address cyber threats. The research presents the theoretical foundations of cyber security threats, reviews global and regional efforts to regulate cyber conduct, and analyzes practical case studies that highlight the vulnerability of digital infrastructures. It concludes by emphasizing the need for a more advanced global legal framework and enhanced international cooperation capable of keeping pace with rapid technological innovation.

Keywords: Cybersecurity – Cyberattacks – Artificial Intelligence – International Responsibility – International Law – Cyber Warfare.