International Journal of Law Research and Studies (IJLRS)
المجلة الدولية للبحوث والدراسات القانونية
IJLRS
Vol. (5), No. (9)
September 2026
الإصدار (5)، العدد (9)

التنظيم الدولي للجرائم السيبرانية الدولية في إطار القانون الجنائي الدولي

فاطمة دربي سعد الشهري
باحثة ماجستير، قسم القانون العام، كلية الحقوق، جامعة الملك عبدالعزيز، المملكة العربية السعودية
mevaalshehri@hotmail.com

رواء غازي المكي
المشرفة الأكاديمية، قسم القانون العام، كلية الحقوق، جامعة الملك عبدالعزيز، المملكة العربية السعودية

المستخلص

أصبحت الجرائم السيبرانية الدولية من أكثر التحديات خطورة على المجتمع الدولي، مزعزعةً بذلك أمن الدول واستقرارها، لما تتسم به من طابع عابر للحدود، وسرعة فائقة في التنفيذ، وصعوبة بالغة في الإسناد، فضلاً عن مقدرتها على إحداث أضرار جسيمة تمس البنى التحتية الحيوية، والأمن الاقتصادي والسياسي للدول، فقد تجاوزت هذه الجرائم الإطار التقليدي للجرائم السيبرانية، لتشكّل تحدياً وتهديداً حقيقياً للسلم والأمن الدوليين، الأمر الذي يستوجب إعادة النظر في مدى إمكانية إخضاعها لأحكام القانون الجنائي الدولي.

يهدف هذا البحث إلى دراسة مفهوم الجرائم السيبرانية الدولية المهددة للسلم والأمن الدوليين وبيان خصائصها وآثارها على أمن واستقرار الدول، والبحث عن مدى إمكانية إدراجها ضمن اختصاص المحكمة الجنائية الدولية، كما يسعى هذا البحث إلى تحليل مدى إمكانية تكييف هذه الجرائم كأحد الجرائم الأربع المنصوص عليها في نظام روما الأساسي للمحكمة الجنائية الدولية، وهي: جريمة الإبادة الجماعية، والجرائم ضد الإنسانية، وجرائم الحرب، وجريمة العدوان.

ويخلص البحث إلى أن الجرائم السيبرانية الدولية المهددة للسلم والأمن الدوليين، على الرغم من عدم النص عليها صراحةً في نظام روما الأساسي للمحكمة الجنائية الدولية، إلا أنه يمكن في أن تندرج ضمن الجرائم الدولية الأربع في نظام روما الأساسي عند توافر عناصر الخطورة البالغة والاعتداء على المصالح المحميّة دولياً، وبالأخص في حالات النزاعات المسلحة وفي حالات الهجمات السيبرانية واسعة النطاق. كما توصي الباحثة بضرورة تطوير قواعد القانون الجنائي الدولي، وإدراج الجرائم السيبرانية المهددة للسلم والأمن الدوليين ضمن اختصاص المحكمة الجنائية الدولية.

الكلمات المفتاحية: الجرائم السيبرانية الدولية، السلم والأمن الدوليين، المحكمة الجنائية الدولية، الاختصاص الجنائي الدولي، الجرائم الأربع الأساسية.

International Journal of Law Research and Studies (IJLRS)
المجلة الدولية للبحوث والدراسات القانونية
Vol. (5), No. (9)
IJLRS
September 2026
الإصدار (5)، العدد (9)

The International Regulation of Cybercrimes within the Framework of International Criminal Law

Fatimah Darbi Saad Alshehri
Master Researcher, Department of Public Law, Faculty of Law, King Abdulaziz University, Kingdom of Saudi Arabia
fatimahdalshehri@gmail.com

Rawaa Ghazi Almakki
Academic Supervisor, Department of Public Law, Faculty of Law, King Abdulaziz University, Kingdom of Saudi Arabia

Abstract

International cybercrimes have become one of the most serious challenges facing the international community, thereby undermining the security and stability of states due to their transnational nature, the exceptional speed with which they can be perpetrated, and the considerable difficulty of attributing responsibility for them. Moreover, such crimes have the capacity to cause severe damage to critical infrastructure and to the economic and political security of states. These crimes have consequently transcended the traditional framework of cybercrime to constitute a genuine challenge and threat to international peace and security, necessitating a reconsideration of the extent to which they may be subject to the provisions of international criminal law.

This research aims to examine the concept of international cybercrimes that threaten international peace and security, and to identify their characteristics and effects on the security and stability of states. It also seeks to explore the extent to which such crimes may fall within the jurisdiction of the International Criminal Court (ICC). Furthermore, the research analyzes the possibility of characterizing these crimes as one of the four crimes established under the Rome Statute of the International Criminal Court: genocide, crimes against humanity, war crimes, and the crime of aggression.

The research concludes that, although international cybercrimes threatening international peace and security are not expressly provided for in the Rome Statute of the International Criminal Court, they may, under certain circumstances, fall within the scope of the four crimes established by the Rome Statute where the requisite elements of gravity and attacks against internationally protected interests are present, particularly in situations of armed conflict and in cases of large-scale cyberattacks. Accordingly, the researcher recommends developing the rules of international criminal law and incorporating cybercrimes that threaten international peace and security within the jurisdiction of the International Criminal Court.

Keywords: International Cybercrimes, International Peace and Securitym, International Criminal Court, International Criminal Jurisdiction, Four Core Crimes.

مقدمة

ظهر للعالم على امتداد العقود الأخيرة تطورات غير معهودة في ميدان التكنولوجيا والفضاء الرقمي، مما أسفر عن ظهور أشكال متطورة من الجرائم العابرة للحدود، وفي مقدمتها الجرائم السيبرانية الدولية المهددة للسلم والأمن الدوليين، والتي أصبحت تشكل تهديدًا حقيقياً للمجتمع الدولي كافة، لقدرتها على استهداف البنية التحتية الحيوية للدولة، وتعطيل مرافقها الأساسية، والإضرار بأمنها القومي والاقتصادي.

وعلى الرغم من تنامي خطورة الجرائم السيبرانية وامتداد آثارها، إلا أنه لا يزال القانون الدولي الجنائي يفتقر إلى قواعد صريحة منظِّمة للمسؤولية الدولية والمسؤولية الجنائية الفردية عن هذا النوع من الجرائم. كما يثور جدلٌ فقهي وقانوني حول مدى إمكانية تكييف الجرائم السيبرانية المهددة للسلم والأمن الدوليين ضمن الجرائم الدولية الأساسية المنصوص عليها في نظام روما الأساسي للمحكمة الجنائية الدولية، وهي جريمة الإبادة الجماعية، والجرائم ضد الإنسانية، وجرائم الحرب، وجرائم العدوان، لا سيما عندما يتم ارتكاب الجرائم السيبرانية في سياق النزاعات المسلحة أو بلوغها درجة من الجسامة تجعلها مماثلة في آثارها الأفعال التقليدية التي تدخل ضمن نطاق هذه الجرائم.

أولاً/ مشكلة الدراسة:

تتمثَّل مشكلة الدراسة في غياب الإطار القانوني المنظِّم للجرائم السيبرانية المهددة للسلم والأمن الدوليين، الأمر الذي يثير العديد من التساؤلات حول مدى إمكانية تكييفها ضمن الجرائم الدولية الأساسية الأربع المنصوص عليها في نظام روما الأساسي، وإسناد المسؤولية الدولية للدول، وإخضاع مرتكبيها للمساءلة أمام المحكمة الجنائية الدولية في ضوء مبدأ الشرعية الجنائية.

من خلال ما سبق تتلخص مشكلة الدراسة في تساؤل رئيسي مفاده: **ما مدى إمكانية تكييف الجرائم السيبرانية الدولية المهددة للسلم والأمن الدوليين ضمن الجرائم الدولية الأساسية الأربع المنصوص عليها في نظام روما الأساسي للمحكمة الجنائية الدولية؟**

ويتفرع عن السؤال الرئيسي عدة أسئلة، ألا وهي:

1- ما مفهوم الجرائم السيبرانية الدولية المهددة للسلم والأمن الدوليين؟

2- ما مدى كفاية قواعد القانون الدولي الجنائي في تنظيم الجرائم السيبرانية المهددة للسلم والأمن الدوليين؟

3- ما الإشكاليات القانونية الناجمة عن تكييف الجرائم السيبرانية الدولية ضمن الجرائم الأربع المنصوص عليها في نظام روما الأساسي؟

4- ماهي آليات تطوير التنظيم الدولي للجرائم السيبرانية الدولية المهددة للسلم والأمن الدوليين ؟

ثانياً/ أهمية الدراسة:

تنبع أهمية الدراسة من عدة اعتبارات قانونية وعملية، يتمثَّل أولها في حداثة موضوع الجرائم السيبرانية المهددة للسلم والأمن الدوليين، وما فرضته من تحديات متزايدة على المجتمع الدولي، وذلك في ظل التطورات التقنية المتسارعة وتزايد الاعتماد على الفضاء السيبراني، الأمر الذي أظهر صوراً إجرامية تجاوزت الحدود التقليدية للقانون الدولي الجنائي.

كما تتمثَّل الأهمية الثانية للدراسة في معالجة القصور التشريعي الدولي في تنظيم المسؤولية عن الجرائم السيبرانية المهددة للسلم والأمن الدوليين، وبيان مدى خضوعها ضمن اختصاص المحكمة الجنائية الدولية وتكييفها ضمن الجرائم الدولية الأساسية المنصوص عليها في نظام روما الأساسي، بصورة تسهم في سد جانب من الفراغ القانوني وتعزيز الإطار القانوني الدولي لمساءلة مرتكبيها وحماية السلم والأمن الدوليين.

ثالثاً/ أهداف الدراسة:

تهدف الدراسة إلى:

1. بيان مفهوم الجرائم السيبرانية الدولية المهددة للسلم والأمن الدوليين وذكر خصائصها وأركانها وصورها.
2. تقييم مدى كفاية قواعد القانون الدولي الجنائي في تنظيم الجرائم السيبرانية.

3. بحث مدى إمكانية تكييف الجرائم السيبرانية المهددة للسلم والأمن الدوليين ضمن الجرائم الدولية الأساسية في نظام روما الأساسي.
4. تحليل إشكاليات إسناد المسؤولية الدولية والمسؤولية الجنائية الفردية عن الجرائم السيبرانية.
5. توضيح آليات التعاون الدولي في مواجهة الجرائم السيبرانية المهددة للسلم والأمن الدوليين وملاحقة مرتكبيها.

رابعاً/ منهجية الدراسة:

1- **المنهج الوصفي:** لتوصيف الجرائم السيبرانية المهددة للسلم والأمن الدوليين وبيان مفهومها وخصائصها وصورها، وإبراز طبيعتها القانونية.

2- **المنهج التحليلي:** لتحليل قواعد القانون الدولي الجنائي ذات الصلة بالجرائم السيبرانية، ولا سيما أحكام نظام روما الأساسي للمحكمة الجنائية الدولية، بهدف بيان مدى إمكانية خضوع الجرائم السيبرانية لاختصاص المحكمة الجنائية الدولية وتكييفها ضمن الجرائم الدولية الأساسية الأربع، وتحليل أركان المسؤولية الدولية والمسؤولية الجنائية الفردية الناشئة عنها.

3- **المنهج التطبيقي:** من خلال تطبيق الدراسة على هجوم ستوكسنت Stuxnet بوصفه أحد أبرز نماذج الهجمات السيبرانية الدولية، وذلك للبحث في مدى إمكانية تكييفه في إطار الجرائم الدولية المنصوص عليها في نظام روما الأساسي، وتحليل ما يثيره من إشكاليات متعلقة بإسناد المسؤولية الدولية والمسؤولية الجنائية الفردية.

خامساً/ حدود الدراسة:

1- **الحدود الموضوعية:** تقتصر الدراسة على الجرائم السيبرانية الدولية المهددة للسلم والأمن الدوليين فقط، مع البحث في مدى إمكانية تكييفها ضمن الجرائم الدولية الأساسية في نظام روما الأساسي، مع بحث إسناد المسؤولية الدولية والمسؤولية الجنائية الفردية عنها.

2- **الحدود المكانية:** تنحصر الدراسة في الجرائم السيبرانية ذات الطابع الدولي المهدد للسلم والأمن الدوليين، وذلك في إطار قواعد القانون الدولي الجنائي دون التقيد بنطاق جغرافي محدد.

3- **الحدود الزمانية:** تتناول الدراسة التطورات المعاصرة للجرائم السيبرانية المهددة للسلم والأمن الدوليين منذ بداية القرن الحادي والعشرين وحتى الوقت الراهن.

سادساً/ الدراسات السابقة:

1- **عبد الإله عبد اللطيف محمد حامد، مدى ملاءمة تجريم السلوك الدولي مع مبدأ الشرعية، المجلة الدولية للدراسات القانونية والفقهية المقارنة، المجلد 1, العدد 3, ديسمبر 2020**

تناول الباحث التحديات المتعلقة بتطبيق مبدأ الشرعية في القانون الدولي الجنائي، وضرورة الالتزام به عند تجريم السلوك الدولي، مع البحث في مدى جواز القياس استثناءً لتحقيق أهداف القانون الدولي الجنائي في مكافحة الجرائم الدولية وحماية الأمن والسلم الدوليين.

أوجه الشبه:

تتفق الدراسة السابقة مع الدراسة الحالية في تناول مبدأ الشرعية في القانون الدولي الجنائي وأهميته في تحديد نطاق التجريم وإسناد المسؤولية الجنائية.

أوجه الاختلاف:

تختلف الدراسة الحالية في أنها تبحث عن مدى إمكانية إخضاع الجرائم السيبرانية ضمن اختصاص المحكمة الجنائية الدولية في ضوء مبدأ الشرعية، وتكييفها ضمن الجرائم الدولية الأساسية المنصوص عليها في نظام روما الأساسي، وما قد يترتب على ذلك من مسؤولية دولية ومسؤولية جنائية فردية، في حين ركزت الدراسة السابقة على مدى توافق تجريم السلوك الدولي بوجه عام مع مبدأ الشرعية دون تخصيصه للجرائم السيبرانية.

2- **رؤى طاهر حميد، آليات تنفيذ أحكام القضاء الدولي الجنائي، رسالة ماجستير، كلية القانون، جامعة القادسية،2025**

تناولت الباحثة آليات تنفيذ أحكام المحاكم الجنائية الدولية في ظل غياب الأجهزة التنفيذية المستقلة، مع تحليلها لجهود المجتمع الدولي في تحقيق العدالة، كما استعرضت أهم التحديات التي تعيق عملية تنفيذ الأحكام، وعلى رأسها السيادة الوطنية ومستوى التعاون الدولي.

أوجه الشبه:

تتفق الدراسة السابقة مع الدراسة الحالية في تناول دور التعاون الدولي في تعزيز فعالية العدالة الجنائية الدولية، ولا سيما من خلال التزام الدول بتنفيذ التزاماتها الدولية والتعاون في ملاحقة مرتكبي الجرائم الدولية وتنفيذ الأحكام الصادرة بحقهم.

أوجه الاختلاف:

تختلف الدراسة الحالية عن الدراسة السابقة في أن الأخيرة انصبَّت على آليات تنفيذ أحكام القضاء الدولي الجنائي بوجه عام، في حين ركَّزت الدراسة الحالية على الجرائم السيبرانية المهددة للسلم والأمن الدوليين وبيان مدى قيام المسؤولية الدولية للدول والمسؤولية الجنائية الفردية عنها.

3- نور أمير الموصلي، الهجمات السيبرانية في ضوء القانون الدولي الإنساني، رسالة ماجستير، الجامعة الافتراضية السورية، 2021

تناولت الباحثة مدى انطباق قواعد ومبادئ القانون الدولي الإنساني على الهجمات السيبرانية، في ضوء ما قد تحدثه من أضرار خطيرة على للبنية التحتية الحيوية وآثار مباشرة على المدنيين، والبحث عن مدى كفاية الحماية القانونية التي يوفِّرها القانون الدولي الإنساني لمواجهة الهجمات السيبرانية.

أوجه الشبه:

تتفق الدراسة السابقة مع الدراسة الحالية في تناول الهجمات السيبرانية في ضوء القانون الدولي، وذكر آثارها على السلم والأمن الدوليين، كما تشترك الدراستان في بحث مدى خضوع هذه الهجمات للقواعد القانونية الدولية المنظمة للنزاعات المسلحة، وإبراز التحديات التي تثيرها الطبيعة التقنية والعابرة للحدود للجرائم السيبرانية المهددة للسلم والأمن الدوليين.

أوجه الاختلاف:

تختلف الدراسة الحالية عن الدراسة السابقة بكونها لا تقتصر على بحث مدى انطباق قواعد القانون الدولي الإنساني ومبادئه على الهجمات السيبرانية أثناء النزاعات المسلحة، بل تمتد للبحث في مدى إمكانية تكييف الجرائم السيبرانية ضمن الجرائم الدولية الأساسية الأربع الواردة في نظام روما الأساسي للمحكمة الجنائية الدولية، مع تحليل أسس قيام المسؤولية الدولية للدول والمسؤولية الجنائية الفردية، ودراسة آليات التعاون الدولي في مكافحة هذه الجرائم وملاحقة مرتكبيها وإخضاعهم للمساءلة أمام القضاء الجنائي الدولي.

4- يزيد صالح المحيميد، الجرائم السيبرانية في القانون الجنائي، رسالة ماجستير، المجلة القانونية،2025

تناول الباحث مفهوم الجرائم السيبرانية وصورها وأطرها القانونية واستعرض التحديات القانونية والتقنية المعيقة لعملية مكافحتها كما اقترح آليات من أجل تطوير منظومة العدالة الجنائية.

أوجه الشبه:

تتفق الدراسة السابقة مع الدراسة الحالية في تناول الجرائم السيبرانية وبيان طبيعتها القانونية وأركان المسؤولية المترتبة عليها.

أوجه الاختلاف:

تختلف الدراسة الحالية في أنها تتناول الجرائم السيبرانية من منظور القانون الدولي الجنائي، بينما تناولت الدراسة السابقة الجرائم السيبرانية في إطار القانون الجنائي الداخلي.

5- وداد بوطلاعة، الهجمات السيبرانية على البنية التحتية الحرجة: دراسة في ضوء القانون الدولي العام ، مجلة حقوق الإنسان والحريات العامة، 2022

تناولت الباحثة الحماية القانونية من الهجمات السيبرانية للبنية التحتية الحرجة في ظل القانون الدولي غير السيبراني، كما قيَّمت مدى شمولية مبادئه وقواعده في ظل غياب القانون الدولي السيبراني، مع دراسة قواعد الحماية المقررة في القانون الدولي لحقوق الإنسان والقانون الدولي الإنساني، والاتفاقيات الدولية ذات الصلة، إلى جانب ذكر الآراء الفقهية والقضائية.

أوجه الشبه:

تتفق الدراسة السابقة مع الدراسة الحالية في تناول الهجمات السيبرانية وآثارها على البنية التحتية الحيوية، كالطاقة والصحة ووتهديدها للسلم والأمن الدوليين، وبيان الإطار القانوني الدولي المنظم لها.

أوجه الاختلاف:

تختلف الدراسة الحالية عن الدراسة السابقة في أن الأخيرة ركزت على الحظر القانوني للهجمات السيبرانية على البنية التحتية الحرجة في ضوء قواعد القانون الدولي لحقوق الإنسان والقانون الدولي الإنساني، بينما تناولت الدراسة الحالية الجرائم السيبرانية المهددة للسلم والأمن الدوليين من منظور القانون الدولي الجنائي، من خلال بحث مدى إمكانية إخضاعها لاختصاص المحكمة الجنائية الدولية وتكييفها ضمن الجرائم الدولية الأساسية.

سابعاً/ هيكل الدراسة:

تتكون الدراسة من مقدمة وثلاثة فصول وخاتمة:

الفصل الأول: الإطار المفاهيمي للجرائم السيبرانية الدولية:

المبحث الأول: ماهية الجرائم السيبرانية الدولية

المطلب الأول: مفهوم الجرائم السيبرانية الدولية:

الفرع الأول: التعريف اللغوي والاصطلاحي والقانوني للجرائم السيبرانية الدولية

الفرع الثاني: المفاهيم القانونية ذات الصلة

المطلب الثاني: خصائص الجرائم السيبرانية الدولية:

الفرع الأول: الطابع التقني والعابر للحدود

الفرع الثاني: الطابع الأمني والدولي

المبحث الثاني: أركان الجرائم السيبرانية الدولية وصورها:

المطلب الأول: أركان الجرائم السيبرانية الدولية:

الفرع الأول: الركن المادي

الفرع الثاني: الركن المعنوي

الفرع الثالث: الركن الشرعي والطابع الدولي

المطلب الثاني: صور الجرائم السيبرانية الدولية

الفرع الأول: الهجمات الموجهة ضد البنى التحتية الحيوية

الفرع الثاني: الهجمات الموجهة ضد الأنظمة العسكرية والأمنية

الفرع الثالث: الهجمات الموجهة ضد الأنظمة الصحية والمالية

المبحث الأول: ماهية الجرائم السيبرانية الدولية

تتبوأ الجريمة الدولية مركزًا فريدًا في بنية القانون الجنائي العام، لانطوائها على خصائص تميّزها عن الجريمة الوطنية، فهي لا تُختزل في كونها أفعالًا مجرَّمة تُرتكب داخل النطاق الإقليمي لدولة بعينها، وإنما تشكّل اعتداءً جسيمًا ومباشرًا على المصالح الجوهرية القائم عليها المجتمع الدولي. ويتجسَّد هذا الاعتداء إمّا في تهديد السلم والأمن الدوليين، أو في ارتكاب انتهاكات دولية واسعة النطاق، كما هو الشأن في جرائم الإبادة الجماعية، والجرائم ضد الإنسانية، وجريمة العدوان، وجريمة الحرب.

وإذا كانت الجريمة الدولية قد احتلّت مكانة استثنائية في منظومة القانون الجنائي العام، فإن التحولات العميقة التي أنتجتها الثورات الرقمية أسهمت في توسيع نطاق هذه الجريمة وإعادة تشكيل الصور التقليدية لها، فقد أدى التطور المتسارع في تقنيات المعلومات والاتصال، والانتشار الواسع لشبكات الإنترنت والفضاء السيبراني إلى نشوء بيئة افتراضية عابرة للحدود، ألغت القيود الإقليمية التي طالما ارتبط بها النشاط الإجرامي ، فبرزت الجريمة السيبرانية الدولية المهددة للسلم والأمن الدوليين بوصفها نمطًا حديثًا من أنماط الجرائم الدولية، لا تقل خطورة عن صورها التقليدية.

وانطلاقًا من ذلك، يهدف هذا المبحث في المطلب الأول إلى البحث في مفهوم الجرائم السيبرانية الدولية، ومن ثم ينتقل في المطلب الثاني للبحث في الخصائص الجوهرية لها والتي تميّزها عن غيرها من الجرائم.

المطلب الأول: مفهوم الجرائم السيبرانية الدولية:

تباينت آراء الفقه الدولي بشأن تحديد مفهوم الجريمة الدولية، ويُعزى ذلك إلى حداثة نشأة القانون الدولي الجنائي، حيث إن قواعده لا تزال في طور التطور والتبلور، إذ تخضع هذه القواعد لعملية تطور مستمرة تفرضها طبيعة الجرائم الدولية المستحدثة.[1]

فمن جهة، يُعدّ هذا القانون فرعًا من فروع القانون الدولي العام، وتعتمد غالبية قواعده على العرف الدولي، حتى تلك القواعد التي صيغت في صورة قواعد وضعية، إذ لا تُعدّ في جوهرها سوى قواعد كاشفة أو مقرّرة لقواعد عرفية سابقة. ومن جهة أخرى، فإن نظام روما الأساسي للمحكمة الجنائية الدولية لم يتضمن تعريفًا صريحًا للجريمة الدولية، الأمر الذي فتح المجال أمام الفقه الدولي للاجتهاد في محاولة تحديد مفهومها وبيان طبيعتها التي تميّزها عن غيرها من الجرائم.[2]

إنّ الخطورة البالغة التي تنطوي عليها الجرائم الدولية تبرّر إخضاعها لمنظومة قانونية متميّزة، تتسم بصرامة إجرائية وموضوعية، وتعتمد على أدوات قانونية استثنائية تختلف عن تلك المقرّرة للجرائم التقليدية.

وفي إطار التطورات الحاصلة على الجرائم الدولية، برزت أنماط إجرامية جديدة تعكس التحولات المتسارعة في مختلف المجالات، ولا سيما المجال التكنولوجي، فقد أدى هذا التطور إلى ظهور الجريمة السيبرانية الدولية المهددة للسلم والأمن الدوليين كأحد أبرز صور الجرائم الدولية المستحدثة، حيث تُعد امتدادًا لجرائم التقنية المعلوماتية، وتتميّز بتعدد مسمياتها وتنوع أساليب ارتكابها، تبعًا لتطور الوسائل التقنية المستخدمة فيها.

الفرع الأول: التعريف اللغوي والاصطلاحي والقانوني للجرائم السيبرانية الدولية:

أولاً/ التعريف اللغوي للجريمة السيبرانية الدولية:

يتكون مصطلح الجريمة السيبرانية الدولية من ثلاث مصطلحات، وهم: الجريمة Crime، والسيبرانية Cyber، والدولية International.

تعرَف الجريمة لغةً بأنها: الفعل "جرَم"، والمصدر "جُرم"، ويطلق على مرتكب الجريمة "المجرم". ويدل الجرم في اللغة على الذنب والإثم والتعدي. كما ورد في لسان العرب أن الجرم يأتي بمعنى الذنب والتعدي، ويرتبط في أصله بمعنى القطع.

وقد ورد لفظ " المجرمين" في قوله تعالى: (إِنَّ الْمُجْرِمِينَ فِي ضَلَالٍ وَسُعُرٍ)،[3] المجرمون هنا يُقصد بهم: الكافرون.

---

[1] سليم، عهد محمود، الطبيعة الفريدة للجريمة الدولية وانعكاساتها على النظام القضائي الدولي، المجلة العربية للنشر العلمي، العدد 86، 2025، ص 569

[2] انظر: سليم، عهد محمود، الطبيعة الفريدة للجريمة الدولية وانعكاساتها على النظام القضائي الدولي، المرجع السابق، ص 569

[3] [سورة القمر: الآية 47]

وقد ورد لفظ " الجرم" في الحديث :" أعظم المسلمين في المسلمين جرماً من سأل عن شيءٍ لم يُحرَّم عليه فحُرّم من أجل مسألته".[4]

تعرَّف السيبرانية بأنها مشتقة من المصطلح الإنجليزي Cyber ، وهو من المصطلحات الحديثة، ويستخدم للدلالة على كل ما يرتبط بالحاسوب ، وتقنية المعلومات، والواقع الافتراضي. وقد عرّف قاموس أكسفورد مصطلح Cyber بأنه: صفة تطلق على كل ما يرتبط بثقافة الحاسب الآلي، أو تقنية المعلومات، أو الواقع الافتراضي.[5]

أما الدولية، فتعرَّف بأنها: ما يوجد أو يحدث أو يتم بين الدول ، أو ما يتعلق بأكثر من دولة أو يمتد أثره اليها.[6]

ثانياً/ التعريف الاصطلاحي للجريمة السيبرانية الدولية:

أولاً/ تعريف الجريمة السيبرانية:

يعرَف ثورستن سيلين الجريمة بأنها: "كل سلوك يخالف الأعراف الاجتماعية، سواء كان هذا السلوك مخالفاً للقانون الجنائي أم لا".[7]

وتُعرَّف بأنها: الفعل أو الامتناع غير المشروع، الذي يخل بالمصلحة الأساسية الصادر عن الإرادة الجنائية والمقرر له القانون عقوبة أو تدبير احترازي.[8]

وتعرَّف السيبرانية بأنها: هجوم عبر الفضاء الإلكتروني بهدف السيطرة على المواقع الالكترونية أو البنية التحتية المحمية إلكترونياً إما لتعطيلها، أو تدميرها، أو الإضرار بها.[9]

بناءً على التعريفات السابقة، تُعرَّف الجريمة السيبرانية بأنها: الجريمة التي تقوم بتهديد سلامة الأمن السيبراني،[10] ويتم ارتكابها باستخدام الحاسب الآلي من خلال الأنظمة أو الشبكات، وتشمل الجريمة السيبرانية جميع الجرائم التي يتم ارتكابها في الفضاء السيبراني.

ثانياً/ تعريف الجريمة الدولية:

تعرَّف الجريمة الدولية بأنها:" كل فعل يعد انتهاكاً للمصالح التي يحميها القانون الدولي ويقرر لمقترفها عقوبة".[11] وتعرّف بأنها: سلوك إرادي غير مشروع صادر عن فرد بإسم الدولة أو بتشجيع أو برضا منها، ويكون منطوياً على مساس بمصلحة دولية يحميها القانون.[12]

ويعرّفها الفقيه كرافن بأنها: الفعل الذي يتعارض مع أحكام القانون الدولي ويترتب عليه مسؤولية دولية، وهي لا تكون إلا بالنسبة لفعل جسيم يحدث اضطراب وإخلال بالأمن العام للمجتمع الدولي. [13]

---

(4) البخاري، كتاب الاعتصام بالكتاب والسنة، حديث رقم 2789، مسلم، كتاب الفضائل، حديث سعد بن أبي وقاص رضي الله عنه رقم 611

(5) الصحفي، روان عطية الله، الجرائم السيبرانية، المجلة الالكترونية الشاملة متعددة التخصصات، العدد 24، 2020، ص 5-7

(6) قاموس أكسفورد الإنجليزي ، دار نشر جامعة أكسفورد، تاريخ الاطلاع: 12 أبريل 2026
متاح على الرابط : https://www.oed.com

(7) د. الحسبان، عماد، د. الضمور، عدنان ، د.التميمي، عز الدين، د.الخزاعلة، ياسر، الجرائم المستحدثة المعلوماتية، الالكترونية، السيبرانية، دار الخليج للنشر والتوزيع،2024 ، ص 17

(8) د. الحسبان، د. الضمور، د. التميمي، د. الخزاعلة، المرجع السابق، ص 16

(9) أ. العتيبي، زياد محمد، جرائم السيبرانية المرتكبة عبر الوسائط الرقمية بيان مفهومها من حيث: أشكالها، خصائصها، أركانها، والدافع من ارتكابها، المجلة الأكاديمية العالمية للدراسات القانونية، المجلد3 ،العدد 1، 2021 ، ص 4

(10) مهمل، أسامة، الإجرام السيبراني، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، 2018، ص 25

(11) أ.حامد، عبد الإله عبد اللطيف محمد، مدى ملاءمة تجريم السلوك الدولي مع مبدأ الشرعية، المجلة الدولية للدراسات القانونية والفقهية المقارنة،2020، ص 132

(12) د.أحمد، رحمة الله حبوب محمد، أنواع الجريمة الدولية وعناصرها في القانون الدولي الجنائي، المجلة الأفريقية للدراسات المتقدمة في العلوم الإنسانية والإجتماعية، 2022، ص 341

(13) انظر: سليم، عهد محمود، الطبيعة الفريدة للجريمة الدولية وانعكاساتها على النظام القضائي الدولي، المرجع السابق ، ص 569

باستقراء التعريفات السابقة للجريمة الدولية يتضح لنا أنها واقعة غير مشروعة دوليًا، تُرتكب بفعل أو امتناع عن فعل يؤثر على مصالح محمية للجماعة الدولية، وقد يكون ارتكابها بموافقة أو برضا الدولة، وتترتب عليها مساءلة قانونية وعقاب دولي لاعتبارها جريمة تمس مصالح عليا للمجتمع الدولي.

وعلى الرغم من اختلاف هذه التعريفات في صياغتها، فإنها تلتقي في التأكيد على الطابع الخاص للجريمة الدولية، سواء من حيث جسامة الفعل المرتكب، أو طبيعة المصالح المُعتدى عليها، أو نطاق المسؤولية المترتبة عنها.[14]

ثالثاً: التعريف القانوني للجريمة السيبرانية الدولية:

أولاً/ تعريف الجريمة السيبرانية:

عرَفتها منظمة الأمم المتحدة في المؤتمر العاشر لمنع الجريمة ومعاملة المجرمين لعام 2000 بأنها: "أي جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، أو في نطاق نظام حاسوبي أو شبكة حاسوبية".[15]

أما اتفاقية بودابست لمكافحة جرائم الإنترنت لعام 2001 ، فلم تضع تعريف للجريمة السيبرانية، ولكنها حددت الأفعال التي تعد جرائم سيبرانية، مثل الجرائم المرتكبة ضد سلامة أو سرية نظم وبيانات الحاسب الآلي، وجرائم الاحتيال المتعلقة بالحاسب الآلي، بالإضافة إلى الجرائم التي تتعلق بالمحتوى والتي يتم استعمال الحاسب الآلي لارتكابها.

كما عرَّف الاتحاد الدولي للاتصالات بأنها: "الأفعال التي ترتكب ضد أفراد أو جماعات لدافع إجرامي، وبنية إلحاق الضرر بسمعتهم أو التسبب بأذى نفسي أو جسدي لهم، أو خسائر مالية لهم، وذلك باستخدام شبكات الاتصال الحديثة مثل الإنترنت أو الهواتف المحمولة".[16]

إلا أن التعريفات السابقة لا تزال مرتبطة بمفهوم الجريمة السيبرانية بمدلولها العام، ولا توفر أساساً كافياً لتحديد مفهوم الجريمة السيبرانية الدولية في إطار القانون الجنائي الدولي، إذ أن الأخيرة تشترط توافر عنصر إضافي رئيسي يتمثَّل في جسامة الفعل ومدى تأثيره على المصالح الجوهرية للمجتمع الدولي.

ثانياً/ تعريف الجريمة الدولية:

على الرغم من المكانة التي تحتلها الجريمة الدولية في إطار القانون الدولي الجنائي، إلا أنه لم يتم اعتماد تعريف دولي موحد لها حتى الآن،[17] إذ اقتصرت معظم الاتفاقيات الدولية على تحديد الأفعال التي تندرج ضمن الجرائم الدولية وذكرت أركانها وآثارها.[18] ويُلاحظ أن هذا الاتجاه التشريعي يركّز على تعداد الأفعال التي تشكِّل اعتداءً جسيماً على المصالح الجوهرية للمجتمع الدولي، بدلًا من صياغة تعريف عام وموحد للجريمة الدولية.

ثالثًا/ تعريف الجريمة السيبرانية الدولية المهددة للسلم والأمن الدوليين:

على الرغم من تنامي الاعتماد على الفضاء السيبراني وما أسفر عنه من استحداث صور جديدة من الأفعال غير المشروعة المنطوية عليها آثار عابرة للحدود، إلا أن المجتمع الدولي لم يتوصل حتى الآن إلى صياغة تعريف قانوني موحَّد للجريمة السيبرانية الدولية المهددة للسلم والأمن الدوليين. ويعود ذلك للعديد من الاعتبارات، على رأسها حداثة الجريمة السيبرانية

---

(14) سليم، عهد محمود، المرجع السابق، ص 569

(15) الحجار، عدنان، بشير، فايز، الأدلة الرقمية وإثبات الجرائم السيبرانية ما بين التأصيل والتأويل، مجلة جامعة الاستقلال للأبحاث، المجلد 6 ، العدد 1 ، 2022، ص 129

(16) المحيميد، يزيد صالح، الجرائم السيبرانية في القانون الجنائي، المجلة القانونية، المجلد 25 ، العدد 3 ، 2025 م، ص 2225.

(17) العازمي، عبد الله خلف، الجرائم الدولية "خصائصها، وأركانها، وصورها"، جامعة الأزهر، كلية الشريعة والقانون بأسيوط، العدد 35، 2023 ، ص 734

(18) ويُعتبر نظام روما الأساسي للمحكمة الجنائية الدولية لعام 1998 أبرز الاتفاقيات الدولية في مجال القانون الجنائي الدولي، حيث لم يتجه لوضع تعريف عام وموحد للجريمة الدولية، وإنما اكتفى بتحديد الجرائم التي تدخل ضمن الاختصاص الموضوعي للمحكمة، وقد نصت المادة 5 منه على أربع جرائم رئيسية تعتبر من أخطر الانتهاكات الماسّة بمصالح المجتمع الدولي بأكمله، وهي: جريمة الإبادة الجماعية، والجرائم ضد الإنسانية، وجرائم الحرب، وجريمة العدوان. ومن ثم، يظهر أن نظام روما الأساسي قد اعتمد على أسلوب تحديد صور وأركان الجرائم الدولية بدلًا من وضع تعريف للجريمة الدولية.

مقارنةً بالجرائم الدولية التقليدية، حيث تعد هذه الجريمة من الجرائم المستحدثة،[19] وذلك لأن قواعد القانون الدولي الجنائي قد نشأت في مرحلة لم تكن فيها الجرائم السيبرانية من ضمن التصورات القائمة عند صياغة تلك القواعد.

كما أن التطور المتسارع للتكنولوجيا جعل من الصعب صياغة تعريف موحد وثابت يتم استيعاب فيه جميع صور السلوك الإجرامي السيبراني، وذلك نظرًا للتغير المستمر لوسائل ارتكاب هذا النوع من الجرائم وتطور أدواته بصورة مستمرة.

بالإضافة إلى ذلك، فإن تباين مواقف الدول حول الطبيعة القانونية لبعض الجرائم السيبرانية يشكِّل عائقًا رئيسياً أمام الاتفاق على تعريف موحد، إذ تتباين الدول بشأن ما إذا كانت الجرائم السيبرانية المهددة للسلم والأمن الدوليين قد تندرج ضمن إطار الجرائم الدولية أو تعتبر مجرد أفعال غير مشروعة خاضعة لقواعد المسؤولية الدولية للدول، وعلى وجه الخصوص فيما يتعلق بمعايير خطورة الفعل وجسامته، وآثاره على السلم والأمن الدولي، ومدى إمكانية إسناده إلى جهة أو دولة معينة.

وعلى الرغم من عدم وجود تعريف دولي للجريمة السيبرانية الدولية، إلا أن الإطار القانوني الدولي يتيح العديد من القواعد والمبادئ التي من الممكن الاستناد إليها في تحديد طبيعة هذا النوع من الجرائم وآثارها على السلم والأمن الدوليين.

حيث قد وضع ميثاق الأمم المتحدة الإطار العام لحماية السلم والأمن الدوليين، ولا سيما من خلال حظره لاستخدام القوة، فهي مبادئ أضحت موضع جدل عند البحث في مدى انطباقها على الجرائم السيبرانية التي قد تفضي إلى آثار مماثلة للأفعال التقليدية المهددة للأمن الدولي.

علاوةً على ذلك، فإن الخلاف بين الدول حول التكييف القانوني للجرائم السيبرانية المهددة للسلم والأمن الدوليين يشكِّل عائقًا أمام إرساء مفهوم موحَّد، إذ لا تزال مواقف الدول تتباين بشأن المعايير التي من الممكن بموجبها اعتبار الجرائم السيبرانية المهددة للسلم والأمن الدوليين جريمة دولية، وليس مجرد فعل غير مشروع يخضع لقواعد المسؤولية الدولية.

ويرتبط هذا الخلاف بمدى جسامة الضرر الناجم عن هذه الجرائم، وطبيعة الأهداف المقصودة، وتأثير الفعل على السلم والأمن الدوليين، ومدى إمكانية إسناده إلى دولة أو أفراد معينين.

وعليه، فإن مفهوم الجريمة السيبرانية الدولية لا يزال في مرحلة التشكُّل والتطور، ولم يُعترف به حتى الآن بوصفه جريمة دولية مستقلة في القانون الجنائي الدولي، حيث لا يوجد حتى الآن تعريف موحّد ومتفق عليه دوليًا لمفهوم الجريمة السيبرانية الدولية المهدِّدة للسلم والأمن الدوليين ضمن اتفاقية دولية ملزمة، إذ تكتفي الاتفاقيات الدولية القائمة، مثل اتفاقية بودابست بتنظيم صور محددة من الجرائم السيبرانية دون التطرق صراحةً إلى ربطها بمستوى تهديد السلم والأمن الدولي .

كما أن الجهود الفقهية والدولية، بما في ذلك ما ورد في دليل تالين، لا تقدم تعريفًا جامعًا ملزمًا، وإنما تضع أطرًا تفسيرية لتقييم متى يمكن أن ترقى الهجمات السيبرانية إلى مستوى تهديد السلم والأمن الدولي، إلا أن النقاش الفقهي والقانوني يسير نحو البحث عن إمكانية استخدام الوسائل السيبرانية كأداة لارتكاب الجرائم الدولية التقليدية عند توافر أركانها وشروطها.

ونظرًا لعدم وجود تعريف موحّد ومتفق عليه دوليًا لمفهوم الجريمة السيبرانية المهدِّدة للسلم والأمن الدولي في الاتفاقيات الدولية، فقد سعت الباحثة إلى وضع تعريف لهذه الجريمة بما يتلاءم مع طبيعة البحث وأهدافه، فعرّفتها بأنها: هي كل هجوم سيبراني منظم أو واسع النطاق يُرتكب عمدًا باستخدام الحاسب الآلي أو الشبكات المعلوماتية، ويهدف لإحداث ضرر جسيم بالأنظمة الحيوية للدول أو بالبنية التحتية الحيوية لها، بما من شأنه زعزعة الاستقرار وتهديد السلم والأمن الدوليين.

ويرتكز هذا التعريف على الجمع بين عنصرين رئيسيين، أولهما الطبيعة السيبرانية للفعل من حيث وسيلة الارتكاب، وثانيهما الصفة الدولية للفعل من حيث الخطورة والآثار والارتباط بالمصالح المحمية في القانون الجنائي الدولي.

الفرع الثاني: المفاهيم القانونية ذات الصلة:

ترتبط الجريمة السيبرانية الدولية ارتباطًا متيناً بالعديد من المفاهيم القانونية التي قد تتداخل معها من حيث الطبيعة أو الوسيلة أو الأثر القانوني أو النطاق، وذلك يستلزم توضيح حدود العلاقة بينها، تفادياً للخلط بين المفاهيم المتشابهة.

[19] يقصد بالجرائم المستحدثة: مجموعة الأفعال الإجرامية الحديثة التي نشأت بفعل التطور العلمي والتقني، والتي تجاوزت في طبيعتها وأساليب ارتكابها الإطار التقليدي للجريمة، الأمر الذي جعلها تشكل خطرًا على المصالح الاجتماعية والأمنية، بما يستوجب تبني آليات قانونية ووسائل فعّالة لمواجهتها والحد من آثارها، أ. شيهاني، عمر، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، 2017، ص 291

فبعض تلك المفاهيم يعتبر وسيلة لارتكاب الجريمة، كالهجمات السيبرانية، وبعضها يشكِّل السياق الذي تقع فيه هذه الجريمة، كالحرب السيبرانية، في حين يعتبر بعضها هو البيئة المرتكب فيها الجريمة، كالفضاء السيبراني، في حين يشكِّل بعضها الآخر آليات الحماية القانونية والتقنية لمكافحتها، كالأمن السيبراني.

ومن ثم، فإن إبراز الفرق بين هذه المفاهيم وبيان الرابطة القانونية بينها وبين الجريمة السيبرانية الدولية يعتبر أمرًا لازمًا لتحديد نطاق الجريمة السيبرانية الدولية وتمييزها عن المفاهيم الأخرى القريبة منها.

أولاً/ الهجمات السيبرانية: قد نرى ارتباط مصطلح السيبرانية Cyber بمصطلح الهجمات Attacks، فقد عرّفت القاعدة 92 من دليل تالين الهجمات السيبرانية بأنها: العملية السيبرانية الهجومية أو الدفاعية، والتي من المُتوقّع أن تؤدي إلى إصابات، أو وفاة أشخاص، أو إلحاق أضرار، أو تدمير الممتلكات.[20]

ويستند هذا التعريف إلى ما تقضي به المادة 49/1 من البروتوكول الإضافي الأول الملحق باتفاقيات جنيف لعام 1949، والتي تنص على: "أعمال العنف ضد الخصم، سواء أثناء الهجوم أو أثناء الدفاع".[21]

كما نصَّ دليل تالين 1 لعام 2013 ودليل تالين 2 لعام 2017 على تعريف للهجمات السيبرانية، فعرَّفها بأنها:" عملية سيبرانية، هجومية كانت أم دفاعية، يُقصد بها أو يُتوقع منها على نحو معقول التسبب في إصابة، أو وفاة أشخاص، أو إلحاق أضرار بالأعيان، أو تدميرها".[22]

من الملاحظ غياب الاتفاق الفقهي الدولي على تعريف قانوني موحد وجامع لمفهوم الهجمات السيبرانية، إذ تعددت التعريفات الفقهية وتباينت أسسها، فبينما ذهب اتجاه إلى النظر إلى الجريمة السيبرانية بوصفها وسيلة للهجوم، رأى اتجاهٌ آخر أنها تمثِّل محلاً أو هدفًا للهجوم بحد ذاته، في حين ركز اتجاهٌ ثالث على الآثار المترتبة على الهجمات السيبرانية باعتبارها معيار للتعريف والتمييز.

فقد ذهب جانب من الفقه إلى قصر تعريف الهجمات السيبرانية على الأداة المستعملة في الهجوم، فعرّفها بعضهم بأنها: هجوم من خلال الفضاء السيبراني بهدف السيطرة على المواقع الإلكترونية أو البنية التحتية، بغرض تعطيلها والإضرار بها.[23]

وفي مقابل ذلك، توسّع فقهاء آخرون في تعريف الهجمات السيبرانية استنادًا إلى الهدف من الهجوم، فعرَفها البعض بأنها: كل فعل يفسد وظائف شبكة المعلومات لأغراض سياسية ماسّة بالأمن القومي.[24]

ويرى أنصار هذا الاتجاه أن الاستناد على الهدف في تعريف الهجمات السيبرانية أدق وذلك يرجع لسبب رئيسي، وهو أن الاعتماد على الهدف أكثر اتساقًا من الناحية المنطقية، ووفقًا لهذا الرأي، فإن استخدام أدوات سيبرانية متقدمة لقطع كابلات الاتصالات البحرية التي تنقل البيانات والمعلومات هجومًا سيبرانيًا، متى كان الهدف المقصود هو تعطيل أو تدمير بنية تحتية حيوية.[25]

وذهب جانب آخر من الفقه إلى تعريف مفهوم الهجمات السيبرانية استنادًا إلى الآثار المترتبة عليها، فعرَّفها البعض بأنها: قيام دول أو كيانات أخرى من غير الدول بشنّ هجمات إلكترونية إما ضمن إطار متبادل أو من جهة واحدة فقط.[26]

وفي نظرنا نرى أن الرأي الثاني الذي يربط مفهوم الهجمات السيبرانية بالهدف المنشود يتمتَّع بقدر كافٍ من الوجاهة المنطقية، لأن الأداة المستخدمة قد تتغير وتتطور مع التطورات التقنية، كما أن الآثار قد لا تتحقق أو قد تتماثل مع أفعال غير سيبرانية. أما الهدف هو الذي يُظهر الغاية العدائية الكامنة خلفه.

---

[20] انظر: القاعدة 92، دليل تالين "2" لعام 2017

[21] Article 491 of the First Additional Protocol to the Geneva Conventions of 1949 https://www.icrc.org/sites/default/files/external/doc/en/assets/files/other/icrc_002_0321.pdf

[22] انظر: القاعدة 30، دليل تالين "1" لعام 2013 ، القاعدة 92، دليل تالين"2" لعام 2017

[23] د.رمضان، إبراهيم السيد أحمد، مواجهة الهجمات السيبرانية في ضوء أحكام القانون الدولي، مجلة العلوم القانونية والاقتصادية، العدد 1، 2025 ، ص 1755

[24] د.رمضان، إبراهيم السيد أحمد، المرجع السابق، ص 1755

[25] المرجع السابق، ص 1758

[26] المرجع السابق، ص 1758

ومع ذلك، الاعتداد بمعيار الهدف وحده يظل قاصرًا عن تقديم وصف قانوني دقيق لمفهوم الهجمات السيبرانية، إذ يؤدي لإغفال عنصر رئيسي متمثل في طبيعة الوسيلة المستخدمة، وما إذا كان الفعل قد تم تنفيذه من خلال استغلال الفضاء السيبراني ذاته بوصفه نطاقًا لتنفيذ الهجوم.

واستنادًا إلى ما سبق عرضه من تعريفات فقهية لمختلف الاتجاهات التي تناولت مفهوم الهجمات السيبرانية، خلصت الباحثة إلى تعريف جامع يستوعب العناصر الأساسية المشتركة بين تلك التعريفات، وعليه، تُعرّف الباحثة الهجمات السيبرانية بأنها: أفعال عدائية غير مشروعة تُنفذ باستخدام التقنيات الرقمية المتطورة، وترتكب في زمن السلم أو النزاع، وتستند في جوهرها إلى الوصول غير المشروع للأنظمة الحيوية والبنية التحتية الحيوية للدولة بقصد تعطيلها أو تدميرها، سعيًا لتحقيق أهداف سياسية، أو عسكرية، أو اقتصادية.

ثانياً/ الحرب السيبرانية: والتي وتعرّف بأنها: أساليب الحرب ووسائلها المعتمدة على تكنولوجيا المعلومات والمستخدمة في سياق النزاعات المسلحة.[27]

ثالثاً: الحصار السيبراني: والذي يعرَّف بأنه منع دولة معينة بواسطة الهجمات السيبرانية، من نقل أو تلقي أو نقل المعلومات خارج حدودها لدوافع سياسية، بهدف إضعاف الدولة وإضعاف مؤسساتها واقتصادها ومجتمعها.[28]

ويظهر من التعريفات السابقة الارتباط بين الهجمات السيبرانية والحرب السيبرانية والحصار السيبراني، حيث توجد علاقة عموم وخصوص، فالهجمات السيبرانية تمثِّل الأداة التي يستند عليها كلاً من الحصار السيبراني والحرب السيبرانية.

فإذا تم استخدام الهجمات السيبرانية في إطار النزاع المسلح أو من أجل تحقيق أهداف عسكرية، فإنها تأخذ وصف الحرب السيبرانية، أما إذا تم توظيفها بصورة منهجية لعزل الدولة وتقييد تدفق المعلومات والاتصالات إليها أو منها، بهدف إضعاف قدراتها السياسية أو الاجتماعية أو الاقتصادية أو، فإنها تأخذ وصف الحصار السيبراني.

فالهجمات السيبرانية، يمكن أن تكون جزءًا من عمليات هجومية منظمة تنفذها الدول في سياق النزاعات المسلحة، فتسمَّى بالحرب السيبرانية، حيث تعتمد الحرب السيبرانية على استخدام الهجمات السيبرانية كامتداد للأعمال العدائية بين الدول، إذ قد تتزامن الهجمات السيبرانية مع النزاعات المسلحة التقليدية كما قد تحدث بصورة مستقلة.

وعلى الرغم من تباين المفاهيم السابقة من حيث الطبيعة القانونية، إلا أنها مرتبطة بالجريمة السيبرانية الدولية ارتباطًا متيناً، حيث تمثِّل الهجمات السيبرانية أداةً لارتكابها، في حين تمثِّل الحرب السيبرانية والحصار السيبراني المجال الذي تحدث فيه هذه الجرائم. كما أن خطورة الآثار الناتجة عنها قد تجعلها مؤثرة على السلم والأمن الدوليين، الأمر الذي يطرح إشكالات التكييف في إطار القانون الجنائي الدولي.

كذلك يرتبط مفهوم الجريمة السيبرانية الدولية ببعض المفاهيم، وهي:

أولاً: الفضاء السيبراني: قد نرى أيضاً ارتباط مصطلح السيبراني Cyber بمصطلح الفضاء Space، فنجد ارتباط وثيق بين الجريمة السيبرانية والفضاء السيبراني، والذي يعرَف بأنه: "البيئة التفاعلية الحديثة، وتشمل عناصر مادية وغير مادية، مكوَنة من مجموعة من الأجهزة الرقمية، وأنظمة الشبكات والبرمجيات، والمستخدمين سواء مشغلين أو مستعملين".[29]

ثانياً: الأمن السيبراني: قد نرى أن مصطلح السيبراني Cyber لطالما ارتبط بمصطلح الأمن Security، فنجد استخدامات عديدة لمصطلح الأمن السيبراني فيما يتعلق بالأمن الالكتروني وأمن المعلومات، والذي يعرَف بأنه: "حماية الشبكات وأنظمة

---

[27] د. لطفي، وفاء، الجهود الدولية في مكافحة جرائم الإرهاب السيبراني: التجربة الماليزية نموذجاً، مجلة كلية الاقتصاد والعلوم السياسية، المجلد 23 ، العدد 1 ،2022 م، ص 161

[28] Velenczei، Dora Vanda، "Recognising Cyber Blockades as Crimes Against Humanity: Can International Criminal Law Keep Up?"، Proceedings of the 19th International Conference on Cyber Warfare and Security ICCWS 2024، Vol. 19، No. 1، 2024، p. 414 available at: https://doi.org/10.34190/iccws.19.1.1948

[29] د. زروقة، إسماعيل، الفضاء السيبراني والتحول في مفاهيم القوة والصراع، مجلة العلوم القانونية والسياسية، جامعة محمد بومضياف، الجزائر، المجلد 10، العدد 1، 2019 ، ص 1107

تقنية المعلومات وأنظمة التقنيات التشغيلية، ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحتويه من بيانات، من أي اختراق، أو تعطيل، أو تعديل، أو دخول، أو استخدام، أو استغلال غير مشروع".[30]

يرتبط مفهوم الجريمة السيبرانية الدولية المهددة للسلم والأمن الدوليين بمفهومي الفضاء السيبراني والأمن السيبراني، وذلك لأن الفضاء السيبراني يعد البيئة التي ترتكب فيها الأفعال الإجرامية من خلال الشبكات الرقمية والأنظمة، بينما يتمَّثل الأمن السيبراني في مجموعة الوسائل والإجراءات التي تهدف إلى حماية تلك البيئة وعناصرها من الاعتداءات غير القانونية المهددة لأمنها وسلامتها.

وتتضح أهمية هذا الارتباط في إطار القانون الجنائي الدولي عندما تتعدى الجريمة السيبرانية مسألة الاعتداء على الأنظمة، لتصبح مستهدفةً بذلك البنى التحتية الحيوية للدول، ومزعزعةً بذلك أمن الدول واستقرارها.

بناءً على ما سبق، فإن الفضاء السيبراني يعتبر نطاق حدوث الجريمة السيبرانية، بينما يمثِّل الأمن السيبراني آليات مواجهتها والحد من تداعياتها، في حين أن الجريمة السيبرانية الدولية تتحدد بمدى خطورة الفعل وامتداد آثاره الماسَّة بمصالح المجتمع الدولي.

المطلب الثاني: خصائص الجرائم السيبرانية الدولية:

تنطوي الجريمة السيبرانية الدولية على جملة من الخصائص الجوهرية التي تميّزها عن غيرها من الجرائم، كما تنفرد بسمات خاصة تميّزها عن الجرائم السيبرانية التي يقتصر نطاقها وآثارها على الإقليم الوطني، حيث تتسم باتساع النطاق الجغرافي والطابع العابر للحدود. تُفضي هذه الخصائص إلى إشكاليات قانونية معقَّدة، تنعكس بصورة مباشرة على فعالية منظومة العدالة الجنائية الدولية. وتأسيسًا على ذلك، سنتناول هذه الخصائص في فرعين رئيسيين، ألا وهي: الطابع التقني والعابر للحدود، والطابع الأمني والدولي.

الفرع الأول: الطابع التقني والعابر للحدود:

أولاً/ الاعتماد على الوسائل التقنية المتطورة:

يعتبر الحاسب الآلي أداة مباشرة لتنفيذ الجريمة السيبرانية، إذ أن هذا النوع من الجرائم يعتمد بشكل رئيسي على الحاسب الآلي والتقنيات الخاصة به، فهو الأداة الرئيسية لارتكاب هذه الجريمة، فلا يستطيع منفذيها ارتكابها إلا باستخدام الحاسب الآلي المتصل بشبكات الانترنت واستخدام الأجهزة الذكية، إذ أنه يستلزم توافر وسائل تقنية متطورة نظراً لطبيعة هذه الجريمة الحديثة،[31]حيث تتميز باتخاذها تقنية المعلومات موضوعاً للجريمة، أو أداةً لها، أو وسيلة لتنفيذها،[32] فمن المهم أن يمتلك منفذيها المعرفة الكافية والخبرة العالية في التعامل مع الحاسب الآلي والأجهزة الذكية.

كما تتسم بدرجة عالية من التنظيم والتعقيد التقني، حيث تُرتكب في إطار سياسات ممنهجة تتبناها الدول، بما يقرّبها من مفهوم الجرائم الدولية التقليدية من حيث خطورتها وآثارها.

ثانياً/ السرعة الفائقة في عملية التنفيذ:

تتسم الجرائم السيبرانية بصفة عامة سواءً في نطاقها الوطني أو الدولي بالسرعة الفائقة من ناحية التنفيذ،[33] فيمكن تنفيذ الجريمة خلال ثواني معدودة، وتتسم أيضاً بسرعة الانتشار، فيمكن نشر برمجيات عبر الشبكات بشكل سريع جداً، بالإضافة إلى سرعة التأثير، لأنه من السهل تحقيق الكثير من الأضرار للدولة في وقت وجيز وبأسلوب هادئ.

---

[30] انظر: الهيئة الوطنية للأمن السيبراني، تاريخ الاطلاع: 12 أبريل 2026
متاح على الرابط: https://nca.gov.sa/pages/about.html

[31] العتيبي، زياد محمد، جرائم السيبرانية المرتبكة عبر الوسائط الرقمية، المجلة الأكاديمية العالمية للدراسات القانونية، المرجع السابق، ص 2

[32] Vitvitskaya، S. S.، Vitvitsky، A. A.، & Isakova، Yu. I.، "Cybercrime: Concept، Classification، and International Counteraction،" Legal Order and Legal Values، Vol. 1، No. 1، 2023، p. 127
Available at: https://doi.org/10.23947/2949-1843-2023-1-1-126-136

[33] د. عبدالرزاق، رانا مصباح عبد المحسن، آليات مكافحة الجرائم السيبرانية في المملكة العربية السعودية، المجلة القانونية، المجلد 15، العدد 5 ، 2023، ص 13

ثالثاً/ الطابع غير المادي لمحل الجريمة:

غالباً ما ينصرف الاعتداء في هذه الجريمة على البيانات والنظم المعلوماتية غير المادية، كاختراق قواعد البيانات أو تعطيل البنية التحتية الرقمية للدول، وذلك أيضاً ما يميّزها عن الجرائم التي تنحصر في الاعتداء على الممتلكات المادية الملموسة.

رابعاً/ جرائم ناعمة:

تسمى الجريمة السيبرانية بالجريمة الناعمة Soft Crime، وذلك لاختلاف طبيعتها عن الجرائم التقليدية التي تتسم بالعنف، أي أن عنصر العنف المباشر فيها غير متواجد فلا تحمل أي شكل من أشكال القوة الجسدية أو المجهود العضلي فهي ذات طابع غير مادي، أي أنها لا تقوم باستهداف أمور مادية، بل تستهدف الشبكات والمعلومات لاعتمادها على التخطيط المنظم والخبرة الكافية بالأجهزة الذكية، فهي تنصب على المعلومات المخزنة داخل نظام المعلومات.[34]

خامساً/ صعوبة عملية الإثبات:

إذ تعتبر من أعقد الجرائم وأكثرها صعوبة من ناحية الإثبات، لوقوعها في الفضاء السيبراني غير الملموس، ولأن غالبية البيانات عبارة عن رموز من الصعب قراءتها، ولسرعة محو الأدلة، زيادةً على ذلك عدم وجود الأثار المادية الملموسة، وهو ما يسمى بالآثار المعلوماتية الرقمية والتي يمكن من خلالها حل القضية.[35]

سادساً/ قابلية الأدلة للمحو والتلاشي:

تتَّسم الأدلة الرقمية في الجرائم السيبرانية بإمكانية حذفها أو تعديلها أو إتلافها بسرعة، دون أن تترك أثراً مادياً ملموساً،[36] مما يفرض تحديات فنية وقانونية جسيمة على الجهات المختصة بالتحقيق، ويتضح ذلك بشكل خاص عند جمع الأدلة وحفظها بما يضمن سلامتها وصلاحيتها للاستخدام ضمن الإجراءات القضائية.

سابعاً/ الطابع العابر للحدود:

تُعدّ الطبيعة العابرة للحدود الإقليمية من الخصائص الجوهرية للجريمة السيبرانية الدولية المهددة للسلم والأمن الدولي، فهي تُرتكب في بيئة افتراضية غير محدودة تُشكّل مسرحًا كاملًا للفعل الإجرامي، مما يتيح من إمكانية تنفيذ أفعال عدوانية دون الحاجة إلى التواجد المادي في إقليم الدولة المتضررة، حيث قد يصدر الفعل الإجرامي من إقليم دولة معينة وتتحقق آثاره في دولة أخرى.

وبهذه الطريقة، يتمكّن المنفذين من تنفيذ الهجمات السيبرانية من أي مكان دون أن يخضعوا لحرس الحدود.[37]

الفرع الثاني: الطابع الأمني والدولي:

أدّى التحوّل المتسارع في الفضاء السيبراني على تكريس الطابع الأمني للجريمة السيبرانية الدولية بصورة جلية، إذ لم يعد هذا الفضاء مقتصرًا على كونه مجالًا تقنيًا لتبادل البيانات والمعلومات، بل أضحى ميدانًا حقيقياً للتهديدات الأمنية ذات الأبعاد الاستراتيجية.

فالهجمات السيبرانية الموجهة ضد البنى التحتية للدول تُعد اعتداءً مباشرًا على أمنها الوطني والاقتصادي، لما تنطوي عليه من قدرة على تعطيل المرافق الحيوية وإحداث شلل واسع في القطاعات الأساسية، كقطاع الطاقة، والأنظمة المالية والمصرفية، وشبكات النقل والاتصالات، بما يخلّ باستقرار الدولة ويهدد أمنها.

ويتعمّق هذا الطابع الأمني بفعل الطبيعة الخاصة للفضاء السيبراني، بوصفه فضاءً افتراضيًا عابرًا للحدود الإقليمية، يصعب إخضاعه للمفاهيم التقليدية للسيادة والرقابة الإقليمية.

---

(34) نصار، غادة، الإرهاب والجريمة الإلكترونية، القاهرة، العربي للنشر والتوزيع، 2017 م، ص 38

(35) د. الكندري، مريم أحمد علي ، الجرائم السيبرانية في الاقتصاد الرقمي دراسة فقهية تأصيلية، مجلة العلوم الشرعية، جامعة الإمام محمد بن سعود الإسلامية، المجلد 3 ، العدد 75، 2025، ص 191

(36) الصحفي، روان، مرجع سابق، ص 12

(37) الديربي، عبدالعال، إسماعيل، محمد، الجرائم الإلكترونية، المركز القومي للإصدارات القانونية، القاهرة، 2012 م، ص 53

ومن الضروري الإشارة إلى سمتين جوهريتين يجب توفرهما في الجريمة السيبرانية لتُصنَّف على أنها جريمة دولية مهددة للسلم والأمن الدولي، وهما:

أولاً: أن ينطوي الفعل المرتكب على خرق للقيم الإنسانية الراسخة لدى المجتمع الدولي، أو إلحاق الضرر بمصلحة مشتركة للمجتمع الدولي.[38]

ثانياً: أن يترتب على ارتكاب هذا الفعل خطر جسيم على المجتمع الدولي أو إخلال بالسلم والأمن الدولي.[39]

وعليه، فإنها متى بلغت من الجسامة حدّ الاعتداء على المصالح الجوهرية للمجتمع الدولي، لا تخرج عن الإطار المفاهيمي للجريمة الدولية، بل تشكّل امتدادًا معاصرًا لها، يخضع لمعيار الخطورة ذاته الذي يقوم على طبيعة المصلحة المعتدى عليها واتساع آثار الفعل الإجرامي، وقد استقر الفقه الجنائي الدولي على أن معيار الخطورة في الجرائم الدولية ليس لمجرد تكرار الفعل أو عدد الضحايا، بل في طبيعة المصلحة المعتدى عليها.[40]

يتضح من السابق أن معيار الخطورة وطبيعة المصلحة المعتدى عليها يعد معيارًا حاسمًا في توصيف الجريمة الدولية، وهو ما ينسجم مع الاتجاه الغالب في الفقه الجنائي الدولي، غير أن تحديد هذه المصالح في سياق الجرائم السيبرانية يظل محل نقاش فقهي، خاصةً في ظل غياب تعريف دولي جامع للجريمة السيبرانية الدولية المهددة للسلم والأمن الدولي.

ومن ثم، يكتسب هذا النوع من الجرائم السيبرانية بعدًا أمنيًا دوليًا يتجاوز الإطار الجنائي الداخلي، ليندرج ضمن فئة التهديدات غير التقليدية للسلم والأمن الدوليين، كما تتضاعف الخطورة الأمنية بالنظر إلى ما تتسم به من عنصر المفاجأة وسرعة التنفيذ، إذ يمكن أن تُلحق أضرارًا جسيمة وواسعة النطاق خلال فترات زمنية وجيزة، دون أن تُتاح للدول المستهدفة فرصة كافية لاتخاذ تدابير وقائية أو ردعية فعالة.[41]

وعلى الرغم من التطور المستمر في تقنيات الحماية والأمن السيبراني، فإن محدودية فعالية الإجراءات الدفاعية في مواجهة هذا النوع من الهجمات تؤكد أنها لم تعد مجرد سلوك إجرامي عابر، بل غدت تهديدًا أمنيًا حقيقيًا يمس المصالح الجوهرية للدول والمجتمع الدولي على حد سواء،[42] ويبرر إدراجها ضمن نطاق الاهتمام المتزايد للقانون الدولي الجنائي.

المبحث الثاني: أركان الجرائم السيبرانية الدولية وصورها

الجرائم السيبرانية الدولية، شأنها شأن الجرائم في نطاق القانون الداخلي، أركان يقوم عليها وجودها القانوني، إذ لا تتحقق إلا بتوافر مجموعة من الأركان الأساسية التي تُشكِّل بنيتها القانونية، كما تتخذ صوراً متعددة ومتطورة تتسم بالتجدد المستمر بسبب التطورات التقنية المتسارعة. ومن ثم، فإن دراسة أركان هذه الجرائم وصورها المختلفة تعتبر أمراً ضرورياً لفهم الطبيعة القانونية لها وتحديد المسؤولية المترتبة عليها.

ومن ثم، سوف نتناول في هذا المبحث مطلبين، سنخصص المطلب الأول للبحث في أركان الجرائم السيبرانية الدولية، وسنخصص المطلب الثاني للبحث في صور الجرائم السيبرانية الدولية.

المطلب الأول: أركان الجرائم السيبرانية الدولية:

يُقصد بأركان الجريمة: العناصر الأساسية التي يتعين توافرها قانونًا لقيام الجريمة، بحيث يترتب على تخلف أي ركن منها انتفاء الوصف الجرمي وعدم قيام المسؤولية الجنائية. وتُعد هذه الأركان عناصر عامة ومشتركة بين مختلف الجرائم، إذ تتوافر في جميع صور السلوك الإجرامي، وتشكّل في مجموعها البنيان القانوني للجريمة.[43]

---

[38] ناجي، محمد سمير، المحكمة الجنائية الدولية" المبادئ التي يقوم عليها نظامها الأساسي"، المجلة الجنائية القومية، المجلد 49، العدد 1، ص 16
[39] ناجي، محمد سمير، المرجع السابق، ص 16
[40] سليم، عهد محمود، الطبيعة الفريدة للجريمة الدولية وانعكاساتها على النظام القضائي الدولي، المرجع السابق، ص 570
[41] د. عبدالرزاق، رانا مصباح عبد المحسن، آليات مكافحة الجرائم السيبرانية في المملكة العربية السعودية، المرجع السابق، ص 13
[42] م.د محمود، سيناء على ،التحديات الأمنية للدول في الفضاء السيبراني، قضايا سياسية، العدد 80 ، ص 320
[43] د. الظفيري، فايز عايد، القواعد العامة في قانون الجزاء الكويتي، الطبعة 5، مطبعة المقهوي، 2016-2017، ص 58

وقد اختلف الفقه الجنائي بشأن تحديد أركان الجريمة؛ فذهب اتجاهٌ فقهي إلى أن الجريمة تقوم على ثلاثة أركان، هي: الركن القانوني أو الشرعي، والمتمثل في وجود نص قانوني يجرّم الفعل ويقرر له جزاءً جنائيًا، والركن المادي، الذي يتمثل في السلوك الإجرامي المجرّم قانونًا، والركن المعنوي، الذي يعبر عن الإرادة الإجرامية للجاني.[44]

في حين يرى اتجاهٌ فقهي آخر أن الجريمة تنحصر في ركنين فقط، هما الركن المادي والركن المعنوي،[45] دون إدراج الركن القانوني ضمن أركان الجريمة.

وعلى الرغم من هذا الخلاف الفقهي، فإن هذا البحث يتبنى الاتجاه الأول القائل بأن الجريمة تقوم على ثلاثة أركان، هي: الركن المادي والمعنوي والشرعي أو القانوني، باعتبار أن الركن القانوني شرطًا جوهريًا يمنح الفعل وصف التجريم ويؤسس للمسؤولية الجنائية، بما يضمن التزام القانون الدولي بمبدأ الشرعية الجنائية.

وتأسيسًا على ما سبق بيانه، وباعتماد الاتجاه الأول، فإن الجرائم السيبرانية الدولية، شأنها شأن الجرائم التقليدية، تقوم على ثلاثة أركان جوهرية تشكِّل بنيانها القانوني، هم: الركن المادي والركن المعنوي والركن الشرعي أو القانوني، بالإضافة الى ركنٍ رابع وهو الركن الدولي باعتباره عنصرًا حاسمًا في إضفاء الصفة الدولية على الجرائم السيبرانية وتمييزها عن غيرها من الجرائم ذات الطابع الداخلي.

الفرع الأول: الركن المادي:

يعرَف الركن المادي بأنه: النشاط المادي الملموس الصادر عن الجاني، والذي يتخذ مظهراً خارجياً يتدخل القانون لتجريمه وترتيب الجزاء الجنائي عليه،[46] ويتكون الركن المادي من ثلاثة عناصر، وهي: السلوك الإجرامي، العلاقة السببية، النتيجة الإجرامية.

أولاً: السلوك الإجرامي:

يعرَف السلوك الإجرامي بأنه: الفعل أو الامتناع الذي يُخرج الجريمة من حيز الفكر والتجريد إلى العالم الواقعي المادي والملموس، بما يتيح التثبت من مظاهره الخارجية، ومن ثم يسمح بتدخُّل القانون بتوقيع الجزاء الجنائي.[47]

ويتخذ السلوك الإجرامي صورتين أساسيتين، هما: السلوك الإيجابي، المتمثِّل في مخالفة نص قانوني ينهى عن إتيان مثل هذا السلوك، يتمثَّل ذلك في تنفيذ هجوم سيبراني متعمد على بنية تحتية حيوية لدولة أخرى، مثل اختراق شبكات الطاقة أو نظم النقل، بما يؤدي إلى تعطيل الخدمات الأساسية وإلحاق أضرار جسيمة، مخالفاً بذلك قواعد القانون الدولي العام، والسلوك السلبي أو الامتناع، المتمثِّل في مخالفة نص قانوني يأمر بإتيان سلوك معين، فيتحقق ذلك من خلال الإخلال بواجب قانوني دولي أو وطني ذا بُعد دولي يفرض على الدولة أو على القائمين على إدارة وحماية نظم المعلومات الحيوية اتخاذ تدابير معيَّنة لضمان أمنها وسلامتها.

على سبيل المثال، إخلال المسؤولين عن أمن المعلومات في الدولة بواجب قانوني مفروض عليهم، كالامتناع عن اتخاذ الإجراءات اللازمة لحماية المعلومات الحيوية للبنى التحتية، أو الإخفاق في عملية تأمين أنظمة التحكم الصناعي في البنية التحتية للدولة، مما يُفضي إلى حدوث هجمات سيبرانية عابرة للحدود.[48]

بناءً على ما تقدم، فإن السلوك الإجرامي في الجرائم السيبرانية الدولية المهددة للسلم والأمن الدوليين، سواء اتخذ صورة الفعل الإيجابي أو الامتناع، فإنه يشكّل الركيزة الأساسية لقيام الركن المادي، متى ثبتت العلاقة السببية بالنتيجة الإجرامية المتمثِّلة في الخطر الجسيم الذي يهدد السلم والأمن الدولي أو المصالح الدولية المحمية.

(44) د. حسني، محمود نجيب، شرح قانون العقوبات، القسم العام، الطبعة 6، دار النهضة العربية،1989، ص63
(45) د. سرور، أحمد فتحي، الوسيط في قانون العقوبات، القسم العام، الطبعة 6، دار النهضة العربية،1996، ص 270
(46) الريثي، محمد مشلوي يحيى، جرائم الأمن السيبراني في النظام السعودي، مجلة العلوم التربوية والدراسات الإنسانية، العدد 45، 2025 ، ص 349
(47) د. الظفيري، فايز عايد، المرجع السابق، ص 328
(48) محمود، أحمد رشيد، الركن الشرعي في الجرائم الدولية، كلية القانون، جامعة ديالي، 2018، ص 12

ثانياً: العلاقة السببية:

تعرَّف العلاقة السببية بأنها: العلاقة التي تربط بين السلوك الإجرامي والنتيجة المترتبة عليه،[49] إذ تُعد عنصرًا اساسياً من عناصر الركن المادي للجريمة.

في القانون الدولي الجنائي، لا تختلف أهمية العلاقة السببية عن مثيلتها في القوانين الداخلية، إذ يُشترط أن يكون السلوك الإجرامي قد أدّى بالفعل إلى النتيجة الإجرامية.

لذلك، تكتسب العلاقة السببية أهمية خاصة عند تطبيقها على الجرائم السيبرانية ذات الطابع الدولي، ففيها قد لا تتحقق النتيجة الإجرامية بشكل فوري، كما قد تتدخل عوامل تقنية معقدة ومتعددة في إحداثها، الأمر الذي يقتضي إثبات وجود علاقة سببية تُسند النتيجة الإجرامية إلى السلوك السيبراني غير المشروع، متى ثبت أن هذا السلوك شكّل عاملاً حاسماً أو مساهماً بقدر كافٍ في إحداث الضرر وتعريض المصلحة الدولية المحمية لخطر جسيم.

ثالثاً: النتيجة الإجرامية:

تُعدّ النتيجة الإجرامية عنصراً رئيسياً في قيام الجريمة الدولية، إذ يتطلب تحققها توافر عنصر النتيجة الإجرامية ضمن أركان الجريمة، إذ إن الجريمة الدولية بطبيعتها تنطوي على اعتداء على مصلحة دولية يحميها القانون الدولي الجنائي، فلا يقتصر التجريم الدولي على مجرد صدور سلوك معين، بل يشترط أن يكون هذا السلوك من شأنه أن يُلحق ضرراً فعلي بالمصلحة الدولية المحمية.[50]

وكما هو الحال في الجريمة الدولية بوجه عام، تُعدّ النتيجة القانونية في الجرائم السيبرانية الدولية عنصراً جوهرياً في تحقق الركن المادي، إذ إن السلوك السيبراني غير المشروع لا يُجرَّم لمجرد مخالفته لقواعد تقنية أو تنظيمية، وإنما لِما ينطوي عليه من مساس فعلي أو تهديد خطير لمصلحة دولية يحميها القانون الدولي الجنائي.

لذلك، تكتسب هذه النتيجة أهمية خاصة في إطار الجرائم السيبرانية الدولية المهددة للسلم والأمن الدولي، نظراً للطبيعة غير المادية لها، ومع ذلك فإنها تنطوي على اعتداء جسيم على المصالح الدولية المحمية.

وعليه، فإن النتيجة في هذا النوع من الجرائم تغدو هي المعيار الحاسم في قيام الركن المادي، حتى في حالة غياب الضرر المادي المباشر.

الفرع الثاني: الركن المعنوي:

يُعرّف الركن المعنوي بأنه: ذلك العنصر الذي يتمثل في الإرادة المصاحبة للفعل الإجرامي، والمتمثلة في اتجاه إرادة الجاني إلى إحداث نتيجة يجرّمها القانون، وهو ما يُعرف بالقصد الجنائي، حيث يقوم على ما يسبق ارتكاب الجريمة من تفكير وتدبير، وإعداد نفسي قائم على إرادة واعية وإدراك معتبرين قانونًا، مع علم الجاني بما يترتب على سلوكه من نتائج وآثار.[51]

وتبرز أهمية هذا الركن على نحو خاص في الجرائم السيبرانية الدولية، نظراً لما تتسم به من تعقيد تقني وتخطيط مسبق وطابع عابر للحدود.

ويقصد بالقصد العام عنصرَي العلم والإرادة، فالعلم يقتضي أن يكون الجاني مدركاً لماهية سلوكه السيبراني غير المشروع، على نحو خالٍ من الجهالة، بما في ذلك طبيعة الوسائل التقنية المستخدمة، ونطاق الهجوم السيبراني، والمصالح الدولية التي يمسّها فعله.

كما يتطلب العلم أن يكون الجاني قادراً على توقّع النتيجة الإجرامية المترتبة على هذا السلوك، سواء تمثَّلت في إحداث ضرر فعلي بالبنى التحتية الرقمية أو الحيوية، أو في تعريضها لخطر جسيم.

---

[49] د. الظفيري، فايز عايد، المرجع السابق، ص 333
[50] محمود، أحمد رشيد، المرجع السابق، ص 12
[51] الحفناوي، منصور، الشبهات وأثرها في العقوبة الجنائية في الفقه الإسلامي مقارنًا بالقانون، مطبعة الأمانة، 1986 ، ص 134

أما الإرادة، فتتجلى في اتجاه نية الجاني إلى ارتكاب الفعل المجرَّم،[52] بحيث يصدر هذا الفعل السيبراني عن إرادة حرة ومقصودة، أي أن الجاني يعلم أن أفعاله من شأنها أن تؤدي إلى تعطيل الأنظمة، أو الإخلال بأمن المعلومات، أو المساس بالمصالح الدولية المحمية، ومع ذلك يمضي في تنفيذها.

أما القصد الخاص، فيتجسَّد في الغاية أو الهدف المحدد الذي دفع الجاني إلى ارتكاب الجريمة السيبرانية الدولية، وهو ما يميّز هذا النوع من الجرائم عن غيره من الأفعال غير المشروعة ذات الطابع التقني البحت.

ويتمثَّل القصد الخاص، على سبيل المثال، في نية الإضرار بأمن دولة معينة، أو التأثير على استقرارها السياسي، أو الاقتصادي، أو تعطيل منشآتها الحيوية، ويُعدّ توافر هذا القصد ركناً جوهرياً لإثبات المسؤولية الجنائية على المستوى الدولي، لاسيما في الحالات التي تُرتكب فيها الأفعال السيبرانية في سياق النزاع المسلح أو الهجوم الموجّه ضد المصالح الدولية المحمية.

وقد أكّد نظام روما الأساسي للمحكمة الجنائية الدولية على الأهمية الجوهرية للركن المعنوي، حيث نصَّت الفقرة 1 من المادة 30 على أنه: " لا يسأل الشخص جنائياً عن ارتكاب جريمة تدخل في اختصاص المحكمة، ولا يكون عرضة للعقاب على هذه الجريمة إلا إذا تحققت الأركان المادية مع توافر القصد والعلم". [53]

لذلك، يشكِّل الركن المعنوي في الجرائم السيبرانية الدولية المهددة للسلم والأمن الدوليين معيارًا فارقًا في تمييز هذا النوع من الجرائم عن غيرها من الجرائم الدولية، إذ أن انتفاء نية الإضرار بالبنية التحتية للدولة أو المساس باستقرارها السياسي أو الاقتصادي، يحول دون إسباغ الوصف الإجرامي على الفعل.

الفرع الثالث: الركن الشرعي والطابع الدولي:

أولاً/ الركن الشرعي للجرائم السيبرانية الدولية:

ويقصد بالركن الشرعي في الجرائم الدولية: القاعدة التجريمية الدولية التي يقررها العرف الدولي أصالةً، أو التي تتضمنها الاتفاقيات الدولية.[54]

ويمثِّل الركن الشرعي في الجرائم السيبرانية الدولية الأفعال الصادرة عن الدولة والتي تكون مخالفة لقواعد ومبادئ القانون الدولي الجنائي، بما يجعل الدولة مسؤولة عن أفعالها على الصعيد الدولي إذا تسببت في أضرار لدولة أخرى عبر الفضاء السيبراني. وتُستمد القاعدة التجريمية الدولية في هذا المجال مصدرها من المعاهدات الدولية، أو من قواعد القانون الدولي العرفي غير المكتوبة، أو من المبادئ العامة للقانون الدولي.[55]

فعلى سبيل المثال، إذا قامت دولة بتنفيذ أو دعم هجوم سيبراني ينطلق من إقليمها ويستهدف أنظمة حيوية لدولة مجاورة، كشبكات الطاقة أو الاتصالات أو الأنظمة المصرفية، وترتب على ذلك تعطيل الخدمات الأساسية أو إلحاق أضرار جسيمة، وثبت أن هذا الفعل يشكل مخالفة لقواعد القانون الدولي المكتوبة أو العرفية، فإن الدولة تتحمل المسؤولية الدولية، بما في ذلك الالتزام بإصلاح الضرر أو التعويض عن الخسائر التي لحقت بالدولة المتضررة.

وفي المقابل، إذا كان الفعل الصادر عن الدولة في المجال السيبراني مشروعاً ومتفقاً مع قواعد القانون الدولي، كاتخاذ تدابير سيبرانية دفاعية مشروعة أو تنظيم سياساتها الرقمية لتحقيق مصلحة اقتصادية داخلية دون مساس بحقوق الدول الأخرى، فلا يترتب على ذلك قيام المسؤولية الدولية.

---

(52) الحفناوي، منصور، المرجع السابق ، ص 135

(53) "لأغراض هذه المادة، يتوافر القصد لدى الشخص عندما :أ يتعمد هذا الشخص، فيما يتعلق بسلوكه، ارتكاب هذا السلوك؛ ب يتعمد هذا الشخص، فيما يتعلق بالنتيجة، التسبب في تلك النتيجة أو يدرك أنها ستحدث في إطار المسار العادي للأحداث - 3 .لأغراض هذه المادة، تعني لفظة "العلم" أن يكون الشخص مدركاً أنه توجد ظروف أو ستحدث نتائج في المسار العادي للأحداث. وتفسر لفظتا "يعلم" أو "عن علم" تبعا لذلك"، نظام روما الأساسي للمحكمة الجنائية الدولية

(54) محمود، أحمد رشيد، المرجع السابق، ص 16

(55) المرجع السابق، ص 14

ويُبرز هذا الركن الفارق الجوهري بين القانون الجنائي الداخلي والقانون الجنائي الدولي، إذ يشترط في الجريمة الداخلية وجود نص قانوني مكتوب يقرر التجريم والعقاب التزاماً بمبدأ الشرعية الصارم، في حين يكفي في الجريمة الدولية أن يكون الفعل خاضعاً لقاعدة تجريمية دولية، سواء كانت مكتوبة أم غير مكتوبة، بما يسمح بالاستناد إلى الأعراف الدولية والمبادئ العامة المعترف بها دولياً في تحديد الطبيعة الإجرامية للفعل.[56]

ثانياً/الطابع الدولي للجرائم السيبرانية الدولية:

إضافةً إلى الأركان السابقة، يشترط لقيام الجرائم السيبرانية الدولية توافر ركن أساسي آخر يتمثل في الركن الدولي، ويُقصد به: أن يكون الفعل محلّ التجريم معاقبًا عليه بموجب قواعد القانون الدولي الجنائي، وأن يترتب عليه إضرار أو اعتداء على مصلحة دولية جوهرية تحظى بالحماية وفقًا لقواعد القانون الدولي، بحيث لا يُقاس معيار دولية الجريمة بكونها تمسّ مرتكبها أو ضحيتها فحسب، وإنما بمدى جسامة الاعتداء الواقع على المصالح الأساسية للمجتمع الدولي.[57]

يُعدّ الطابع الدولي أحد الأركان الجوهرية المميّزة للجريمة الدولية، إذ يضفي عليها طابعها الخاص الذي يخرجها عن نطاق الجرائم الوطنية البحتة ويجعلها محل اهتمام المجتمع الدولي بأسره. وفي المقابل، يقوم الركن الشرعي على مبدأ الشرعية الجنائية، الذي يقتضي ضرورة وجود نص قانوني سابق يجرّم الفعل ويوضح أركانه ويحدد العقوبة المقررة له.

وفي هذا الإطار، تصبح الجريمة السيبرانية غير مكتملة إذا انتفى الركن الدولي فيها، حتى لو توافرت بقية الأركان، إذ قد تُصنّف الأفعال ذات الصلة في هذه الحالة ضمن الجرائم السيبرانية الداخلية وفقًا لقوانين العقوبات الوطنية، مثل جرائم أمن الدولة أو الجرائم المعلوماتية الداخلية. لذلك، يشترط أن يكون الفعل صادرًا من دولة ضد دولة أخرى، بما يمنح الجريمة صفتها الدولية ويحدد نطاق المسؤولية الدولية للدولة والمسؤولية الجنائية الفردية للقادة والأشخاص المكلفين بتنفيذها.

المطلب الثاني: صور الجرائم السيبرانية الدولية:

تتخذ الجرائم السيبرانية الدولية صورًا متعددة تتباين في أساليبها وأهدافها، غير أنّ أخطر هذه الصور وأكثرها ارتباطًا بتهديد السلم والأمن الدوليين تتمثل في الهجمات السيبرانية الموجّهة ضد البنى التحتية الحيوية للدول، الأنظمة العسكرية والأمنية، والأنظمة الصحية والمالية.

الفرع الأول: الهجمات الموجهة ضد البنى التحتية الحيوية:

تعرَّف الهجمات السيبرانية على البنية التحتية الحيوية بأنها: الاعتداءات رقمية تستهدف الأنظمة الرقمية الحيوية للدولة بهدف تعطيل الخدمات الأساسية أو التأثير سلبًا على الأمن الوطني والاستقرار، وتشمل استهداف القطاعات الحيوية.[58]

فهذه البنى، لما تمثّله من ركائز أساسية لاستقرار المجتمعات وضمان استمرارية المرافق الحيوية، تُعدّ هدفًا استراتيجيًا للهجمات السيبرانية، ويُضفي استهدافها بعدًا أمنيًا خطيرًا على الفعل الإجرامي، يجاوز كونه مجرد سلوك إجرامي تقني، ليغدو تهديدًا مباشرًا للمصالح الجوهرية المشتركة للمجتمع الدولي.

فالبنية التحتية الحيوية، التي تشمل القطاعات الأساسية مثل الطاقة، والمواصلات، والمياه، والاتصالات، تعد العمود الفقري لاستمرار عمل الدولة واستقرارها، وأي اختراق أو تعطيل لها يمكن أن يفضي إلى أضرار جسيمة تشكل تهديدًا للسلم والأمن الدوليين.

فتعتمد سلامة واستقرار هذه البنى التحتية الحيوية على حمايتها بصورة فعّالة ضد التهديدات المختلفة، بما في ذلك الهجمات السيبرانية، نظرًا لأهميتها الحيوية في دعم الأمن الوطني واستدامة الخدمات العامة.

---

(56) المرجع السابق، ص 16

(57) العازمي، عبد الله خلف، الجرائم الدولية "خصائصها، وأركانها، وصورها"، المرجع السابق ، ص 748

(58) Watney, Murdoch. "Cybersecurity Threats to and Cyberattacks on Critical Infrastructure: A Legal Perspective." Proceedings of the 21st European Conference on Cyber Warfare and Security (ECCWS 2022), University of Johannesburg, South Africa, 2022, Vol. 21, No. 1, p. 319–327. https://doi.org/10.34190/eccws.21.1.196.

ولكن، لم تسلم هذا القطاعات من التعرض للهجمات السيبرانية، مما يضع حياة البيئة البشرية تحت تهديد مباشر واختبارًا حقيقيًا لقدرة الأنظمة على الصمود، ما يزيد من تعقيد إدارة المخاطر وتأمين استمرارية العمل في القطاعات الأساسية للدول.[59]

حيث قد شهد العقدان الأخيران عدداً من الهجمات البارزة التي كشفت هشاشة البنى التحتية الحيوية أمام التهديدات السيبرانية، ومن أبرز هذه الحوادث: الهجمات واسعة النطاق التي استهدفت أوكرانيا في يونيو 2017، والتي شملت محطات الطاقة ، وأدت إلى تعطيل أنظمة تشغيلية حيوية.[60]

ومن الأمثلة أيضاً على الهجمات السيبرانية على قطاع الطاقة، الهجمات السيبرانية التي تستهدف الشبكات الكهربائية لتعطيلها، حيث يتم ذلك من خلال القيام باختراق الأنظمة ونشر الفيروسات مما يؤدي لتعطيل أنظمة التحكم في البنية التحتية الحيوية.[61]

كما يعد هجوم Stuxnet الذي استهدف أجهزة الطرد المركزي التي تستخدم في تخصيب اليورانيوم في منطقة إيران أحد أبرز الأمثلة على الهجمات السيبرانية على البنية التحتية الحيوية،[62] فقد تم نشر فيروسات استهدفت نظام التشغيل Windows، وتحديداً برنامج Siemens SCADA، وتم تدمير أجهزة الطرد المركزي الإيرانية فعطّلت البرنامج النووي الإيراني، وذلك لأهداف عسكرية.[63]

وفي عام 2008، تعرضت مرافق الطاقة في البرازيل لهجمات سيبرانية، أسفرت عن انقطاع واسع للتيار الكهربائي، بما في ذلك توقف قطارات الأنفاق وإشارات المرور، وتعطل سد "إيتايبو"، ثاني أكبر محطة لتوليد الطاقة في البلاد، وهو ما أثر على حياة أكثر من 60 مليون شخص، وتُبرز هذه الحادثة خطورة الهجمات السيبرانية على البنية التحتية الحيوية للطاقة وقدرتها على تهديد الأمن القومي وسلامة المواطنين.[64]

وفي عام 2017، شهدت المملكة العربية السعودية هجومًا سيبرانيًا خطيرًا باستخدام برمجيات مخصصة للصناعات البترولية، حيث تسللت للشبكات الصناعية واستهدفت قطاع النفط والغاز البتروكيماويات، وأدت إلى خسائر اقتصادية كبيرة للشركات العاملة في هذه القطاعات.[65]

وفي عام 2019، شنت مجموعات قرصنة منظمة من إيران سلسلة هجمات سيبرانية متقدمة استهدفت شبكات المعلومات والبنية التحتية في السعودية، والإمارات، وقطر، والكويت، والبحرين، واستمرت هذه الهجمات لفترات طويلة بهدف تعميق تأثيرها وضمان تحقيق أهداف استراتيجية بعيدة المدى.[66]

كما أن أنظمة الاتصالات والمعلومات لم تسلم من هذه الهجمات السيبرانية، والتي تُعرّف بأنها: أفعال متعمّدة تستهدف البنية التحتية الحيوية، بما في ذلك الشبكات وأنظمة المعلومات، بهدف تعطيلها أو اختراقها أو إتلافها أو الوصول غير المصرّح به إلى البيانات المخزّنة أو المتبادلة داخلها.[67]

تُعد هذه الهجمات أحد أخطر التهديدات التقنية الحديثة، لاستهدافها البنية التحتية المعلوماتية التي تستند عليها الحكومات والشركات وحتى الأفراد.

---

[59] بوطلاعة، وداد، الهجمات السيبرانية على البنية التحتية الحرجة دراسة في ضوء القانون الدولي العام، مجلة حقوق الإنسان والحريات العامة، المجلد 7، العدد 2، 2022، ص 333

[60] م.د محمود، سيناء علي، التحديات الأمنية للدول في الفضاء السيبراني، المرجع السابق، ص 319

[61] زهران، سحر جمال، الجوانب القانونية الدولية لجريمة الإرهاب الإلكتروني، مجلة السياسة والاقتصاد، المجلد 5، العدد 4، 2019، ص 75.

[62] زهران، سحر جمال، المرجع السابق، ص 75

[63] Kelly، Michael، "The Stuxnet Attack on Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought،" Business Insider، Business Insider Inc.، 20 November 2013، Available at: https://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previously-thought-2013-11 Accessed: 31 July 2015

[64] م.د محمود، سيناء علي، المرجع السابق، ص 319

[65] المرجع السابق ، ص 319-320

[66] م.د محمود، سيناء علي، المرجع السابق ، ص 319-320

[67] Watney، Murdoch، "Cybersecurity Threats to and Cyberattacks on Critical Infrastructure: A Legal Perspective،" Proceedings of the 21st European Conference on Cyber Warfare and Security ECCWS 2022، University of Johannesburg، South Africa، 2022، pp. 319–327، Available at: https://doi.org/10.34190/eccws.21.1.196

- **أبرز صور الهجمات الموجهة ضد أنظمة الاتصالات والمعلومات :**[68]

1- الدخول على الأنظمة المعلوماتية:

يكون ذلك عن طريق الدخول على أنظمة الحاسب الآلي أو الوصول بصورة غير مشروعة إلى الأنظمة والبيانات، ويشمل هذا الدخول العديد من الأفعال، على سبيل المثال: حجب البيانات، حجب الأنظمة، أونقلها أو تعديلها أو إتلافها بأي شكل من الأشكال.

وقد جرَّمت اتفاقية مجلس أوروبا لمكافحة الجرائم الإلكترونية هذا النوع من الأفعال، حيث نصَّت المادة 4 من الاتفاقية بأن الدخول على البيانات يكون عن طريق: الإتلاف العمدي أو حذف البيانات أو الإفساد أو التغيير أو الحجب غير المشروع لبيانات الحاسب الآلي.[69]

كما جرّمت اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية "مالابو" هذا النوع من الأفعال في الفقرة 2/أ من المادة 29 ،[70] وكذلك في الفقرة 1 من المادة 8 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.[71]

2- هجوم الحرمان من الخدمة DDOS:

حيث يتم تعطيل الأنظمة من خلال إغراق الخوادم أو الوسائط الشبكية بطلبات مكثفة تحول دون وصول الاستخدام المشروع.

ويُعد هذا النوع من أكثر أنواع الهجوم تعقيدًا، إذ يعتمد على استخدام عدد كبير من الأجهزة الحاسوبية والتقنيات الرقمية لتنفيذ هجوم منسق يستهدف الخوادم أو البنية التحتية الشبكية، مما يؤدي إلى منع المستخدمين من الوصول إلى الخدمات.

ويمكننا توضيح آلية عمل هذا الهجوم من خلال تصور عدد هائل من الأجهزة التي تحاول الاتصال بخادم واحد في الوقت ذاته، في ظل محدودية قدرة المعالجة وعرض النطاق، الأمر الذي يؤدي إلى عجز الخادم عن الاستجابة للطلبات الحقيقية بسبب انشغاله بالطلبات الوهمية.[72]

ومن أبرز الأمثلة على الهجمات السيبرانية هنا هي: الهجمات التي تقوم باستهداف البنى التحتية للشبكات الحكومية، بهدف تدمير البيانات أو التشويش عليها أو تعطيل التواصل الحيوي لها.[73]

3- البرمجيات الخبيثة Malware:

وهي إنتاج أو توزيع أو حيازة أدوات تُستخدم في إساءة استخدام الحاسب الآلي، وتشمل هذه الأدوات البرمجيات الخبيثة، والأجهزة التقنية، وغيرها من البيانات التي تمكّن من الدخول غير المشروع إلى الأنظمة واعتراض البيانات والتدخل فيها،

---

(68) انظر: الجرائم التي تنتهك سرية وسلامة وتوافر بيانات وأنظمة الحاسوب، مكتب الأمم المتحدة المعني بالمخدرات والجريمة، تاريخ الاطلاع: 4 مايو 2026، متاح على الرابط:
https://www.unodc.org/e4j/zh/cybercrime/module-2/key-issues/offences-against-the-confidentiality--integrity-and-availability-of-computer-data-and-systems.html

(69) نصَّت الفقرة 1 من المادة 4 على أنه:" التدخل في البيانات: ١. تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية في قانونها الوطني، إذا ما ارتكبت عمداً: إتلاف بيانات حاسوبية، حذفها، إفسادها، تعديلها أو تدميرها"، الاتفاقية المتعلقة بالجريمة الإلكترونية "اتفاقية بودابست لعام 2001

(70) نصَّت الفقرة أ من المادة 29 على أنه:" الهجمات على أنظمة الحاسوب: تلتزم الدول الأطراف باتخاذ التدابير التشريعية و/أو التنظيمية اللازمة لتجريم الأفعال التالية: الدخول غير المصرح به، أو محاولة الدخول غير المصرح به، إلى جزء من نظام حاسوبي أو إلى النظام بالكامل، أو تجاوز حدود الدخول المصرح به"، اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية "مالابو" لعام 2014

(71) نصَّت الفقرة 1 من المادة 8 على أنه:" الاعتداء على سلامة البيانات 1- :تدمير أو محو أو إعاقة أو تعديل أو حجب بيانات تقنية المعلومات قصدا وبدون وجه حق"، الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010

(72) انظر: الجرائم التي تنتهك سرية وسلامة وتوافر بيانات وأنظمة الحاسوب، مكتب الأمم المتحدة المعني بالمخدرات والجريمة، المرجع السابق، متاح على الرابط:
https://www.unodc.org/e4j/zh/cybercrime/module-2/key-issues/offences-against-the-confidentiality--integrity-and-availability-of-computer-data-and-systems.html

(73) الخريصي، زعل بن سعيد، جرائم الإرهاب السيبراني ودور السياسة الخارجية السعودية في مواجهتها من منظور الأمن الوطني والقانون الدولي، مجلة الأندلس للعلوم الإنسانية والاجتماعية، العدد 73، 2023 ، ص 201.

بهدف إصابة الأنظمة المستهدفة بغرض المراقبة، وجمع البيانات منها، وفرض السيطرة عليها.[74]

وقد جرّمت المادة 9 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات هذا السلوك تحت مسمى "إساءة استخدام وسائل تقنية المعلومات".[75]

وتتعدد صور البرمجيات الخبيثة المستخدمة في هذا السياق، ومن أبرزها:[76]

1- الدودة Worm: برنامج خبيث قادر على الانتشار ذاتيًا دون تدخل المستخدم.

2- الفيروس Virus: برمجية خبيثة تتطلب تفاعل المستخدم للانتشار.

3- حصان طروادة Trojan Horse: برنامج خبيث يتخفى في صورة برنامج مشروع لخداع المستخدم وحثّه على تثبيته، بما يتيح التجسس أو إلحاق الضرر بالنظام.

4- برامج التجسس Spyware: برمجيات تُستخدم لمراقبة الأنظمة بشكل خفي وجمع المعلومات وإرسالها إلى الجهة المهاجمة.

الفرع الثاني: الهجمات الموجهة ضد الأنظمة العسكرية والأمنية:

تلعب التكنولوجيا دوراً محورياً في تطوير القدرات العسكرية الحديثة، حيث تربط الوحدات العسكرية ببعضها البعض، مما تتيح إمكانية تبادل المعلومات العسكرية والأمنية بسرعة عالية، وتسرّع عملية إصدار الأوامر العسكرية، فضلاً عن إمكانيتها من تنفيذ عمليات دقيقة عن بُعد.[77]

غير أن هذه الميزة قد تتحول إلى نقطة ضعف جوهرية في حال غياب الأمن السيبراني الكافي، إذ قد تؤدي هذه الهجمات التي تستهدف الشبكات التابعة للمؤسسات العسكرية والأمنية إلى اختراقها والسيطرة عليها. مما يترتب على ذلك آثار خطيرة قد تصل إلى إيقاع خسائر بشرية في صفوف العسكريين والمدنيين، وتهديد للأمن والسلم الدوليين.[78]

وبناءً عليه، فإن الهجمات السيبرانية الموجهة ضد الأنظمة العسكرية قد تؤدي إلى نتائج تماثل في خطورتها آثار استخدام القوة العسكرية التقليدية، من حيث القدرة على تعطيل البنية التحتية للدولة وإلحاق أضرار جسيمة بقدراتها الدفاعية والأمنية.

ومن الأمثلة البارزة على الهجمات الموجهة ضد الأنظمة العسكرية: الهجمات السيبرانية التي استهدفت القوات المسلحة الأوكرانية والشبكات العسكرية لها، والتي نُسبت إلى جهات سيبرانية مرتبطة بروسيا، حيث كان الهدف منها اختراق أنظمة الاتصالات العسكرية وجمع المعلومات وإضعاف كفاءة العمليات العسكرية.

كما يشهد عام 2008 واقعة اختراق شبكات وزارة الدفاع الأمريكية، إذ تعد مثالاً بارزاً على استهداف الأنظمة العسكرية ، حيث تمكن المهاجمون من النفاذ إلى شبكات عسكرية واستخباراتية، وذلك يكشف عن حجم المخاطر التي تشكِّلها الهجمات السيبرانية على أمن الدول.[79]

---

(74) الجرائم التي تنتهك سرية وسلامة وتوافر بيانات وأنظمة الحاسوب، مكتب الأمم المتحدة المعني بالمخدرات والجريمة، المرجع السابق, متاح على الرابط: https://www.unodc.org/e4j/zh/cybercrime/module-2/key-issues/offences-against-the-confidentiality--integrity-and-availability-of-computer-data-and-systems.html

(75) نصَّت المادة 9 على أنه:" جريمة إساءة استخدام وسائل تقنية المعلومات 1- :إنتاج أو بيع أو شراء أو استيراد أو توزيع أو توفير :أ - أية أدوات أو برامج مصممة أو مكيفة لغايات ارتكاب الجرائم المبينة في المادة السادسة إلى المادة الثامنة .ب- كلمة سر نظام معلومات أو شيفرة دخول او معلومات مشابهة يتم بواسطتها دخول نظام معلومات ما بقصد استخدامها لأية من الجرائم المبينة في المادة السادسة إلى المادة الثامنة 2- .حيازة أية أدوات أو برامج مذكورة في الفقرتين أعلاه، بقصد استخدامها لغايات ارتكاب أي من الجرائم المذكورة في المادة السادسة إلى المادة الثامنة"، الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010، المرجع السابق

(76) الجرائم التي تنتهك سرية وسلامة وتوافر بيانات وأنظمة الحاسوب، المرجع السابق ، متاح على الرابط: https://www.unodc.org/e4j/zh/cybercrime/module-2/key-issues/offences-against-the-confidentiality--integrity-and-availability-of-computer-data-and-systems.html

(77) د.صلاح عبداللاه ربيع، محمد، الهجمات السيبرانية بين مشروعيتها كوسيله للدفاع الشرعي وادانتها كاعتداء غير مشروع دراسة تحليلية في ضوء القانون الدولي، مجلة الدراسات القانونية والاقتصادية، المجلد 10، العدد 1، 2024، ص 42

(78) د.صلاح عبداللاه ربيع، محمد، المرجع السابق، ص 42

تندرج الهجمات السابقة ضمن أنماط التجسس السيبراني الدولي متى تمت بدعم مباشر أو غير مباشر من دولة أخرى، ولاسيما عندما يكون الهدف منها الحصول على معلومات ذات قيمة استراتيجية.

ومن الأمثلة على الهجمات الموجهة ضد الأنظمة الأمنية، هي الهجمات التي تعرضت لها مملكة النرويج، والتي نُسبت مسؤوليتها إلى جهات سيبرانية مدعومة من الصين، حيث قد استهدفت هذه الهجمات البنية التحتية المعلوماتية للقطاع الأمني، وتمكن منفذوها من الحصول على صلاحيات إدارية عالية المستوى أتاحت لهم النفاذ إلى الأنظمة المركزية المستخدمة من قبل مؤسسات الإدارة العامة للدولة.[80]

ومن الأمثلة أيضاً، الهجوم الذي استهدف مكتب إدارة شؤون الموظفين الأمريكي OPM في عام 2015، حيث تم اختراق الأنظمة والوصول لبيانات شخصية وأمنية لملايين من الموظفين الحكوميين، بمن فيهم الأفراد العاملين في الأجهزة الأمنية والاستخباراتية.[81]

الفرع الثالث: الهجمات الموجهة ضد الأنظمة الصحية والمالية:

أولاً/الهجمات الموجهة ضد الأنظمة الصحية:

تتعرض البنية التحتية للخدمات الصحية على المستوى العالمي، سواء في أوقات السلم أو النزاعات، لمخاطر الهجمات السيبرانية التي تستهدف تعطيل أنظمة الحوسبة الإلكترونية الطبية، وسلاسل التوريد الطبية، والأجهزة الطبية الحيوية.

تنبع خطورة هذه الهجمات من قدرتها على إيقاف تقديم الرعاية الصحية، مما يهدد حياة المرضى وكوادر القطاع الصحي، ويؤثر سلبًا على انتظام توزيع المستلزمات الطبية الأساسية، ويعرّض فعالية الخدمات الصحية العامة للخطر بشكل كبير.[82]

تحدث مثل هذه الهجمات من خلال برامج الفدية الضارة، على سبيل المثال، سُجّلت أول حالة وفاة لسيدة ألمانية كانت نتيجة لهجوم سيبراني على مستشفى في مدينة دوسيلدوف بعد أن تم نقلها لمستشفى آخر بسبب تعطل الخدمات الصحية.[83]

ثانياً/ الهجمات الموجهة ضد الأنظمة المالية:

والتي تعني استهداف القطاع المالي في دولةٍ ما، فعلى سبيل المثال، تعرّضت الدولة أ لهجمات DDOS من قِبل الدولة ب على القطاع المالي لها، نتج عن هذه الهجمات عدم تمكّن مواطني الدولة أ من الوصول للخدمات المصرفية، وتعطل أجهزة الصراف الآلي لهذه الدولة.

ومن الأمثلة على الهجمات السيبرانية الموجهة ضد الأنظمة المالية، الهجوم الذي تم استهداف فيه البنك المركزي لبنغلاديش عام 2016، والذي نُسب لمجموعة Lazarus المرتبطة بكوريا الشمالية. حيث تمكن المهاجمون من اختراق نظام التحويلات المالية الدولي SWIFT ، وإصدار أوامر تحويل غير مشروعة أدت إلى سرقة مبالغ مالية كبيرة من حسابات البنك وتحويلها لمؤسسات مالية أجنبية.[84]

---

(79) انظر: الحرب السيبرانية، تاريخ الاطلاع: 13 مايو 2026 ، متاح على الرابط:
https://www.ebsco.com/research-starters/political-science/cyberwarfare-overview

(80) انظر: أهم 10 هجمات إلكترونية على المنظمات الدفاعية والحكومية في عام 2021، تاريخ الاطلاع: 13 مايو 2026، متاح على الرابط:
https://ats.ae/ar/غير-مصنف/أهم-10-هجمات-إلكترونية-على-المنظمات-الدف/

(81) انظر: الحرب السيبرانية، المرجع السابق, تاريخ الاطلاع : 13 مايو 2026 ، متاح على الرابط:
https://www.ebsco.com/research-starters/political-science/cyberwarfare-overview

(82) بوطلاعة، وداد، الهجمات السيبرانية على البنية التحتية الحرجة دراسة في ضوء القانون الدولي العام، المرجع السابق، ص 331

(83) انظر: شارولت ميتشل، أول حالة وفاة بسبب هجمة سيبرانية على خدمات الرعاية الصحية، صحيفة الدايلي ميل البريطانية ، 2020 ، تاريخ الاطلاع: 12 مايو 2026، متاح على الرابط: World's first healthcare cyberattack death after German hospital had to turn woman away due to hack | Daily Mail Online

(84) BankInfoSecurity، "Bangladesh Bank Attackers Hacked SWIFT Software،" Available at: https://www.bankinfosecurity.com/report-swift-hacked-by-bangladesh-bank-attackers-a-9061 Accessed: 10 May 2026

يعتبر هذا الهجوم نموذجاً بارزاً للهجمات السيبرانية المدعومة من الدول والتي تستهدف الأنظمة المالية، حيث كان الغرض منه تحقيق مكاسب مالية غير مشروعة لصالح كوريا الشمالية التي كانت تدعم المهاجمين.

الخاتمة

تناولت هذه الدراسة موضوع التنظيم الدولي للجرائم السيبرانية الدولية في إطار القانون الجنائي الدولي، حيث تم البحث فيها عن تكييف الجرائم السيبرانية المهددة للسلم والأمن الدوليين في ضوء القانون الجنائي الدولي، وذلك انطلاقًا من التطور المتسارع للتقنيات الرقمية وما صاحبه من ظهور أنماط جديدة من الجرائم العابرة للحدود، والتي أصبحت تُشكل تحديًا واقعياً للقواعد التقليدية للقانون الدولي، ولا سيما في مجال المسؤولية الدولية.

وقد أظهرت الدراسة أن الجرائم السيبرانية لم تعد مجرد جرائم تقنية، بل أصبحت في بعض صورها تشكل تهديدًا مباشرًا للسلم والأمن الدوليين، حيث قد ترتقي متى ما توافرت أركانها وتحققت آثارها الخطيرة إلى مستوى الجرائم الدولية الأربع التي نص عليها نظام روما الأساسي، سواء بوصفها جرائم حرب ، أو جرائم عدوان، أو جرائم ضد الإنسانية، أو حتى جريمة إبادة جماعية في حال اقترانها بالقصد الجنائي الخاص.

كما كشفت الدراسة عن وجود قصور في التنظيم الدولي القائم في مواجهة هذا النوع من الجرائم، وذلك من حيث غياب التنظيم القانوني الدولي للهجمات السيبرانية الخطيرة، وفيما يتعلق بآليات الإسناد وإثبات المسؤولية الدولية والمسؤولية الجنائية الفردية، الأمر الذي يحد من فعالية العدالة الجنائية الدولية في التصدي لهذا النوع من الجرائم ومساءلة مرتكبيها.

وبناءاً على ما سبق، خلصت الدراسة إلى أن مواجهة الجرائم السيبرانية الدولية المهددة للسلم والأمن الدوليين تقتضي تطوير الأطر القانونية الدولية بصورة تواكب طبيعة الفضاء السيبراني، وذلك من خلال تطوير نظام روما الأساسي، وإبرام اتفاقية دولية متخصصة، وتعزيز التعاون الدولي في مجال تبادل المعلومات والأدلة الرقمية، وتطوير أيضاً وسائل التحقيق والإسناد التقني، بالإضافة إلى تكريس مبدأ عدم الإفلات من العقوبة، وتعزيز الحماية التقنية والقانونية للبنى التحتية الحيوية للدول.

النتائج والتوصيات

أولاً/ النتائج:

1. خلصت الدراسة إلى أن الهجمات السيبرانية متى بلغت درجة من الخطورة والأثر الذي قد تهدد فيه السلم والأمن الدولي، فإنها تكون قابلة للتكييف ضمن الجرائم الدولية الأربع، نظراً لما قد تُحدثه من آثار مشابهة.
2. 2خلصت الدراسة إلى وجود قصور تشريعي في الإطار القانوني الدولي القائم فيما يخص تنظيم الجرائم السيبرانية المهددة للسلم والأمن الدوليين، خصوصاً فيما يتعلق بآليات الإسناد وإثبات المسؤولية الدولية والمسؤولية الجنائية الفردية.
3. خلصت الدراسة إلى ضرورة تطوير نظام روما الأساسي بما يتيح إدراج الهجمات السيبرانية المهددة للسلم والأمن الدوليين ضمن نطاق الجرائم الدولية، بما يعزّز من فعالية العدالة الجنائية الدولية في مواجهة الجرائم الدولية الحديثة والمتطورة.
4. خلصت الدراسة إلى أن الجرائم السيبرانية قد ترقى إلى جريمة عدوان في حال استهدافها لسيادة الدولة وأثرت في وظائفها السيادية بصورة تعادل استخدام القوة المسلحة، كما يمكن تكييفها كجريمة حرب في حال ارتكابها أثناء نزاع مسلح واستهدافها لأعيان مدنية أو منشآت محمية.
5. خلصت الدراسة إلى أن الجرائم السيبرانية الدولية المهددة للسلم والأمن الدوليين قد ترقى إلى جرائم ضد الإنسانية في حال نُفذت بصورة ممنهجة أو واسعة النطاق ضد السكان المدنيين، وقد تصل بعض صور هذا النوع من الجرائم إلى مستوى جريمة الإبادة الجماعية في حال اقترنت بالقصد الخاص المتعلق بتدمير جماعة قومية أو إثنية أو دينية.
6. خلصت الدراسة إلى أن الاتفاقيات الدولية القائمة، وعلى الرغم من تناولها الجرائم السيبرانية، إلا أنها لا تحتوي على تنظيم شامل ومباشر للهجمات السيبرانية الموجهة ضد البنية التحتية الحيوية للدول، سواءاً من حيث التجريم أو آليات الحماية.

ثانياً/ التوصيات:

1. توصي الدراسة بتوسيع نطاق اختصاص المحكمة الجنائية الدولية بما يتيح تكييف الجرائم السيبرانية الدولية الخطيرة ضمن الجرائم الدولية الأربع متى توافرت أركانها القانونية وآثارها المهددة للسلم والأمن الدولي.
2. توصي الدراسة بتعديل أحكام نظام روما الأساسي بما يكفل النص صراحةً على اعتبار الجرائم السيبرانية الدولية الخطيرة كأحد الجرائم الدولية الأربع وإحدى وسائل ارتكابها.
3. توصي الدراسة بضرورة إبرام اتفاقية دولية متخصصة تُعنى بتنظيم الهجمات السيبرانية الخطيرة، وتضع إطار قانوني محدد وواضح لتحديد شروط تكييفها ضمن الجرائم الدولية.
4. توصي الدراسة بتعزيز آليات التعاون الدولي في إطار تبادل المعلومات الاستخباراتية والأدلة الرقمية، بالإضافة إلى تطوير آليات تقنية تساعد في عمليات التحقيق في الجرائم السيبرانية.
5. توصي الدراسة على تكريس مبدأ عدم الإفلات من العقوبة، إذ يجب مساءلة مرتكبي هذا النوع من الجرائم جنائياً على الصعيد الدولي، بما في ذلك مرتكبيها الذين يتم دعمهم من قبل الدول، وذلك لضمان عدم استغلال طبيعة هذه الجرائم التقنية كوسيلة للإفلات من المسؤولية الجنائية الدولية.
6. توصي الدراسة بتعزيز آليات الحماية التقنية والقانونية للبنى التحتية الحيوية للدول، بما يقلل من خطر استهدافها ويضمن استمرارية الخدمات الرئيسية.

قائمة المراجع

المراجع العربية:

المصادر الشرعية:

1. القرآن الكريم.
2. البخاري، كتاب الاعتصام بالكتاب والسنة.
3. مسلم، كتاب الفضائل.

الكتب:

1. الحسبان، عماد، والضمور، عدنان، والتميمي، عز الدين، والخزاعلة، ياسر، الجرائم المستحدثة: المعلوماتية، الإلكترونية، السيبرانية، دار الخليج للنشر والتوزيع، 2024.
2. حسني، محمود نجيب، شرح قانون العقوبات، القسم العام، الطبعة السادسة، دار النهضة العربية، 1989.
3. الحفناوي، منصور، الشبهات وأثرها في العقوبة الجنائية في الفقه الإسلامي مقارنًا بالقانون، مطبعة الأمانة، 1986.
4. الديربي، عبدالعال إسماعيل، ومحمد، الجرائم الإلكترونية، المركز القومي للإصدارات القانونية، القاهرة، 2012م.
5. سرور، أحمد فتحي، الوسيط في قانون العقوبات، القسم العام، الطبعة السادسة، دار النهضة العربية، 1996.
6. الظفيري، فايز عايد، القواعد العامة في قانون الجزاء الكويتي، الطبعة الخامسة، مطبعة المقهوي، 2016–2017.
7. نصار، غادة، الإرهاب والجريمة الإلكترونية، القاهرة، العربي للنشر والتوزيع، 2017م.

الدراسات السابقة:

1. أ. حامد، عبد الإله عبد اللطيف محمد، «مدى ملاءمة تجريم السلوك الدولي مع مبدأ الشرعية»، المجلة الدولية للدراسات القانونية والفقهية المقارنة، 2020.
2. أحمد، رحمة الله حبوب محمد، «أنواع الجريمة الدولية وعناصرها في القانون الدولي الجنائي»، المجلة الأفريقية للدراسات المتقدمة في العلوم الإنسانية والاجتماعية، 2022.

3. بوطلاعة، وداد، "الهجمات السيبرانية على البنية التحتية الحرجة: دراسة في ضوء القانون الدولي العام"، مجلة حقوق الإنسان والحريات العامة، المجلد 7، العدد 2، 2022.
4. الحجار، عدنان، وبشير، فايز، «الأدلة الرقمية وإثبات الجرائم السيبرانية ما بين التأصيل والتأويل»، مجلة جامعة الاستقلال للأبحاث، المجلد 6، العدد 1، 2022.
5. الخريصي، زعل بن سعيد، «جرائم الإرهاب السيبراني ودور السياسة الخارجية السعودية في مواجهتها من منظور الأمن الوطني والقانون الدولي»، مجلة الأندلس للعلوم الإنسانية والاجتماعية، العدد 73، 2023.
6. الديربي، عبدالعال إسماعيل، ومحمد، «الجرائم الإلكترونية»، المركز القومي للإصدارات القانونية، القاهرة، 2012.
7. رمضان، إبراهيم السيد أحمد، «مواجهة الهجمات السيبرانية في ضوء أحكام القانون الدولي»، مجلة العلوم القانونية والاقتصادية، العدد 1، 2025.
8. الريثي، محمد مشلوي يحيى، «جرائم الأمن السيبراني في النظام السعودي»، مجلة العلوم التربوية والدراسات الإنسانية، العدد 45، 2025.
9. زروقة، إسماعيل، «الفضاء السيبراني والتحول في مفاهيم القوة والصراع»، مجلة العلوم القانونية والسياسية، جامعة محمد بوضياف، الجزائر، المجلد 10، العدد 1، 2019.
10. زهران، سحر جمال، «الجوانب القانونية الدولية لجريمة الإرهاب الإلكتروني»، مجلة السياسة والاقتصاد، المجلد 5، العدد 4، 2019.
11. سليم، عهد محمود، «الطبيعة الفريدة للجريمة الدولية وانعكاساتها على النظام القضائي الدولي»، المجلة العربية للنشر العلمي، العدد 86، 2025.
12. الصحفي، روان عطية الله، «الجرائم السيبرانية»، المجلة الإلكترونية الشاملة متعددة التخصصات، العدد 24، 2020.
13. صلاح عبد اللاه ربيع، محمد، «الهجمات السيبرانية بين مشروعيتها كوسيلة للدفاع الشرعي وإدانتها كاعتداء غير مشروع: دراسة تحليلية في ضوء القانون الدولي»، مجلة الدراسات القانونية والاقتصادية، المجلد 10، العدد 1، 2024.
14. العازمي، عبد الله خلف، «الجرائم الدولية: خصائصها، وأركانها، وصورها»، جامعة الأزهر، كلية الشريعة والقانون بأسيوط، العدد 35، 2023.
15. عبد الرزاق، رانا مصباح عبد المحسن، «آليات مكافحة الجرائم السيبرانية في المملكة العربية السعودية»، المجلة القانونية، المجلد 15، العدد 5، 2023.
16. العتيبي، زياد محمد، «جرائم السيبرانية المرتكبة عبر الوسائط الرقمية: بيان مفهومها من حيث أشكالها، خصائصها، أركانها، والدافع من ارتكابها»، المجلة الأكاديمية العالمية للدراسات القانونية، المجلد 3، العدد 1، 2021.
17. الكندري، مريم أحمد علي، «الجرائم السيبرانية في الاقتصاد الرقمي: دراسة فقهية تأصيلية»، مجلة العلوم الشرعية، جامعة الإمام محمد بن سعود الإسلامية، المجلد 3، العدد 75، 2025.
18. لطفي، وفاء، «الجهود الدولية في مكافحة جرائم الإرهاب السيبراني: التجربة الماليزية نموذجًا»، مجلة كلية الاقتصاد والعلوم السياسية، المجلد 23، العدد 1، 2022م.
19. محمود، أحمد رشيد، الركن الشرعي في الجرائم الدولية، كلية القانون، جامعة ديالي، 2018.
20. محمود، سيناء علي، «التحديات الأمنية للدول في الفضاء السيبراني»، قضايا سياسية، العدد 80.
21. المحيميد، يزيد صالح، «الجرائم السيبرانية في القانون الجنائي»، المجلة القانونية، المجلد 25، العدد 3، 2025م.
22. مهمل، أسامة، «الإجرام السيبراني»، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، 2018.
23. ناجي، محمد سمير، «المحكمة الجنائية الدولية: المبادئ التي يقوم عليها نظامها الأساسي»، المجلة الجنائية القومية، المجلد 49، العدد 1.

الاتفاقيات والبروتوكولات الدولية:

1. اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية (اتفاقية مالابو) لعام 2014.

2. الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010.
3. اتفاقية بودابست بشأن الجرائم المعلوماتية.
4. البروتوكول الإضافي الأول إلى اتفاقيات جنيف لعام 1949.
5. دليل تالين "2" لعام 2017.(Tallinn Manual 2.0).
6. نظام روما الأساسي للمحكمة الجنائية الدولية.

المواقع الإلكترونية العربية:

1. الهيئة الوطنية للأمن السيبراني.
2. https://nca.gov.sa/ar/
3. أهم 10 هجمات إلكترونية على المنظمات الدفاعية والحكومية في عام 2021.
https://ats.ae/ar/الدف-المنظمات-على-إلكترونية-هجمات-10-أهم/مصنف-غير/
4. الحرب السيبرانية، متاح على الرابط:
https://www.ebsco.com/research-starters/political-science/cyberwarfare-overview
5. شارولت ميتشل، أول حالة وفاة بسبب هجمة سيبرانية على خدمات الرعاية الصحية، صحيفة الدايلي ميل البريطانية ، 2020، متاح على الرابط: World's first healthcare cyberattack death after German hospital had to turn woman away due to hack | Daily Mail Online
6. الجرائم التي تنتهك سرية وسلامة وتوافر بيانات وأنظمة الحاسوب، مكتب الأمم المتحدة المعني بالمخدرات والجريمة، متاح على الرابط:
https://www.unodc.org/e4j/zh/cybercrime/module-2/key-issues/offences-against-the-confidentiality--integrity-and-availability-of-computer-data-and-systems.html
7. قاموس أكسفورد الإنجليزي ، دار نشر جامعة أكسفورد , متاح على الرابط : https://www.oed.com

الدراسات الأجنبية:

1. Kelly, Michael, "The Stuxnet Attack on Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought," Business Insider, Business Insider Inc., 20 November 2013. Available at: Business Insider Accessed: 31 July 2015.
2. Velenczei, Dora Vanda, "Recognising Cyber Blockades as Crimes Against Humanity: Can International Criminal Law Keep Up?", Proceedings of the 19th International Conference on Cyber Warfare and Security (ICCWS 2024), Vol. 19, No. 1, 2024.
3. Vitvitskaya, S. S., Vitvitsky, A. A., & Isakova, Yu. I., "Cybercrime: Concept, Classification, and International Counteraction," Legal Order and Legal Values, Vol. 1, No. 1, 2023.
4. Watney, Murdoch. "Cybersecurity Threats to and Cyberattacks on Critical Infrastructure: A Legal Perspective." Proceedings of the 21st European Conference on Cyber Warfare and Security (ECCWS 2022), University of Johannesburg, South Africa, 2022, Vol. 21, No. 1.

المواقع الإلكترونية الأجنبية:

1. Article 491 of the First Additional Protocol to the Geneva Conventions of 1949 https://www.icrc.org/sites/default/files/external/doc/en/assets/files/other/icrc_002_0321.pdf.

2. Bangladesh Bank Attackers Hacked SWIFT Software
https://www.bankinfosecurity.com/report-swift-hacked-by-bangladesh-bank-attackers-a-9061.
3. Kelly، Michael، "The Stuxnet Attack on Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought،" Business Insider، Business Insider Inc.، 20November 2013، Available at: https://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11.