مجلة كفة الميزان

دراسات قانونية و سياسية محكمة برؤية تحليلية

نافذة معرفية في عالم القنون و السياسة تجمع
بين التحليل الاكاديمي و الرؤية الواقعية

العدد الرابع - السنة الأولى - المجلد الأول / شوال 1447 الموافق نيسان 2026

توجه جميع المرسلات الى رئيس التحرير على العنوان التالي

مجلة كف الميزان - اربيل - العراق
تلفون : 009647738223272
info@tip-scale.com

تتوفر نصوص و البحوث كاملة في الموقع التالي
www.tip-scale.com

رقم الايداع
3105-1502

كفة الميزان

سياسية النشر

تعنى مجلة كف الميزان بمشاركات الأبحاث الرصينة والدراسات والتعليقات على الأحكام القضائية وملخصات رسائل الماجستير وأطاريح الدكتوراه والتقارير العلمية عن الندوات والمؤتمرات وعرض الكتب الجديدة ومراجعتها باللغة العربية والإنكليزية، كما تدعوكم المجلة للتفاعل معها وإغناء الأعداد الصادرة عنها وفق سياسة النشر الخاصة بها والمتمثلة بالآتي:

1- مجلة كف الميزان هي مجلة دورية تصدر شهرياً عن دار هاتريك للنشر والتوزيع في أربيل- العراق.

2- المجلة مختصة بنشر أبحاث العلوم الإجتماعية (القانونية والسياسية والاقتصادية)، أو عرض رسائل الماجستير وأطاريح الدكتوراه، أو التعليقات على الأحكام القضائية، أو التقارير العلمية عن الندوات والمؤتمرات، أو عرض الكتب الجديدة ومراجعتها في العلوم القانونية والسياسية وباللغتين العربية والإنكليزية.

3- تحتفظ المجلة بحقوق النشر والطبع كافة، كما تعبر جميع آراء المؤلفين الواردة في البحث أو المادة العلمية عن وجهة نظرهم، ولا تُعَدُّ المجلة مسؤولة عنها، استناداً لمبدأ استقلالية الرأي، وتلتزم المجلة بالحفاظ على حقوق الملكية الفكرية للمؤلفين..

4- المجلة غير ملزمة برد أصول البحوث أو التعليقات على الأحكام القضائية أو ملخصات الكتب ورسائل الماجستير أو أطاريح الدكتوراه سواء نشرت أم لم تنشر، مع خصم جميع المصاريف في حال عدم النشر.

5- تكون الأولوية بالنشر حسب الأسبقية بالحصول على قبول نشر للبحوث، وفي حال رغبة الباحث بالنشر المستعجل يستوفى مبلغ إضافي على أجور النشر النهائية للبحث، طبقاً لما متاح على موقع المجلة الإلكتروني.

6- يشترط بالمادة العلمية المراد نشرها بالمجلة، أن لا تكون قد سبق نشرها في مجلة أو دورية أو مؤتمر علمي، بتعهد يقدمه الباحث، وبخلافه يتحمل الباحث المسؤولية القانونية والمالية كافة.

7- يلتزم الباحث بعدم إرسال بحثه أو مادته العلمية إلى أي جهة أخرى لغرض النشر، حتى يصله رد المجلة بصلاحية بحثه أو مادته العلمية للنشر من عدمه خلال مدة شهرين من تاريخ استلام المجلة للبحث أو المادة العلمية، وبخلافه تحتفظ المجلة بحقوقها القانونية والمالية كافة.

8- يتعين على الباحث أن يلتزم بشروط وأسلوب النشر المعتمد من المجلة والمتاح على موقع المجلة الإلكتروني (https://tip-scale.com/)، وبخلافه لا تتحمل المجلة مسؤولية التأخر بقبول أو نشر البحث أو المادة العلمية.

9- يجب على الباحث مراعاة الأمانة العلمية في البحث العلمي والدراسة الأكاديمية وفي مقدمتها أخلاقيات البحث العلمي وبنود لجنة أخلاقيات النشر (Committee On Publication Ethics) مثال ذلك، توثيق المراجع والمصادر والنصوص القانونية والعلمية ومراعاة الموضوعية والمنهجية في الكتابة، وبخلافه يتحمل الباحث المسؤولية القانونية والإدارية والمالية الكاملة عن أي انتهاك أو تجاوز لهذه الأخلاقيات طبقاً للقوانين والتعليمات الوطنية أو الدولية.

10- تخضع جميع البحوث العلمية المراد نشرها بالمجلة لتدقيق نسبة الانتحال (turnitin) ضماناً لعدم نشر البحوث مسروقة النص جزئياً أو كلياً، وبخلافه يتحمل الباحث المسئولية القانونية والمالية والإدارية الكاملة.

11- تخضع المادة العلمية التي تنشرها المجلة للتحكيم الشفاف والمراجعة العلمية المتخصصة (Peer-reviewed process) فضلاً عن التدقيق اللغوي (للغة العربية واللغة الإنكليزية)، ويكون للمجلة صلاحية الموافقة على النشر فيها من عدمه استناداً إلى الآراء الأولية لهيئة تحرير المجلة أو آراء المحكمين المتخصصين.

13- يمنح كل باحث نسخة ورقية من العدد المنشور فيه بحثه، فضلاً عن نسخة مستلة عن بحثه، ولا تتحمل المجلة أجور إرسال النسخة الورقية للباحث.

14- تعمل المجلة وفق آلية وسياسة النشر المفتوح (Open Access).

15- تلتزم المجلة بمنح الباحث قبول النشر حين استكمال جميع المتطلبات على أن يذكر فيه المجلد والعدد وسنة النش

Publication Policy

KAFEET_ALMEZAN Journal focuses on contributions of rigorous research, studies, comments on judicial rulings,

summaries of master's theses and doctoral dissertations, scientific reports on conferences, and book reviews in both Arabic and English. The journal invites you to interact with it and enrich the published issues according to its publication policy, as follows:

1. KAFEET_ALMEZAN Journal is a peer-reviewed monthly journal published by Hatrick Publishing and Distribution company in Erbil, Iraq.

2. The journal specializes in publishing research in the fields of social sciences (legal, political, and economic), presenting master's theses, doctoral dissertations, comments on judicial rules, scientific reports on conferences, and reviews of new books in both Arabic and English languages.

3. The journal reserves all rights of publication and printing. All opinions expressed in the research or scientific material are solely those of the authors, and the journal is not responsible for them, based on the principle of independence of opinion, the journal is committed to preserving the intellectual property rights of authors.

4. The journal is not obliged to return the original research, comments on judicial rules, book summaries, master's theses, or doctoral dissertations, whether published or not, with all costs deducted in case of non-publication.

5. Priority for publication is based on the order of receiving research acceptance. In case the researcher wishes to expedite publication, an additional fee is applied on the final publication costs of the research, as available on the journal's website.

6. The scientific material intended for publication in the journal should not have been previously published in any magazine, periodical, or scientific conference, as per a commitment provided by the researcher. Otherwise, the researcher bears full legal and financial responsibility.

7. The researcher should not submit their research or scientific material to any other entity for the purpose of publication until they receive a decision on whether the journal accepts their research or scientific material

for publication within two months from the date of the journal's receipt of the research or scientific material. Otherwise, the journal reserves all legal, financial, and administrative rights.

8. The researcher must adhere to the conditions and style of publication approved by the journal and available on the journal's website. Otherwise, the journal is not responsible for any delay in accepting or publishing the research or scientific material.

9. The researcher must observe scientific integrity in scientific research and academic study, including research ethics and the codes of the Committee on Publication Ethics. This includes proper citation of references, sources, legal texts, and scientific texts, as well as ensuring objectivity and methodology in writing. Otherwise, the researcher is fully responsible for any violations or deviations from these ethics, in accordance with national or international laws and regulations.

10. All scientific research intended for publication in the journal is subject to plagiarism checking (Turnitin) to ensure that the research is not partially or entirely plagiarized. Otherwise, the researcher is fully responsible for any legal, financial, and administrative liability.

11. The scientific material published by the journal is subjected to transparent peer review and specialized scientific review, in addition to linguistic review (in Arabic and English). The journal has the right to approve or reject publication based on the preliminary opinions of the journal's editorial board or specialized reviewers.

12. Each researcher is granted a hard copy of the issue in which their research is published, as well as a copy of their research. The journal does not cover the costs of sending the hard copy to the researcher.

13. The journal operates according to the Open Access publication model.

14. The journal is committed to providing the researcher with the acceptance of publication upon completing all the requirements, specifying the volume, issue, and year of publication, except for research extracted from master's theses and doctoral dissertations."

الحماية القانونية من جرائم الانظمة الرقمية والمعلوماتية

اشراف

الأستاذ الدكتور موسى الابراهيم

الطالب

مهند محسن عبد

المستخلص:

يهدف البحث إلى دراسة جرائم الدخول والبقاء غير المشروع ضمن الأنظمة المعلوماتية، وهي واحدة من أبرز الجرائم السيبرانية التي نشأت نتيجة للتطورات التكنولوجية واستخدام الإنترنت. تُمثل هذه الجرائم تهديدًا كبيرًا للأمن السيبراني، حيث يشمل الاختراق غير المشروع للأنظمة المعلوماتية بهدف الحصول على البيانات أو تدميرها أو التحكم بها دون إذن من صاحب النظام. وقد تم تقسيم البحث إلى عدة محاور، حيث تم تناول في المبحث الأول جرائم الاختراق المعلوماتي، بما في ذلك تطورها وأسباب نشوئها، ودوافع وأساليب جريمة الاختراق السيبراني. تم التركيز على تحديد الفرق بين الهجمات السيبرانية والجريمة السيبرانية، حيث تُعتبر الأولى أكثر تطورًا وتعقيدًا وتشمل أنشطة دولية أو عسكرية. وفي المبحث الثاني، تم التعرض لجرائم إتلاف المعطيات الرقمية، مثل الهجمات التي تستهدف تدمير البيانات أو تعطيل أنظمة المعلومات. كما تم تناول الفروق بين التسلل السيبراني والهجوم السيبراني والإرهاب السيبراني. وقد تم التوصل إلى مجموعة من النتائج المهمة التي تسلط الضوء على التحديات الأمنية التي تواجه الأفراد والدول في مجال حماية أنظمتها المعلوماتية، وأهمية تحسين التشريعات الوطنية والدولية لمكافحة هذه الجرائم. كما تم تقديم توصيات هامة تهدف إلى تعزيز الأمن السيبراني وزيادة الوعي المجتمعي حول هذه الأنواع من الجرائم.

الكلمات المفتاحية: الجرائم السيبرانية ،الأمن السيبراني، اختراق الأنظمة المعلوماتية ،الهجمات الإلكترونية، التشريعات القانونية.

Abstract:

The research is divided into several sections. This research aims to study crimes of unauthorized access and remaining within information systems, which are among the most prominent cybercrimes that have arisen as a result of technological developments and the use of the internet. These crimes represent a significant threat to cybersecurity, as they include the unauthorized intrusion into information systems with the aim of obtaining, destroying, or controlling data without the permission of the system owner. The research is divided into sections, with the first section addressing cyber intrusion crimes, including their development, causes of emergence, motives, and methods of cyber intrusion. The focus is on defining the difference between cyberattacks and cybercrime, as the former is considered more sophisticated and complex and includes international or military activities. The second section addresses crimes of digital data destruction, such as attacks that aim to destroy data or disrupt information systems

Discussing the differences between cyber intrusion, cyberattack, and cyberterrorism. A number of important findings were reached, highlighting the security challenges facing individuals and nations in protecting their information systems, and the importance of improving national and international legislation to combat these crimes. Important

recommendations were also presented aimed at strengthening cybersecurity and increasing public awareness about these types of crimes.

Keywords: Cybercrime, Cybersecurity, Information Systems Hacking, Cyberattacks, Legal Regulations.

المقدمة

لقد أحدثت التكنولوجيا ثورة هائلة في مختلف مجالات الحياة البشرية، وأثر هذا التطور بشكل كبير على الأمن السيبراني وظهور أشكال جديدة من الجرائم، أبرزها الجرائم المعلوماتية أو ما يعرف بالجرائم السيبرانية. هذه الجرائم، التي تتمثل في الدخول غير المشروع إلى الأنظمة المعلوماتية واعتداءات أخرى على الشبكات الرقمية، باتت تشكل تهديدًا كبيرًا للأفراد والمؤسسات والدول على حد سواء. فالتطور التكنولوجي السريع في مجال الاتصالات والإنترنت قد سهل للأفراد في أي مكان بالعالم الوصول إلى المعلومات والأنظمة الرقمية، مما ساهم في زيادة ظاهرة الجرائم السيبرانية بأنواعها المختلفة، مثل اختراق البيانات، التسلل، الهجمات الإلكترونية، والتجسس السيبراني.

من أهم هذه الجرائم هو "جريمة الدخول غير المشروع والبقاء داخل الأنظمة المعلوماتية"، والتي تعني الاعتداء على الأنظمة الرقمية بغرض سرقة أو تخريب البيانات أو حتى استخدام الأنظمة في أغراض غير مشروعة. لقد تزايدت هذه الأنواع من الجرائم بسبب إقبال الأفراد على استخدام الإنترنت وزيادة تعقيد الهجمات السيبرانية التي تشمل الهجمات العسكرية والسياسية

أهمية البحث:

تكتسب دراسة هذه الجرائم أهمية خاصة في ظل تزايد الاعتماد على الإنترنت في الحياة اليومية، وتطور التقنيات التي تمكّن الأفراد من تنفيذ هجمات سيبرانية بسهولة وفعالية. يشمل هذا التهديد البنية التحتية الرقمية للدول، مثل شبكات

الكهرباء، المياه، وحتى الأنظمة العسكرية. ومن هنا تبرز الحاجة الملحة لفهم أبعاد هذه الجرائم ووضع التشريعات المناسبة لمكافحتها.

إشكالية البحث:

تتمثل إشكالية البحث في كيفية تصنيف الجرائم السيبرانية بشكل دقيق، والتمييز بين الأنواع المختلفة من الجرائم السيبرانية مثل الاختراق، الهجوم، والإرهاب السيبراني. هذا التمييز يعد أمرًا بالغ الأهمية لتوفير استراتيجية فعالة لمكافحة هذه الجرائم، حيث أن بعض الجرائم تتطلب استجابة قانونية وأمنية مختلفة عن غيرها.

منهجية البحث:

يعتمد البحث على المنهج التحليلي المقارن، حيث يتم دراسة تطور الجرائم السيبرانية وتقديم تعريفات مفصلة لكل نوع من هذه الجرائم. كما يستعرض البحث الأساليب القانونية والتشريعية التي اتبعتها الدول لمكافحة هذه الجرائم، ويركز على المقارنة بين الأنظمة القانونية في العالم العربي والعالم الغربي في معالجة هذه الظاهرة.

خطة البحث:

يتناول البحث في المبحث الأول تطور الجرائم السيبرانية وتحديد الأنواع المختلفة مثل الاختراق الإلكتروني، التسلل، الهجمات الإلكترونية، وعلاقة كل منها بالأمن السيبراني. في المبحث الثاني، سيتم التركيز على الحماية القانونية من هذه الجرائم، مع تحليل التشريعات الدولية والمحلية في مجال مكافحة الجرائم المعلوماتية. أخيرًا، سيتم تقديم بعض التوصيات التي تهدف إلى تطوير سياسات أمنية فعالة لمكافحة الجرائم السيبرانية.

المبحث الأول

جرائم الدخول والبقاء غير المشروع ضمن الأنظمة المعلوماتية

إن التقدم الحضاري الذي اجتاح العالم في العصر الحديث أثر في كافة نواحي الحياة الإنسانية من سلوكيات وغيرها وقد طال هذا التأثير نوعية الجريمة والمجرم وأصبح ملموسا لدى كل المختصين والمهتمين بعلم الإجرام والمجرمين. ومن نتائج التطور الحضاري الذي اجتاح العالم الحديث تقنية المعلومات التي نعتبر العامل الأساسي الذي أحدث ثورة هائلة في مجال الاتصالات واستخدامات الحاسب الآلي والإنترنت للأغراض المختلفة وفي نفس الوقت ساهمت في إنتاج وتطوير كثير من السلوكيات التي تعتبر إجراماً وفقاً لقوانين وقواعد التجريم ولا شك أن لها الأثر البالغ على حياة أفراد مجتمعات العالم وعلى القطاع العام والخاص ومن هذه الجرائم التي تم استحداثها ما يسمى بالجرائم السيبرانية[1].

وبناءً على ما تقدم سوف نقوم بتقسيم هذا المبحث إلى مطلبين حيث سنعالج في المطلب الأول طبيعة جرائم الاختراق المعلوماتي أما في المطلب الثاني سوف نتطرق إلى دوافع وأساليب جريمة الاختراق السيبراني .

[1] إسلام هديب، الأمن السيبراني، الهجمات السيبرانية والجرائم السيبرانية، مرجع سابق، ص33.

المطلب الأول

طبيعة جرائم الاختراق المعلوماتي

تطورت الجريمة السيبرانية بشكل كبير على مر السنوات وذلك نتيجة للتقدم التكنولوجي وانتشار استخدام الإنترنت والتكنولوجيا الرقمية، وبعد التغييرات الصناعية والقفزات الكبيرة في مجال العلم والتكنولوجيا منذ نهايات قرن الثامن عشر وحتى قرن العشرين ظهرت الكثير من الأساليب الجديدة في النزاعات المسلحة، فالثورة الصناعية تعد من أهم الأسباب التي أدت إلى تغيير ماهية النزاعات المسلحة لتصبح ذات آثار مدمرة أكثر من السابق. إن تطور العلم والتكنولوجيا وظهور الأدوات والأساليب الحديثة أدى إلى تطور عظيم في وسائل القوة والأسلحة كظهور أسلحة الدمار الشامل والحرب السيبرانية[1].

وبعد غزو روسيا (الإتحاد السوفيتي (سابقاً) للفضاء وبدء سباق التسلح النووي، قامت الحكومة الأمريكية بتكليف مؤسسة راند (RAND) بدراسة مسألة استراتيجية ألا وهي كيفية ضمان استمرارية الاتصالات بين السلطات الأمريكية في حالة نشوب حرب نووية.

فتمخض عن دراسات هذه المؤسسة وجوب بناء شبكة لامركزية تعتمد على تحويل الرسائل إلى بيانات رقمية فقامت وزارة الدفاع الأمريكية في عام 1969 بتنفيذ هذا المشروع وأسمتها شبكة الأربانت (Arpanet) إذ ربطت هذه الشبكة مجموعة

---

[1] زهراء عماد محمد كلنتر، المسؤولية الدولية الناشئة عن الهجمات السيبرانية، مرجع سابق، ص44.

من الجامعات الأمريكية وتجلت فائدتها في نقل المعلومات بسرعة هائلة بين أجهزة كمبيوتر عملاقة ، ثم توسعت بعد ذلك ودخلت مرحلة العالمية إثر ربطها بجامعات ومراكز أبحاث في أوروبا وأصبحت تسمى شبكة الإنترنت (Internet) أي الشبكة العالمية.

و من بعد هذه الحقبة بدأ انتشار استخدام الإنترنيت، وأسهم ظهور الشبكات المختلفة في توسع شبكة الإنترنت التي أصبحت وسيلة رئيسية في الاتصالات، إلا إن الثورة الحقيقية في عالم الإنترنت كانت ظهور شبكة الويب العالمية (www)، وهي خدمة سهلة الاستخدام تعتمد في عرض المعلومات على النصوص والصور والصوت و الفيديو[1]، وانتشر بذلك استخدام الإنترنت بسرعة هائلة و أصبحت شبكة الإنترنيت من مظاهر التطور العلمي الحديث المستخدمة في نقل المعلومات بسرعة تفوق التصور و أصبح بالإمكان الحصول على المعلومات فيها بمجرد الاتصال بالشبكة، فالمعلومات التي تخزنها وتنشرها هذه الشبكة وأنظمتها، لا تعد حكراً على أحد.

إن هناك صعوبة في تحديد بداية معينة لنشوء الجرائم السيبرانية، حيث أن الحواسيب الإلكترونية كانت موجودة منذ فترة بعيدة، ولكن تختلف عما هي عليه الحواسيب الحالية سواء من حيث الشكل أو السرعة والدقة والتطور الحالي الذي يعتبر نتائج لتطور كبير عبر سنين عديدة. إلا أن البعض يرجع حدوث أول جريمة متصلة بالحاسوب إلى عام 1801، عندما أقدم صاحب مصنع للنسيج

---

[1] منير محمد الجنبيهي وممدوح محمد الجنبيهي، امن المعلومات الإلكترونية، مرجع سابق، ص9.

في فرنسا ويدعى جوزيف جاكورد على تصميم لوحة إلكترونية وكانت أول نموذج للوحة الحاسوب الحالي لتقويم هذه اللوحة بتكرار مجموعة من الخطوات المستخدمة لحياكة أنواع من المنسوجات، الأمر الذي آثار مخاوف بعض العاملين في المصنع من تأثير تلك اللوحة على وظائفهم مما دفعهم إلى تخريب تلك اللوحة[1].

بينما يرجع البعض الآخر البداية الحقيقية لظاهرة الجرائم السيبرانية إلى عام 1958 حيث بدأ معهد ستانفورد الدولي للأبحاث في الولايات المتحدة الأمريكية رصد حالات ما سمي في ذلك الحين بإساءة الإلكترونية استخدام الحاسوب بصورة منظمة.

ورغم استمرار تطور ظاهرة الجريمة السيبرانية خلال حقبة السبعينات، إلا أن الحالات التي سجلت في تلك الفترة الزمنية كانت قليلة، وقد تعود أسباب تلك القلة إلى كون مكمن الخطر كان داخليا، ويكاد أن يكون خطرا ينحصر بين العاملين على الأنظمة الحاسوبية نفسها حيث كانوا هم فقط من يستطع الوصول إلى تلك الأنظمة بصورة مباشرة ولم يكن هناك اتصال بتلك الأنظمة من العالم الخارجي، كما أن سبب قلتها أيضا إلى عدم الإبلاغ عن الكثير من تلك الجرائم لكون الشركات والوكالات كانت تحرص على عدم اهتزاز الثقة بها وبأنظمتها

---

[1] عدنان النقيب، الجرب الإلكترونية في ضوء بروتكولي سبع وسبعين الملحقين باتفاقيات جنيف الأربع لسنة تسع وأربعين (الهجمات السيبرانية)، مرجع سابق، ص36.

الحديثة، وأعقبت تلك الحقبة الزمنية إجراء دراسات ومقالات صحفية بشأن الجريمة السيبرانية من قبل كثير من الباحثين الصحفيين[1].

وكذلك في تلك الفترة الزمنية ظهر الاهتمام العربي بظاهرة الجريمة السيبرانية وتمثل ذلك في صدور العديد من الدراسات العلمية والمؤلفات العربية ذات الشأن بالجريمة السيبرانية وعقد الندوات المختلفة ذات الصلة بذلك حيث عقدت في 1986 ندوة أمن المعلومات في الحاسبات الآلية والتي تبناها مركز المعلومات الوطني التابع لوزارة الداخلية السعودية.

ومع تطور الجرائم وإنتشارها، شرعت الدول بتنظيم فضائها السيبراني ومكافحة الجرائم السيبرانية عن طريق تجريم الأفعال وتحديد العقوبات المناسبة لها، ومن أول الدول التي قامت بتنظيم الجرائم السيبرانية هي الدول الغربية وذلك لإعتمادها على شبكات الكمبيوتر والإنترنت بوقت مبكر كالولايات المتحدة و بلجيكا وفرنسا وسويسرا ، ثم بعد ذلك ظهرت الحاجة إلى تنظيم هذه الجرائم في البلدان العربية فقامت البعض منها بإصدار تنظيم الجرائم السيبرانية ضمن تشريعات خاصة بها كالإمارات العربية المتحدة و سوريا[2]، و أغلبية الدول العربية الأخرى إكتفت بتنظيم المعاملات والتواقيع الإلكترونية والتجارة الإلكترونية كالعراق ولبنان .

---

[1] سميرة بيطام، تطور الجريمة السيبرانية والآليات القانونية للتصدي لها في ظل التحولات الجيوسياسية، مرجع سابق، ص57.

[2] القانون الاتحادي الإماراتي رقم 34 لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية، وقانون مكافحة الجرائم الإلكترونية السوري رقم 20 لسنة 2022.

المطب الثاني

دوافع وأساليب جريمة الاختراق السيبراني

إن البشرية قد باتت، تُواجهُ في العصر الراهن ظاهرةً إجراميةً حديثة، ذات امتداد فضائيّ، وعابر للحدود من خلال ما يُعرف بجرائم المعلوماتية، أو "الإجرام الفضائي" Cybercrime؛ ولم تعد ضحية هذه الجرائم شخصاً منفرداً، رجلاً أم امرأة بل برزت ضحايا متعدّدة النوعية والعددية ، وسوف نحاول في هذا الفرع أن نقوم بالتفريق بين الجريمة السيبرانية والهجمات السيبرانية وتعريف كل واحدة على حدي وبيان التداخل بينهم وذلك على الشكل الاتي:

أولاً: الهجمات السيبرانية:

تعددت التعريفات التي تناولت مصطلح الهجمات السيبرانية على ضوء الاجتهادات الفقهية، والممارسات العملية الدولية، فالهجمات السيبرانية مصطلح يستخدم من قبل فئات عديدة من الناس؛ للإشارة إلى أشياء مختلفة كالإشارة إلى وسائل القتال وأساليبه، تلك التي تتألف من عمليات في الفضاء الإلكتروني والتي يمكن أن ترتقي إلى مستوى النزاع المسلح، أو تُجرى في سياقه، ضمن المعني المقصود في القانون الدولي، فنذكر بعض أقوال فقهاء القانون الدولي من تعريفاتهم وتوجيهاتهم نحو الهجمات السيبرانية على ما يلي:

فعرفه البعض بقولهم: "هجوم عبر الأنترنت يقوم على التسلل إلى مواقع الكترونية غير مرخص بالدخول إليها، بهدف تعطيل أو إتلاف البيانات المتوفرة فيها أو

الاستحواذ عليها، وهي عبارة عن سلسلة هجمات الكترونية تقوم بها دولة ضد أخرى[1]".

ثانياً: الجريمة السيبرانية:

لم يكن من السهولة بمكان على الفقه والتشريع أن يصلا لتعريف شامل ودقيق للجرائم السيبرانية، إذ يظل هذا النوع من الجرائم عصياً على التعريف الجامع المانع نظرا لما يشهده العصر الحالي من تطور مستمر على كل من الصعيد التقني والعلمي في مجالات الاتصالات تقنية المعلومات، وما صاحب ذلك من تطور شهدته شبكة الإنترنت أدى إلى ميلاد فئات جديدة من السلوك الإجرامي ومرتكبيه، والذي يتطور بتطور هذه التقنيات.

وعلى هذا الصعيد فقد تعددت وكثرت الجهود التي بذلت لمواجهة هذه الظاهرة المستحدثة في مجال الإجرام التقني على المستويات الدولية والإقليمية والوطنية، فبرغم من تنامي هذه المجهودات إلا أنها لم تتفق على وضع تعريف موحد حول مفهوم الجرائم المرتبطة بتقنية المعلومات، حيث أفرزت هذه الجهود عدداً من التعريفات التي اختلفت فيما بينها وتراوحت بين الضيق والاتساع.

بخلاف الهجمات السيبرانية التي يستهدف مرتكبوها الأمن القومي والسياسي للدولة أو يقوم هؤلاء بتخريب الشبكات التي تتحكم بالبنية التحتية الأسا في الدولة

---

[1] إسماعيل محمود الرزاز، الحماية القانونية من الهجمات والجرائم السيبرانية، مركز المحمود لتوزيع الكتب القانونية، مصر، 2023، ص17.

وتدميرها بقصد إرباكها، وزعزعة النظام فيها لتحقيق أهداف أمنية أو عسكرية أو سياسية، وقد تبنت الجمعية العامة للأمم المتحدة تعريف للجرائم السيبرانية مفاده أنها كل جريمة ترتكب بواسطة نظام رقمي أو شبكة رقمية أو داخل نظام رقمي، أي أنها كل جريمة يمكن أن ترتكب داخل بيئة إلكترونية سواء وقعت على هذه البيئة أو من خلالها أو بواسطة هذه البيئة.

كما عرفتها الاتفاقية الأوروبية للجرائم السيبرانية بأنها جريمة تشمل كافة الأنشطة غير القانونية أو غير المشروعة والتي ترتبط بأجهزة الحاسب الآلي وباستخدام شبكة الإنترنت، كما قسمت هذه الاتفاقية جرائم تقنية المعلومات إلى عدة طوائف، منها طائفة الجرائم التي تقع على سلامة المعلومات وخصوصيتها، وطائفة الجرائم ذات الصلة بالكمبيوتر، وطائفة الجرائم التي تتعلق بالمحتوى الإلكتروني، والجرائم التي تتعلق بالملكية الفكرية والعلامات التجارية[1].

ومن هنا يتضح أن التعريفات الفقهية قد فرقت بين الجرائم السيبرانية وجرائم الإنترنت، وذلك برغم الارتباط بين طائفتي هذه الجرائم، حيث إن التمييز بينهما يتمثل في أن جرائم الإنترنت تتطلب اتصالاً بالشبكة الدولية، أما الجرائم السيبرانية فيمكن أن ترتكب دون توافر شبكة الإنترنت مثل جرائم تخريب النظم المعلوماتية، والاعتداء على حق المؤلف[2].

---

[1] اتفاقية أوروبا المتعلقة بالجريمة الإلكترونية (بودابست) لعام 2001.

[2] عاطف عباس عبد الحميد، جرائم تقنية المعلومات وحقوق الملكية الفكرية، المؤسسة العربية للعلوم والثقافة، مصر، 2022، ص23.

وبذلك يمكن القول إن الهجمات والجرائم السيبرانية بينهما عموم وخصوص فإذا كانت صادرة من دول لأهداف سياسية أو عسكرية أو امنيه أو زعزعة النظام العام فهي الهجمات السيبرانية وإن كانت صادرة من أفراد ضد شركات أو مؤسسات فهي الجرائم السيبرانية.

المبحث الثاني

جرائم اتلاف المعطيات الرقمية

يستخدم الفضاء السيبراني لإتمام تعاملات الكترونية متنوعة، سواءً للدول أم المؤسسات والكيانات الأخرى والأفراد، ومن هذه التعاملات ما قد يشكل جرائم، تمس الأفراد والكيانات الخاصة كالشركات، ومن أمثلتها الجرائم السيبرانية ذات الصبغة الجنائية، والتسلل السيبراني، ومنها كذلك ما قد ينتج عنه أضراراً أو ربما يرقى لتهديد أمن الدول، مثل الهجمات السيبرانية، والحرب السيبرانية، والتجسس السيبراني.

ومع تشابه هذه الممارسات باعتبارها تتم الكترونياً ومن خلال الفضاء السيبراني، إلا أنها ليست متماثلة أو مترادفة، فلكل منها خصائص مميزة، وقد يؤدي الخلط بينها إلى صعوبة أكاديمية، تتمثل في عدم معالجته أو دراستها بشكل صحيح، وصعوبات عملية تتعلق بكيفية الرد المقبول من جانب الدول على كل منها، وكذلك الصعوبات تشريعية، حيث تقوم معظم الدول بتنظيم تلك العمليات وطنياً، باعتبارها نوع واحد يتعلق بالجريمة السيبرانية ذات الصبغة الجنائية، كالنصب أو السرقة، ولا تفرد تلك مساحة تنظيمية لباقي العمليات السيبرانية، التي هي من

الخطورة بحيث تستهدف الأنظمة الالكترونية لمؤسسات الدول، وقد تكافئ الآثار الناتجة عنها، وما ينتج عن هجوم مسلح تقليدي، ويتطلب الأمر معالجة كل منها بنصوص تتوافق مع تعريفها وطبيعتها وخصائصها المميزة، وآثارها المحتملة[1].

بناءً على ما سبق سوف نقوم بتقسيم هذا المبحث إلى مطلبين، نتناول في المطلب الأول التمييز بين التسلل والهجوم والإرهاب السيبراني، بينما في المطلب الثاني نتناول تمييز الجريمة السيبرانية عن غيرها من المفاهيم المقاربة الأخرى.

المطلب الأول

التمييز بين التسلل والهجوم والإرهاب السيبراني

ولأغراض الدراسة، نبدأ بالتمييز بين هذه الممارسات، وذلك بتعريف كل منها، وتحديد خصائصها المميزة، ثم نقوم بتحليل ما قد يميز كل منها عن الآخر، وذلك على النحو التالي.

أولاً: التسلل السيبراني.

عندما تبدأ العمليات الإلكترونية بالوصول غير المصرح به إلى داخل شبكة الكترونية ما، إذ يتم تخزين أو تداول البيانات السرية، أو المحمية، ومجرد الوصول غير المشروع إلى المعلومات، يمثل جوهر التطفل الإلكتروني، حيث يقيم المتسلل

---

[1] محمد عادل محمد عسكر، وضع العمليات السيبرانية في القانون الدولي مع التطبيق على ممارسة التجسس وقت السلم، بحث تخرج منشور في كلية الحقوق، جامعة المنصورة، مصر، 2020، ص268.

داخل شبكة معلومات تابعة لبلد ما، أو كيان آخر غير الدولة، أو الشركة، أو الأفراد، دون متابعة اتخاذ مزيد من الإجراءات.

وبذلك يمكن القول، بأن هذا التطفل يمثل خطوة أولى لجميع العمليات السيبرانية الأخرى، وبعد اختراق الأنظمة الالكترونية، يكون لدى الدخيل عدة خيارات، حسب للهدف الذي يريد تحقيقه، فإما أن يقف عند حد التسلل دون المتابعة لتحقيق هدف آخر، وإما أن يتابع القيام بعمليات أخرى، كنقل المعلومات السرية التي تم الاطلاع عليها دون تعديل، وذلك إلى دولة أو كيان أو أفرد، وهو ما يعرف بالتجسس الإلكتروني، أو تعديل هذه المعلومات، أو محوها، أو التحكم في الأنظمة الإلكترونية، أو البنية التحتية للدولة، أو تعطيلها، والتي تصنف على أنها هجوم الكتروني، والتي إذا تكررت فإنها تصنف كحرب سيبرانية [1].

ثانياً: الهجوم السيبراني. إن القاعدة (30) من "دليل تالين"حددت تعريف الهجوم السيبراني باعتباره: "عملية إلكترونية هجومية أو دفاعية، يتوقع وفقاً للطريقة العادية للأشياء أن يتسبب في أضرار جسيمة كإصابة أو موت أشخاص، أو تلف أو تدمير أشياء، ونلاحظ أن الأمثلة الواردة في تعريف أضرار الهجوم السيبراني، وبعضها لا يمكن إصلاحه كموت أشخاص، أو تلف أو تدمير أشياء،

---

[1] أنظر اتفاقية مجلس اوربا المتعلقة بالجريمة الالكترونية لعام 2001، https://rm.coe.int/budapest-convention-in-arabic/1680739173 ، تاريخ الزيارة: 2025/2/9.

وهي نفس الآثار التي يمكن أن تحدث نتيجة لاستخدام القوة، أو هجوم عسكري مسلح من دولة على أخرى[1].

كما عرفه مركز استراتيجية الأمن السيبراني الألماني، بأنه: "هجوم من خلال الفضاء السيبراني، الموجه لإلحاق الضرر بأنظمة تكنولوجيا المعلومات لبلد ما، عن طريق تعديلها_ كلها أو بعضها _أو تحريفها، أو تدميرها' وهذه الآثار ناتجة عما يسمى ب "القنبلة الذكية"، وهو برنامج أو أوامر الكترونية، تتسبب في إغلاق نظام الكتروني أو شبكة الكترونية، أو محو بيانات أو برامج على الشبكة. وأدرجت الاستراتيجية الإلكترونية للمملكة المتحدة السيبرانية، ثلاثة أشكال يمثل كل منها هجوما الكترونياً، وهي: "التلاعب بآليات تبادل المعلومات الالكترونية، "واعتراض موجات الراديو"، وتعطيل الاتصالات الالكترونية.

وقد عرف دليل الجيش الأمريكي للعمليات السيبرانية والإرهاب السيبراني لعام 2005 " الهجوم السيبراني" بأنه: السلوك المتعمد لأنشطة التخريب لأجهزة الكمبيوتر أو الشبكات، بقصد إلحاق الضرر، أو تحقيق أهداف اجتماعية أو إيديولوجية أو دينية أو سياسية أو أهداف آخري أو ترهيب أي شخص، أو أي جهة، لتحقيق تلك الأهداف ووفقاً للدليل، تهدف الهجمات السيبرانية إلى تحقيق أهداف أربعة رئيسة، وهي:

---

[1] أحمد عبيس نعمة الفتلاوي، الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية والسياسية، العدد الرابع، السنة الثامنة، كلية جامعة بابل، العراق، 2016، ص14.

1) التلاعب بحقيقة المعلومات وما يتعلق بأمانتها، وذلك بتعديلها بشكل خاطئ وبلا قيمة.
2) إخفاء المعلومات وجعلها غير متاحة للمستخدمين المصرح لهم باستخدامها.
3) كسر سرية المعلومات والكشف عنها للمستخدمين غير المصرح لهم،
4) إتلاف المعلومات مادياً بمسحها أو إتلافها.

وفي عام 2011، نشرت قيادة إدارة الأمن السيبراني في الولايات المتحدة الأمريكية دليلاً، حددت فيه الهجوم السيبراني على أنه: عمل عدائي يحدث باستخدام الكمبيوتر، والشبكات والأنظمة السيبرانية ذات الصلة، ويهدف إلى تعطيل أو تدمير التلاعب بأنظمة الإنترنت لدولة ما، أو المعلومات المخزنة على حواسيبها، أو وظائف هذه الأجهزة، ويتم تنفيذ هذا الهجوم بوسائل متعددة بما في ذلك المراسلات الالكترونية المزيفة، أو الرسائل المفخخة، ويتميز الهجوم بأن آثاره عادةً ما تكون منفصلة من الناحية الجغرافية عن نقطة إطلاقه [1])، ونلاحظ أن التعريف ركز على غرضين للهجوم، وهما إتلاف الأنظمة الالكترونية أو المعلومات ذات الصلة، أو تدمير البنية التحتية والمادية المرتبطة بتشغيل واستخدام هذه الانظمة.

---

[1] منى الأشقر جبور، الامن السيبراني: التحديات ومستلزمات المواجهة، اللقاء السنوي الأول للمختصين في أمن وسلامة الفضاء السيبراني، جامعة الدول العربية، المركز القانوني للبحوث القانونية والقضائية، بيروت، 2012، ص 3.

كما عرف الفقه الدولي الهجوم السيبراني بأنه: "أي عمل يهدف إلى تفويض وظائف شبكة الكمبيوتر لأغراض سياسية، أو امنية، أو اقتصادية، تصب في مصلحة دول معينة، وبالمثل فهي: "أي محاولات لتغير، أو تعطيل، أو تدمير أنظمة الكمبيوتر، أو الشبكات أو المعلومات أو البرامج المحملة عليها أو التي تعمل من خلالها"، ويمتد نطاقها وتأثيراتها إلى ما هو أبعد من ذلك، حيث يمكن استخدامها لتعطيل المنشآت الحيوية للدول والتي تعتمد على الذكاء الاصطناعي في تشغيلها، مثل محطات الكهرباء والمياه، ومحطات الطاقة النووية وإشارات المرور، وغيرها[1].

ثالثاً: الجريمة السيبرانية.

إن الهجوم السيبراني كما ذكرنا سابقاً هو عبارة عن التصرفات الإلكترونية التي تتسبب في قتل أو دمار أو أضرار مادية تقوم بها دولة أو مجموعة مسلحة ضد دولة أخرى. بينما الجريمة السيبرانية تشمل مجالاً أوسع بكثير من ذلك أي تتضمن كل النشاطات الإلكترونية غير القانونية بما في ذلك استخدام الوسائل المعتمدة على الكمبيوتر لإرتكاب أعمال غير قانونية في التشريعات الوطنية.

إن الحداثة التي تتميز بها الجريمة السيبرانية و إختلاف النظم القانونية و الثقافية بين الدول أدت الى عدم الإتفاق على تعريف موحد لهذا النمط من الجرائم خشية

---

[1] محروس نصار غريب، الجريمة المعلوماتية، مجلة التقني، العدد9، المجلد 24، هيئة التعليم التقني، بغداد، 2011، ص 120.

حصرها في مجال ضيق[1]، لذلك ظهرت عدة اتجاهات في تعريف الجريمة السيبرانية فمن الفقهاء من إعتمد على وسيلة إرتكاب الجريمة كأساس لتعريفه، وهذا ما ذهب اليه مكتب تقييم التقنية في الولايات المتحدة (OTA) إذا عرفها بأنها: الجرائم التي تؤدي فيها البيانات الكمبيوترية والبرامج المعلوماتية دوراً رئيسياً[2]، كما عرفت بأنها " الجرائم التي يستخدم فيها الحاسوب و شبكاته العالمية كوسيلة مساعدة لإرتكاب الجريمة كاستخدامه في النصب والإحتيال وغسل الأموال وتشويه السمعة والسب.

المطلب الثاني

تمييز الجريمة السيبرانية عن غيرها من المفاهيم المقاربة الأخرى

نتيجة التطور التقني المتسارع، واستخدام التقنيات الحديثة في عمليات الإجرام السيبراني، أدى ذلك إلى ظهور العديد من المصطلحات والمفاهيم التي تتشابه بعضها البعض الآخر، في مجالات التكنولوجيا والمعلوماتية، حيث يتداخل مفهوم الهجمات السيبرانية مع غيرها من المصطلحات، وبالتالي سنقوم بتوضيح هذه المصطلحات فيما يلي:

---

[1] محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2004، ص43.

[2] محمد عبيد الكعبي، الجرائم الناشئة عن استخدام غير المشروع لشبكة الإنترنت، دار النهضة العربية، القاهرة، 2009 ص33.

1- **العمليات المعلوماتية** [1]: هي تلك الإجراءات التي تستخدم للتأثير على معلومات أنظمة العدو والدفاع عن معلومات وأنظمة الشخص الذي يقوم بهذه الاعمال، وتكمن خطورتها في إنها في الحقيقة تستخدم تكنولوجيا المعلومات الحديثة للتأثير على الصديق والعدو وشن هجوم على قلب وعقل العدو، وعلى الأصدقاء والحلفاء والمحايدين لكسبها.

وهي عمليات واسعة النطاق تجري في نطاقها جميع الحروب والعمليات في إطار المعلوماتية، وهي تختلف عن الحرب في عصر المعلومات المقصود منها استخدام تكنولوجيا المعلومات وتوظيفها كأداة تمد الأطراف المتصارعة بوسائل ذات أهمية كبيرة في تنفيذ العمليات العسكرية التي قد تستهدف أهدافاً لا علاقة لها بالمعلوماتية، والهجمات السيبرانية هي جزء صغير من هذه العمليات.

ويقصد بحرب المعلومات بوصفها فرعاً من العمليات المعلوماتية تعني الاستخدام المترابط لقدرات وخصائص الهجمات السيبرانية، وعمليات شبكات الكمبيوتر (التي تشمل الهجمات على شبكات الحاسوب، واستغلال شبكات الحاسوب، والتجسس في مجال شبكات الحاسوب)، والعمليات النفسية، والحيل العسكرية والعمليات

---

[1] يراد بالمعلوماتية مجموعة من الاتصالات الكونية والالكترونية التي يمكن أن تنقل المعلومات في التو واللحظة من و إلى أي مكان في الكون- شيماء فاضل عادل، المعلوماتية والخروب المعاصرة (نموذج تطبيقي: الحرب على العراق 2003)، مجلة جامعة تكريت للعلوم القانونية والسياسية، العدد 2، السنة 1، العراق، 2018، ص 179.

المنسقة، مع قدرات داعمة ودفاعية للتأثير على معلومات العدو ووقفها، وتخريبها، وسرقتها مع حماية عمليات صنع القرار في المؤسسات الوطنية [1]).

2- **الحرب المعلوماتية النفسية:** يقصد بحرب المعلومات النفسية هي تلك الأعمال التي تهدف إلى طمس الحقائق ونشر الأكاذيب والشائعات في المجتمع والتأثير على الخصم من أجل القيام بأفعال يهدف الفاعل إلى تحقيقها من قبل خصمه، وتكون لتحقيق أهداف سياسية، أو عسكرية أو اجتماعية.

وهي ليست حرب رسائل المعلومات التي تعتمد على إستغلال المعلومات والتلاعب بها، بل هي مكون مركزي في مجالات الحرب النفسية والخداع والدعاية وكشف معلومات يحرص الخصم على إخفائها، وتختلف كلتا هاتين الحربين عن حرب قراصنة المعلومات التي تستخدم أنظمة المعلومات والشبكات الالكترونية بطرق غير مشروعة للحصول على المعلومات المخزنة في الحواسيب والشبكات المرتبطة بها، وتجري غالباً بأهداف مالية أو اقتصادية.

3- الحرب الإلكترونية: يراد بالحرب الالكترونية الإجراءات الالكترونية التي تشمل استخدام الانظمة والوسائل الالكترونية في كشف الاشعة الكهرومغناطيسية المنبعثة من الأنظمة الالكترونية للعدو ووسائله الالكترونية المختلفة، مع الاستخدام المتعمد للطاقة الكهرومغناطيسية للتأثير على هذه الأنظمة والوسائل

---

[1] رياض مهدي عبد الكاظم وآلاء طالب خلف، المعلوماتية والحروب الحديثة- دراسة حالة الحرب الأمريكية على العراق، عام 2003، مجلة واسط للعلوم الإنسانية، العدد29، مجلد 11، مصر، 2015، ص 19.

لمنع العدو، وحرمانه أو الحد من استغلاله للمجال الكهرومغناطيسي، وكذلك حماية الموجات الكهرومغناطيسية المنبعثة من النظم والوسائل الالكترونية من استطلاع العدو لها أو تأثيره عليها. فالحرب الالكترونية أوسع من الحرب السيبرانية فهي حرب مسارها الرئيسي الشبكات الرقمية والالكترونية والوسائل التكنولوجية الأخرى [1].

4- **الاستطلاع الإلكتروني:** يقصد بالاستطلاع الالكتروني تلك الإجراءات المتخذة للبحث واعتراض الموجات الكهرومغناطيسية بغرض التعرف الفوري للتهديد لتقليل قدرة العدو على شن الهجمات عبر هذه الموجات. والاستطلاع يختلف عن التداخل الالكتروني الذي يقصد به ان يكون مجموعة من الإجراءات المتخذة لمنع العدو من الاستخدام الفعال للطيف الكهرومغناطيسي والحد منه باستخدام القدرات الالكترونية [2].

5- **الهجمات على شبكات الحاسوب**[3]: تعتبر عمليات معلوماتية أو عمليات مصممة بغرض حرمان أو تقليص أو إتلاف المعلومات الموجودة في أجهزة الكمبيوتر وشبكاتها أو أجهزة الكمبيوتر والشبكات نفسها، سواء وصلت هذه العمليات إلى حالة الحرب أم كانت مجرد عمليات معلوماتية لم تصل إلى حد

---

[1] خالد وليد محمود، الهجمات عبر الانترنت: ساحة الصراع الالكتروني الجديدة، المرجع السابق، ص11

[2] أنظر قانون التوقيع الالكتروني والمعاملات الالكترونية العراقي رقم 78، لسنة 2012، http://esttf.motrans.gov.iq/wp- ، تاريخ الزيارة: 2025/5/9.

[3] محمد أمين الشوابكة، جرائم الحاسوب والانترنت (الجريمة المعلوماتية)، الطبعة الثالثة، دار الثقافة للنشر والتوزيع، عمان، 2009، ص 35.

النزاع المسلح، وجوهر هذه الهجمات هو اعتمادها على سبيل من البيانات لتنفيذ الهجوم، بخلاف وهو موجود في الهجمات الالكترونية من اعتمادها على الإشعاع الكهرومغناطيسي، أو ما هو الهدف من الهجمات الالكتروني من خلال استهداف المنشآت والبنية التحتية المرتبطة بالفضاء السيبراني وتدميرها، أو تعطيلها، وليس فقط شبكات الكمبيوتر.

والمقصود من التجسس على المعلوماتي " استخدام وسائل تقنية المعلومات الحديثة للدخول بشكل غير مسموح وغير قانوني، إلى أنظمة المعلومات الالكترونية الخاصة بالدولة والحكومات والتنصت عليها، بقصد الاستحصال على ما لديها من معلومات مهمة تتعلق بنظامها وأسرارها، وتشمل جميع أنواع المعلومات العسكرية والسياسية والأمنية والاقتصادية والعلمية والاجتماعية"[1].

5- الأمن السيبراني: يراد بمفهوم الأمن السيبراني تلك الانشطة التي تؤمن حماية الموارد البشرية، والمالية والبنية التحتية المتعلقة بتقنيات الاتصالات والمعلومات، والتأكد من أن هذه الأنشطة تقلل الخسائر والأضرار التي تنتج في حال إدراك المخاطر والتهديدات، كما تتيح هذه الإجراءات إلى إعادة الوضع إلى ما كان عليه بأسرع وقت بدون أن تتوقف دورة الإنتاج والحركة اليومية، بحيث لا تتحول الاضرار إلى خسائر دائمة، والتهديدات السيبرانية هي الاحداث والتهديدات التي تؤثر بشكل طبيعي أو بفعل بشري، (بصورة عمدية أو غير عمدية على فضاء السايبر) أو تلك الحوادث والتهديدات التي تعمل من خلال القضاء السيبراني أو

---

[1] ضرغام جابر عطوش آل مواش، جريمة التجسس المعلوماتي، المركز العربي للدراسات والبحوث العلمية، ومكتبة دار السلام القانونية، بغداد، 2016، ص89.

بأي صورة مرتبطة به، أما التحريض (الاثارة) السيبرانية فهو استخدام الحواسيب والنظم المرتبطة بها من أجل تقليل قوة الخصم والتأثير عليه واضطهاده، ويسعى المستخدم لهذه الوسيلة إلى معاقبة الخصم أو التأثير على عقائد الخصم وسلوكياته من دون قصد التسبب بأضرار مادية، كهجمات مجموعة على المواقع الحكومية كردة فعل على اعتقال مؤسس موقع ويكي ليكس. يقصد بالجرائم السيبرانية بأنها شكل من أشكال الجرائم المرتبطة بالحاسوب والتي تستخدم تكنولوجيا الشبكة الدولية للمعلومات (الانترنت)، وتغطي جميع الجرائم التي ترتكب في الفضاء السيبراني [1].

[1] وسيم شفيق الحجار، الأمان في الفضاء السيبراني ومكافحة الجريمة السيبرانية في المنطقة العربية، توصيات سياساتيه، منشورات الأمم المتحدة، الاسكو، 2015، ص 30.

الخاتمة

في نهاية هذا البحث، نجد أن الجرائم السيبرانية أصبحت من أبرز التهديدات التي تواجه العالم في العصر الحديث. إذ تتطور هذه الجرائم بشكل مستمر مع التقدم التكنولوجي، مما يستدعي استجابة فعالة من قبل الحكومات والمؤسسات الأمنية. من خلال دراسة التطور التاريخي للجرائم السيبرانية والتمييز بين أنواعها، توصلنا إلى أهمية وجود تشريعات قوية لمكافحة هذه الجرائم وحماية الأفراد والمؤسسات من أضرارها.

في ختام هذا البحث، يمكن القول إن الجرائم السيبرانية أصبحت اليوم واحدة من أكبر التحديات التي تواجه الدول والمجتمعات في العصر الرقمي. هذه الجرائم التي تتم عبر الفضاء الإلكتروني، وتستهدف الأفراد والمؤسسات على حد سواء، تتسم بتعقيدها وظهورها المستمر نتيجة للتطورات التكنولوجية السريعة. مع ازدياد الاعتماد على الإنترنت والتكنولوجيا في مختلف المجالات الحياتية، ظهرت حاجة ملحة لوضع أطر قانونية وتنظيمية تتصدى لهذه الجرائم التي لا تعترف بالحدود الجغرافية أو القانونية.

إن تطور الجرائم السيبرانية لا يقتصر على الأضرار المالية أو المادية فحسب، بل يمتد إلى تهديدات تمس الأمن القومي وتشمل الهجمات السيبرانية الموجهة ضد البنية التحتية الحيوية مثل محطات الطاقة والمياه، مما يجعلها تشكل تهديدًا استراتيجيًا للدول. وفي ظل هذه المخاطر، تبرز أهمية تعزيز التعاون

الدولي لتطوير آليات قانونية فعالة لمكافحة هذه الجرائم وحماية الفضاء السيبراني.

نتائج البحث:

تزايد الجرائم السيبرانية بسبب النمو المستمر في استخدام الإنترنت والتكنولوجيا الرقمية.

ظهور أنواع متعددة من الجرائم السيبرانية التي تستهدف المؤسسات الحكومية والخاصة.

ضرورة تطوير التشريعات الوطنية والدولية لمواكبة تطور هذه الجرائم.

التداخل بين الهجمات السيبرانية والجريمة السيبرانية يسبب صعوبة في تحديد أنواع الجرائم.

تزايد استخدام الحرب السيبرانية والهجمات الإلكترونية من قبل الدول لتحقيق أهداف سياسية وعسكرية.

توصيات البحث:

ضرورة تحديث وتطوير التشريعات القانونية في الدول العربية لمواكبة تطور الجرائم السيبرانية.

تعزيز التعاون الدولي في مكافحة الجرائم السيبرانية من خلال اتفاقيات ومؤتمرات دولية.

زيادة الوعي المجتمعي والمؤسساتي حول خطر الجرائم السيبرانية وسبل الحماية منها، مع التركيز على أهمية الأمن السيبراني.

المصادر والمراجع:

كتب قانونية:

1. إسلام هديب، الأمن السيبراني، الهجمات السيبرانية والجرائم السيبرانية ، دار مصر للنشر ،مصر ،2024.
2. منير محمد الجنبيهي وممدوح محمد الجنبيهي، أمن المعلومات الإلكترونية ، دار الفكر الجامعي ، مصر ،2025.
3. عدنان النقيب، الجرائم الإلكترونية في ضوء بروتوكولي سبع وسبعين الملحقين باتفاقيات جنيف الأربع لسنة تسع وأربعين (الهجمات السيبرانية ، المركز العربي للنشر والتوزيع، مصر ، 2022.
4. سميرة بيطام، تطور الجريمة السيبرانية والآليات القانونية للتصدي لها في ظل التحولات الجيوسياسية.
5. إسماعيل محمود الرزاز، الحماية القانونية من الهجمات والجرائم السيبرانية، مركز المحمود لتوزيع الكتب القانونية، مصر، 2023.
6. عاطف عباس عبد الحميد، جرائم تقنية المعلومات وحقوق الملكية الفكرية، المؤسسة العربية للعلوم والثقافة، مصر، 2022.
7. محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2004.
8. محمد عبيد الكعبي، الجرائم الناشئة عن استخدام غير المشروع لشبكة الإنترنت، دار النهضة العربية، القاهرة، 2009.

9. أحمد عبيس نعمة الفتلاوي، الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية والسياسية، العدد الرابع، السنة الثامنة، كلية جامعة بابل، العراق، 2016.

10. منى الأشقر جبور، الأمن السيبراني: التحديات ومستلزمات المواجهة، اللقاء السنوي الأول للمختصين في أمن وسلامة الفضاء السيبراني، جامعة الدول العربية، المركز القانوني للبحوث القانونية والقضائية، بيروت، 2012.

11. محروس نصار غريب، الجريمة المعلوماتية، مجلة التقني، العدد9، المجلد 24، هيئة التعليم التقني، بغداد، 2011.

12. محمد أمين الشوابكة، جرائم الحاسوب والانترنت (الجريمة المعلوماتية)، الطبعة الثالثة، دار الثقافة للنشر والتوزيع، عمان، 2009.

13. ضرغام جابر عطوش آل مواش، جريمة التجسس المعلوماتي، المركز العربي للدراسات والبحوث العلمية، ومكتبة دار السلام القانونية، بغداد، 2016.

قوانين:

1. القانون الاتحادي الإماراتي رقم 34 لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية.

2. قانون مكافحة الجرائم الإلكترونية السوري رقم 20 لسنة 2022.

3. قانون التوقيع الإلكتروني والمعاملات الإلكترونية العراقي رقم 78، لسنة 2012.

اتفاقيات:

1. اتفاقية أوروبا المتعلقة بالجريمة الإلكترونية (بودابست) لعام 2001.
2. اتفاقية مجلس أوروبا المتعلقة بالجريمة الإلكترونية لعام 2001.

أبحاث ومقالات:

1. خالد وليد محمود، الهجمات عبر الانترنت: ساحة الصراع الإلكتروني الجديدة، المرجع السابق.
2. رياض مهدي عبد الكاظم وآلاء طالب خلف، المعلوماتية والحروب الحديثة– دراسة حالة الحرب الأمريكية على العراق، عام 2003، مجلة واسط للعلوم الإنسانية، العدد29، مجلد 11، مصر، 2015.
3. شيماء فاضل عادل، المعلوماتية والخروب المعاصرة (نموذج تطبيقي: الحرب على العراق 2003)، مجلة جامعة تكريت للعلوم القانونية والسياسية، العدد 2، السنة 1، العراق، 2018.
4. وسيم شفيق الحجار، الأمان في الفضاء السيبراني ومكافحة الجريمة السيبرانية في المنطقة العربية، توصيات سياساتية، منشورات الأمم المتحدة، الاسكو، 2015.