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

TUJR
مجلة جامعة تكريت للحقوق
Tikrit University Journal for Rights

IRAQI Academic Scientific Journals
العراقية المجلات الاكاديمية العلمية

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

كلية القانون
College of Law

The legal importance of cybersecurity

Prof. Dr. Ban Hikmat Abdul Karim
College of Law, Al-Mustansiriya University, Baghdad, Iraq

tujr@tu.edu.iq

The researcher. Nour Saad Mohammed

College of Law and Political Science, University of Iraq, Baghdad, Iraq

tujr@tu.edu.iq

Article info.

Article history:
- Received 14 June 2024
- Accepted 20 May 2025
- Available online 1 September 2025

Keywords:

-Cybersecurity

- Cyberattacks

- Electronic Elections

.

Abstract: The recent development in information technology and its application in all areas of life have led to the emergence of what is known as cybersecurity and cybercrime.

Cyberspace is a borderless world, and therefore the state's activities here are cross-border. They are not limited to the borders of a specific state, but rather their activities are global, via the Internet, i.e., via satellites. This creates the greatest challenges to the state's security and sovereignty, as well as to human rights, including the right to freedom of expression, the right to privacy, and the right to vote and run for office.

These rights are relevant to the cyber world, where cyber activities have the greatest impact on society. Both the international and local communities are concerned with addressing the phenomenon of cybercrime and its impact on the electronic electoral

process, and with establishing legal regulation for it.

© 2023 TUJR, College of Law, Tikrit University

الأهمية القانونية للأمن السيبراني

أ.د. بان حكمت عبد الكريم

كلية القانون، الجامعة المستنصرية , بغداد ، العراق

tujr@tu.edu.iq

أ. م. نور سعد محمد

كلية القانون والعلوم السياسية, الجامعة العراقية ، بغداد، العراق

tujr@tu.edu.iq

معلومات البحث :

تواريخ البحث:
- الاستلام : ١٤/ حزيران/ ٢٠٢٤
- القبول : ٢٠ / ايار/ ٢٠٢٥
- النشر المباشر: ١/ ايلول/٢٠٢٥

الكلمات المفتاحية :

- الامن السيبراني
- الهجمات السبيرانية
- الانتخابات الالكترونية.

الخلاصة: ان التطور الحاصل في تكنلوجيا المعلومات في الآونة الأخيرة واستخدام هذا التطور التكنلوجي في كافة مجالات الحياة أدى الى ظهور ما يعرف (بالأمن السيبراني والجريمة السيبرانية).فالفضاء السيبراني هو عالم بلا حدود وبالتالي ان أنشطة الدولة هنا تكون عابرة للحدود فهي لا تقف عند حدود دولة معينة وانما تكون أنشطتها عالمية عبر الانترنيت أي عبر الأقمار الصناعية فهنا تخلق أكبر التحديات لأمن وسيادة الدولة وكذلك حقوق الانسان منها ما تكون كالحق في التعبير والحق في الخصوصية والحق في الانتخاب والترشيح.

فهذه الحقوق تكون ذات صلة بالعالم السيبراني التي تكون فيها الأنشطة السيبرانية أكبر إثر على المجتمع، وان اهتمام المجتمع الدولي والمحلي على حداً سواء بمعالجة ظاهرة الجريمة السبيرانية وتأثيرها على العملية الانتخابية الالكترونية ووضع التنظيم القانوني لها.

© ٢٠٢٣, كلية القانون، جامعة تكريت

المقدمة : تُعد الجرائم السيبرانية ظاهرة عالمية وذلك لزيادة عدد أجهزة تكنولوجيا المعلومات والاتصالات ذات الصلة بالإنترنيت، ففي عام ٢٠١٦ اشارت التقديرات إلى إن تكلفة الجرائم السيبرانية قد تصل إلى (٢,١) ترليون دولار على مستوى العالم بحلول عام ٢٠١٩.

تشير كذلك التقديرات إلى أن أكثر ممن ٨٠% من أفعال الجريمة السيبرانية تتخذ شكل من اشكال الجريمة المنظمة لاسيما مع انشاء الأسواق السوداء للجرائم السيبرانية، والفايروسات الحاسوبية، وإدارة شبكات الحواسيب، وجميع البيانات الشخصية والمالية، وبيع البيانات، الهدف منها هو الحصول على الربح من المعلومات المالية [١].

والسبب في زيادة الإجرام السيبراني هو أن شبكة الإنترنيت تُتيح لهم الفرصة بشكل كبير للمجرمين المنظمين لجمع الأرباح الطائلة عن طريق مخططات احتيالية، والوصول الى المشتبه بهم، والقبض عليهم، والحصول على اعترافهم، وتوجيه المهمة لهم، ومثولهم امام الحكمة المختصة بتطبيق القانون عليهم، اصبحت قاعدة قديمة لأن المشبه به في الجرائم السيبرانية قد يكون خارج الاختصاص القضائي لتلك المحكمة الماثل امامها.

لهذا لابد من اتباع اجراءات خاصة فيما تخص مرحلة التحقيق والمحاكمة [٢]، فيما تحص تطبيق القانون اتجاه هؤلاء المجرمين وكذلك التعاون على تسليمهم وأيضًا تقديم تقارير الخبراء، وبالتالي

---

(١) تُعرف الجريمة المنظمة انها: (ظاهرة إجرامية إذ يكون خلفها جماعات معينة استخدام العنف المخاطر الإجرامي وتهدف إلى الربح، يُنظر: محمود شريف بسيوني، الجريمة المنظمة عبر الوطنية ما هيتها ووسائل مكافحتها دولياً وعربياً، دار الشروق، القاهرة، ط١، ٢٠٠٤، ص١١، ولهذا وقد اعتمدت اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية وتم عرضها للتوقيع والتصديق والانضمام لها بموجب قرار الجمعية العامة للأمم المتحدة بدورتها (٥٥) بتاريخ ١٥/ نوفمبر/ ٢٠٠٠ ودخلت حيز النفاذ في ٢٩/ سبتمبر/ ٢٠٠٣، يُنظر: وثيقة الأمم المتحدة U.N.DOG.AVRES/55/25 2006

(١) حيث نصت المادة (٢) من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية إلى تقنيات التحقيق الخاصة وهي المراقبة الإلكترونية أو غيرها من اشكال المراقبة والعمليات السرية.

يستغل المجرم السيبراني عدم تكييف القانون الجنائي مع بيئة الإنترنيت ويكون المسؤول عن تطبيق القانون غير مجهز بالوسائل اللازمة للتحقيق فيها شكل سليم.

هذا وأن التحديات القانونية والتقنية في المؤسسة إلى تفرضها هذه الجريمة (الجريمة السيبرانية) هي ذات مسألة عالمية لا يمكن التعامل معها إلا باستراتيجية متماسكة والأخذ بنظر الاعتبار اصحاب المصلحة وضمن الإطار التعاون الدولي.

وبناءً على ما تقدم سوف نقوم بتقسيم هذا المبحث إلى مطلبين إذ يتحدث المطلب الأول عن مفهوم الأمن السيبراني واهدافه وهو بدوره يُقسم إلى فرعين، يتكلم الفرع الأول عن تعريف الأمن السيبراني واهدافه، أما الفرع الثاني يتناول دور الأمن السيبراني في حماية العملية الانتخابية وتحقيق النماذج التي تعرضت لهجمات الأمن السيبراني.

أهمية البحث:

تكمن أهمية البحث في بيان مفهوم الامن السيبراني ومحاوره واهميته وبيان لدور المهم للأمن السيبراني بتأثيره على العملية الانتخابية الالكترونية والعمل على حماية العملية الانتخابية الالكترونية من أي اعتداء او خرق او اتلاف لكي يمنع حدوث وقوع الجريمة السيبرانية.

مشكلة البحث:

تتبلور مشكلة البحث من خلال التساؤلات التالية:

١. ما هو مفهوم الامن السيبراني؟

٢. ما هي اهم الصور للأمن السيبراني؟

٣. ما هو تأثير الامن السيبراني على العملية الانتخابية الكترونية؟

٤. ما هي الهجمات السيبرانية؟

٥. ما هي محاور الامن السيبراني؟

منهجية البحث:

اعتمدنا في دراسة بحثنا على المنهج التحليلي والمقارن في بيان فاعلية ودور الامن السيبراني في إتمام العملية الانتخابية الكترونية.

اهداف البحث:

يهدف بحثنا هذا الى بيان أهمية مفهوم الامن السيبراني واهم الصور التي تمثل الاعتداء على بيانات الكترونية ومدى تأثيرها على سير العملية الانتخابية الالكترونية وبيان أهمية الاتفاقية الدولية (بوداسيت) المتعلقة بمكافحة الجريمة السيبرانية.

هيكلية البحث:

قسمنا بحثنا إلى مبحثين بحيث سنتناول المبحث الأول (مفهوم الامن السيبراني وأهدافه) اما المبحث الثاني (دور الامن السيبراني في حماية العملية الانتخابية الالكترونية وبعض نماذج الهجمات)

المبحث الأول

مفهوم الأمن السيبراني واهدافه

أن النمو الحاصل في جميع خدمات المجتمع ولاسيما الاقتصادي منها يرتبط ارتباط وثيق بالتطور التكنولوجي الحاصل في الوقت الحاضر حيث ان تكنلوجيا المعلومات والاتصالات تسمح ويستطيع من خلالها تبادل ماديات وافعال البيانات ويتم تبسيط هذه العملية وتطبيق هذا الواقع الافتراضي على جميع مفاصل المجتمع وخدماته وبالتالي فإن الاعتماد على الخدمات الرقمية ينتج عنه مخاطر ومن هذه المخاطر ما يعرف ب(الأمن السيبراني)، فهو له أشكال كثيرة ينتج عنه عواقب سلبية كبيرة، فعن بعض الدول يُعد الأمن السيبراني أي (التهديدات السيبرانية) خطر تجاري، بينما يُعدها البعض الآخر مخاطر تكنولوجية [١].

بينما تم إجراء إحصائيات لعام ٢٠٢٢ إذ قدر تكلفة الجريمة السيبرانية على الاقتصاد العالمي حوالي (١ ترليون)؛ أي أكثر من ٥٠% مما كان متوقع في عام ٢٠١٨ [٢].

---

for designing, developing and managing natural 1) S.G.SA.R.I.Neel, linguistic as framework(language processing tools, Big Data society 2022, January.
(2) P.lyenar, Garther Board of Directors Survey, Garther, 2020.

المطلب الأول

تأثير الهجمات الالكترونية على مؤسسات الدولة

ان هذه الهجمات الالكترونية تؤثر تأثيراً سلبياً على مؤسسات الدولة وتعمل على عرقلة عملها وهي تتمثل بالاتي :

١. أن هذه الهجمات تؤدي إلى فقدان البيانات الحساسة مثل المعلومات الشخصية، أرقام بطاقات الائتمان.

٢. أن مجرم أو مرتكب جرائم الجريمة المعلوماتية أو الإلكترونية قدرته على بيع البيانات على شبكة الانترنيت Dark Web، أو يقوم هنا المجرم بطلب فدية مالية من ضحاياه، وهذا بدوره يؤثر على التنظيم المالي والقانوني وعلى سمعة المؤسسة.

٣. أن المجرم الإلكتروني يستطيع أن يستخدم المعلومات الشخصية عن طريق انتحال شخصية معينة أو قيامه بسرقة ما يتعلق بالمستمسكات الثبوتية لهذا الشخص.

٤. أن النتائج التي تتمثل بالحوادث الناتجة من الأمن السيبراني هي تتمثل بالخسائر المالية؛ لأن الحوادث الإلكترونية تتطلب استرداد أو معالجة مكلفة فيما يتعلق بالبيانات المسربة، وهذا بدوره يؤدي إلى الحاق ضرر جسيم بالنسبة للمستهلك، وهذا يؤدي إلى فرض غرامات على أساس اللوائح المعتمدة في كل دولة [١].

(1) Man in the Middle Attack, Kaymera, (online), Available on the website http://kaymera.com/how-does-the-man-in-the-middle-attack-work (Accessed 18 June 2020)

٥. أن الهجمات الإلكترونية تنتج عنها تعطيل الخدمة المقدمة بشكل كلي، إذ تتميز الهجمات التي تسمى (DDOS) على إطلاق مواقع الويب الذي يخص المؤسسة؛ ففي عام ٢٠١٦ كانت أول هذه الهجمات السابقة الذكر إلى أيقاف (Twitter, PayPal) عن العمل [١].

(2) I.Vasiu and V.Lucian, Cyber Security as an essential Sustainable factor, Economic development European Journal of Sustainable Development, No.7(4), pp.177- 178, 2018.

المطلب الثاني

تعريف الأمن السيبراني ومحاوره

يُعرف الأمن السيبراني على أنه عملية حماية واستعادة أنظمة الحاسوب، والشبكات، والأجهزة، والبرامج من أي أنواع الهجمات الإلكترونية)، ويُعرف تكنولوجيا المعلومات على أنه (مكافحة التهديدات التي توجه ضد الأنظمة والتطبيقات المتصلة بالشبكة سواء كانت تلك التهديدات تنشأ من داخل المنظمة أو خارجها) [١].

وبناءً على ما تقدم يمكننا تعريف الأمن السيبراني على أنه عباره عن بيئة معقده يتكون من مشاركة أطراف مختلفة من الأفراد وكذلك البرمجيات والخدمات التي تكون ذات صله بالتواصل مع شبكات الإنترنيت وتكنولوجيا المعلومات والاتصالات، وأن هذه البيئة الإلكترونية تقدم فوائد منها المساعدة على بناء اقتصاد متطور، وهنا على المسؤولين حماية البيانات والأنظمة من خلال التشفير ووضع اتفاقيات سرية لتجنب مخاطر الأمن السيبراني.

(3) A.Lukehart, 2022 Cyber Attack Statistics, Data and trends, parachute 2022, (online), Available: from https://parachute.cloud/2022-cyber-attack-statistics-data-and-trends/, (Accessed 18 June 2020).

المطلب الأول

محاور الامن السيبراني

- **الفرع الأول: أساسيات الأمان**

يتمثل هذا المحور في السرية التي تعني الحفاظ على خصوصية البيانات ومنع الإفصاح عنها للآخرين الغير مصرح لهم؛ إذ تكون عن طريق حماية البيانات الشخصية كما هو موضح في المخطط أدناه.

ومع ملاحظة السماح بالدخول يتم من هوية المستخدم قبل السماح له بالدخول للنظام عن طريق عدة وسائل وهي:

١. شيء يخص كل شخص مثل بصمة العين، أو الأصبع، أو البصمة الوراثية...الخ.
٢. وسيلة خاصة بالشخص وهي البطاقة الشخصية (البطاقة الموحدة).
٣. وسيلة خاصة بالشخص أي خاصة بالنظام الذي يسمح له بالدخول وهي كلمة المرور الخاصة به.

- **الفرع الثاني: السلامة**

الذي نعني به دقة وتطابق البيانات في كل مراحلها من تخريب، واسترجاع، ونقل، ويتم التعديل عليها من قبل الأشخاص المسموح لهم، كع ملاحظة يتم التأكيد من أمن هذه البيانات عن طريق التحقق من مطابقة البيانات المرسلة في المستقبل لمنع حدوث فقدان المعلومات، إذ يكون ذلك عن طريق التحكم

في الاصدار للتعديل على البيانات من شخص واحد أو عمل نسخة احتياطية صحيحة لإرجاع البيانات المفقودة [١].

- **الفرع الثالث: توفر البيانات**

وهو توفر المعلومات بشكل دقيق واكتشاف وضعف وبطء النظام والعمل على تحقيق حالة الضغط على النظام.

- **الفرع الرابع: الهوية الشخصية**

التي تعني هو كل ما يدل على الشخص بذاته لأن هناك نوعين من الهوية الشخصية وهي:

أ- الهوية الحقيقية للشخص: تتضمن المعلومات الشخصية للشخص، أي البطاقة أو الهوية التي تعطى للشخص من أول يوم وجوده في الحياة.

ب- الهوية الإلكترونية للشخص: تتضمن كل المعلومات التي يختارها الشخص سواء كانت بالنشر أو المشاركة عن طريق القضاء الإلكتروني.

- **الفرع الخامس: الاحتياطات**

وتعني التوعية والمعرفة بأساليب الاختراق والحروب السيبرانية، وعمل نسخ احتياطي بصورة دائمة؛ إذ يتم حفظها بمكان آمن والعمل على تحديث البرامج ونظام التشغيل بصوره مستمرة وكذلك فحص الأجهزة والبرامج قبل استخدامها [٢].

---

١) الهيئة العامة للمنشآت الصغيرة والمتوسطة، الأمن السيبراني، بحث منشور على الموقع الإلكتروني: (https://www.monshaat.gov.sa/sites/default/files ، تاريخ الزيارة ٩/ ١٠/ ٢٠٢٤.

(٢) الهيئة العامة للمنشآت الصغيرة والمتوسطة، الأمن السيبراني، مصدر سبق ذكره.

المبحث الثاني

دور الأمن السيبراني في حماية العملية الانتخابية الإلكترونية وبعض النماذج من الهجمات

قد ذكرنا سابقًا أن الأمت السيبراني بأنه الفضاء الإلكتروني الذي يقوم على حماية كافة الموارد البشرية والخدمات في المجتمع منها الاجتماعية، والاقتصادية، والسياسية، التي تكون مرتبطة بتقنية تكنولوجيا المعلومات والاتصالات؛ فهو يهدف إلى الحد من الخسائر والتهديدات إذ يعمل على إعادة الحال لما كان عليه، فضلًا عن ذلك أنه يقوم بتجميع وسائل، وسياسات، وإجراءات أمنية، كما أنه يقوم في حالة وقوع التهديدات أو الخطر بتلاقي ذلك الخطر والتهديد عن طريق التدريب أو ممارسات وتقنيات تكون قادرة على مواجهة التهديد والخطر؛ لأن تلك التقنيات الحديثة، يمكن إن تُستخدم في حماية البيئة السيبرانية وكل ما يتعلق بمفاصل الدولة مستخدميها.

لهذا توجد هيئة وطنية أو مديرية خاصة بالأمن السيبراني هدفها العمل على حماية الشبكات وأنظمة تقنية المعلومات بما فيها الأنظمة التشغيلية ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات وما تحتويه من بيانات من أي اختراق، أو تعطيل، أو دخول، أو استخدام، أو استغلال غير المشروع، وكذلك يحتوي هذا المفهوم على أمن المعلومات والأمن الرقمي والإلكتروني [١].

وقياسًا على ما تقدم نلاحظ أن الأمن السيبراني له دور في حماية العملية الانتخابية الإلكترونية لأنه يعمل على توفير الحماية الكافية لأمن المعلومات الإلكترونية؛ من خلال مرحلة التصويت الإلكتروني وجميع مراحل العملية الانتخابية الإلكترونية، لأن تلك العملية الانتخابية الإلكترونية عملية حساسة وجوهرية فنتيجة نجاحها يعكس الصورة الأفضل للدولة؛ من خلال توفير كافة مستلزمات التقنيات

(١) الهيئة العامة للمنشآت الصغيرة والمتوسطة– الأمن السيبراني– مصدر سبق ذكره.

الإلكترونية الخاصة بالعملية الانتخابية الإلكترونية، وتوفير أمن المعلومات والبيانات الخاصة بالتصويت الإلكتروني، فهر تعكس سيادة الدولة وفرض هيبتها من دون تدخلات خارجية أو داخلية تؤثر على سير العملية الانتخابية الإلكترونية، ومن وجهة نظر الباحثة أن نجاح العملية الانتخابية الإلكترونية هو نجاح العملية السياسية التي تتعلق بسيادة الدولة، كون أن الأخيرة هي التي تبسط هيبتها وقدرتها على التحكم بكافة زمام الأمور وسلوكيات الفرد، لاسيما أن بعض أو غالبية الدول اتجهت إلى تطبيق ما يسمى بالحكومة الإلكترونية [١].

وبالتالي فأن أي خلل يصيب الماديات الفنية والقانونية للوسائل الإلكترونية بشكل يؤثر على البينات المعلوماتية يؤدي إلى ما يسمى بالجريمة الانتخابية الإلكترونية [٢]، أن ما تم ذكره يدل على اختراق أمني معلوماتي خطر وهو ما نتج عنه الجريمة السيبرانية، تعددت التعاريف حول هذا المفهوم إذ عرفها البعض على أنها (الدخول بغير وجه حق إلى جهاز حاسوب مستقل أو مرتبط بأخر بواسطة شبكة محلية لغرض ارتكاب فعل يجرمه الشرع والقانون)، وعرفها البعض الأخر على أنها (الجرائم التي تتم بواسطة الكومبيوتر أو أحد وسائل التقنية الحديثة على كومبيوتر آخر أو أحد وسائل التقنية الحديثة مع ضرورة توفر شبكة الإنترنيت) [٣].

---

(١) نهلا عبد القادر، الجرائم المعلوماتية، ط١، المكتبة الوطنية، الأردن، ٢٠١٠، ص٦٢.

(٢) الجرائم الإلكترونية قد تحدث في مناطق لا تعالج مثل هذا النوع من الجريمة لعدم وجود قانون خاص بها؛ إذ كان أحد الدروس التي قدمها فايروس (بقة الحب) وانتشار في العالم اجمع، الحق هذا الفايروس خسائر جمه بالمؤسسات الحكومية تقدر بملايين الدولارات، كما استطاع مكتب التحقيقات الفيدرالية هوية مرتكب الفعل الغير المشروع هو طالب في الفلبين، وجدوا لا يوجد قانون يستطيع من خلاله محاكمة هذا المجرم فعمدت الفلبين إلى إصدار قانون يمكن عن طريقه محاكمة هذا المجرم وهي قوانين إلكترونية، إذ هي تجرم الأفعال التي يتم ارتكابها عبر الشبكات الإلكترونية، كما أن هذا الفايروس أصاب حوالي (٢٠٠) ألف محور إلكتروني عالمي من ضمنها مجلس العموم البريطاني، والبيت الأبيض، ووزارة الدفاع الأمريكية، وشركة فورد، وقواعد عسكرية أمريكية، وغيرها من الشركات المتعددة الجنسيات إلى درجة تسمية هذا الفايروس ب(الفايروس القاتل القادم من مانيلا).

(٣) اسمامه مهل، الإجرام السيبراني، رسالة ماجستير مقدمة إلى مجلس كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، ٢٠١٨، ص٩.

والبعض الآخر يعرفها على أنها (نشاط إجرامي تستخدم فيه تقنية الحاسوب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود) [١].

وبناًء على ما تقدم يمكننا تعريف الجريمة السيبرانية على أنها الجرائم التي تُرتكب بواسطة التقنيات الحديثة، الغاية منها هو الاستيلاء، أو التجسس، أو التزوير، أو الاحتيال الإلكتروني، الذي يُطال سمعة الأمن المعلوماتي الرقمي؛ فهي السلوك غير المشروع أو النشاط الإجرامي المنافي للأخلاق، كما أنها تمثل جرائم العصر الرقمي التي تتم بواسطة الوسائل الإلكترونية الحديثة هدفها هو المساس بسيادة دولة معينة، والعمل على اختراق الأجهزة الأمنية بواسطة شبكة الإنترنيت؛ فهي من الجرائم العابرة للحدود.

(١) د. أحمد قرعان، الجرائم الإلكترونية، ط١، دار وائل للنشر والتوزيع، عمان، ٢٠١٧، ص١٩.

المطلب الأول

صور الامن السيبراني

ان الامن السيبراني له عدة صور

- **الفرع الاول: الاعتداء السيبراني على معطيات الحاسوب الآلي**

يكون الاعتداء عن طريق إتلاف البيانات والمعلومات والبرامج أو يتم التلاعب بتلك المعلومات المخزونة داخل الحاسوب، ويكون الاتلاف عن طريق أصابه الحاسوب الآلي بالفايروس.

- **الفرع الثاني: الاعتداء عن طريق الاستيلاء والنصب والاحتيال السيبراني**

ويحدث عن طريق الاعتداء على نفسه أو لغيره على مال منقول أو على سند أو يتم توقيع هذا السند، ويكون بالاحتيال أو اتخاذ اسم كاذب أو انتحال صفة غير صحيحة [١].

- **الفرع الثالث: الاعتداء بطريق الانتحال [٢]**

ويكون على نوعين:

أ- انتحال شخصية فردية:

ويكون بسبب التنامي المتزايد لشبكة الإنترنيت الذي اعطى المجرمين قدرة أكبر على جمع المعلومات الشخصية المطلوبة، الغاية منها هو الاستفادة من ارتكاب جرائمهم فتنتشر عن طريق مواقع التواصل الاجتماعي الكثير من الإعلانات المشبوه والتي يكون هدفها هو محاولة الاستيلاء على

---

(٢) يُنظر م(٤٥٧) من قانون العقوبات العراقي رقم ١١١ لسنة ١٩٦٩ المعدل.

(٣) يُنظر م(٢٦٠) من قانون العقوبات العراقي رقم ١١١ لسنة ١٩٦٩ المعدل.

معلومات اختيارية من الضحية، مثلما يتم الإعلان عن جائزة ثمينة الغرض من ورائها هو جمع أكبر قدر من المال عن طريق المساهمة بمبلغ لجمعية خيرية وهنا لابد من إفشاء الأسرار عن معلومات سرية، الأمر الذي يؤدي إلى الاستيلاء على رصيد في المصرف، أو البنك، أو السحب من بطاقة ائتمانية، أو يتم الإساءة إلى سمعة الضحية.

ب- انتحال شخصية المواقع:

يحدث باختراق الجهاز الأمني وتتم عملية الانتخال بهجوم يشنه المجرم على المواقع لكي يتم السيطرة عليها من قبله، أو يحاول المجرم أن يخترق موقع لأحد مقدمي الخدمة المشهورين، وبعد ذلك يقوم بتركيب البرنامج الخاص به مما ينتج عنه أن يتجه أي شخص إلى موقعه بالاكتفاء بكتابة أسم الموقع المشهور [١].

- **الفرع الرابع: الابتزاز والتهديد السيبراني [٢]**

يحدث عن طريق نشر صور أو معلومات سواء كانت صحيحة أم غير صحيحة عن المجنى عليه لغرض الحصول على المال أو أي غرض غير مشروع.

- **الفرع الخامس: التوصيات السيبراني [٣]**

هنا يتم استخدام برنامج في جهاز الشخص المجنى عليه أو الضحية وعن طريقه يمكن الاطلاع والاستماع إلى جميع ما موجود في الجهاز من فيديوهات، ومراسلات، ومحادثات...الخ، إذ يتم ادخال هذا إلى جهاز الضحية عن طريق البريد الإلكتروني أو عن طريق مواقع يتم زيارتها من قبل الضحية؛ فيقوم الضحية بأنزال برنامج ومنها برنامج التنصت فيقوم المجرم باستخدام وسائل احتيالية أو أي وسيلة

---

(١) أ. روان بنت عطية الله الصحفي، الجرائم السيبرانية، المجلة الإلكترونية الشاملة متعددة التخصصات، العدد ٢٤، ٢٠٢٠، ص١٨ وص١٩.

(٢) يُنظر المواد (٤٣٠ و٤٣١) من قانون العقوبات العراقي رقم ١١١ لسنة ١٩٦٩ المعدل.

(١) يُنظر م(٣٢٨) من قانون العقوبات العراقي رقم ١١١ لسنة ١٩٦٩ المعدل.

غش لكي يغري المجنى عليه بأن البرنامج يحتوي على العاب أو غيرها من الأمور الأخرى الغير المشروعة، أما جريمة التنصت فتكون أما بالألفاظ هو مشاهدة البيانات من خلال الشبكة المعلوماتية، أو من خلال أحد أجهزة الحاسوب، أو تكون عن طريق اعتراض ما هو مرسل عبر الشبكة المعلوماتية أو أحد الأجهزة الحاسوبية.

- **الفرع السادس: الاعتداء السيبراني على الأمن**

مثل أنشاء مواقع لمنظمات إرهابية على الشبكة المعلوماتية أو أحد أجهزة الحاسوب، أو نشرها لتسهيل الاتصال بقيادات تلك المنظمات، أو أي من اعضائها، أو ترويج أفكارها، أو تمويلها، أو نشر كيفية تصنيع الأجهزة الحارقة، أو المتفجرات، أو أي إداه تُستخدم في الأعمال الإرهابية والدخول غير المشروع إلى موقع إلكتروني أو نظام معلوماتي مباشرة، أو عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسوب للحصول على بيانات تمس الأمن الداخلي أو الخارجي للدولة أو اقتصادها الوطني [١].

وقياسًا على ما ذُكر سابقًا أن الجريمة السيبرانية تتحقق بمجرد اختراق الجدار الأمني أو الجهاز الأمني الإلكتروني الذي يضم البيانات المادية للحكومة، وذكرني سابقًا صور تحقق الجريمة السيبرانية هي الاعتداء بطريق الابتزاز، والتنصت، والاحتيال، والانتحال، والاختراق الأمني، وبهذه الصور التي ينتج عنها الجريمة السيبرانية؛ فهي هنا تمس سيادة الدولة وتهز أمن المجتمع السياسي وتؤثر على كافة هياكل ومؤسسات الدولة وعملها، بما فيها الانتخابات سواء كانت تقليدية أم إلكترونية؛ فإن أي خلل يمس أجهزة الدولة الأمني أو اختراقه أو قرصنته يصيب العملية الانتخابية الإلكترونية، لأن البيانات المادية يتم التعرض إليها إذا ما تم اختراق الأمن المعلوماتي الذي يخص البيانات الإلكترونية في أية مرحلة من مراحل العملية الانتخابية الإلكترونية.

---

(٢) يُنظر المواد من (١٥٦ إلى ٢٢٢) من قانون العقوبات العراقي رقم ١١١ لسنة ١٩٦٩ المعدل، وكذلك يُنظر المواد (٢ فقرة/ سابعًا) و(٣ فقرة/ ثالثًا) من قانون مكافحة الإرهاب العراقي رقم ١٣ لسنة ٢٠٠٥.

يتم الاعتداء على البيانات المادية لحاملي البطاقة الانتخابية الإلكترونية، أو الأجهزة المعدة للتصويت الإلكتروني، أو حتى يتم الاعتداء على تلك البيانات المادية الإلكترونية حتى في المرحلة التمهيدية للانتخابات الإلكترونية؛ فإن الجريمة الانتخابية الإلكترونية تُرتكب بمجرد تعرض البيانات المادية أو الأجهزة الموردة لاستخدام التصويت الإلكتروني إلى إتلاف أو الاعتداء الكلي أو الجزئي للبيانات المادية الإلكترونية، أو عن طريق القرصنة، أو الاحتيال، أو التزوير، أو السرقة الإلكترونية، أو حتى عن طريق الإرهاب الإلكتروني، أو أية وسيلة أخرى غير مشروعة تستخدم فقد لغرض ارباك العملية الانتخابية الإلكترونية، وبهذا فأن جميع الصور التي ذكرت في موضوع الأمن السيبراني ينتج عنها الجريمة الانتخابية الإلكترونية.

المطلب الثاني

النماذج التي تعرضت للهجمات السيبرانية:

الهجمات السيبرانية بين الصين والولايات المتحدة الأمريكية إذ أكدت شركة (كوكل) عام ٢٠١٠ أن الهجوم قد حدث في منتصف شهرين، الأول وكان مصدره الصين وقد ذكرت الشركة أن أكثر من (٢٠) شركة أخرى تعرضت للهجوم، إذ تم استهداف أكثر من (٣٤) منظمة، ونتيجة هذا الهجوم أكد الكونغرس الأمريكي سعيه إلى أن يحقق لما ادعت به شركة (كوكل) بأن الحكومة الصينية قد استخدمت خدمات الشركة للتجسس على نشطاء حقوق الإنسان، وقد استهدف الهجوم عشرات المنظمات [١].

وكان كذلك من بين الأهداف التي تعرضت للهجوم السيبراني هي شركة (ياهو سيمانتك، نورثروب، عزومان، مورغان ستانلي، بلاك بيري) [٢].

وأطلق على هذا الهجوم (عملية أورورا) من قبل (دميتري البيروفيتش) نائب رئيس ابحاث التهديدات في شركة الأمن السيبراني (إنتل سيكسوريتي)، إذ كشفت هذه الشركة أن (أورورا) كان جزء من مسار الملف على الجهاز المهاجم الذي تضمنه في اثنين من ثنائيات البرامج الضارة التي قالت أنها مرتبطة بالهجوم [٣].

---

(١) د. فراس جمال شاكر، الحروب المعلوماتية في المجال الأمني والعسكري (أمريكا والصين)، ط١، دار العربي للنشر والتوزيع، القاهرة، ٢٠٢٣، ص١٩٦.

(2) Tom Ramstac. Congress to Investigate Google Charges of Chinese Internet Sying, January, No.13, 2010, p1-2.

(3) KMZETTER.Operaion "Aurora" Hit Google, others by George Kutz, Januar, No.14, 2010, p1-2.

ولهذا فأن الهجمات السيبرانية هي فعل يقلص من قدرات ووظائف شبكة الكومبيوتر لغرض قومي أو سياسي من خلال استغلال نقطة ضعف معينة تمكن المهاجم من التلاعب بالنظام [١].

وعرفها (مايكل شميث) على أنها مجموعة من الإجراءات التي تتخذها الدولة للهجوم على نظم المعلومات المعادية بهدف التأثير والإضرار بها أو الدفاع عن نظم المعلومات الخاصة بالدولة المهاجمة [٢].

اتعمد المجلس الأوروبي الطابع الدولي للجرائم السيبرانية منذ عام ١٩٧٦، وقم تم إنشاء ما يعرف باتفاقية (بودابست) لمقاومة جرائم السيبرانية والاتصالات عام ٢٠٠١، تم التصديق على هذه الاتفاقية بعدما أدركت الدول بمدى خطورة الجريمة السيبرانية بوصفها جريمة عابرة للحدود؛ فتم التوقيع عليها من قبل (٣٠) دولة من ضمنها العاصمة المجرية (بودابست)، منها تضمن دول الأعضاء من الاتحاد الأوروبي منها (كندا، اليابان، أمريكا، جنوب إفريقيا)، والهدف من هذه الاتفاقية هو المعالجة الدولية للإشكاليات الجريمة السيبرانية وتجاوزها للحدود الدولية بما يساعد الدول على مكافحة هذه الجريمة وتعقب مرتكبيها، والمساعدة على الاستدلال عليهم وضبطهم وهي تشمل جوانب عده منها جرائم الإنترنيت من بينها الإرهاب، وعمليات تزوير بطاقات الأتمان، وغيرها.

وبهذا تُعد اتفاقية (بوداسيت) الاتفاقية الأوروبية لمكافحة الجرائم السيبرانية التي دخلت حيز التنفيذ عام ٢٠٠٤؛ فهي خطوة مهمة على مستوى التعاون بين الدول لوضع إطار عالمي للتعاون الدولي

(4) Cyber Attack and the use of force: Matthew G.Waxman, the Xale Joumal of International Back to the Future of Article, Vol.36, 2011, p.423.
(5) Computer Network Attack and the of Michael N.Sehmitt thoughts on a Nomative framework, force in International Law, Joumal Columbia of Transnational law, 1998, p.885.

في مواجهة تلك الجرائم المرتبطة بالقضاء السيبراني، ونجحت في ذلك من خلال إعطاء حق الانضمام للاتفاقية لأي دولة ولم يقتصر ذلك الحق على الدول الأوروبية فقط [١].

1بناءً على ما تقدم نلاحظ دور أو تأثير الأمن السيبراني في العملية الانتخابية إذ ازدادت الأنشطة السيبرانية على الرغم من أن نصف سكان العالم اتجهوا إلى صناديق الاقتراع (٢٠٢٤) مثل امريكا، والهند، المملكة المتحدة، البرتغال، بلجيكا، ...الخ، كما أن تقرير الوكالة الأوروبية للأمن السيبراني الذي سنظهره في الجدول ادناه بمدى تأثير الهجمات السيبرانية على الانتخابات في بعض الدول.

الدولة	السنة	الطريقة المستخدمة	الهدف
امريكا الشمالية	٢٠٢٠	١. خرق البيانات الانتخابية. ٢. فشل الموقع الإلكتروني للحملة. ٣. برمجيات الفدية الخبيثة.	١. المواقع الإلكترونية الحكومية والمتعلقة بالانتخابات. ٢. المواقع الإلكترونية لحملات المرشحين. ٣. نظام التحقق من الناخبين.
أوروبا	٢٠٢١	محأولة التصيد الاحتيالي (التصيد الاحتيالي لسرقة البيانات)	أعضاء البرلمان
أمريكا اللاتينية	٢٠٢٣	هجوم غير محدد	نظام التصويت عبر الإنترنيت للمواطنين المقيمين في الخارج
عالمي	٢٠٢٣	١. التصيد الاحتيالي. ٢. اختراق البيانات.	١. أعضاء البرلمان. ٢. الجامعات، والصحفيون، والقطاع العام،

(١) د. فراس جمال شاكر، مصدر سابق، ص٤٩٦ وص٤٩٨.

		٣. هجمات غير محددة.	ومنظمات المجتمع المدني الأخرى.

الخاتمة:

بعد اكمال بحثنا هذا توصلنا الى عدة استنتاجات والتوصيات التالية:

أولاً: الاستنتاجات

١. لاحظنا ان الامن السبيراني هدفه حماية امن المعلومات من الاختراق والاعتداء على امن المعلومات والتصدي لما يعرف بالهجمات السبيرانية او الجريمة السيبرانية.
٢. مواكبة التطور التكنلوجي والعمل على استخدامه بصورة صحيحة لكي يتجنب حدوث مايسمى بالجريمة السيبرانية.
٣. الامن السيبراني هدفه العمل على مكافحة الجريمة الالكترونية والوقاية منها او الخد من وقوعها من خلال تامين وحماية امن المعلومات من أي هكر او خرق او اعتداء وتتوفر هذه الحماية بواسطة توفير كادر متخصص ذو كفاءة عالية من العلم والمعرفة بهذا المجال الأمني الحساس.

ثانياً: التوصيات

١. العمل على تعديل بالإضافة لقانون الانتخابات وضرورة النص على مصطلح الامن السيبراني والجريمة الانتخابية الالكترونية ووضع الالية المتخصصة لحل هذه المسالة الخطرة والنص على مكافحتها ووضع العقوبة المناسبة لها التي تمس امن وسيادة الدولة.
٢. ضرورة حث العراق للانضمام لاتفاقية بودابست التي تنص على مكافحة الجريمة السيبرانية لان أي مساس بالأمن السيبراني لدولة العراق اولاي دولة يؤدي للمساس بسيادة وامن الدولة خاصة في ممارسة العملية الانتخابية الالكترونية لتجنب وقوع الجريمة الالكترونية لأن الأخيرة يعمل على مكافحتها والحد او الوقاية الامن السيبراني.

٣. ضرورة اعداد فريق متطور من فريق مختص في مجال الامن السيبراني ذو مستوى من الكفاءة والخبرة للتصدي لاي خرق او اعتداء او هكر لأمن المعلومات واعداد أجهزة فائقة الدقة للعمل على التصدي أي اعتداءات وخروقات لأمن المعلومات.

المصادر:

أولاً: الكتب

١. نهلا عبد القادر، الجرائم المعلوماتية، ط١، المكتبة الوطنية، الأردن، ٢٠١٠.

٢. د. أحمد قرعان، الجرائم الإلكترونية، ط١، دار وائل للنشر والتوزيع، عمان، ٢٠١٧.

٣. د. فراس جمال شاكر، الحروب المعلوماتية في المجال الأمني والعسكري (أمريكا والصين)، ط١، دار العربي للنشر والتوزيع، القاهرة، ٢٠٢٣.

ثانياً: البحوث

١. الهيئة العامة للمنشآت الصغيرة والمتوسطة، الأمن السيبراني، بحث منشور على الموقع الإلكتروني: https://www.monshaat.gov.sa/sites/default/files، تاريخ الزيارة ٩/ ١٠/ ٢٠٢٤.

٢. أ. روان بنت عطية الله الصحفي، الجرائم السيبرانية، المجلة الإلكترونية الشاملة متعددة التخصصات، العدد ٢٤، ٢٠٢٠.

ثالثاً: الرسائل

١. اسمامه مهل، الإجرام السيبراني، رسالة ماجستير مقدمة إلى مجلس كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، ٢٠١٨.

رابعاً: القوانين

خامساً: الكتب الأجنبية

1. S.G.SA.R.I.Neel, linguistic as framework for designing, developing and managing natural language processing tools, Big Data society 2022, January.
2. P.lyenar, Garther Board of Directors Survey, Garther, 2020
3. Man in the Middle Attack, Kaymera, (online), Available on the website http://kaymera.com/how-does-the-man-in-the-middle-attack-work (Accessed 18 June 2020)
4. I.Vasiu and V.Lucian, Cyber Security as an essential Sustainable factor, Economic development European Journal of Sustainable Development, No.7(4), 2018.
5. A.Lukehart, 2022 Cyber Attack Statistics, Data and trends, parachute 2022, (online), Available: from https://parachute.cloud/2022-cyber-attack-statistics-data-and-trends/, (Accessed 18 June 2020).
6. Tom Ramstac. Congress to Investigate Google Charges of Chinese Internet Sying, January, No.13, 2010.
7. KMZETTER.Operaion "Aurora" Hit Google, others by George Kutz, Januar, No.14, 2010.
8. Cyber Attack and the use of force: Matthew G.Waxman, the Xale Joumal of International Back to the Future of Article, Vol.36, 2011, p.423.
9. Computer Network Attack and the of Michael N.Sehmitt thoughts on a Nomative framework, force in International Law, Joumal Columbia of Transnational law, 1998.