الأمن السيبراني و أثره على دول العالم
Cybersecurity and Its Impact on World Nations

سي عبد القادر حنان، طالبة دكتوراه(*)
كلية الحقوق والعلوم السياسية بسوسة، تونس
asswadhanane@gmail.com

تاريخ الاستلام: 2024/03/01 تاريخ القبول للنشر: 2024/03/30

****

ملخص:

إن مصطلح "الأمن السيبراني" يشير إلى جوانب الأمن المتعلقة بالمعلومات وتكنولوجيا المعلومات. وتتعلق هذه الجوانب بحماية البيانات الرقمية والشبكات والأنظمة الحاسوبية من التهديدات الإلكترونية والهجمات السيبرانية. في سياق سيبيريا، فإن مصطلح "مواجهة الأمن السيبراني" يشير ببساطة إلى التحديات والمخاطر التي تواجهها المؤسسات والحكومات في تأمين بنيتها التحتية الرقمية وبياناتها في المنطقة السيبيرية. تتضمن هذه التحديات عادةً محاولات اختراق الأنظمة الحاسوبية، وسرقة المعلومات الحساسة، والتجسس الإلكتروني، وانتشار البرامج الضارة، والهجمات السيبرانية الأخرى التي يمكن أن تؤدي إلى تعطيل الأنظمة أو سرقة البيانات أو حتى تخريب البنية التحتية الرقمية بشكل عام. لمواجهة تلك التحديات، تحتاج المؤسسات والحكومات في سيبيريا إلى اعتماد استراتيجيات شاملة للأمن السيبراني تتضمن تطوير السياسات والإجراءات الأمنية، وتنفيذ تقنيات الحماية الأمنية المتقدمة، وتدريب الكوادر على التعامل مع التهديدات السيبرانية بفعالية. كما يجب أيضًا تعزيز التعاون الدولي وتبادل المعلومات بين الدول لمكافحة الجرائم السيبرانية وتعزيز الأمن الرقمي في المنطقة بشكل عام.

الكلمات المفتاحية: الأمن؛ السيبراني؛ الجرائم؛ الإشكالات؛ الحلول

Abstract:

The term "cybersecurity" refers to aspects of security related to information and information technology. These aspects involve protecting digital data, networks, and computer systems from electronic threats and cyber attacks. In the context of Siberia, the

*المؤلف المرسل. الإيميل: asswadhanane@gmail.com

term "cybersecurity confrontation" simply refers to the challenges and risks that institutions and governments face in securing their digital infrastructure and data in the Siberian region.

These challenges typically include attempts to penetrate computer systems, steal sensitive information, engage in electronic espionage, spread malware, and other cyber attacks that could lead to system disruption, data theft, or even sabotage of digital infrastructure in general To address these challenges, institutions and governments in Siberia need to adopt comprehensive cybersecurity strategies that include developing security policies and procedures, implementing advanced security protection technologies, and effectively training personnel to deal with cyber threats. It is also necessary to enhance international cooperation and information exchange between countries to combat cybercrime and enhance digital security in the region as a whole.

Keywords: Security; Cybersecurity; Crimes; Challenges; Solutions.

مقدّمة:

مع ظهور الحواسيب وتزايد استخدام الإنترنت في العديد من مجالات الحياة، ظهرت العديد من الآثار السلبية والمخاطر الناشئة عن هذا التوسع الكبير. فكلما زاد الاعتماد على هذه التقنيات في التنمية، زادت المخاطر المرتبطة بحماية المعلومات، وكلما زاد الاعتماد العالمي على تكنولوجيا المعلومات والاتصالات زاد التعرض للجرائم الإلكترونية.

ولذلك أصبح أمن الفضاء السيبراني أولوية بالنسبة للعديد من البلدان، ودفع التهديد المتزايد لأمن الفضاء السيبراني العديد من البلدان إلى بذل جهود متضافرة لوضع تشريعات لمكافحة الجريمة السيبرانية. ولذلك تبنت العديد من الدول استراتيجيات تدعم الجانب العسكري للفضاء السيبراني، ليس فقط ضد الهجمات التي قد يقوم بها أفراد أو قراصنة إلكترونيون، ولكن أيضا ضد إمكانية استخدام الدول لهذا المجال الجديد في الصراعات، وبالتالي، على المستوى الدولي هناك حاجة إلى توحيد الجهود الدولية لتطوير الأطر القانونية والتنظيمية والإجرائية لمواجهة المخاطر السيبرانية وتبعاتها تعزيز أشكال التعاون الدولي لمكافحة تهديدات الأمن السيبراني، ومعالجة الاستجابات القانونية الدولية للتهديدات في الفضاء السيبراني ومكافحتها من أجل الحفاظ على أمن الفضاء السيبراني.

تتناول هذه الدراسة الأمن السيبراني والجريمة السيبرانية والجهود الدولية لمكافحة الجريمة السيبرانية والصعوبات التي تواجهها.
وتستخدم الدراسة المنهج الوصفي والتحليلي والمقارن كمناهج علمية للتعامل مع الأمن السيبراني والجريمة السيبرانية والجهود الدولية لمكافحة الجريمة السيبرانية والصعوبات التي تواجهها.

سؤال البحث.

ما هي المبادرات المتخذة لمكافحة هذا النوع من الجريمة؟ ما هي الصعوبات التي تواجه الجهود الدولية للقضاء عليها؟

المبحث الأول:ماهية الأمن السيبراني والجريمة السيبرانية؟

سوف تتطرق هذه الدراسة إلى التعريف والغرض منه، ومفهوم الجريمة السيبرانية، والخصائص التي تميزها عن غيرها من الجرائم التقليدية، وأنواعها وأشكالها، والتي يمكن تنظيمها من حيث المطالب الثلاثة التالية:

المطلب الأول: مفهوم الأمن السيبراني وأهدافه وأبعاده

يعد الأمن السيبراني من الموضوعات المستجدة التي غيرت رؤية المجتمع الدولي لمفهوم الأمن العام. لذا، نحاول في المبحثين التاليين إعطاء مفهوم الأمن السيبراني هدفه وأهميته:

الفرع الأول: مفهوم الأمن السيبراني وأهدافه

أولاً: تعريفه:

على الرغم من وجود عدة تعريفات للأمن السيبراني، إلا أنها تتلخص جميعها في مفهوم واحد: توفير الحماية السيبرانية بهدف ضمان توافر واستمرارية نظم المعلومات واتخاذ التدابير اللازمة لحماية الأفراد والدول من المخاطر السيبرانية.

ثانياً: أهدافه:

-**البنية التحتية لأمن المعلومات وحماية بيانات المواطنين**: كل ما يتعلق ببيانات المواطنين يحتاج إلى حماية قوية وتخزينها في مكان آمن.

وتلعب حماية شبكات المعلومات والاتصالات دورًا رئيسيًا في تدفق البيانات بين المواطنين والدول، أو من طرف إلى آخر، وفي حال تعرضها للتشويش أو التعطيل أو الاختراق، فلا مفر من تأثر هذه الاتصالات وتعطلها، مما قد يعطل سير العمل والخدمات هناك فهم طبيعة هذا المهاجم وأهدافه من خلال معرفة التقنيات والأساليب المختلفة التي يستخدمها هذا المهاجم من أجل منع هذا الهجوم بطريقة علمية وتقنية.

الفرع الثاني:أهمية الأمن السيبراني وأبعاده

أولا: أبعاده

- 1البعد العسكري:

كانت بدايات الإنترنت في الأساس في بيئة عسكرية، ثم في بيئة علمية وأكاديمية، تمثلت في الإنجازات العلمية التي تساهم في تفوق دولة على أخرى، مثل الأبحاث التي تفيد في

تطوير القدرات العسكرية والتنافس الأشد بين الاتحاد السوفيتي والولايات المتحدة الأمريكية في مجالات الوصول إلى الفضاء الخارجي وتطوير الأسلحة النووية. انتقل العالم إلى عالم التعامل مع الجرائم الإلكترونية في سياق الاتفاقيات الدولية
كمثال على الهجمات والاختراقات التي كانت لها عواقب وخيمة، إما من خلال اندلاع نزاع مسلح لاحق، كما حدث بين روسيا وجورجيا، أو من خلال قطع اتصالات الإنترنت بين الدولة ومواطنيها وتعطيل الدوائر الحكومية في إستونيا، ما حدث في جورجيا وإستونيا وكوريا الجنوبية وإيران تتراكم الحالات، بما في ذلك الكهرباء والمياه والاتصالات السلكية واللاسلكية.
إن التفوق النسبي للقوة السيبرانية يكمن في قدرتها على ربط الوحدات العسكرية ببعضها البعض من خلال الشبكات العسكرية في الفضاء الإلكتروني، مما يؤدي حتمًا إلى هجمات إلكترونية مضادة ضد شبكات القوات العسكرية، مما يؤدي إلى تدمير قواعد البيانات وما يتبع ذلك من مخاطر) [1]

2 - الجوانب القانونية:

تترتب على أنشطة الأفراد والمنظمات والحكومات في الفضاء السيبراني تبعات والتزامات قانونية تتطلب اهتمامًا خاصًا لحل النزاعات التي قد تنشأ عنها، حيث ظهرت حقوق أخرى مثل الحق في الوصول إلى شبكات المعلومات العالمية، كما أن بعض المفاهيم بحاجة إلى مواكبة التحولات التي صاحبت ظهور مجتمع المعلومات، حيث اتسعت لتشمل ومن الأمثلة على ذلك الحق في إنشاء المدونات، والحق في إنشاء مجتمعات إلكترونية والحق في حماية ملكية برامج المعلومات.

ثانياً: أهميته:

تهدف الهجمات الإلكترونية إلى الوصول إلى البيانات الحساسة للمؤسسات والمستخدمين أو حذفها أو تهديدها،ويحتاج الجميع الآن إلى وجود الأمن السيبراني في المؤسسات والشركات والمصانع والهيئات الحكومية وحتى في المنزل. لقد أصبح الأمن السيبراني حاجة ملحة بعد ظهور ما سُمي بالثورة الصناعية الرابعة، أو ثورة البيانات. أحد أهداف الأمن السيبراني هو مواجهة المخاطر السيبرانية، وقد سبق الإشارة إلى أن أحد أهم المخاطر في قلب الفضاء السيبراني هو الجريمة السيبرانية. لذلك يشرح هذا المطلب ماهية الجريمة السيبرانية وأنواعه[2]ا.

المطلب الثاني: تعريف هذا النوع من الجريمة الجريمة وأنواعها

الفرع الأول: تعريف الجريمة السيبرانية

تُعرَّف بأنها: "أي فعل أو نشاط غير قانوني أو غير مشروع يستخدم فيه الحاسوب كوسيلة أو موضوع للجريمة، أو أي فعل إجرامي يكون فيه الحاسوب وسيلة أو موضوعاً لفعل غير مشروع، أو أي تقنية متقدمة لتكنولوجيا المعلومات أو نظم التطوير

[1] بارة سمير،المن السيبراني في الجزائر،المجلة الجزائرية للأمن الانساني،العدد4،2017،ص 260
[2] أمنة أم يوسف،فوائد الامن الانساني،2021،ص 161

أي فعل أو امتناع عن فعل قد ينتهك الملكية المادية أو المعنوية ناتج بشكل مباشر أو غير مباشر عن تدخل
كما يمكن تأييد هذا التعريف لأنه يشمل جميع الجرائم التي يمكن ارتكابها في البيئة السيبرانية ويشمل جميع أشكال الجريمة السيبرانية، حيث إنه لم يحصر الجريمة السيبرانية في مجالات محددة، حيث إن العديد من الأفعال السيبرانية لا تفلت من العقاب[3].

الفرع الثاني: أنواعها

على الرغم من تعدد أنواع الأفعال التي تهدد الأمن السيبراني، وتباين أهدافها والجهات التي تقوم بها، إلا أنه يمكن سرد بعض منها على النحو التالي:
1-التعرض لسرية الاتصالات التي تؤثر على الوصول إلى أنظمة البريد الإلكتروني والدردشة ونقل الملفات والوصول إلى المعلومات دون إذن. على غرار التنصت على المكالمات الهاتفية والاطلاع على البريد الإلكتروني الخاص ودخول المنزل لتفتيشه، ففي الدول التي تحترم فيها القواعد القانونية يشترط عادة الحصول على إذن مسبق من السلطات المختصة، وفقا للقواعد القانونية، وهذه الأفعال سواء من قبل فرد أو من قبل سلطة عامة الحقوق وتعتبر جريمة ضد الحقوق.
2-التلاعب بالمعلومات التي تحتويها بعض الأنظمة أو تشويهها أو إتلافها، سواء بالاختراق المادي أو بإرسال برامج أو فيروسات خاصة، يعد اعتداء على الملكية وحق التمتع بها والتصرف فيها. كما أنه في حالة وجود نية الإضرار، بالإضافة إلى التدخل في سلامة عمل موقع خاص أو تجاري، سواء تحقق الضرر المطلوب أو لم يتحقق، فإن الجرائم المعتادة التي تستخدم الإنترنت لتنفيذها، مثل السرقة والاحتيال والخداع والتغرير بالقُصَّر وتسهيل الدعارة والتسهيل، وتشجيع الأنشطة غير المشروعة، والاعتداء على الملكية الفكرية، كل هذه الجرائم يعاقب عليها القانون الوضعي ولا تحتاج إلى إذن مسبق من السلطات المختصة في الدول التي تحترم القواعد القانونية، كما هو مقرر هنا.
3- الجرائم التي تندرج في إطار الجريمة المنظمة، مثل غسل الأموال والإرهاب، والتي تهدد أمن الأفراد والدول في الفضاء السيبراني والفضاء التقليدي على حد سواء [4]

المطلب الثالث:خصائص الجريمة السيبرانية وأشكالها

الفرع الأول: خصائصها

أولاً: الجرائم التي ترتكب من خلال الأجهزة الإلكترونية كالحاسب الآلي والهواتف النقالة:

ليندا شرابسة،السياسة الدولية و الإقليمية في مجال مكافحة الجريمة الالكترونية،مجلة الدراسات و الألبحاث المجلد 1،العدد2019،1ص 392[3]

[4] جبور منى الأشقر،السيبرانية هاجس العصر،جامعة الدول العربية،لبنان،المجلد1،المركز العربي لبحوث القانونية و القضائية،2019،ص220

وهما أداتان يدخل من خلالهما المجرمون إلى شبكة الإنترنت لتنفيذ جرائمهم.
ثانياً: الجرائم المستترة: وهي جرائم لا يسهل اكتشافها بسبب مهارات الضحية التقنية مقارنة بالجاني، وربما بسبب مهارات الجاني التقنية والعلمية المتقدمة، أو قدرته على إخفائها، أو خوف الضحية من الإبلاغ عن الجريمة لتجنب التشهير بنفسه.
ثالثاً: الجرائم سريعة التنفيذ: سرعة ارتكاب الجريمة في جزء من الثانية فقط، وقد لا تتطلب أي إعداد قبل تنفيذها.
رابعا:الجرائم عن بعد: يمكن للجاني أن ينفذ الجريمة وهو في بلد بعيد عن الضحية.
خامساً: الجريمة العابرة للحدود الوطنية: فالجريمة العابرة للحدود الوطنية: فالعالم متصل بشبكة واحدة لا تعرف حدوداً جغرافية ويمكن أن تخلق مشاكل قضائية من حيث التحقيقات والمحاكمات بسبب تعقيد الإجراءات التي تحكمها الاتفاقيات والمعاهدات والعلاقات الدولية والتضارب بين الاثنين حول أي القوانين يجب أن تطبق [5]
سادسًا: الجرائم التي يصعب إثباتها: وتكمن صعوبات إثبات الجرائم في أن متابعتها والكشف عنها يكون عرضيًا ويصعب حصرها في أماكن محددة، ولا تترك آثارًا واضحة أو لا يمكن رؤيتها بالعين المجردة، وهي مجرد أرقام تدور في السجلات والمواقع الإلكترونية، والجرائم غير المكتشفة أكثر شيوعًا من المكتشفة وتكمن الصعوبات في كونها جرائم لا تترك أثراً بعد ارتكابها، وصعوبة الحفاظ على آثارها تقنياً (إن وجدت)، وأنها تتطلب خبرة فنية ويصعب التعامل معها من قبل المحققين التقليديين، وأن ارتكاب الجريمة يعتمد على الخداع والغموض في تحديد هوية مرتكبيها، من بين أسباب أخرى.
سابعًا: الجريمة الناعمة: على عكس الجريمة التقليدية، فهي جريمة غير عنيفة لا تتطلب أدنى جهد.
ومن ذلك أن المجرمين الإلكترونيين يتميزون بدرجة عالية من المهارة، حيث يعتمدون على ذكائهم ودهائهم وقدرتهم العقلية مع الإلمام بالأساليب الإلكترونية لإتلاف البرامج واختراق الحواجز الأمنية، وقد تكون دوافع المجرمين الإلكترونيين بدافع المال، حيث يلجأون إلى أساليب غير مشروعة بسبب البطالة علماً أنهم قد يكونون مدفوعين أيضاً بدوافع أيديولوجية أو سياسية، أو بدوافع التجسس أو انتهاك الخصوصية[6].

الفرع الثاني:أشكال الجريمة السيبرانية

-1خطر الكوارث الطبيعية أو العرضية على الكابلات البحرية:

تلعب الكابلات البحرية دورًا مهمًا في توفير خدمات الاتصالات بين دول العالم في مجالات مثل الإنترنت وشبكات الحاسب الآلي وغيرها، ومنذ عام 2005، أصبحت

محمد عبد الرحمان ونصيرات وائل،الجهود الدولية في مكافحة الجرائم المعلوماتيةو الصعوبات التي
[5] تواجهها،المؤتمر الدولي لمكافحة الجرائم المعلوماتية،جامعة الامام محمد بن سعود الإسلامية ،ص11
أميرة عبد العظيم المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام ،مجلة الشريعة و القانون المجلد3،العدد 35ص361.[6]

الكابلات البحرية منذ عام 2005، ولكن في نطاق التقدم والتطور تحولت هذه الكابلات إلى تقنيات خفيفة الوزن وصغيرة الحجم, لا تقع في المياه العميقة، مما يعرضها لعدد من المشاكل التي تؤثر سلبًا على أعمال البنية التحتية.

2- التجسس الإلكتروني:

وهو نوع من أنواع التجسس التقليدي عالي التقنية، وتنطوي معظم هجمات التجسس السيبراني المتقدمة التي تندرج ضمن هذه الفئة على الاستحواذ غير المشروع على معلومات حساسة بغرض الحصول على ميزة اقتصادية أو استراتيجية أو عسكرية.

والتجسس السيبراني هو التجسس الذي يستخدم التكنولوجيا الإلكترونية للحصول على المعلومات، وهناك أنواع مختلفة من التجسس السيبراني، بما في ذلك التجسس الفردي والتجسس باستخدام الشبكات السلكية والتجسس القائم على الأقمار الصناعية[7].

3-الإرهاب السيبراني

الإرهاب السيبراني هو استخدام مصادر المعلومات - وسائل الإعلام والكمبيوتر والإنترنت والفضائيات - للتخويف أو الإكراه لأغراض سياسية أو للإقناع الفكري أو للتثقيف السلبي والعدائي.

ويرتبط الترهيب والإكراه لأغراض سياسية أو للإقناع الفكري أو التثقيف السلبي والعدائي والإرهاب المعلوماتي إلى حد كبير بدرجة عالية من تطور تكنولوجيا المعلومات والإعلام في جميع مجالات الحياة في العالم.

ويمكن للإرهاب السيبراني أن يشل أنظمة القيادة والسيطرة والاتصالات، فيعطل روابط الاتصال بين الوحدات والقيادة المركزية، ويعطل أنظمة الدفاع الجوي، إلخ.

4-الحرب السيبرانية:

تعتمد الحرب السيبرانية الناجحة على فرق متعددة من خبراء الحرب السيبرانية، لكل منهم مسؤوليات ومهارات فريدة.ويقوم العاملون بتخطيط وإدارة وتنفيذ الأنشطة الهجومية والدفاعية في الفضاء السيبراني.

المبحث الثاني: الجهود الدولية والإقليمية لمكافحة الجرائم السيبرانية .

المطلب الأول: الجهود الدولية لمكافحة الجريمة السيبرانية

يركز هذا المطلب على جهود الأمم المتحدة والمنظمات الدولية مثل منظمة التعاون الاقتصادي والتنمية والاتحاد الدولي للاتصالات.

الفرع الأول: جهود الأمم المتحدة لمكافحة الجريمة السيبرانية

أوصى المجلس الاقتصادي والاجتماعي التابع للأمم المتحدة (ECOSOC) بأن تضطلع المنظمات الدولية بدور رئيسي في منع الجريمة وصياغة سياسة العدالة الجنائية الدولية.وفي عام 1950، أقرت الجمعية العامة للأمم المتحدة هذه التوصية وأنشأت لجنة الخبراء الاستشارية لمنع الجريمة ومعاملة المجرمين. واللجنة مسؤولة عن مكافحة

[7] إدريس عطية،المرجع السابق،ص 109

الجريمة وإسداء المشورة للأمين العام وإعداد البرامج وصياغة الخطط ورسم السياسة المتعلقة بالتدابير الدولية في مجال منع الجريمة ومعاملة المجرمين.
وفي أعقاب مؤتمر الأمم المتحدة لمنع الجريمة ومعاملة المجرمين الذي عقد في كيوتو، اليابان، في عام 1970، استعيض عن اللجنة الاستشارية بمجلس منع الجريمة ومكافحتها بناء على توصية من المجلس الاقتصادي والاجتماعي في عام 1971. ويُعقد مؤتمر الأمم المتحدة لمنع الجريمة ومعاملة المجرمين كل خمس سنوات ويهدف إلى تعزيز تبادل المعارف والخبرات بين الخبراء الوطنيين وتعزيز التعاون الدولي والإقليمي في مجال مكافحة الجريمة.وتركز هذه الدراسة على عمل الأمم المتحدة من خلال مؤتمر منع الجريمة ومعاملة المجرمين فيما يتعلق بالجرائم التكنولوجية والحاسوبية وهو يشير هنا إلى مؤتمر الأمم المتحدة السابع لمنع الجريمة ومعاملة المجرمين، الذي عُقد في ميلانو، إيطاليا، في عام 1985.) [8]
وقد أقرّ مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة المجرمين، الذي عقد في هافانا، كوبا، في عام 1990، هذه المبادئ ووضع المبادئ التوجيهية النهائية في إطار التحضير الإقليمي للمؤتمر الثامن.
وشدد المؤتمر أيضا على أن التطورات الجديدة في العلم والتكنولوجيا يجب أن تطبق في كل مكان من أجل الصالح العام ومن أجل منع الجريمة منعا فعالا[9]. كما شدد المؤتمر على أن العلم والتكنولوجيا يمكن أن يخلق أشكالا جديدة من الجريمة، وأنه ينبغي اتخاذ التدابير المناسبة ضد التجاوزات التي يمثلها هذا العلم والتكنولوجيا. وتطرق المؤتمر إلى مسألة الخصوصية التي قد تنتهك بالاطلاع على البيانات الشخصية المخزنة في النظم الحاسوبية، وذكر المؤتمر أن ذلك يعد انتهاكاً لحقوق الإنسان واعتداءً على كرامة الحياة الخاصة، وأنه ينبغي اعتماد ضمانات مناسبة لكفالة السرية ولضمان اطلاع الأفراد.

الفرع الثاني: جهود المنظمات الدولية في مكافحة الجريمة السيبرانية

الاتحاد الدولي للاتصالات، المنظمة الدولية للشرطة الجنائية(ITU) ، المنظمة الدولية للشرطة الجنائية (الإنتربول)/المنظمة الأوروبية للشرطة الجنائية(EUROPOL) ، منظمة التعاون الاقتصادي والتنمية(OECD) ، هيئة الإنترنت للأسماء والأرقام المخصصة(ICANN) ، المنظمة الدولية للمعايير ,(ISO) واللجنة الكهروتقنية الدولية (IEC)، وفرقة عمل هندسة الإنترنت(IETF) ، ومنظمة التعاون الاقتصادي لآسيا والمحيط الهادئ(APEC) ، ومنظمة الدول الأمريكية(OAS) ، ورابطة دول جنوب شرق آسيا(ASEAN) ، وجامعة الدول العربية(LAS) ، والاتحاد الأفريقي(AU) ، والعديد من المنظمات الأخرى تم الاضطلاع بها.
جامعة الدول العربية والاتحاد الأفريقي، وتستخدم منظمتان هنا كأمثلة على ذلك:

أولاً، منظمة التعاون الاقتصادي والتنمية.(OECD)

[8] عبابنة،ص 156
[9] عبابنة،ص 158

بدأت هذه المنظمة، التي تهدف إلى تحقيق أعلى مستويات النمو الاقتصادي والانسجام بين التنمية الاقتصادية والاجتماعية، في التركيز على الجرائم الإلكترونية بعد عام 1978، عندما وضعت سلسلة من الأدلة والمبادئ التوجيهية المتعلقة بتكنولوجيا المعلومات. وكان دليل حماية الخصوصية وأنظمة نقل البيانات من أوائل الأدلة التي اعتمدها مجلس المنظمة في عام 1980، وأوصى الدول الأعضاء بالامتثال لها. وفي عام 1983، نشرت منظمة التعاون والتنمية في الميدان الاقتصادي تقريراً بعنوان "تحليل الجرائم المتعلقة بالحاسوب والسياسة القانونية الجنائية"، والذي استعرض السياسات الجنائية القائمة والمقترحات الخاصة في عدد من الدول الأعضاء وتضمن ما يلي:

الحد الأدنى من أفعال إساءة استخدام الحاسوب التي ينبغي لكل دولة تجريمها، بما في ذلك مايلي:[10]

-الاستخدام غير المصرح به أو الوصول غير المصرح به إلى أنظمة وموارد الحاسب الآلي

- النسخ أو التدمير أو التخريب

-الإفصاح غير المصرح به عن المعلومات المعالجة آلياً، بما في ذلك البيانات والبرمجيات، والإعاقة غير القانونية للوصول إلى موارد الحاسوب عن طريق منع أو تعطيل استخدام الحاسوب أو برمجياته أو البيانات المخزنة فيه.

وفي عام 1992، أعدت منظمة التعاون والتنمية الاقتصادية توصيات ومبادئ توجيهية بشأن نظم المعلومات، وأوصت بأن تنص التشريعات الجنائية للدول الأعضاء على المبادئ العامة التالية:

- حدود الجمع: ينبغي فرض حدود على جمع البيانات.

-جودة البيانات: جودة البيانات: يجب أن تكون البيانات ذات صلة بالغرض الذي ستستخدم من أجله.

تقييد الغرض: تقييد الاستخدام: يجب أن تكون الأغراض التي يمكن استخدام البيانات الشخصية من أجلها محدودة ومحددة مسبقًا.

-تقييد الاستخدام: تقييد الاستخدام: يفرض التزامًا بعدم الكشف عن البيانات الشخصية أو تقديمها لأشخاص غير مصرح لهم.

قيود الاستخدام: قيود الاستخدام: تفرض التزامًا بعدم الكشف عن البيانات الشخصية أو تقديمها لأشخاص غير مصرح لهم.

-ضمانات الأمن: يجب وضع تدابير وإجراءات أمنية مناسبة وقوية حول البيانات.

-المشاركة الشخصية: حق الشخص المعني في الوصول إلى البيانات المتعلقة به والاطلاع عليها والتحكم في صحتها.

[10] مشوش مراد،الجهود الدولية لمكافحة الاجرام السيبراني،مجلة الواحات للبحوث والدراسات ،المجلد12،العدد 2،،ص 709

-المساءلة: يجب مساءلة الأفراد والكيانات المخولة بالوصول إلى البيانات والاطلاع عليها والتعامل معها في حال خرقهم لإجراءات ضمان حماية البيانات الشخصية) مشوش، 2019، صفحة 710(.

ثانياً: الاتحاد الدولي للاتصالات(ITU)

اعتمد المؤتمر العالمي لتنمية الاتصالات لعام 2006 القرار رقم 45 الذي اعتمده المؤتمر العالمي لتنمية الاتصالات في عام 2006، وطلب فيه من المدير العام لإدارة تنمية الاتصالات تنظيم اجتماع بشأن الأمن السيبراني ومكافحة الرسائل الإلكترونية التطفلية وتقديم تقرير يتضمن النتائج التي توصل إليها إلى مؤتمر المندوبين المفوضين لعام 2006.

واعتُمدت سلسلة من التوصيات في مجالي الأمن السيبراني والبريد الإلكتروني غير المرغوب فيه، وفي مايو 2007 أطلق الأمين العام للاتحاد الدولي للاتصالات جدول الأعمال العالمي للأمن السيبراني لوضع إطار عمل للتصدي للجريمة السيبرانية في ضوء الاتفاقيات الدولية[11].

وفي أكتوبر 2007، أُنشئ فريق خبراء رفيع المستوى يضم أكثر من 100 خبير، قدم تقريره وتوصياته في يونيو 2008، ونُشرت استراتيجية عالمية في 11 ديسمبر 2008. وتشمل الاستراتيجية المجالات التالية: التدابير القانونية، والتدابير التقنية والإجرائية، والهياكل التنظيمية وبناء القدرات، والتعاون الدولي).

المطلب الثاني: الجهود الإقليمية في مكافحة الجريمة السيبرانية

من بين المعاهدات والاتفاقيات التي تعالج التعاون الدولي في مجال مكافحة الجريمة السيبرانية، تعد الاتفاقيات والمعاهدات الدولية عموماً، من أهم أشكال التعاون الدولي، لا سيما في مجال مكافحة الجرائم الناشئة عن الجريمة السيبرانية: اتفاقية بودابست لمكافحة الجريمة السيبرانية، واتفاقية اتفاقية جامعة الدول العربية بشأن

والتوصية الصادرة عن مجلس أوروبا بشأن الجرائم الجنائية الإجرائية المتعلقة بتكنولوجيا المعلومات، وترد أدناه مناقشة التوصيات الصادرة عن مجلس أوروبا بشأن الجرائم الجنائية الإجرائية المتعلقة بتكنولوجيا المعلومات:

الفرع الأول: توصيات مجلس أوروبا

أدى التطور السريع لتكنولوجيا الحاسوب والإنترنت وإدراك الدول الأوروبية لأهمية مراجعة الإجراءات الجنائية إلى صدور توصية مجلس أوروبا رقم: 13/95 المؤرخة 11 أيلول/سبتمبر 1995 بشأن مسألة الإجراءات الجنائية المتعلقة بالتكنولوجيا وتكنولوجيا المعلومات والعقوبات الوطنية التي تتناسب مع التطورات في هذا المجال توصية مجلس أوروبا رقم: 13/95 المؤرخة 11 سبتمبر 1995 بشأن مسألة الإجراءات

[11] نوايسة عبد إله،جرائم تكنولوجيا المعلومات،شرح الأحكام الموضوعية في قانون جرائم الإلكترونية،الأردن،دار وائل لنشر و التوزيع،عمان،ص 211

الجنائية المتعلقة بالتكنولوجيا وتكنولوجيا المعلومات والعقوبات الوطنية التي تتناسب مع التطورات في هذا المجال.

-ينبغي توضيح إجراءات تفتيش الحواسيب ومصادرة المعلومات الواردة في الحواسيب ومراقبة المعلومات العابرة في القانون.

-يجب أن تسمح الإجراءات الجزائية للدولة للمفتشين بمصادرة برامج الحاسوب والمعلومات الواردة في المعدات بنفس شروط إجراءات التفتيش العادية، ويجب إبلاغ الشخص المسؤول عن المعدات بأن النظام

ينبغي أن يتم تفتيشه وينبغي إخطاره بأن المعلومات ستتم مصادرتها.

-أثناء عملية التفتيش، يجب أن يسمح لسلطات الإنفاذ بتوسيع نطاق التفتيش ليشمل أنظمة حاسوبية أخرى في ولايتها القضائية متصلة بالنظام الخاضع للتفتيش ومصادرة المعلومات الواردة فيه فقط إذا كان ذلك ضرورياً، مع احترام تدابير الحماية المقررة.

ويجب أن يوضح قانون الإجراءات الجنائية أن الإجراءات التقليدية المتعلقة بالوثائق تنطبق أيضا على المعلومات الواردة في الحواسيب.

-ويجب أن تطبق إجراءات المراقبة والتسجيل في مجال التحقيق الجنائي عند الضرورة في مجال تكنولوجيا المعلومات ويجب توفير السرية والاحترام للمعلومات التي يفرض القانون حماية خاصة لها.

- .ينبغي إلزام موظفي الوكالات الحكومية والمؤسسات الخاصة التي تقدم خدمات الاتصالات السلكية واللاسلكية بالتعاون مع المراقبة والتسجيل من قبل سلطات التحقيق.

-ومن أجل الكشف عن الحقيقة، ينبغي تعديل القانون الإجرائي من خلال إصدار أمر للأشخاص الذين بحوزتهم معلومات، سواء كانت برامج أو قواعد بيانات أو بيانات متعلقة بالحاسوب، بتسليمها.

-وينبغي تمكين سلطات التحقيق من إصدار أمر للأشخاص الذين بحوزتهم بيانات شخصية بالوصول إلى نظم المعلومات أو الوصول إلى المعلومات الواردة فيها، لاتخاذ التدابير اللازمة لتمكين المحققين من الوصول إليها)[12].

-يجب تطوير نظم التعامل مع الأدلة الإلكترونية وتوحيدها. يجب تطبيق الوثائق الإجرائية الخاصة بالأدلة التقليدية على الأدلة الإلكترونية حتى تكون معترفاً بها بين مختلف الدول.

-وينبغي تشكيل وحدات خاصة لمكافحة الجرائم الحاسوبية وإعداد برامج تدريبية خاصة لتزويد موظفي العدالة الجنائية بالمعارف في مجال تكنولوجيا المعلومات.

-وقد تتطلب إجراءات التحقيق الوصول إلى أنظمة حاسوبية أخرى خارج الدولة والتدخل السريع، ويجب وضع قواعد قانونية واضحة لتمكين هذه الإجراءات من تجنب انتهاك السيادة الوطنية والقانون الدولي.

[12] الزهراني،المرجع السابق،ص 752

ولذلك كان من الضروري إبرام اتفاقيات تنظم متى وكيف يمكن اتخاذ مثل هذه الإجراءات.مكافحة الجريمة السيبرانية في ضوء الاتفاقيات الدولية 79

-يجب أن تكون هناك إجراءات سريعة وملائمة ونظام اتصالات يمكّن سلطات التحقيق من الاتصال بالسلطات الأجنبية لجمع أدلة معينة، ويجب أن تأذن هذه الأخيرة بإجراءات التفتيش والحجز [13]

الفرع الثاني:اتفاقية بودابست بشأن مكافحة الجرائم الإلكترونية

في نهاية عام 2001، تم التوقيع في بودابست، عاصمة المجر،على أول اتفاقية دولية لمكافحة الجريمة السيبرانية. وتماشياً مع هذا التطور، أبرم مجلس أوروبا اتفاقية بودابست

وفي 8 تشرين الثاني/نوفمبر 2001 وقُدمت للتصديق عليها في 23 تشرين الثاني/نوفمبر 2001: تم التصديق عليها في 23 تشرين الثاني/نوفمبر 2001. وتتضمن الاتفاقية تعريفاً لأهدافها وقائمة بالجرائم التي يجب على الدول المصدقة عليها أن تحظرها في قوانينها الوطنية، وتعتبر الأولى في مجال مكافحة جرائم المعلوماتية وتشمل العديد من الجرائم الإلكترونية، ومنها: تهدف الاتفاقية إلى مواءمة التشريعات الجديدة في العديد من الدول، وهي ثمرة مشاورات طويلة الأمد بين الحكومات وأجهزة الشرطة وقطاع الحاسوب، وقام بصياغة موادها عدد من الخبراء من مجلس أوروبا بالتعاون مع العديد من الدول، بما في ذلك الولايات المتحدة [14].

كما أنها المعاهدة الوحيدة المتعددة الأطراف المعنية بمكافحة الجرائم المرتكبة بواسطة الحواسيب أو ضدها وباستخدام الإنترنت، وهي ركيزة أساسية لمجلس الاتحاد الأوروبي منذ دخولها حيز النفاذ على مستوى الدول الأعضاء في 1 تموز/يوليو 2004. وكما سبق ذكره، فقد وقّع عليها العديد من الدول غير الأعضاء في مجلس أوروبا، بما في ذلك كندا واليابان وجنوب أفريقيا، وصادقت عليها الولايات المتحدة الأمريكية. الاتفاقية هي دعوة إلى دول العالم للتفاعل مع الإنترنت، وهي ثمرة محاولات عديدة منذ ثمانينيات القرن الماضي حتى ظهورها بصيغتها النهائية في 23 نوفمبر 2001)[15].

وتضمنت هذه الاتفاقية الأقسام التالية:

القسم الأول: تعريف المصطلحات

القسم الثاني: تعريف المصطلحات التدابير الواجب اتخاذها في إطار التشريعات الوطنية.

القسم الثالث: التعاون الدولي: التعاون الدولي.

القسم الرابع: الشروط النهائية للانضمام إلى الاتفاقية.

الفرع الثالث: اتفاقية جامعة الدول العربية لمكافحة الجرائم السيبرنية

---

[13] الزهراني،ص 753

[14] درار،ص 273

[15] درار نسيمةالامن المعلوماتي وسبل مواجهة مخاطره في التعامل الالكتروني ،أطروحة دكتوراه،كلية الحقوق والعلوم السياسية ،جامعة تلمسان،،ص 274

أصدرت جامعة الدول العربية قانوناً استرشادياً لمكافحة الجرائم الإلكترونية.وقد سعت الدول العربية إلى تقنين وتجريم الأفعال غير المشروعة المرتكبة من خلال استخدام الفضاء الإلكتروني من خلال التوقيع على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في 21 ديسمبر 2010، وذلك بهدف تعزيز التعاون بين الدول العربية لمكافحة الجرائم الإلكترونية وحماية سلامة المجتمع وأمنه

ويحث المجلس الدول العربية المصدقة على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات على موافاة الأمانة الفنية للمجلس بالتدابير اللازمة لمواءمة تشريعاتها مع أحكام الاتفاقية، وتجريم الأشكال الجديدة للجريمة الإلكترونية لمنع استخدام الإرهابيين للإنترنت، وضمان منع كافة أشكال الإرهاب الإلكتروني ودعا المجلس إلى زيادة التعاون مع المنظمات الدولية والإقليمية المعنية بمكافحة الجريمة.

كما دعا المجلس الدول العربية إلى التعاون في منع الإرهابيين من إساءة استخدام تكنولوجيا المعلومات والاتصالات والإنترنت للتحريض على دعم الأعمال الإرهابية وتمويل أنشطتهم والتخطيط والإعداد للأعمال الإرهابية وضمان عدم استخدام الإرهابيين لأسلحة الدمار الشامل ومكوناتها (وشدد على أهمية تعزيز التعاون مع الوكالات والمنظمات الدولية المتخصصة لبناء القدرات اللازمة لمواجهة التهديدات والحصول على المساعدة اللازمة لدعم أمن المطارات والموانئ والحدود.

;على الرغم من هذه الجهود الدولية، سواء على مستوى الأمم المتحدة والمنظمات الدولية أو على المستوى الإقليمي، تدعو اتفاقية بودابست على وجه الخصوص الدول إلى مراجعة قوانينها الوطنية والتعاون الدولي لمكافحة الجريمة الإلكترونية التي لا تعرف حدودًا جغرافية. ومع ذلك، هناك صعوبات تواجه هذه الجهود، ويتناول هذا المطلب هذه الصعوبات وكيفية حله[16]ا.

المطلب الثالث:الصعوبات التي تواجهها الجهود الدولية وكيف يمكن حلها

الفرع الأول: الصعوبات التي تواجهها الجهود الدولية

دعا البعض إلى ضرورة إنشاء وحدة خاصة لمكافحة الجريمة السيبرانية، وكذلك وكالات التحقيق الجنائي الوطنية والدولية (الإنتربول)، لتحديد متى ارتكبت الجريمة وتحديد الأدلة ومرتكبيها. وهذا يعني إيجاد الطرائق المناسبة للتعاون الدولي لمكافحة الجرائم المرتكبة ضد البيانات الشخصية وتبادل الخبرات والمعلومات حول هذا النوع من الجرائم ومرتكبيها وسبل مكافحتها. وعلى الرغم من الحاجة إلى التعاون الدولي لمكافحة الجريمة السيبرانية، إلا أن هناك عقبات تعيق ذلك وتجعل هذا التعاون صعباً:

أولا: يوجد نموذج واحد متفق عليه للسلوك الإجرامي، حيث لا تتفق النظم القانونية في جميع أنحاء العالم على أشكال محددة من هذه الجرائم، بما في ذلك ما يسمى باستغلال نظم المعلومات. كما لا يوجد تعريف محدد لما يفترض الاتفاق عليه كجريمة جنائية.

[16] أميرة عبد العظيم،المرجع السابق،ص 499

كما أنها لم تتمكن من مواكبة سرعة التقدم في مجال المعلومات، وبالتالي سرعة الجريمة السيبرانية. أولا: عدم وجود اتفاق بين النظم القانونية المختلفة على صورة موحدة للسلوك الإجرامي في مجال الجريمة الإلكترونية يغري قراصنة الحاسوب بإراقة الدماء.

ثانيا: عدم وجود معاهدات ثنائية أو جماعية بين الدول تسمح بالتعاون المثمر في هذا المجال من الجريمة، وحتى لو وجدت تظل هذه المعاهدات غير كافية لتحقيق الحماية اللازمة في ظل التقدم السريع لأنظمة وبرامج الحاسوب والإنترنت، و ونتيجة لذلك، فإن الجريمة الإلكترونية تتطور بنفس السرعة، مما يثير استياء المشرعين الوطنيين والسلطات الأمنية.كما تتجلى الآثار السلبية في التعاون الدولي الذي تحاول الأمم المتحدة والعديد من الدول الأوروبية الاهتمام به[17]

ثالثا: هناك نقص في التنسيق بشأن الإجراءات الجنائية فيما يتعلق بالجريمة السيبرانية. وعلى وجه الخصوص، فيما يتعلق بالتحقيقات والوصول إلى الأدلة، فمن الصعب للغاية الحصول على الأدلة خارج الحدود من خلال ضبط أو تفتيش بعض نظم المعلومات في مثل هذه الجرائم، بالإضافة إلى صعوبة الحصول على الأدلة نفسها.

قائمة المراجع:

-عبد الله النوايسة، جرائم تقنية المعلومات - شرح الأحكام الموضوعية لقانون الجرائم الإلكترونية، الأردن: دار وائل للنشر والتوزيع، ط1، عمّان.

-محمود أحمد عبابنة،الجريمة المعلوماتية وجوانبها الدولية. الأردن: دار الثقافة للنشر والتوزيع، الأردن: دار وائل للنشر والتوزيع، الطبعة الثانية، المجلد 1، عمان.

- روان بنت عطية الله،الجرائم الإلكترونية: مجلة إلكترونية شاملة متعددة التخصصات، العدد 24.

-أم يوسف أمنر 17 01, 2021 مزايا الأمن السيبراني. تم الاسترجاع 11 أكتوبر 2021، من جريدة التاسيلي:

عسيري، ف. (2002). الأمن السيبراني وحماية المعلومات - تقنية المعلومات. المملكة العربية السعودية.

-بنت نبي ياسمين بلعسل، والحسين عمروش التهديدات السيبرانية والأمن السيبراني في العالم العربي.مجلة نميروس الأكاديمية، المجلد 02، العدد 02.

-جبور منى الأشقر الأمن السيبراني هاجس عصرنا. جامعة الدول العربية، بيروت، لبنان: المجلد 1، المركز العربي للبحوث القانونية والقضائية.

-سمير بالا الأمن السيبراني في الجزائر:السياسات والمؤسسات. المجلة الجزائرية للأمن الإنساني، العدد 04،

[17] شرايسة،ص 250

-شيخة حسين الزهراني التعاون الدولي في مواجهة الهجمات الإلكترونية. مجلة جامعة الشارقة للعلوم القانونية، المجلد 17، العدد 01.
-عبد الفتاح حجازي مبادئ الإجراءات الجنائية في جرائم الحاسب الآلي والإنترنت.مصر: دار الكتب القانونية، المحلة الكبرى، الطبعة الأولى.
-عطية إدريس، مكانة الأمن المعلوماتي في منظومة الأمن القومي الجزائري. مجلة المصداقية، المجلد 01، العدد 01،
-ليندا شلابوسة. السياسات الدولية والإقليمية في مجال مكافحة الجريمة الإلكترونية. مجلة الدراسات البحثية، المجلد 01، العدد 01،
-محمد عبد الجواد أميرة عبد العظيم، المخاطر السيبرانية في القانون الدولي العام وكيفية التعامل معها.مجلة الشريعة والقانون، المجلد 03، العدد 35،
-محمد عبد الرحمن نصيرات وائل، الجهود الدولية والصعوبات في مكافحة الجرائم الإلكترونية. المؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية - المؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية، جامعة الإمام محمد بن سعود الإسلامية، المملكة العربية السعودية.
-مراد مشوش 2019 المبادرات الدولية لمكافحة الجرائم الإلكترونية في واحة البحوث والدراسات. مجلة.المجلد 12، العدد 01،
-نسيمة درال ،الأمن السيبراني في التجارة الإلكترونية وكيفية مواجهة مخاطرها: دراسة مقارنة.) أطروحة دكتوراه، جامعة أبو بكر بلقايد - تلمسان - الجزائر، كلية الحقوق والعلوم السياسية.