

تهديد الجرائم الإلكترونية عبر الحدود: التحديات والاستراتيجيات الدولية لمواجهتها

The Threat of Cross-Border Cybercrimes: International Challenges and Strategies to Combat Them

جديدي ضياء الدين رمضان
المركز الجامعي بركة
مخبر افاق الحوكمة للتنمية المحلية المستدامة
dhiaeddine.djedidi@cu-barika.dz

دراحي شهرزاد*
المركز الجامعي بركة
مخبر افاق الحوكمة للتنمية المحلية المستدامة
Chahrazed.deradji@cu-barika.dz

تاريخ إرسال المقال: 2023 / 06 / 23 تاريخ قبول المقال: 2023 / 08 / 27 تاريخ نشر المقال: 2023 / 09 / 15

الملخص:

مع الاعتماد المتزايد باستمرار على التكنولوجيا والإنترنت، أصبحت الجرائم الإلكترونية تشكل تهديداً كبيراً على الأفراد والمنظمات والحكومات في جميع أنحاء العالم، وذلك أن عمل مجرمي الإنترنت غالبا ما يكون عبر الحدود الوطنية حيث يستخدمون أساليب متطورة لارتكاب جرائمهم التي تتراوح ما بين سرقة البيانات والاحتيال المالي إلى الإرهاب الإلكتروني والتجسس، وعليه تناقش هذه المقالة التحديات التي تطرحها الجرائم الإلكترونية على المستوى الدولي وتكشف الاستراتيجيات المستخدمة لمكافحة هذا التهديد المتزايد، بالإضافة إلى تسلط الضوء على الحاجة إلى التعاون والتنسيق الدوليين بين وكالات إنفاذ القانون وأصحاب المصلحة الآخرين من أجل مكافحة الجريمة السيبرانية بشكل فعال.

الكلمات المفتاحية: الجرائم الإلكترونية ؛ التعاون الدولي ؛ سرقة البيانات ؛ الاحتيال المالي ؛ الإرهاب السيبراني .

Abstract:

With the ever-increasing reliance on technology and the internet, cybercrime has become a major threat to individuals, organizations, and governments around the world. Cybercriminals operate across national borders and use sophisticated methods to commit crimes that range from data theft and financial fraud to cyber

تهديد الجرائم الإلكترونية عبر الحدود: التحديات والاستراتيجيات الدولية لمواجهتها

terrorism and espionage. This article discusses the challenges posed by cybercrime at the international level and explores the strategies being employed to combat this growing threat. The article highlights the need for international cooperation and coordination among law enforcement agencies and other stakeholders in order to effectively combat cybercrime.

Keywords: cybercrime ; international cooperation ; data theft ; financial fraud ; cyber terrorism.

مقدمة:

أصبحت الجريمة الإلكترونية ظاهرة عالمية يمكن أن تتسبب في ضرر كبير للأفراد والمنظمات والحكومات، فلقد خلق استخدام التكنولوجيا والإنترنت فرصاً جديدة للمجرمين لاستغلال نقاط الضعف وارتكاب الجرائم ، ونظراً لكون نشاط مجرمي الإنترنت عبر الحدود الوطنية فلقد كان من الصعب على وكالات تنفيذ القانون تعقبهم وتقديمهم إلى العدالة ، وبهذا أصبحت الجرائم الإلكترونية تهدد الأمن القومي لمختلف البلدان حول العالم مما أدى إلى زعزعة استقرار النظام الدولي وتعطيل الأداء الطبيعي للعلاقات الدولية ، لذلك فقد تطلبت الطبيعة العالمية للجرائم الإلكترونية التعاون والتنسيق الدوليين لمكافحة هذا التهديد المتزايد بشكل فعال .

وبناءً عليه يتجلى الهدف من دراسة هذا الموضوع في تحديد الاستراتيجية التي اعتمدها المجتمع الدولي في مواجهة خطورة هذا النوع من الإجرام، بالرغم من التحديات التي قد تواجهه في تحقيق غايته، وعليه سوف تتمحور هذه الدراسة حول الإجابة على الاشكال التالي :

فكيف جسدت مكافحة الجرائم الإلكترونية على المستوى الدولي ؟

وللإجابة على هذه الإشكالية ارتأينا تقسيم الدراسة الى محورين نعالج في المبحث الأول الإطار القانوني للجرائم الإلكترونية على المستوى الدولي من خلال النظر ومناقشة كل من القوانين والاتفاقيات والمعاهدات الدولية المتعلقة بالجرائم الإلكترونية وكذا تحديات وقيود قوانين الجرائم الإلكترونية الدولية بالإضافة الى التعاون الدولي في مكافحة الجرائم الإلكترونية، أما المبحث الثاني فسوف نخصه لدراسة استراتيجيات الأمن السيبراني سواء ما تعلق منها بأمن الحكومات والمنظمات بالإضافة لأمن الأفراد والتقنيات الناشئة وتأثيرها على الأمن السيبراني.

المبحث الأول : الإطار القانوني للجرائم الإلكترونية على المستوى الدولي

أدى التقدم التكنولوجي إلى ظهور الحاجة إلى إطار قانوني للتحكم في الجرائم الإلكترونية على المستوى الدولي وهذا نظرا لكون ان الجرائم الإلكترونية تشير إلى الأنشطة الإجرامية التي تُرتكب باستخدام أجهزة الكمبيوتر أو الإنترنت أو أي شكل آخر من أشكال التكنولوجيا، فيمكن أن تتراوح هذه الجرائم من القرصنة وسرقة الهوية إلى نشر محتوى غير قانوني أو التجسس عبر الإنترنت¹، ولهذا فالجرائم الإلكترونية مشكلة عالمية تتطلب حلاً عالمياً، وهو ما سوف نستشفه من خلال هذا المبحث المعنون بالإطار القانوني للجرائم الإلكترونية على المستوى الدولي.

المطلب الأول: القوانين والاتفاقيات والمعاهدات الدولية المتعلقة بالجرائم الإلكترونية

يمكن حصر اهم القوانين والاتفاقيات والمعاهدات الدولية المتعلقة بالجرائم الإلكترونية سواء بصفة مباشرة او غير مباشرة في :

أولاً: اتفاقية مجلس أوروبا بشأن الجرائم الإلكترونية

إن اتفاقية مجلس أوروبا المتعلقة بجرائم الإنترنت والمعروفة أيضاً باسم اتفاقية بودابست²، هي أول معاهدة دولية بشأن جرائم الإنترنت، تم تبنيها سنة 2001 وصادقت عليها 65 دولة. تحدد الاتفاقية الإطار القانوني لمكافحة الجريمة السيبرانية من خلال تحديد مختلف الجرائم المتأصلة من الإنترنت كالقرصنة والاحتيال المرتبط بالكمبيوتر والمواد الإباحية للأطفال، كما تحدد إجراءات التحقيق في الجرائم الإلكترونية وملاحقة مرتكبيها ، بما في ذلك جمع الأدلة الإلكترونية واجراءات التحقيق والمتابعة³، وبذلك كانت اتفاقية مجلس أوروبا بشأن جرائم الإنترنت أول صك ملزم متعدد الأطراف لتنظيم جرائم الإنترنت.

حيث تتطلب اتفاقية بودابست من الموقعين وضع القوانين واللوائح التي تجرم الجرائم الإلكترونية وتقديم المساعدة القانونية إلى الموقعين الآخرين في التحقيق والملاحقة القضائية في الجرائم الإلكترونية، فضلا عن إنشائها لشبكة من نقاط الاتصال لتسهيل التعاون وتبادل المعلومات بين الموقعين.

¹ Gordon, S., & Ford, *On the definition and classification of cybercrime*, Journal in computer virology, 2, R. (2006), p 14. .

² الاتفاقية المتعلقة بالجريمة الإلكترونية (بودابست)، الصادرة عن مجلس أوروبا "مجموعة المعاهدات الأوروبية رقم 175"، المؤرخة في 2001/11/23.

³ Weber, A. M, *The council of Europe's convention on cybercrime*, Berkeley Technology Law Journal, 18(1), (2003), p 425.

تهديد الجرائم الإلكترونية عبر الحدود: التحديات والاستراتيجيات الدولية لمواجهةها

وتجدر الإشارة إلى أنه تم الإشادة بالاتفاقية دولياً لنهجها الشامل تجاه جرائم الفضاء الإلكتروني وفعاليتها في تعزيز التعاون الدولي، بالإضافة إلى توفيرها معياراً هاماً يمكن قياس الجهود الوطنية على أساسه على نطاق أوسع⁴، ومع ذلك أثار بعض النقاد الكثير من المخاوف بشأن افتقار الاتفاقية إلى الشفافية وإمكانية انتهاكها للخصوصية والحريات المدنية.

وعلى الرغم من أن الاتفاقية لا تزال أهم صك في هذا المجال، غير أنها مصحوبة الآن بمجموعة من المبادرات الدولية والإقليمية والوطنية أنشأت في بيئة غير مستقرة قد يكون فيها الاتفاق الدولي بعيد المنال.

ثانياً: اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية

تم اعتماد اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية والمعروفة أيضاً باسم اتفاقية باليرمو في عام 2000⁵، وعلى الرغم من أن هذه الاتفاقية تتناول الجريمة المنظمة في المقام الأول إلا أنها تحتوي أيضاً على أحكام بشأن جرائم الإنترنت، حيث تُعرّف الاتفاقية الجريمة الإلكترونية على أنها أي جريمة التي تُرتكب باستخدام نظام أو شبكة كمبيوتر ويعاقب عليها القانون. تتطلب اتفاقية باليرمو من الموقعين وضع القوانين واللوائح التي تجرم الجريمة الإلكترونية وتقديم المساعدة القانونية للأطراف الموقعة الأخرى في التحقيق في الجرائم الإلكترونية وملاحقتها، كما تتطلب الاتفاقية أيضاً من الموقعين التعاون مع بعضهم البعض في منع وقمع الجريمة السيبرانية وتبادل المعلومات وأفضل الممارسات⁶.

لقد تم الإشادة بالاتفاقية لتركيزها على الجريمة المنظمة ونهجها الشامل اتجاه الجريمة السيبرانية، غير أن بعض النقاد قد أثاروا مخاوف بشأن افتقار الاتفاقية إلى آليات التطبيق وإمكانية انتهاكها للخصوصية والحريات المدنية.

⁴ Clough, J. *A world of difference: The Budapest convention on Cybercrime and the challenges of Harmonisation*, Monash University Law Review, 40(3), (2014), p 698.

⁵ اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، اعتمدت بموجب قرار الجمعية العامة للأمم المتحدة 55/25، المؤرخة في 15 نوفمبر 2000.

⁶ Betti, S. *New prospects for inter-state co-operation in criminal matters: The Palermo Convention*, International Criminal Law Review, 3(2), (2003), p 151.

ثالثا: توجيه الاتحاد الأوروبي بشأن الهجمات على أنظمة المعلومات

تم اعتماد توجيه الاتحاد الأوروبي بشأن الهجمات على أنظمة المعلومات والمعروف أيضاً باسم توجيه NIS في عام 2016⁷، و نظراً لكون الأنظمة القديمة التقليدية التي تدير البنى التحتية الوطنية الحيوية يتم رقمتها بشكل متزايد لمراقبة الأداء وكفاءته، فقد تم توجيه اهتمام كبير لتحسين أمنها السيبراني و توجيه أمن أنظمة المعلومات والشبكات NIS هو أول محاولة على المستوى الأوروبي لإنشاء مستوى عالٍ من الأمن السيبراني ، حيث تثير NIS أسئلة حول تحديد النطاق أو تقديم الأدلة أو حشد التمويل، كما يحدد التوجيه إطاراً قانونياً لمنع ومكافحة الجرائم الإلكترونية في الاتحاد الأوروبي. و يتطلب توجيه NIS من الدول الأعضاء في الاتحاد الأوروبي وضع قوانين ولوائح تجرم الجرائم الإلكترونية وتقديم المساعدة القانونية للدول الأعضاء الأخرى في التحقيق في الجرائم الإلكترونية وملاحقتها.

كما يتطلب توجيه NIS أيضاً من الدول الأعضاء في الاتحاد الأوروبي اتخاذ تدابير لمنع وكشف الهجمات الإلكترونية، بما في ذلك إنشاء فرق استجابة لحوادث أمن الكمبيوتر الوطنية وتطوير خطط طوارئ للحوادث السيبرانية ، وتم الإشادة بالتوجيه أيضاً لتركيزه على المنع ونهجه الشامل لجرائم الإنترنت ، ومع ذلك أثار بعض النقاد مخاوف بشأن إمكانية أن ينتهك التوجيه الخصوصية والحريات المدنية⁸.

المطلب الثاني: تحديات وقيود قوانين الجرائم الإلكترونية الدولية

تعد قوانين الجرائم الإلكترونية الدولية مهمة لمعالجة المشكلة العالمية للجرائم الإلكترونية، و على الرغم من وجود هذه القوانين، إلا أن هناك تحديات وقيود مرتبطة بها، التي تتمثل في :

أولاً: الاختلافات في القوانين الوطنية

أحد التحديات الرئيسية لقوانين الجرائم الإلكترونية الدولية هو الاختلافات في القوانين الوطنية. الدول لديها قوانينها ولوائحها الخاصة للتصدي للجرائم الإلكترونية والتي قد تختلف بشكل كبير فلا يتم عادة إعداد القانون دائماً لتلبية متطلبات العولمة والأنشطة الجديدة غير القانونية القائمة

⁷ توجيهات الاتحاد الأوروبي بشأن الهجمات على أنظمة المعلومات، الصادر عن البرلمان الأوروبي ومجلس الاتحاد الأوروبي، المؤرخ في 2016/06/06.

⁸ Michalec, O., Van Der Linden, D., Milyaeva, S., & Rashid, A. *Industry responses to the european directive on security of network and information systems (NIS) understanding policy implementation practices across critical infrastructures*. In *Proceedings of the Sixteenth USENIX Conference on Usable Privacy and Security* . p 301.

تهديد الجرائم الإلكترونية عبر الحدود: التحديات والاستراتيجيات الدولية لمواجهتها

على الاستخدام غير المشروع لتكنولوجيا المعلومات والاتصالات⁹، وهذا ما يجعل من الصعب تطبيق قوانين الجرائم الإلكترونية على المستوى الدولي .
فلدى البلدان تعريفات مختلفة لما يشكل جرائم الإنترنت، وهذا ما قد يؤدي إلى الارتباك والصراعات عند التعامل مع الجرائم الإلكترونية عبر الحدود.

ثانيا: قضايا الاختصاص القضائي

تعد قضايا الاختصاص القضائي تحدياً آخر مرتبطاً بقوانين الجرائم الإلكترونية الدولية و تنشأ قضايا الاختصاص القضائي عندما ترتكب جريمة إلكترونية في بلد ما وتؤثر على بلد آخر وهنا تنشأ مشكلات كثيرة لا سيما في مسألة تحديد الاختصاص القضائي الذي يجب أن تدرج تحته هذه الجريمة¹⁰، و قد يكون من الصعب تحديد الدولة التي لديها سلطة مقاضاة الجاني. في بعض الحالات ، قد ترفض الدول تسليم المجرمين إلى دول أخرى ، مما قد يزيد الأمور تعقيداً.

ثالثا: الافتقار إلى التعاون الدولي:

هناك تحدٍ آخر مرتبط بالقوانين الدولية لمكافحة الجرائم الإلكترونية وهو الافتقار إلى التعاون الدولي، فقد تتردد البلدان في مشاركة المعلومات أو التعاون مع الدول الأخرى في التحقيقات المتعلقة بجرائم الإنترنت، لعدة أسباب يمكن أن تكون بسبب التوترات السياسية أو انعدام الثقة أو الاختلافات في الأنظمة القانونية¹¹.

رابعا: التطورات التكنولوجية

يمكن أن تشكل التطورات التكنولوجية السريعة أيضاً تحدياً لقوانين الجرائم الإلكترونية الدولية، وهذا لأن مجرمي الإنترنت يستحدثون باستمرار أساليبهم وتقنياتهم في ارتكاب الجرائم، لتجنب الكشف والقيام بأنشطتهم بكل فعالية، وهو ما قد لا تتمكن قوانين الجرائم الإلكترونية الدولية من مواكبة هذه التطورات التكنولوجية ، مما يجعل من الصعب مقاضاة الجناة والقبض عليهم¹².

⁹ Foggetti, N ,*Transnational cyber crime, differences between national laws and development of European legislation: by repression?*. Masaryk University journal of Law and technology, 2(2), (2008), p 31.

¹⁰ *Ibid* , p 33.

¹¹ ثامري عمر، التعاون الدولي في مكافحة الفساد، مداخلة منشورة في الموقع [مداخلة كاملة أ. ثامري.pdf](#). تم

الإطلاع عليها يوم الأحد 2023/05/26 على الساعة 12:00، ص 4.

¹² Ledingham, R., & Mills, R. *A preliminary study of autism and cybercrime in the context of international law enforcement*, *Advances in Autism*, 1(1), (2015), p 2.

خامسا: الموارد المحدودة

كما يمكن أن تشكل الموارد المحدودة قيودا على قوانين الجرائم الإلكترونية الدولية، فقد لا تمتلك العديد من البلدان الموارد أو الخبرة اللازمة للتحقيق الفعال في قضايا الجرائم الإلكترونية ومقاضاة مرتكبيها، مما سيؤدي إلى عدم تطبيق قوانين الجرائم الإلكترونية و إفلات مجرمي الإنترنت من العقاب.

المطلب الثالث: التعاون الدولي في مكافحة الجرائم الإلكترونية

أدى الاستخدام المتزايد باستمرار لأجهزة الكمبيوتر وتكنولوجيا المعلومات والاتصالات في عالم -كل شيء فيه إلكتروني- ، إلى فتح مجموعة من الأنشطة الجديدة للجريمة من خلال استغلال الوسائل الإلكترونية على نطاق عالمي ، وعليه تتطلب المكافحة الفعالة لهذه الجرائم والتحقيق فيها ومقاضاة مرتكبيها تعاوناً دولياً بين الدول ووكالات إنفاذ القانون والمؤسسات المدعومة بالقوانين والعلاقات الدولية والاتفاقيات والتوجيهات والتوصيات التي تتوج بمجموعة من المبادئ التوجيهية الدولية لمكافحة الجريمة السيبرانية¹³ ، بغض النظر عن الحدود الوطنية فالتعاون الدولي أمر حاسم في مكافحة الجريمة السيبرانية نظرا لكونها مشكلة عالمية تتطلب حلاً شاملاً تحتاج فيه الدول إلى العمل معاً لتبادل المعلومات والخبرات والموارد لتحديد المجرمين الإلكترونيين والقبض عليهم، ومنع الهجمات الإلكترونية، وتقليل تأثير الجرائم الإلكترونية على الأفراد والمنظمات والحكومات، غير انه توجد بعض تحديات التي تواجه التعاون الدولي مثل قضايا الاختصاص القضائي والاختلافات الثقافية والحوازر اللغوية والاعتبارات السياسية، والتي يمكن معالجتها من خلال الحوار والتعاون وتطوير معايير وأطر مشتركة ، حيث سنفصل في ذلك على النحو التالي :

أولاً: أهمية التعاون الدولي في مكافحة الجرائم الإلكترونية

إن الجريمة الإلكترونية مشكلة عالمية تتطلب حلاً عالمياً، وذلك نظرا لأن مجرمي الإنترنت باستطاعتهم العمل من أي مكان في العالم، وغالباً ما يستخدمون تقنيات متطورة للهروب من الكشف والمقاضاة. لذلك فإن التعاون الدولي أمر حاسم لمكافحة هذه المشكلة لا غنى عنه، حيث يمكن للتعاون الدولي أن يساعد في تبادل المعلومات والخبرات والموارد لتحديد المجرمين الإلكترونيين والقبض عليهم

¹³ Cerezo, A. I., Lopez, J., & Patel, *International cooperation to fight transnational cybercrime. In Second international workshop on digital forensics and incident analysis (WDFIA 2007)* .p 13.

تهديد الجرائم الإلكترونية عبر الحدود: التحديات والاستراتيجيات الدولية لمواجهتها

ومنع الهجمات الإلكترونية، وبالتالي التقليل من تأثير الجرائم الإلكترونية على الأفراد والمنظمات والحكومات¹⁴.

ثانياً: طرق التعاون الدولي في مكافحة الجريمة السيبرانية

هناك عدة طرق يمكن للدول من خلالها العمل معاً لمكافحة الجريمة السيبرانية، وعليه سنحاول فيما يلي تحديد بعض الطرق الأكثر شيوعاً¹⁵:

- مشاركة المعلومات: يمكن للبلدان مشاركة المعلومات حول اتجاهات الجريمة السيبرانية والمجرمين الإلكترونيين والهجمات الإلكترونية، للمساعدة في تحديد الجرائم الإلكترونية ومنعها، حيث يتم مشاركة هذه المعلومات من خلال قنوات مختلفة مثل الإنترنت واليوروبول والمنظمات الإقليمية والدولية الأخرى¹⁶.
- التحقيقات المشتركة: يمكن للبلدان أن تتعاون في التحقيقات المشتركة لتعقب مجرمي الإنترنت وجمع الأدلة لمقاضاتهم، ويشمل ذلك المشاركة في الموارد والخبرات مثل تكنولوجيا الطب الشرعي الرقمي لمساعدة في تحديد وتعقب مجرمي الإنترنت¹⁷.
- تطوير معايير مشتركة: يمكن للبلدان العمل معاً لتطوير معايير مشتركة للأمن السيبراني وحماية البيانات، مما يساعد في إنشاء إطار عمل مشترك لمكافحة الجريمة السيبرانية وتعزيز الأمن السيبراني عبر الولايات القضائية المختلفة.
- بناء القدرات: يمكن للبلدان توفير برامج التدريب وبناء القدرات لتحسين خبرة الأمن السيبراني لوكالات إنفاذ القانون والمدعين العامين والقضاة، وهو ما يساعد في تعزيز قدرتها على اكتشاف جرائم الإنترنت والتحقيق فيها ومقاضاة مرتكبيها.

¹⁴فايزة هوام، حيدرة سعدي، آليات التعاون الدولي في مجال مكافحة جرائم الفساد، مجلة التواصل، المجلد 28،

العدد 01، جوان 2022، ص 170.

¹⁵إيمان بوقصبة، آليات التعاون الدولي لمكافحة الفساد، مجلة الآداب والعلوم الاجتماعية، المجلد 16، العدد 04،

2019، ص 153-156.

¹⁶إلياس عجابي، نحو إطار تشريعي فعال يكرس مبدأ التعاون الدولي في مكافحة الفساد، مجلة الاستاذ الباحث و

الدراسات القانونية والسياسية، العدد 09، المجلد 01، مارس 2018، ص 150.

¹⁷بلقاسم بريشي، محمد سي ناصر، التعاون الدولي في مجال تسليم المجرمين - دراسة تحليلية على ضوء

الاتفاقيات الدولية، مجلة المستقبل للدراسات القانونية والسياسية، المجلد 04، العدد 01، جوان 2020، ص 80.

تهديد الجرائم الإلكترونية عبر الحدود: التحديات والاستراتيجيات الدولية لمواجهتها

- **الإطار التشريعي:** يمكن للبلدان تطوير ومواءمة أطرها التشريعية لضمان أن قوانينها ولوائحها مواكبة لأحدث التطورات في التكنولوجيا والأمن السيبراني، وذلك من أجل توفير أساس قانوني قوي لمحاكمة قضايا الجرائم الإلكترونية.

ثالثاً: التحديات التي تواجه التعاون الدولي

في حين أن التعاون الدولي أمر حاسم في مكافحة الجريمة السيبرانية ، غير أنه توجد العديد من التحديات التي يواجهها التعاون الدولي ووضع مبادئ توجيهية دولية لمكافحة الجريمة السيبرانية العالمية عبر الحدود، فتوجد ضرورة أساسية لمواءمة القوانين الجنائية الداخلية للدول للمعاهدات والاتفاقيات الدولية، فضلاً عن إقرار قضايا الاختصاص القضائي المعقدة وتطوير إجراءات تعاون جديدة لمواجهة الجريمة السيبرانية ومداها وموقعها، فمن الضروري تحديد الجناة عبر الحدود في أي مكان في العالم، ثم التحقيق وتأمين الأدلة الإلكترونية على جرائمهم حتى تقديمهم إلى العدالة في أي ولاية قضائية متوافقة مع العدالة والامتثال لمعايير حقوق الإنسان، و لذلك تتمثل اهم التحديات في التي يجب معالجتها في ¹⁸:

1. **قضايا الاختصاص القضائي:** لدى الدول المختلفة قوانين ولوائح مختلفة تحكم الأمن السيبراني وحماية البيانات، يمكن أن يؤدي ذلك إلى خلق مشكلات تتعلق بالسلطة القضائية عند التحقيق في قضايا الجرائم الإلكترونية التي تتجاوز الحدود ومقاضاة مرتكبيها.
2. **الاختلافات الثقافية:** لدى البلدان المختلفة معايير ثقافية وأنظمة قانونية مختلفة، والتي يمكن أن تخلق تحديات في العمل معاً لمكافحة الجريمة السيبرانية.
3. **حواجز اللغة:** يمكن أن تخلق حواجز اللغة أيضاً تحديات في مشاركة المعلومات والخبرات بين مختلف البلدان.
4. **الاعتبارات السياسية:** يمكن للاعتبارات السياسية أيضاً أن تخلق تحديات في التعاون الدولي ، لا سيما في الحالات التي توجد فيها توترات سياسية أو دبلوماسية بين البلدان.

المبحث الثاني: استراتيجيات الأمن السيبراني

ان الاعتماد المتزايد على التكنولوجيا في العالم الحديث، رافقه أيضاً خطر التهديدات السيبرانية لذلك زادة الحاجة للأمن السيبراني الذي يعد ممارسة لحماية أنظمة الكمبيوتر والشبكات والمعلومات الحساسة من الوصول غير المصرح به أو السرقة أو التلف، وعليه سوف نناقش من خلال هذا المبحث اهم استراتيجيات التي تشكل هذه الممارسة سواء على مستوى الحكومات والمنظمات او على المستوى الفردي، بالإضافة إلى التقنيات الناشئة وتأثيرها على الأمن السيبراني.

¹⁸ Cerezo, A. I., Lopez, J, & Patel,, Previous reference, p 13.

المطلب الأول: استراتيجيات الأمن السيبراني للحكومات والمنظمات

تواجه الحكومات والمنظمات في جميع أنحاء العالم التحدي المتمثل في حماية أصولها ومعلوماتها من الهجمات الإلكترونية، لذلك سوف نخصص هذه الدراسة لنناقش بعض استراتيجيات الأمن السيبراني التي يمكن للحكومات والمنظمات استخدامها لحماية أنظمتها ومعلوماتها.

أولاً: اهم استراتيجيات الامن السيبراني للحكومات والمنظمات

على مدى السنوات العديدة الماضية نشرت العديد من الدول استراتيجيات وطنية للأمن السيبراني في محاولة لتحقيق أو تحسين وضع دولتهم بالنسبة للتهديدات الناشئة من الفضاء السيبراني كما نشرت مراكز الأبحاث والمنظمات الدولية وحتى الشركات الخاصة توصيات حول العناصر التي يجب تضمينها في هذه الاستراتيجيات السيبرانية، وتعد التوصيات الحالية بمثابة تحسين كبير مقارنة بالإرشادات الأصلية التي صدرت في أوائل العقد الأول من القرن الحادي والعشرين ، والتي دعت إلى أحد مسارين للعمل: إما إنشاء فريق الاستجابة لحوادث أمن الكمبيوتر أو إنشاء هيكل قانوني لمكافحة الجريمة السيبرانية وقد كشفت الأبحاث السابقة أن هذين النهجين غير كافيين ، خاصة بالنسبة للبلدان الناشئة ذات القدرات الفنية والإدارية المحدودة لذلك تضمن الإتجاه الدولي توصيات أكثر شمولاً واستراتيجيات منشورة مؤخراً لتحديد 15 عنصراً حاسماً يجب على الدول تضمينها عند وضع استراتيجية وطنية شاملة للأمن السيبراني، تغطي هذه توصيات قضايا السياسة العامة الرئيسية للأطر القانونية ، وبرامج التعليم العام ، والتنسيق السياسي جنباً إلى جنب مع التوصيات العملية والتقنية حول إنشاء المنتديات العامة والخاصة¹⁹، و تتمثل اهم استراتيجيات الامن السيبراني التي يجب على الحكومات و المنظمات العمل بها في:²⁰

1. **تقييم المخاطر:** تتمثل الخطوة الأولى في تطوير استراتيجية الأمن السيبراني في تحديد المخاطر وتقييمها، إذ تحتاج الحكومات والمنظمات إلى تقييم التهديدات المحتملة ونقاط الضعف التي يمكن أن تؤثر على أنظمتها ومعلوماتها. كما يتضمن ذلك تحديد البيانات الحساسة التي تحتاج إلى حماية والعواقب المحتملة لخرق.

¹⁹ Newmeyer, K. P, Elements of national cybersecurity strategy for developing nations. National Cybersecurity Institute Journal, 1(3), (2015), p 9.

²⁰ Ibid , p 10-15.

تهديد الجرائم الإلكترونية عبر الحدود: التحديات والاستراتيجيات الدولية لمواجهتها

2. **الإطار الأمني:** تحتاج الحكومات والمنظمات إلى تطوير إطار أمني شامل يتضمن سياسات وإجراءات ومبادئ توجيهية لحماية أنظمتها ومعلوماتها. ويجب أن يغطي إطار العمل الأمني جميع جوانب الأمن السيبراني ، بما في ذلك ضوابط الوصول وأمن الشبكة وتشفير البيانات والاستجابة للحوادث.
3. **تدريب الموظفين:** غالبًا ما يكون الموظفون هم الحلقة الأضعف في الأمن السيبراني، وعليه تحتاج الحكومات والمنظمات إلى توفير تدريب منتظم لموظفيها على أفضل ممارسات الأمن السيبراني، ويتضمن ذلك التدريب على كيفية التعرف على رسائل البريد الإلكتروني المخادعة وكيفية إنشاء كلمات مرور قوية وكيفية الإبلاغ عن الأنشطة المشبوهة.
4. **تحديثات منتظمة:** تحتاج الحكومات والمؤسسات إلى التأكد من أن أنظمتها وبرامجها محدثة بأحدث تصحيحات الأمان والتحديثات، وهما سيساعد في التخفيف من مخاطر الثغرات الأمنية المعروفة التي يمكن لمجرمي الإنترنت استغلالها.
5. **خطة الاستجابة للحوادث:** يتعين على الحكومات والمنظمات أن يكون لديها خطة محددة جيدًا للاستجابة للحوادث للتعامل مع الهجمات الإلكترونية، حيث يجب عليها أن تحدد خطة ودور و مسؤولية كل عضو في الفريق ، وإجراءات احتواء الهجوم مع الخطوات السريعة لاستعادة الأنظمة والبيانات.
6. **النسخ الاحتياطي والاسترداد:** تحتاج الحكومات والمنظمات إلى وجود نظام نسخ احتياطي واسترداد قوي، وهذا يضمن أنه في حالة وقوع هجوم إلكتروني يمكنهم استعادة بياناتهم وأنظمتهم بسرعة.

ثانيا: التحديات في تنفيذ استراتيجيات الأمن السيبراني

تميل نقاط الضعف المتأصلة في الفضاء الإلكتروني والهجمات الإلكترونية المتصاعدة باستمرار إلى تهديد الأمن القومي والاقتصادي والحياة اليومية للمواطنين، ولذلك قامت أكثر من معظم الدولة حول العالم بصياغة استراتيجياتها للأمن السيبراني لمعالجة المخاوف الخطيرة المترتبة عن تفاقم الجرائم الإلكترونية، وتهدف إستراتيجية الأمن السيبراني بشكل خاص إلى تأمين الفضاء الإلكتروني الوطني من نواقل التهديد السيبراني الحاقدة، ولكن نظرًا لتنوع مشهد التهديدات إذ يمكن رؤية اختلافات كبيرة في الإجراءات والنهج الوقائية والدفاعية والهجومية المعتمدة من قبل كل الدول والمنظمات²¹، ولكن رغم هذه

²¹ Shafqat, N, & Masood, A, *Comparative analysis of various national cyber security strategies*. International Journal of Computer Science and Information Security, 14(1), (2016) , p 129.

تهديد الجرائم الإلكترونية عبر الحدود: التحديات والاستراتيجيات الدولية لمواجهتها

الإختلافات فإن التحديات التي تواجهها الحكومات والمنظمات متشابهة لحد بعيد والتي يمكن أن تشمل كل من²² :

1. **التكلفة:** قد يكون تنفيذ استراتيجيات الأمن السيبراني مكلفاً، وتحتاج الحكومات والمنظمات إلى تخصيص موارد كافية لمواجهة مخاطر الأمن السيبراني.
 2. **قيود الموارد:** قد لا تمتلك الحكومات والمنظمات الموارد أو الخبرة اللازمة لتنفيذ استراتيجيات الأمن السيبراني بشكل فعال.
 3. **قلة الوعي:** لا يدرك العديد من الموظفين مخاطر وعواقب الهجمات الإلكترونية، حيث تحتاج الحكومات والمنظمات إلى تثقيف موظفيها حول مخاطر الأمن السيبراني وكيفية التخفيف منها.
 4. **تغيير مشهد التهديد:** يتطور مشهد التهديدات باستمرار، مما يتطلب من الحكومات والمنظمات تكيف استراتيجيات الأمن السيبراني الخاصة بها لمواجهة التهديدات الجديدة.
- وفي الأخير فإن الأمن السيبراني هو قضية حاسمة تحتاج الحكومات والمنظمات لمعالجتها في سبيل حماية أنظمتها ومعلوماتها من التهديدات السيبرانية، لذلك يعد تنفيذ استراتيجية شاملة للأمن السيبراني أمراً ضرورياً للتخفيف من مخاطر الجرائم الإلكترونية .
- و بناءاً عليه تحتاج الحكومات والمنظمات إلى إجراء تقييمات منتظمة للمخاطر وتطوير إطار أمني لها ، وتوفير تدريب للموظفين ، والحفاظ على تحديث الأنظمة والبرامج ، ووضع خطة للاستجابة للحوادث ، وأنظمة النسخ الاحتياطي والاسترداد، في حين أن هناك تحديات في تنفيذ استراتيجيات الأمن السيبراني ، يمكن التغلب عليها من خلال الموارد الكافية والوعي والتكيف مع مشهد التهديد المتغير .

المطلب الثاني: استراتيجيات الأمن السيبراني الفردية

في العصر الرقمي الحالي يقوم الأفراد بتخزين المعلومات الشخصية ومشاركتها عبر الإنترنت مما يجعلهم عرضة للهجمات الإلكترونية، حيث يستخدم مجرمو الإنترنت مجموعة متنوعة من التقنيات لاستغلال الثغرات الأمنية في أجهزة وشبكات الأفراد مثل هجمات التصيد والبرامج الضارة والهندسة الاجتماعية، لذلك من الضروري للأفراد تنفيذ استراتيجيات الأمن السيبراني لحماية معلوماتهم الشخصية ومن أهم هذه الاستراتيجيات مايلي²³ :

أولاً: استخدام كلمات مرور قوية

²² Santos, H., Pereira, T., & Mendes, I .*Challenges and reflections in designing cyber security curriculum*. In 2017 IEEE World Engineering Education Conference (EDUNINE) ,(2017, March), p47-51.

²³ Ibid , p60

تهديد الجرائم الإلكترونية عبر الحدود: التحديات والاستراتيجيات الدولية لمواجهتها

من أبسط الطرق وأكثرها فعالية لحماية المعلومات الشخصية استخدام كلمات مرور قوية و يجب أن تتكون كلمة المرور القوية من ثمانية أحرف على الأقل ، وتتضمن مجموعة من الأحرف الكبيرة والصغيرة والأرقام والرموز ، ويجب ألا تتضمن أي معلومات شخصية أو كلمات قاموس. علاوة على ذلك يجب على الأفراد تجنب استخدام نفس كلمة المرور لحسابات متعددة.

ثانيا: الحفاظ على تحديث البرامج وأنظمة التشغيل

يعد تحديث البرامج وأنظمة التشغيل أمراً بالغ الأهمية في منع الهجمات الإلكترونية، إذ يصدر بائعو البرامج بانتظام تحديثات تعمل على إصلاح الثغرات الأمنية والأخطاء التي يمكن لمجرمي الإنترنت استغلالها، لذلك يجب على الأفراد التأكد من قيامهم بتحديث برامجهم وأنظمة التشغيل الخاصة بهم بانتظام لمنع الهجمات الإلكترونية.

ثالثا: استخدام المصادقة الثنائية

تضيف المصادقة الثنائية (FA2) طبقة إضافية من الأمان لحسابات الأفراد، فيطلب من الأفراد تقديم جزء إضافي من المعلومات مثل رمز يتم إرساله إلى أجهزتهم المحمولة، بالإضافة إلى كلمة المرور الخاصة بهم للوصول إلى حساباتهم ، و هذا يجعل من الصعب على مجرمي الإنترنت الوصول إلى حسابات الأفراد حتى لو كانت لديهم كلمة المرور الخاصة بهم²⁴.

رابعا: تجنب شبكات Wi-Fi العامة

غالبًا ما تكون شبكات Wi-Fi العامة غير آمنة ويمكن لمجرمي الإنترنت استغلالها للوصول إلى أجهزة الأفراد والمعلومات الشخصية، لذلك يجب على الأفراد تجنب الاتصال بشبكات Wi-Fi العامة خاصة عند الوصول إلى معلومات حساسة مثل الخدمات المصرفية عبر الإنترنت أو البريد الإلكتروني.

خامسا: الحذر من عمليات التصيد الاحتيالي

تعتبر عمليات التصيد الاحتيالي أسلوبًا شائعًا يستخدمه مجرمو الإنترنت لخداع الأفراد للكشف عن معلوماتهم الشخصية ، لذلك فالتصيد الاحتيالي هو شكل من أشكال سرقة الهوية عبر الإنترنت يهدف إلى سرقة المعلومات الحساسة مثل كلمات مرور الخدمات المصرفية عبر الإنترنت ومعلومات بطاقة الائتمان من المستخدمين، لذلك قد حظيت عمليات التصيد الاحتيالي بتغطية صحفية واسعة النطاق لأن مثل هذه الهجمات تصاعدت من حيث العدد والتعقيد، و يمكن أن تأتي حيل التصيد الاحتيالي في شكل رسائل بريد

²⁴ Kirda, E., & Kruegel, C, *Protecting users against phishing attacks with antiphish*. In 29th Annual International Computer Software and Applications Conference (COMPSAC'05) , Vol. 1, (2005, July), p 515.

تهديد الجرائم الإلكترونية عبر الحدود: التحديات والاستراتيجيات الدولية لمواجهتها

إلكترونى مزيفة أو رسائل نصية أو مكالمات هاتفية تبدو وكأنها من مصادر مشروعة، فيجب على الأفراد دائماً توخي الحذر من الرسائل غير المرغوب فيها وتجنب النقر فوق الروابط أو تنزيل المرفقات من مصادر غير معروفة²⁵.

سادساً: استخدام الشبكات الخاصة الافتراضية (VPN)

تقوم الشبكات الافتراضية الخاصة (VPN) بتشفير حركة مرور الأفراد على الإنترنت ، مما يجعل من الصعب على مجرمي الإنترنت اعتراض وسرقة المعلومات الشخصية. بالإضافة الى ذلك تعد شبكات VPN مفيدة بشكل خاص عند استخدام شبكات Wi-Fi العامة أو عند الوصول إلى معلومات حساسة مثل الخدمات المصرفية عبر الإنترنت.

لذلك قد أصبحت الشبكات الخاصة الافتراضية VPN وسيلة اتصال للوصول إلى المعلومات وتبادل البيانات وتدفق المعلومات، ولهذا تتطلب العديد من المؤسسات شبكة إنترنت أو VPN للوصول إلى البيانات والوصول إلى الخوادم من أجهزة الكمبيوتر ومشاركة أنواع مختلفة من البيانات بين مكاتبها ومستخدميها ، فتعد بيئة VPN الأمانة ضرورية للمؤسسات لحماية المعلومات والبنية التحتية لتكنولوجيا المعلومات وأصولها²⁶.

وفي الختام ، يعد الأمن السيبراني جانباً أساسياً من الحياة الرقمية فيمكن أن يكون للهجمات الإلكترونية عواقب وخيمة على حياة الأفراد الشخصية والمالية لذلك يجب على الأفراد اتخاذ تدابير استباقية لحماية معلوماتهم الشخصية ، و الاستراتيجيات التي تمت مناقشتها طرق بسيطة و فعالة لتقوية دفاعات الأمن السيبراني للأفراد، فمن خلال استخدام هذه الاستراتيجيات يمكن للأفراد تقليل مخاطر الوقوع ضحية للهجمات الإلكترونية.

المطلب الثالث: التقنيات الناشئة وتأثيرها على الأمن السيبراني

في السنوات الأخيرة أدى التقدم السريع في التكنولوجيا إلى إحداث تغييرات كبيرة في مختلف المجالات، حيث أحدثت التقنيات الناشئة مثل الذكاء الاصطناعي (AI) والتعلم الآلي (ML) و blockchain وإنترنت الأشياء (IoT) والحوسبة السحابية ثورة في العالم الرقمي، و في حين أن هذه

²⁵ Kirda, E., & Kruegel, C, *Previous reference*, p 517.

²⁶ Pedapudi, S. M., & Vadlamani, N, *A Comprehensive Network Security Management in Virtual Private Network Environment*. In 2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC), (2022, May), p1362.

تهديد الجرائم الإلكترونية عبر الحدود: التحديات والاستراتيجيات الدولية لمواجهتها

التقنيات قد جلبت العديد من الفوائد إلا أنها خلقت أيضاً تحديات جديدة فيما يتعلق بالأمن السيبراني²⁷، وبناءاً عليه تستكشف هذه الجزئية تأثير التقنيات الناشئة على الأمن السيبراني من خلال مايلي:

أولاً: الذكاء الاصطناعي (AI) والتعلم الآلي (ML)

ظهر الذكاء الاصطناعي والتعلم الآلي كأدوات قوية لتعزيز الأمن السيبراني، فيمكن لهذه التقنيات اكتشاف الهجمات الإلكترونية والاستجابة لها في الوقت الفعلي، كما يمكن للذكاء الاصطناعي أيضاً تحديد نقاط الضعف المحتملة وتطوير استراتيجيات للتحقق منها، ويعمل التعلم الآلي على تحليل كميات هائلة من البيانات وتحديد الأنماط لاكتشاف الحالات الشاذة التي قد تشير إلى الهجمات الإلكترونية، ولذلك هناك مجموعة واسعة من التقاطعات متعددة التخصصات بين الأمن السيبراني والذكاء الاصطناعي (AI) فمن ناحية يمكن إدخال تقنيات الذكاء الاصطناعي مثل التعلم العميق في الأمن السيبراني لإنشاء نماذج ذكية لتنفيذ تصنيف البرامج الضارة واكتشاف التسلل واستشعار التهديدات الاستخباراتية، و من ناحية أخرى ستواجه نماذج الذكاء الاصطناعي العديد من التهديدات السيبرانية ، والتي ستزعج عينتها وتعلمها وقراراتها ، و بالتالي تحتاج نماذج الذكاء الاصطناعي إلى تقنيات محددة للدفاع والحماية للأمن السيبراني وذلك لمكافحة التعلم الآلي العدائي ، والحفاظ على الخصوصية في التعلم الآلي ، والتعلم الفيدرالي الأمن²⁸، ومع ذلك يمكن أن يكون الذكاء الاصطناعي والتعلم الآلي عرضة للهجمات الإلكترونية، حيث يمكن للقراصنة التلاعب بخوارزميات الذكاء الاصطناعي والتعلم الآلي لخلق إيجابيات أو سلبيات كاذبة مما يؤدي إلى نتائج غير دقيقة، لذلك كان من الضروري وجود تدابير أمنية قوية لحماية هذه التقنيات.

ثانياً: بلوك تشين

تتمتع تقنية Blockchain بإمكانية إحداث ثورة في الأمن السيبراني من خلال توفير نظام لامركزي يضمن معاملات آمنة، ينشئ Blockchain دفتر عام يسجل جميع المعاملات بطريقة آمنة وشفافة، فيصعب اختراق هذه التقنية لأنها تتطلب إجماعاً من جميع المشاركين في الشبكة لتغيير دفتر ، بالإضافة إلى ذلك يمكن استخدام blockchain لحماية البيانات الحساسة من خلال توفير طريقة آمنة لتخزين المعلومات ونقلها، ومع ذلك فإن blockchain ليست محصنة ضد الهجمات الإلكترونية فيمكن للقراصنة استغلال الثغرات الأمنية في البرنامج ويمكن اختراق الشبكة إذا وافق غالبية المشاركين على إجراء تغييرات على دفتر .

²⁷ Pedapudi, S. M., & Vadlamani, N ,*Previous reference* , p1377

²⁸ Li, J. H ,*Cyber security meets artificial intelligence: a survey. Frontiers of Information Technology & Electronic Engineering*, 19(12), (2022, May), p 1462.

تهديد الجرائم الإلكترونية عبر الحدود: التحديات والاستراتيجيات الدولية لمواجهتها

فتقدم Blockchain نهجًا مبتكرًا لتخزين المعلومات وتنفيذ المعاملات وأداء الوظائف وبناء الثقة في بيئة مفتوحة حيث يعتبر الكثيرون blockchain بمثابة اختراق تقني للتشفير والأمن السيبراني مع حالات استخدام تتراوح من أنظمة العملات المشفرة المنتشرة عالميًا مثل Bitcoin ، إلى العقود الذكية والشبكات الذكية عبر إنترنت الأشياء وما إلى ذلك، ولكن على الرغم من أن blockchain قد تلقى اهتمامًا متزايدًا في كل من الأوساط الأكاديمية والصناعية في السنوات الأخيرة إلا أن أمان وخصوصية blockchain لا يزالان في قلب النقاش عند نشر blockchain في تطبيقات مختلفة²⁹.

ثالثًا: إنترنت الأشياء (IoT)

إنترنت الأشياء هي شبكة من الأجهزة المترابطة التي تجمع البيانات وتشاركها، فقد أحدثت هذه التكنولوجيا ثورة في الطريقة التي نعيش ونعمل بها لذلك كانت هناك زيادة في استخدام إنترنت الأشياء (IoT) في العالم، والتي أصبحت مؤخرًا مجال اهتمام متزايد حيث يتم استخدامها على نطاق واسع للعديد من التطبيقات والأجهزة مثل أجهزة الاستشعار اللاسلكية والأجهزة الطبية وأجهزة الاستشعار المنزلية الحساسة وغيرها أجهزة إنترنت الأشياء ذات الصلة، و نظرًا للطلب على طرح منتجات إنترنت الأشياء الجديدة بسرعة في السوق غالبًا ما يتم التغاضي عن الجوانب الأمنية حيث يستغرق الأمر وقتًا للتحقيق في جميع نقاط الضعف المحتملة ، وهذا لأن أجهزة إنترنت الأشياء تعتمد على الإنترنت وتتضمن معلومات حساسة وسرية و بالتالي أثارت مخاوف أمنية³⁰ بشأنها ، وذلك لأن أجهزة إنترنت الأشياء معرضة للهجمات السيبرانية كثيرًا كونها تفتقر إلى التدابير الأمنية اللازمة، و يمكن للقراصنة استخدام أجهزة إنترنت الأشياء للوصول إلى الشبكات وسرقة المعلومات الحساسة، بالإضافة إلى ذلك فإنه يمكن التلاعب بأجهزة إنترنت الأشياء لأداء أنشطة ضارة مثل إطلاق هجمات رفض الخدمة الموزعة (DDoS) و عليه كان من الضروري وجود تدابير أمنية قوية لحماية أجهزة إنترنت الأشياء.

رابعًا: حوسبة سحابية

الحوسبة السحابية هي نموذج تكنولوجي ناشئ ينقل المفاهيم التكنولوجية والحاسوبية الحالية إلى حلول شبيهة بالمرافق مشابهة لأنظمة الكهرباء والمياه، تقدم السحابة مجموعة واسعة من الفوائد بما في ذلك موارد الحوسبة القابلة للتكوين، والمدخرات الاقتصادية ، ومرونة الخدمة، ومن هنا أصبحت الحوسبة

²⁹ Zhang, R., Xue, R., & Liu, L, *Security and privacy on blockchain*. ACM Computing Surveys (CSUR), 52(3), (2019), p 1.

³⁰ Al Hayajneh, A., Bhuiyan, M. Z. A., & McAndrew, I, *Improving Internet of Things (IoT) security with software-defined networking (SDN)*. Computers, 9(1), (2020), p 8.

تهديد الجرائم الإلكترونية عبر الحدود: التحديات والاستراتيجيات الدولية لمواجهتها

السحابية تقنية أساسية للشركات والأفراد على حد سواء ، فتتيح الحوسبة السحابية للمستخدمين تخزين البيانات والوصول إليها عبر الإنترنت ، مما يجعلها أكثر ملاءمة وسهولة الوصول إليها ، ومع ذلك فإن الحوسبة السحابية معرضة للهجمات الإلكترونية ، و يمكن للقراصنة استغلال الثغرات الأمنية في البرنامج للوصول إلى البيانات الحساسة³¹ ، بالإضافة إلى ذلك قد لا يكون لدى موفري الحوسبة السحابية دائماً تدابير أمنية قوية ، مما قد يؤدي إلى انتهاكات للبيانات و لذلك فمن الضروري وجود تدابير أمنية قوية لحماية أنظمة الحوسبة السحابية.

وفي الأخير نرى ان التقنيات الناشئة قد جلبت العديد من الفوائد للعالم الرقمي، غير انها في مقابل ذلك خلقت تحديات جديدة من حيث الأمن السيبراني و لذلك كان من الضروري وجود تدابير أمنية قوية لحماية هذه التقنيات.

فرغم امكانية استخدام الذكاء الاصطناعي والتعلم الآلي لتعزيز الأمن السيبراني ، لكنهما قد يكونان أيضاً عرضة للهجمات السيبرانية، إضافة إلى ذلك يمكن أن توفر Blockchain طريقة آمنة لتخزين البيانات ونقلها، ولكنها ليست محصنة ايضاً ضد الهجمات الإلكترونية، كما يمكن أن تكون أجهزة إنترنت الأشياء عرضة للهجمات السيبرانية لأنها غالباً ما تفتقر إلى التدابير الأمنية اللازمة ، وعليه يمكن القول أنه و لضمان حماية اللازمة لهذه التقنيات وضمان سلامة المعلومات الحساسة، يجب أن تتضافر جهود المجتمع الدولي و المنظمات الدولية لإيجاد الآليات والتدابير الأمنية القوية و ذات فعالية في مواجهة الهجمات السيبرانية.

الخاتمة :

نظراً لأن العالم أصبح مترابطاً بشكل متزايد استمر خطر الجرائم الإلكترونية في النمو مما أثر على الأفراد والشركات والحكومات على حد سواء، وعلى الرغم من التحديات أثبت التعاون الدولي على أنه أداة فاعلة في مكافحة الجرائم الإلكترونية، ففي السنوات التي أعقبت نشر "مكافحة الجرائم الإلكترونية على المستوى الدولي"، قطع المجتمع العالمي خطوات كبيرة في تعزيز الأمن السيبراني ومكافحة التهديدات السيبرانية، فعملت الحكومات معاً لتبادل المعلومات الاستخباراتية وتنسيق التحقيقات وتطوير قوانين وأنظمة جديدة لمواجهة التهديدات الناشئة، كما حسّنت وكالات تنفيذ القانون قدراتها على تعقب مجرمي الإنترنت، ولعبت المنظمات الدولية مثل الأمم المتحدة والإنتربول دوراً متزايد الأهمية في تسهيل التعاون العالمي بشأن قضايا الأمن السيبراني.

³¹ Carlin, S., & Curran, K ,*Cloud computing security. In Pervasive and Ubiquitous Technology Innovations for Ambient Intelligence Environments. IGI Global, (2013), p 12.*

تهديد الجرائم الإلكترونية عبر الحدود: التحديات والاستراتيجيات الدولية لمواجهتها

وفي حين أن مكافحة الجرائم الإلكترونية لم تنته بعد، ساعدت الدروس المستفادة من النجاحات والإخفاقات السابقة في تمهيد الطريق لعالم رقمي أكثر أماناً ومرونة، ومع استمرار الأفراد والمنظمات في التكيف مع مشهد التهديدات المتطورة ، ستظل أهمية التعاون الدولي في مكافحة الجرائم الإلكترونية دائماً على نفس القدر من الأهمية .

ومن خلال هذه الورقة البحثية يمكن ان نقدم جملة من التوصيات لمكافحة الجرائم الإلكترونية على المستوى الدولي وذلك باتباع نهج منسق ومتعدد الأوجه يتضمن التعاون بين الحكومات ووكالات تنفيذ القانون والشركات الخاصة والجمهور، و فيما يلي بعض التوصيات لمكافحة الجريمة السيبرانية على المستوى الدولي:

- تعزيز التعاون الدولي؛ فيجب على الحكومات العمل معاً لتبادل المعلومات والاستخبارات حول التهديدات السيبرانية وتنسيق التحقيقات، وتطوير قوانين ولوائح جديدة لمواجهة التهديدات الناشئة، كما يجب أن تستمر المنظمات الدولية مثل الأمم المتحدة والإنتربول في لعب دور نشط في تسهيل التعاون العالمي بشأن قضايا الأمن السيبراني.
- تطوير قوة عاملة ماهرة ؛ فيجب أن تعمل الحكومات والصناعات الخاصة معاً لتطوير قوة عاملة ماهرة من خبراء الأمن السيبراني الذين يمكنهم المساعدة في منع التهديدات السيبرانية والاستجابة لها ويشمل ذلك الاستثمار في برامج التعليم والتدريب، فضلاً عن تعزيز الشراكات بين الأوساط الأكاديمية والصناعية والحكومية.
- زيادة الوعي العام؛ فرفع مستوى الوعي العام حول مخاطر الجرائم الإلكترونية أمر ضروري للحد من انتشارها، إذ يجب أن تعمل الحكومات والصناعات الخاصة معاً لتثقيف الجمهور حول أهمية ممارسات الأمن السيبراني الجيدة مثل استخدام كلمات مرور قوية، وتحديث البرامج باستمرار، وتوخي الحذر عند النقر على الروابط أو تنزيل المرفقات
- تطوير المعايير الدولية ؛ فيمكن أن يساعد تطوير المعايير الدولية للأمن السيبراني في تعزيز الاتساق وأفضل الممارسات عبر مختلف البلدان والمناطق، ويتضمن ذلك معايير تطوير البرامج الآمنة وحماية البيانات والاستجابة للحوادث.
- تعزيز البنية التحتية الحيوية فيجب أن تعمل الحكومات والصناعات الخاصة معاً لتحديد وحماية البنية التحتية الحيوية مثل شبكات الطاقة وأنظمة النقل والشبكات المالية من التهديدات السيبرانية، وهذا يشمل الاستثمار في تكنولوجيا الأمن السيبراني وتدريب أولئك الذين يقومون بتشغيل وصيانة البنية التحتية الحيوية.

تهديد الجرائم الإلكترونية عبر الحدود: التحديات والاستراتيجيات الدولية لمواجهتها

- تعزيز المعايير الدولية فيمكن أن يساعد تطوير معايير وقواعد سلوك دولية للفضاء الإلكتروني على تعزيز السلوك المسؤول وردع الجهات الخبيثة، وهذا يشمل تعزيز سلوك الدولة المسؤول ، وحماية حقوق الإنسان على الإنترنت ، وضمان تطبيق القانون الدولي على الفضاء السيبراني. ومن خلال اتخاذ هذه الخطوات يمكن للحكومات ووكالات الدولية العمل معاً لمكافحة الجريمة الإلكترونية على المستوى الدولي وإنشاء عالم رقمي أكثر أمناً وأماناً، وذلك عن طريق تنفيذ المعاهدات و الاتفاقيات الدولية و ماتضمنته من آليات و تدابير لمواجهة الهجمات السببرانية.

قائمة المصادر والمراجع:

أولاً: الاتفاقيات:

- 1- الاتفاقية المتعلقة بالجريمة الإلكترونية (بودابست)، الصادرة عن مجلس أوروبا "مجموعة المعاهدات الأوروبية رقم 175"، المؤرخة في 2001/11/23.
- 2- اتفاقية الامم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، اعتمدت بموجب قرار الجمعية العامة للأمم المتحدة 55/25، المؤرخة في 15 نوفمبر 2000.
- 3- توجيهات الاتحاد الأوروبي بشأن الهجمات على أنظمة المعلومات، الصادر عن البرلمان الأوروبي ومجلس الاتحاد الأوروبي، المؤرخ في 2016/06/06.

ثانياً: المقالات:

- 1- إيمان بوقصبة، آليات التعاون الدولي لمكافحة الفساد، مجلة الآداب والعلوم الإجتماعية، المجلد 16، العدد 04، 2019.
- 2- إلياس عجابي، نحو إطار تشريعي فعال يكرس مبدأ التعاون الدولي في مكافحة الفساد، مجلة الاستاذ الباحث و الدراسات القانونية والسياسية، العدد 09، المجلد 01، مارس 2018.
- 3- بلقاسم بريشي، محمد سي ناصر، التعاون الدولي في مجال تسليم المجرمين - دراسة تحليلية على ضوء الاتفاقيات الدولية، مجلة المستقبل للدراسات القانونية والسياسية، المجلد 04، العدد 01، جوان 2020
- 4- فايزة هوام، حيدرة سعدي، آليات التعاون الدولي في مجال مكافحة جرائم الفساد، مجلة التواصل، المجلد 28، العدد 01، جوان 2022.

ثالثاً: المواقع الانترنت:

تهديد الجرائم الإلكترونية عبر الحدود: التحديات والاستراتيجيات الدولية لمواجهتها

1- ثامري عمر، التعاون الدولي في مكافحة الفساد، مداخلة منشورة في الموقع مداخلة كاملة أ.

ثامري.pdf. تم الإطلاع عليها يوم الأحد 2023/05/26 على الساعة 12:00.

Articles :

1. Al Hayajneh, A., Bhuiyan, M. Z. A., & McAndrew, I, **Improving Internet of Things (IoT) security with software-defined networking (SDN)**. Computers, 9(1), (2020).
2. Betti, S. **New prospects for inter-state co-operation in criminal matters: The Palermo Convention**, International Criminal Law Review, 3(2), (2003).
3. Carlin, S., & Curran, K ,**Cloud computing security**. In Pervasive and Ubiquitous Technology Innovations for Ambient Intelligence Environments. IGI Global, (2013).
4. Cerezo, A. I., Lopez, J., & Patel, **International cooperation to fight transnational cybercrime**. In Second international workshop on digital forensics and incident analysis (WDFIA 2007).
5. Clough, J. **A world of difference: The Budapest convention on Cybercrime and the challenges of Harmonisation**, Monash University Law Review, 40(3), (2014).
6. Foggetti, N ,**Transnational cyber crime, differences between national laws and development of European legislation: by repression?**. Masaryk University journal of Law and technology, 2(2), (2008).
7. Gordon, S., & Ford, **On the definition and classification of cybercrime**, Journal in computer virology, 2, R. (2006).
8. Kirda, E., & Kruegel, C, **Protecting users against phishing attacks with antiphish**. In 29th Annual International Computer Software and Applications Conference (COMPSAC'05) , Vol. 1, (July, 2005).
9. Ledingham, R., & Mills, R. **A preliminary study of autism and cybercrime in the context of international law enforcement**, Advances in Autism, 1(1), (2015).
10. Li, J. H ,**Cyber security meets artificial intelligence: a survey**. Frontiers of Information Technology & Electronic Engineering, 19(12), (May, 2022).
11. Michalec, O., Van Der Linden, D., Milyaeva, S., & Rashid, A. ,**Industry responses to the european directive on security of network and information systems (NIS) understanding policy implementation practices across critical infrastructures**. In Proceedings of the Sixteenth USENIX Conference on Usable Privacy and Security.
12. Newmeyer, K. P, **Elements of national cybersecurity strategy for developing nations**. National Cybersecurity Institute Journal, 1(3), (2015).
13. Pedapudi, S. M., & Vadlamani, N, **A Comprehensive Network Security Management in Virtual Private Network Environment**. In 2022 International



- Conference on Applied Artificial Intelligence and Computing (ICAAIC), (May, 2022).
14. Santos, H., Pereira, T., & Mendes, I, **Challenges and reflections in designing cyber security curriculum.** In 2017 IEEE World Engineering Education Conference (EDUNINE) ,(March, 2017).
15. Shafqat, N., & Masood, A, **Comparative analysis of various national cyber security strategies.** International Journal of Computer Science and Information Security, 14(1), (2016).
16. Weber, A. M, **The council of Europe's convention on cybercrime,** Berkeley Technology Law Journal, 18(1), (2003).
17. Zhang, R., Xue, R., & Liu, L, **Security and privacy on blockchain.** ACM Computing Surveys (CSUR), 52(3), (2019)