PISSN : 2572-0007 - EISSN : 2661-7250

الجريمة السيبرية والجهود الدولية لمكافحتها

Cyber crime and international efforts to combat it

نعيمة حاجي

جامعة العربي التبسي ـ تبسة (الجزائر)، naima.hadji@univ-tebessa.dz

تاريخ الاستلام: 10/ 05 / 2021 تاريخ القبول: 08/ 08 / 2021 تاريخ النشر: 25/ 08 / 2021

ملخص:

يعتبر الفضاء الالكتروني أو السيبري مجالا لتوسعة الخدمات والمعاملات والأنشطة ووصولها إلى أكبر عدد من الأشخاص والتجمعات في جميع دول العالم، متجاوزا حدود الزمان والمكان، إلا أنه لا يخلو من المخاطر، نتيجة القرصنة الإلكترونية والاختراقات التي تعرف بالجريمة السيبرية.

وكلما تطور النشاط الإلكتروني تطور النشاط الإجرامي، وبالمقابل تطورت معه أساليب مكافحته، بهدف توفير أكبر قدر من الحماية والأمان، وضمان الاستخدام الآمن للفضاء السيبري، الأمر الذي أدى إلى ضرورة التعاون الدولي والإقليمي لمواجهتها، والذي يفرضه الطابع العالمي للجريمة السيبرية.

الكلمات المفتاحية: اختراق؛ جريمة؛ سيبراني؛ سيبري؛ قرصنة؛ هاكر.

***

Abstract:

The electronic or cyber space is a field for expanding services, transactions and activities and reaching the largest number of people and gatherings in all countries of the world, exceeding the limits of time and space, but it is not without risks, as a result of electronic piracy and breaches known as cybercrime.

As electronic activity develops, criminal activity develops, and in return, methods of combating it have evolved, with the aim of providing greater protection and security, and ensuring the safe use of cyberspace, which led to the need for international and regional cooperation to confront it, which is imposed by the global character of cybercrime.

Keywords: Breakthrough; e-crime; Electronic; cyber; hacking; Transnational.

مقدمة

أدى الانتشار السريع للحواسيب الإلكترونية والإنترنيت في العالم كله إلى خلق فرص جديدة للنشاط البشري، وزادت تقنية المعلومات في قوة البشر، كما فتحت تلك التقنية الباب أمام المجرمين ليرتكبوا جرائم سيبرية على صعيد دولي، وقد جرى تطور نوع جديد من الرصد والتحقيق الجنائي لمحاربة الجرائم التقنية يعرف باسم **"العلم الجنائي المعلوماتي"**، ويعمل المحققون السيبيريون والشرطة الإلكترونية على رصد قراصنة ولصوص الإنترنيت، وتشمل الجرائم السيبرية كمّا كبيرا من النشاطات الإجرامية، بداية من عمليات النصب المصرفية والائتمانية، مرورا بالتخريب الإلكتروني وصولا إلى اهتمام القراصنة بالتجسس الصناعي والإرهاب، إلا أن كل جريمة ينفذها مجرمون تقنيون تقابَل بخبراء معلوماتية يراقبون شبكة الانترنيت.

وبالتالي فإن هذه الدراسة تنطلق من الإجابة على الإشكالية التالية: **ما هي الأبعاد المختلفة للجريمة السيبرية ؟ وإلى أي مدى يمكن تقييم الجهود الإقليمية والدولية في التصدي لها والحد منها؟**

وقد استندت هذه الدراسة على ثلاثة فرضيات، كالتالي:

الفرضية الأولى: فرص المجرمين في تنفيذ أفعالهم والإفلات من المساءلة القانونية يرتبط بقوة حواسيبهم الإلكترونية ومهاراتهم في استعمالها.

الفرضية الثانية: أهم عامل يعتمد عليه مجرمو الإنترنيت هو **الهوية المجهولة**، فلا يمكن التعرف على الشخص الذي يعرض أو يطلب خدمة الكترونية مثلا أنه محتال وأن عمله غير شرعي، أو أنه ليس زبونا حقيقيا حتى، وفي بعض الأحيان فإنه لا يكون مجهول الهوية وحسب خلال ارتكاب جريمته بل يستحيل تتبعه أيضا، وبالتالي فإن فرص نجاح عمليات ملاحقة قانونية لهؤلاء المجرمين عبر الحدود ضئيلة جدا، خاصة وأن آلية العمل بين الأجهزة الأمنية ـ والتي تعمل تحت سقف قوانين الدول ـ تحدها في أغلب الأحيان السياسة الداخلية للدولة، إضافة إلى الطابع العالمي لشبكة الإنترنيت، حيث لا تتوفر قوى أمنية وطنية أو دولية لمكافحة الجرائم الإلكترونية، وغالبا ما تكون هذه الجرائم خالية من المخاطرة بالنسبة للمجرمين، كونها تنفذ عن بعد، كما أن عائداتها ضخمة في كثير من الأحيان بالنسبة لمرتكبيها، وبالمقابل فهي تخلف أضرارا جسيمة بالنسبة للضحايا.

الفرضية الثالثة: الجريمة السيبرية جريمة عابرة للحدود في الكثير من الحيان، حيث أنها ترتكب ضمن الفضاء السيبري الذي لا يخضع لحدود الزمان والمكان، مما يستدعي ضرورة تكثيف الجهود الدولية لمكافحتها والحد منها، ولأن هذا النوع من الجرائم يكون باستخدام شبكة الإنترنيت العالمية، فإن الجريمة المرتكبة عبرها هي جريمة عالمية، أو كما أصطلح عليه بالجريمة العبر وطنية، ثم أن التكنولوجيا تأخذ اتجاها تطوريا متسارعا جدا، وبالتالي فإن الجهود أيضا لمحاربتها يفترض أن تواكب هذا التطور وتسير معه ضمن مسار متوازي.

وتهدف دراسة هذا النوع من الجرائم إلى معرفة جوانبها المختلفة ومسبباتها وتحديد مستوى الخطر الذي تشكله بالنسبة لأمن الأفراد والتجمعات، ومن ثمة تقييم مستوى التعاون الدولي والإقليمي الذي حققه المجتمع الدولي في سبيل مواجهتها والتصدي لها والحد منها.

ولتحقيق الأهداف المذكورة أعلاه فقد اعتمدت هذه الدراسة على مزيج من المناهج، خاصة المنهج التاريخي، المنهجين الوصفي والتحليلي، وفي بعض المواضع تم استخدام المنهج الإحصائي.

وقد اقتضت الإحاطة بالجوانب المختلفة للدراسة الخطة التالية:

أولا: مفهوم الجريمة السيبرية

ثانيا: أساليب الاحتيال الإلكترونية
ثالثا: الجهود الدولية لمواجهة الجريمة السيبرية

أولا: مفهوم الجريمة السيبرية

لم يتفق الفقه الجنائي على تسمية موحدة للجريمة السيبرية، حيث يطلق عليها تسميات عديدة: الجريمة الالكترونية، الجريمة المعلوماتية، جرائم إساءة استخدام تكنولوجيات المعلومات والاتصال، جرائم الكمبيوتر والإنترنيت (فريق مجمع البحوث والدراسات، 2015)، وأرى أن التسمية الأشمل والأكثر استخداما خاصة من الهيئات الدولية والوطنية التي تُعنى بمكافحة هذا النوع من الجرائم، هي تسمية "الجريمة السيبرية أو السيبرانية"، وهي تعريب للكلمة الإنجليزية Cyber crime أي جريمة الفضاء الإلكتروني أو جريمة الإنترنيت، وقد مرت بمراحل تطور عديدة، كما أنها عمل إجرامي يختفي وراءه العديد من الدوافع أو الأسباب وكذلك الأهداف.

1. تعريف الجريمة السيبرية

تعرّف المنظمة الدولية للشرطة الجنائية "الإنتربول" الجريمة السيبرية كما يلي: « **يشير مصطلح "الجريمة السيبرية البحتة" إلى الجرائم المرتكبة ضد أجهزة الكمبيوتر وأنظمة المعلومات، حيث يتمثل الهدف في الوصول غير المأذون به إلى جهازٍ ما أو منع الوصول إلى مستخدمٍ شرعي** » (https://interpol.int)، وهو تعريف مختصر يستوعب الجوانب العامة التي تصف الجريمة السيبرية، من حيث المحل والهدف دون الإشارة إلى الطرف المرتكب للفعل الإجرامي الذي قد يكون فردا أ مجموعة مشكلة لعصابة منظمة، كما تم تعريفها خلال مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين لسنة 2000 على أنها: « أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، والجريمة تلك تشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية» (نهلا عبد القادر المومني، 2010)، ويظهر من خلاله أنه وضح الجوانب الأساسية التي يمكن أن يتخذها العمل الإجرامي ضمن البيئة الإلكترونية، وأضاف الأداة التي يتم من خلالها ارتكاب هذا النوع من الجرائم

من خلال التعريفين السابقين يمكن تعريف الجريمة السيبرية كما يلي: الجريمة السيبرية هي تلك الجريمة التي يرتكبها فرد أو مجموعة ضد أجهزة الكمبيوتر وأنظمة المعلومات من خلال الوصول غير الشرعي أو الاختراق ضمن البيئة الإلكترونية، مهما كان الهدف منها سواء تعلق الأمر بالإضرار بالضحية أو تحقيق منافع للمجرم، أو كليهما معا .

كما أشار الموظفون المكلفون بإنفاذ القانون لدى هيئة الأمم المتحدة إلى مجموعة من الأفعال التي تشكل الجريمة السيبرية الآخذة في التصاعد، ويدخل في نطاق هذه الأفعال: الاحتيال الحاسوبي وانتحال الشخصية، وإنتاج أو توزيع أو حيازة مواد إباحية فيها استغلال جنسي للأطفال، ومحاولات التصيد الاحتيالي، والاختراق غير المشروع لأنظمة الحاسوب بما في ذلك القرصنة، ورجّح الموظفون المختصون أسباب تصاعد مستويات الجريمة السيبرية إلى تزايد قدرة تقنيات عدم الكشف عن الهوية عند استخدام تكنولوجيا المعلومات والاتصالات، فضلا عن تنامي تسويق أدوات إساءة استخدام الحاسوب (مكتب الأمم المتحدة المعني المخدرات والجريمة، 2013).

2. التطور التاريخي للجريمة السيبرية

قبل الخوض في تاريخ ظهور الجريمة السيبرية، يجب التوضيح أولا أن المخاطر التي يتعرض لها الفضاء السيبري أو البيئة المعلوماتية لا تكون دائما متعمدة (أيمن عبد الله فكري، 2017)، بل قد تكون عارضة أيضا، فرضتها طبيعة تعقد فضاء المعلومات وحداثته أيضا، والجريمة السيبرية تعد من المخاطر المتعمدة، التي يتوفر

فيها عنصر القصد الجنائي، وقد ظهرت هذه الأخيرة باختراع الإنترنيت، وتطورت من حيث أساليب ارتكابها مع مرور الزمن، وذلك تماشيا مع التطور التكنولوجي، خاصة في ما يتعلق باختراع جهاز الحاسوب والهواتف المحمولة وغيرها، ويمكن شرح ذلك كما يلي:

1.2. الظهور الأول للجريمة السيبرية

الجريمة المعلوماتية أو السيبرية هي جريمة حديثة نسبيا، وذلك بسبب ارتباطها بتكنولوجيا متطورة هي تكنولوجيا المعلومات، الأمر الذي جعلها تتسم بخصائص ومميزات تجعل منها مفهوما متميزا عن باقي الجرائم، كما أنها جلبت معها نوع جديد من المجرمين يطلق عليهم مجرمي المعلوماتية (نهلا عبد القادر المومني، 2010)، ومن المؤكد أن هناك صعوبة في تحديد أول جريمة سيبرية حدثت في تاريخ البشرية، الأمر الذي جعل الآراء تتباين بشأن ذلك، خاصة وأن الحواسيب تطورت مع الزمن، ودخلت تدريجيا في مناحي الحياة السياسية والاقتصادية والأمنية والاجتماعية والترفيهية وغيرها، مما يقتضي إدراج احتمالين، حيث:

الاحتمال الأول: أول جريمة متصلة بالحاسوب تعود إلى سنة 1801م عندما قام جوزيف جاكوارد Joseph Jacquard بصنع لوحة الكترونية تقوم بتكرار مجموعة من الخطوات لحياكة النسيج، وهو ما أثار مخاوف بعض العمال الأمر الذي دفعهم إلى تخريبها، وهو احتمال ضعيف بالرغم من أن بعض الباحثين يعتبرونه صورة من صور الإجرام السيبري، وأرى أنه حتى لو تم اعتباره كذلك فهو بتناسب وطريقة ارتكاب الجريمة ودوافعها مع الزمن الذي حدثت فيه.

الاحتمال الثاني: أول ظهور للجريمة السيبرية كانت بتاريخ 1958م، حيث بدأ معهد ستانفورد الدولي للأبحاث في الولايات المتحدة الأمريكية يرصد حالات إساءة لاستخدام الحاسوب، أو بمعنى آخر استخدام الحاسوب بطرق غير مشروعة أو لأغراض غير مشروعة، وهو الاحتمال المرجح، حيث يشكل الفعل المرتكب صورة جلية للجريمة السيبرية المعروفة في الوقت الحاضر، وحسب ما تم تعريفه سابقا.

2.2. تطور الجريمة السيبرية في فترة السبعينات

بانتشار الحواسيب وتدخلها في شتى مناحي الحياة انتشرت الجريمة السيبرية وتنوعت أساليبها وتطورت، وأضحت أكثر خطورة، وأكثر صعوبة من إمكانية التحكم فيها أو الحد منها، حيث حدثت العديد من الجرائم السيبرية، أبرزها جريمة وقعت سنة 1966 استهدفت سرقة بنك مينيسوتا الأمريكي، التي تعتبر أول سرقة الكترونية يتعرض لها بنك (فريق مجمع البحوث والدراسات، 2015)، وقد سجلت العديد من الجرائم السيبرية في فترة السبعينات إلا أنها إجمالا كانت قليلة.

وترى الدراسة التي أجراها فريق بحث مجمع البحوث والدراسات، التابع إلى أكاديمية السلطان قابوس لعلوم الشرطة بسلطنة عمان، بعنوان {الجريمة الالكترونية في المجتمع الخليجي وكيفية مواجهتها} أن سبب ذلك يعود إلى أن الخطر الذي يهدد الحواسيب هو خطر داخلي بين العاملين على الأنظمة الحاسوبية نفسها، حيث أنهم هم فقط من كانوا يستطيعون الوصول إلى تلك الأنظمة بصورة مباشرة، كما لم يكن هناك اتصال بالعالم الخارجي كما هو اليوم، حيث توسعت شبكة الانترنيت لتشمل أعدادا ضخمة جدا من الموصولين بها، وكذلك أن المؤسسات والبنوك المستهدفة كانت لا تعمد إلى إفشاء أسرارها وما تتعرض له من اختراقات حاسوبية لأنظمتها، حتى لا تهتز الثقة التي تتمتع بها بين الجمهور (فريق مجمع البحوث والدراسات، 2015)، وقد ظهرت في فترة السبعينات بعض التشريعات التي تجرم بعض الممارسات المتعلقة بإساءة استخدام الحواسيب.

3.2. تطور الجريمة السيبرية في فترة الثمانينات

في فترة الثمانينات نشطت الصحافة والأبحاث الأكاديمية التي تكشف هذه الجرائم وتعرّف بها على نحو دفع إلى وضع تشريعات بخصوص جرائم الإنترنيت وبشكل عام قوانين الملكية الفكرية، كما برز في هذه الفترة اهتمام الدول والتشريعات العربية بالجريمة السيبرية من خلال إصدار قوانين وعقد ندوات ومؤتمرات لتوعية ودراسة الجوانب المختلفة لهذه الظاهرة الخطيرة.

4.2. تطور الجريمة السيبرية في فترة التسعينات ومطلع الألفية الثالثة

في سنوات التسعينات ومطلع الألفية الثالثة حدثت تطورات عملاقة في مجال استخدام الإنترنيت، فبعد أن كان مجالها محصورا، أصبحت تستخدم في المجالات التجارية وكذلك الاستخدامات الفردية، وارتفع عدد الموصولين بها (الإنترنيت) بشكل كبير جدا، حيث بلغ مستخدموها عام 1996 ما يقارب 40 مليون مستخدم، وفي سنة 2011 حوالي 2.3 مليار مستخدم، أي ما يعادل أكثر من 3/1 سكان العالم، يمثل 60% منهم من سكان الدول النامية، ولا يتجاوز 45% من هؤلاء المستخدمين سن 25 سنة، وفي سنة 2014 تجاوز عدد المستخدمين أكثر من 3 مليار مستخدم، الأمر الذي صعب على المختصين التحكم فيها أو رصدها، حيث أصبحت تتجاوز الحدود الجغرافية والإقليمية.

5.2. واقع الجريمة السيبرية في الوقت الحالي

تعتبر الجريمة السيبرية في الوقت الحالي **"جريمة عبر وطنية"** أي عابرة للحدود، حيث أن حدودها هي العالم الافتراضي، وقد توقعت الأمم المتحدة أنه بحلول عام 2020 سوف يتفوق عدد الأجهزة المتصلة بالشبكة العنكبوتية على عدد البشر بنسبة ستة إلى واحد، مما سيؤدي إلى تغيير المفاهيم الحالية للإنترنت (الأمم المتحدة، ص xxi)، وبهذا العدد الهائل والإحصاءات الصادمة يمكن تصور حجم الجرائم وتنوعها والتفنن في طرق ارتكابها.

3. دوافع الجريمة السيبرية

تتنوع الأسباب والدوافع التي تؤدي إلى ارتكاب الجريمة السيبرية، حيث أن مرتكبيها يسعون من خلالها إلى تحقيق أغراض شخصية أو أغراض خاصة بنشاط هيئات معينة أو أغراض سياسية وأمنية أو مخابراتية لدول وحكومات، وقد أحصت الدراسة التي أجراها فريق بحث مجمع البحوث والدراسات، التابع إلى أكاديمية السلطان قابوس لعلوم الشرطة بسلطنة عمان، حول {الجريمة الالكترونية في المجتمع الخليجي وكيفية مواجهتها} أهم الأسباب والدوافع التي تؤدي إلى ارتكابها، وهي كالتالي:

1.3. الرغبة في جمع المعلومات وتعلمها

جاء في دراسة حول قرصنة الأنظمة أو الهاكرز HACKERS أن أخلاقيات القراصنة تقوم على مبدأين أساسيين، يتمثل الأول في أن الدخول إلى أنظمة الحاسب الآلي يمكن أن تعلمك كيف يسير العالم، أما المبدأ الثاني فيتمثل في جمع المعلومات، حيث يفترض أنه يجب أن يكون غير خاضع للحدود، وغالبا ما يصرح قراصنة الأنظمة أن هدفهم من التهكير هو التعلم فقط وإتاحة نسخ المعلومات دون قيود، حيث يتعاونون في شكل مجموعات ويتقاسمون المعلومات التي يجمعونها من خلال القرصنة الالكترونية ويستخدمونها في أنشطة هادفة، ولو بشكل غير مشروع ويخالف الأنظمة.

2.3. تحقيق أرباح ومكاسب مادية

يسعى المخترقون لأنظمة الحواسيب في الكثير من الأحيان إلى تحقيق مكاسب مادية لصالحهم الشخصي، أو حتى لمصلحة جهات معينة، نذكر على سبيل المثال الهاكر الجزائري المعروف باسم "الهاكر المبتسم" الشاب العشريني حمزة بن دلاج، مصنف ضمن أخطر الهاكرز في العالم، حيث اقتحم مواقع الحسابات المصرفية لأكثر من 217 بنكا مختلفا على مستوى العالم وحصول على أربعة مليارات دولار، كما قام بالهجوم على أكثر من 8000

موقع فرنسي مما أدى إلى غلقها، وتسبب أيضا في خسائر مالية فادحة للعديد من الشركات المالية، حيث كان يقوم بتحويل جزء من هذه الأموال إلى فلسطين وعدد من الدول الإفريقية الفقيرة (https://www.marefa.org).

3.3. الاستيلاء على المعلومات

في هذه الحالة يكون الهدف من الحصول على المعلومة من الحواسيب هو تهديد الضحية أو ابتزازها ماليا، أو حتى جسديا، أو بهدف تنافسي، ككشف أسرار شركة منافسة.

4.3. قهر النظام وإثبات التفوق على تطور الوسائل التقنية

الهاكر يقضي ساعات طويلة أمام شاشة حاسبه، حتى يكشف المواقع والأنظمة ويخترقها، ليثبت فقط تفوقه على أي تطور تقني في مجال التكنولوجيا .

5.3. إلحاق الأذى بأشخاص أو جهات

يكون هدف المجرم في هذه الحالة الانتقام وإلحاق الأذى بجهة معينة كحكومة أو هيئة أو شخص ما، دون السعي من وراء ذلك إلى تحقيق مكاسب شخصية.

6.3. تهديد الأمن القومي والعسكري: أصبح من الممكن أن يتم التهديد الأمني والقومي باستخدام التكنولوجيا، وذلك من خلال شن هجمات الكترونية على مواقع حكومات وأنظمة معينة، والتجسس عليها، وتوجيه تهديدات بأشكال وصور أو أنماط مختلفة، وغالبا تكون غير متوقعة.

ثانيا: أساليب الاحتيال الإلكترونية

أشار إعلان سلفادور بشأن الاستراتيجيات الشاملة لمواجهة التحديات العالمية، المرافق لقرار الجمعية العامة رقم 230/65 إلى أنَّ:" **تطور تكنولوجيات المعلومات والاتصالات وزيادة استخدام الإنترنيت يهيئان فرصا جديدة للمجرمين ويسِّران تنامي الجريمة**" (إعلان سلفادور، 2011)، وبالتالي فإن الأساليب والطرق التي يستخدمها المجرمون السيبريون تتطور وتتوسع وتتعقد أكثر تماشيا مع تطور تكنولوجيات الإعلام والاتصال، وبالتالي فهناك أساليب كثيرة جدا، يتم شرح أبرزها وأكثرها استخداما من خلال ما يلي:

1. أسلوب الاختراق والقرصنة

كمحاولة للسيطرة بشكل غير قانوني على نظام تشغيل ملفات محفوظة في حواسيب أناس آخرين أو في خوادم الشركات يمكن لقرصان المعلومات أن يكون عضوا في منظمة إجرامية، وعوضا عن القيام بعمليات ابتزاز في الشارع والتي يُجبر فيها الناس على دفع المال مقابل إبقاء أعمالهم سارية، يمكن لمجموعة منظمة من قراصنة المعلوماتية القيام بعملياتهم عبر الإنترنيت، وبالتالي يجبرون الضحية على دفع المال أو يقومون بتدمير أنظمة التشغيل لديه، كما يمكن لتلك المجموعات أن تعمل على صعيد دولي، وتكون عادة مدعومة من قبل الحكومات.

وبالتالي يمكن لجميع قواعد الملفات والبيانات المحفوظة في الحواسيب الالكترونية أن تكون معرضة للتلف أو السرقة، حيث أن مهمة عملية الاختراق سهلة جدا، وتحتاج عادة إلى أقل من 04 ساعات، وفي كثير من الحالات لا تحتاج لأكثر من 05 دقائق، هذا ما ورد على لسان جيم سيتل الذي كان يرأس وحدة الجرائم الإلكترونية في مكتب التحقيقات الفدرالي .

كان قراصنة المعلومات خلال بداية عصر الحواسيب الآلية لا يهتمون بأكثر من فهم أساليب عمل أنظمة التشغيل، فقد كان الأوائل منهم (قراصنة المعلومات) مجرد مبرمجين عاديين يبحثون عن أساليب فعّالة لتمرير المعلومات عبر الشبكات الالكترونية البطيئة، ومنذ تلك الفترة بدأت كلمة قرصان المعلوماتية تأخذ طابعا إجراميا، أما اليوم فقد أصبحت القرصنة المعلوماتية تعرف قضائيا على أنها **{اختراق عن سابق تصميم وإصرار لحاسوب إلكتروني بنوايا سيئة}**، كما أن جميع مستعملي الحواسيب معرضون للاختراق بغض النظر عن مستوى الأمن الذي يضنون أنهم يتمتعون به، سواء من خلال استعمال برامج الحماية من الفيروسات أو غير ذلك من برامج الأمن أو استعمال كلمات سر صعبة.

وقد تحول قراصنة المعلوماتية إلى عصابات إجرامية منظمة تقوم بجرائم غاية في الاحترافية، وذلك بسبب تطور تقنية المعلومات، وسواء تعلق الأمر بالمعدات أو البرامج فإن الإنتاج قد ازداد من ناحية الأمن والحماية، وبالتالي ازداد تعقيد وحدّة الهجمات وازداد تركيزها على أهدافها، وبالتالي أصبحت مقاومتها أمرا صعبا، ويمكن إدراج نموذج عن جرائم تم الاعتماد فيها على أسلوبي الاختراق والقرصنة والمتمثلة في: جريمة السطو الإلكترونية على مصرف Security Pacific National Bank في لوس أنجلس سنة 1978من قبل Mark Rifkin Stanly .

وقد كانت واحدة من أضخم عمليات السطو على المصارف، حيث ألقي القبض على موظف يدعى ستانلي مارك ريفكين يشغل منصب خبير المعلوماتية لدى البنك عرف في محيطه المهني بالذكاء والتفوق، حيث كان على وشك تحقيق جريمة كاملة، فقد اختفت 10 ملايين و200 ألف دولار من المصرف في تحويل عبر الهاتف في خريف ذلك العام، ولم يحتاج الرجل إلى أسلحة أو أقنعة أو حتى إلى سيارة للهروب، ولم يكتشف أي أحد أن هناك سرقة داخل البنك، قبل أن يعلمهم مكتب التحقيقات الفيدرالي بذلك، وقد كانت تلك أكبر سرقة قد تعرض لها مصرف في تلك الحقبة (securityartwork.es).

قام بعملياته بعد فتح حساب في مصرف سويسري مدعيا أنه تاجر ألماس، في 25 أكتوبر 1978 دخل ريفكن إلى غرفة الحوالات وحفظ شيفرات عمليات ذلك اليوم، ثم اتصل في وقت لاحق من ذلك اليوم بقسم الحوالات مستعملا اسم مايك هانستن، وقال أنه يعمل في قسم العلاقات الدولية التابعة للمصرف، ليتم تحويل مبالغ الحوالات لذلك اليوم إلى حسابه، ثم توجه إلى سويسرا لإتمام الجزء الثاني من خطته، حيث اشترى ألماسا بقيمة تعادل مئات الدولارات، وقام بتهريبه إلى الو. م.أ وبدأ عملية بيعه على نحو فوري، لكن ألقي القبض عليه قبل منتصف ليل 05 نوفمبر من نفس السنة وإعترف بعد أشهر بجريمته، وحكم عليه بالسجن 08 سنوات، إضافة إلى استعادة البنك المبلغ المسروق وتحقيق ربح إضافي قدّر بـ 05 مليون دولار أمريكي لصالح المصرف من جراء بيع الماس.

2. أسلوب الفيروس الالكتروني

الفيروس هو برنامج يكرر نفسه على نظام الكمبيوتر عن طريق دمج نفسه في البرامج الأخرى، حيث يحتوي على مجموعة من الأوامر الخاصة بكيفية انتشاره داخل الملفات، ويحدث آثارا تخريبية (رابحي عزيزة، 2018/2017)، يتصف برنامج الفيروس بأن له تأثير كبير على برامج الحاسب الآلي لما له من قدرة على إحداث تغيير في البرامج والبيانات المتداولة على الجهاز تصل إلى حد الإتلاف الكلي للبرامج، وقد نشأ مع الأيام الأولى

لاختراع الحاسب، وكان جون فاننيومان وهو رائد علم الحواسيب قد قام بوضع أسس هذا الفيروس سنة 1949، وقد بدأت تظهر الفيروسات فعليا سنة 1959 على هيئة كود غريب يظهر في حواسيب بعض الشركات بعد عدة ساعات من العمل (صغير يوسف، 2013).

يرجّح الخبراء وجود ما يقارب 100 ألف فيروس على شبكة الإنترنيت كما يجري التعرف على عدد يتراوح ما بين 20 و30 فيروسا في كل يوم، والمعركة ما بين صانعي الفيروسات وما بين بائعي برامج الحماية ضد الفيروسات مستمرة ولا نرى نهاية قريبة لها، حيث أن آلية تلك المعركة تتغير باستمرار، كما أن أغلب الفيروسات تُصنع على سبيل المزاح الثقيل، إلا أن الفيروسات الناجحة والفعالة قد تسبب خسائر مالية ضخمة، ومن بين أشهر الجرائم السيبرية التي اعتمدت هذا النوع من الفيروسات_جريمة الحرمان من الخدمات من خلال مهاجمة موقع الرهانات البريطاني bluesq.com المعروف باسم الساحة الزرقاء في أكتوبر 2004 عن طريق فيروس حصان طروادة Trojan Horse (يحي الشريف حنان، 2018/2017).

3. أسلوب الدودة الإلكترونية

هذا الأسلوب عبارة عن برنامج إلكتروني خبيث يطلق عليه اسم الدودة، وبعكس الفيروس فإن الدودة الإلكترونية لا تُلصق نفسها بملف، فهي برنامج مستقل بذاته يعمل في عمق الشبكات الإلكترونية، متى وصلت عمليات النسخ إلى مستوى معين فإنها تعوق عمل الشبكة، وأشهر نموذج للدودة الإلكترونية دودة **حشرة الحب التي أطلقت بتاريخ 05 ماي عام 2000م**، حيث ظهرت في بادئ الأمر في الفيليبين إلا أن تأثيرها وصل العالم كله، كان الضحايا يتلقونها كأنها رسالة حب إلكترونية مكتوب فيها عبارة (I love You)، إلا أن فتح هذه الرسالة يؤدي إلى تدمير المعلومات (يحي الشريف حنان، 2018/2017)، وقد انتشر البرنامج الخبيث بسرعة كإصابة خوادم الشركات الضخمة ومن ثمة وسائل الإعلام والحكومات وحواسيب ملايين الأفراد وتدمير المعلومات الموجودة في تلك الأنظمة.

يشير البرنامج نفسه من خلال الولوج إلى قائمة الاتصال في كل حاسوب مصاب، ومن ثمة إرسال رسالة إلكترونية لجميع العناوين الموجودة هناك، كانت الرسالة تحمل نسخة مرفقة من البرنامج اسمها {رسالة حب لك}، جرى الإعلان عن 50 مليون حالة مع حلول 13 ماي سنة 2000، ونتجت عن ذلك أضرار بقيمة 08 مليارات دولار أمريكي، أضطر البنتاقون ووكالة الاستخبارات المركزية ومجلس النواب البريطاني إلى إغلاق نظم البريد الإلكتروني للتخلص من البرنامج، كما اضطرت عدة منظمات لإيقاف شبكاتها الإلكترونية مما أدى إلى خسارتها أعمالها أو تعليق خدماتها (http://natgeo.com).

تلقت شركة أنتل نت في الفلبين ألاف الاتصالات من مستخدمين أوروبيين اشتكوا من رسالة الحب الالكترونية التي أتت من خوادمهم، توجهت الشركة مباشرة إلى مكتب التحقيقات الوطني في الفلبين، وبعد مرور عدة أيام من المراقبة لمحور الاتصالات الأول الذي ظهر فيه الفيروس، نجح المكتب بتحديد رقم هاتف تكرر استعماله بشكل مشبوه، كان رقم الهاتف عنوانه شقة في ضواحي مانيلا، يسكنها شابان يدرسان في برمجة الحواسيب الإلكترونية بالجامعة، اتضح في الأخير أن أحدهما هو من أطلق رسالة الحب، إلا أنه لم يعاقب لأنه لم يكن هناك قانون في الفيليبين يخص الجرائم الإلكترونية (صغير يوسف، 2013)، وقد صرّح الفاعل أنه أطلق

الدودة على سبيل المزاح فقط ولم يكن يقصد الأذى، وقد أعطى صورة سيئة لبقية المراهقين بعدم إخضاعهم للعقاب، وقد حصل على فخر زملائه من الكلية الذين يعتقدون أنه أحسن الصنع بعبقريته.

ثالثا: الجهود الدولية لمواجهة الجريمة السيبرية

لا يمكن حصر كل الجهود الدولية أو الإقليمية لمواجهة الجريمة السيبرية، ولكن يمكن من خلال هذه الدراسة التطرق إلى بعض المبادرات التي قامت بها دول ومنظمات ومراكز بحث وغيرها، حتى يمكن اكتساب تصور أولي حول ما يدور في الساحة الدولية من متابعات وتحقيقات جنائية واتفاقات وشراكات وعقد مؤتمرات وندوات وإجراء دراسات أكاديمية، وتكليف خبراء في ميدان المعلوماتية بوضع حلول وإجراء إحصاءات وغيرها.

1. المتابعة الجنائية العبر وطنية للجريمة السيبرية عن طريق الإنتربول

جاء ضمن التقرير السنوي للمنظمة الدولية للشرطة الجنائية (الإنتربول) لسنة 2018 التوطئة التالية: **«ثمة جانب سيبري في كل جوانب حياتنا، وللأسف، أيضا في أنشطة المجرمين، والمكتب المعني بالقدرات السيبرية هو إحدى الركائز الأساسية التي يقوم عليها التزامنا بمكافحة الجريمة السيبرية »** (تقرير الإنتربول، 2018)، وبالتالي فالإنتربول تساهم في الحد من الجريمة السيبرية ومواجهتها من خلال العديد من أوجه التدخل، يمكن ذكر أهمها في النقاط التالية:

1.1. مساعدة البلدان الأعضاء على إجراء تحقيقات في الجرائم السيبرية

ولأنه لا توجد حدود في الفضاء السيبري، مما يطرح تحديات للشرطة في التحقيق في حوادث الجريمة السيبرية التي قد تشمل المشتبه بهم والضحايا والجرائم، وتمتد إلى عدة بلدان، لذلك تساعد الإنتربول البلدان الأعضاء على إجراء تحقيقات في الجرائم السيبرية، وتحرص على أن تتوفر لدى الشرطة أحدث وأهم المعلومات عن التهديدات السيبرية لتوجيه أعمالها (https://interpol.int).

2.1. المتابعة الجنائية من خلال أجهزة الإنتربول

تتوزع مهام الإنتربول في ما يخص متابعة الجرائم السيبرية بين هياكل مركزية وأخرى إقليمية أهمها:

1.2.1. مهام المركز المتعدد الاختصاصات لمكافحة الجريمة السيبرية

يظم المركز المتعدد الاختصاصات لمكافحة الجريمة السيبرية التابع للإنتربول خبراء الإنترنت من أجهزة إنفاذ القانون والقطاع الصناعي، مهمتهم جمع المعلومات المتوفرة عن الأنشطة الإجرامية في الفضاء السيبري وتوفير المعلومات الاستخباراتية للدول (https://interpol.int)، ويقوم المركز المتعدد الاختصاصات لمكافحة الجريمة السيبرية بمهمة تحليل البيانات السيبرية الواردة من الشركاء في القطاع الخاص والأوساط الأكاديمية والبلدان الأعضاء، حيث أنه في عام 2018 أعد هذا المركز 246 تقريرا عن الأنشطة السيبرية الموجهة إلى البلدان الأعضاء، تضمنت معلومات يمكن الاستناد إليها للتحرك، حيث أتاحت تنفيذ العديد من عمليات الملاحقة الناجحة (تقرير الإنتربول، 2018) .

2.2.1. مهام المكتب المعني بالقدرات السيبرية

يعمل المكتب المعني بالقدرات السيبرية في رابطة أمم جنوب شرق آسيا مع البلدان العشرة التي تتألف منها هذه الرابطة على دعم تحقيقاتها وعملياتها ومعلوماتها، وتُجمَع معلومات عن التهديدات السيبرية من البلدان الأعضاء ومن الجهات الشريكة من القطاع الخاص، ثم تُحوَّل إلى معلومات يمكن استغلالها للتحرك بشكل ملموس، وتعتزم الإنتربول على إنشاء مكاتب مماثلة في بقية المناطق الأخرى (تقرير الإنتربول، 2018).

3.1.التدريب في مجال العمل الشرطي السيبري

إن برامج التدريب الشاملة في مجال مكافحة الجريمة السيبرية والتي تجمع بين التعلم الإلكتروني والتدريب في القاعات تتيح للمشاركين فيها مواجهة تطور الجريمة في المجال الرقمي، وقد عمد الإنتربول ـ حرصا منه على حصول أكبر عدد ممكن من أفراد الشرطة على أشد أشكال التدريب تنوعاـ إلى توسيع نطاق دروسه التدريبية وأماكن توفيرها، وفي عام 2012 ركّزت الدورات التدريبية للمرة الأولى على مسألتي الجريمة السيبرية والفساد في عالم الرياضة، وعُقدت للمرة الأولى في البحرين وتونس.

وازداد عدد هذه الدورات بنسبة 6% قياسا بعددها عام 2011، وارتفع عددها في الشرق الأوسط وشمال أفريقيا بنسبة 40 %، وفي آسيا وجنوب المحيط الهادي بنسبة 36 % (تقرير الإنتربول، 2012)، وفي عام 2018 قدمت دورات تدريبية إلى 164 شخصا من 61 بلدا عضوا، من بينهم عناصر في فرق التدخل الأول ومحققون في الجرائم السيبرية ومحللون للتهديدات السيبرية وصانعون للقرار ومُدّعون عامّون وقضاة (تقرير الإنتربول، 2018).

4.1. الشراكات الدولية

يستحيل على أي جهة بمفردها القضاء على الجريمة السيبرية العابرة للحدود، لذلك يمضي الإنتربول جاهدا في إرساء شراكات متينة مع هيئات إقليمية ودولية أخرى، تشمل أجهزة إنفاذ القانون وغيرها، ففي عام 2012 مثلا توصلت المنظمة إلى عدة اتفاقات تعاون جديدة، وافقت الجمعية العامة على ستة منها وانضمت إلى مجموعة الشركاء قديمي العهد، مثل الأمم المتحدة والاتحاد الأوروبي، وجهات أخرى مثل جماعة شرق أفريقيا والشراكة الدولية المتعددة الأطراف لمكافحة التهديدات السيبرية IMPACT ومشروع التحقق من الأسلحة الصغيرة SAS والسوق المشتركة لبلدان المخروط الجنوبي(تقرير الإنتربول، 2012)، كما أقامت الإنتربول شراكات مع القطاع الخاص، فمثلا عام 2016 وقّع الإنتربول اتفاقات تعاون رسمية مع عدة شركاء من هذا القطاع (تقرير الإنتربول، 2016).

5.1. عمليات جنائية للإنتربول في مجال الجريمة السيبرية

يمكن إدراج أمثلة عنها كما يلي:

1.5.1. عملية بانجيا الخامسة

تمكّنت السلطات في 100 بلد، أثناء عملية بانجيا الخامسة، من إغلاق ما يزيد عن 18000 موقع إلكتروني كانت لها صلة بصيدليات تعمل بشكل غير مشروع على الإنترنت، ومصادرة 4 ملايين وحدة من الأدوية غير المشروعة التي قد تشكل خطرا على الحياة، وتستهدف هذه العملية السنوية السوق السوداء الدولية التي تبيع الأدوية المقلدة وغير المشروعة والتي تهدد صحة مستهلكيها الذين يتناولونها بدون الشك في طبيعتها، وتستهدف العملية أيضا تعزيز الوعي العام بخطر شراء الأدوية عن طريق الإنترنت (تقرير الإنتربول، 2012).

2.5.1. عملية أنماسك: نُفّذت بدعم من الإنتربول عملية دولية استهدفت قراصنة للحواسيب يُعتقد أن لهم صلة بمجموعة "أنونيمُس"، وأفضت إلى اعتقال قرابة 25 شخصا في أمريكا اللاتينية وأوروبا، وشارك في هذه العملية المعروفة بعملية أنماسك، الأرجنتين وإسبانيا وشيلي وكولومبيا عقب سلسلة من الاعتداءات السيبرية المنسقة التي انطلقت من هذه البلدان ضد مواقع إلكترونية تابعة للحكومة الكولومبية، وفضلا عن اعتقال هؤلاء الأشخاص، صودر حوالي 250 جهازا معلوماتيا وهواتف خلوية وبطاقات دفع ومبالغ مالية (تقرير الإنتربول، 2012).

3.5.1. عملية الاحتيال المالي باستخدام البريد الالكتروني {اعتقال "مايك"}

في جويلية 2016، أدت عملية مشتركة بين الإنتربول ولجنة الجريمة الاقتصادية والمالية النيجيرية إلى القبض على" مايك "في نيجيريا، وهو زعيم لشبكة إجرامية دولية ارتكبت آلاف عمليات الاحتيال بالبريد الإلكتروني التي شملت أكثر من 60 مليون دولار أمريكي، وأوقعت ضحايا في جميع أنحاء العالم (تقرير الإنتربول، 2016).

2. تدخل المجتمع الدولي للحد من الجريمة السيبرية

كما سبق بيانه فإن الجريمة السيبرية تشكل قضية عالمية تهم كل الحكومات والمنظمات الدولية والقطاع الخاص أيضا وكذا الأفراد، وقد ظهرت مبادرات جادة لمواجهتها ومحاولة تحقيق مطلب الأمن والأمان في الفضاء السيبراني، تتمثل في توفير هياكل متخصصة وعقد اتفاقيات وتشكيل لجان وتجميع الخبراء للتشاور والنقاش والخروج بحلول بناءة، إضافة إلى إجراء لقاءات وعقد ندوات ومؤتمرات على مستوى دولي وإقليمي، ومحاولة إشراك القطاع الأكاديمي من خلال البحوث والدراسات المتخصصة، ويمكن من خلال هذه الدراسة إعطاء بعض الأمثلة.

1.2. الأمم المتحدة

يعتبر الأمن السيبري من بين القضايا التي نشطت من خلالها الأمم المتحدة، وهي بذلك تؤدي دورا محوريا، خاصة من خلال الاتفاقيات المختلفة التي تتناول فيها القضية وتطرح حلولا لها، وتحاول ربط قنوات التعاون بين الدول والمنظمات الدولية وكذا القطاع الخاص، على أساس الطبيعة العالمية للإجرام السيبري.

2.2. اللجنة الاقتصادية والاجتماعية لدول غرب آسيا (الإسكوا)

تأسست لجنة الأمم المتحدة الاقتصادية والاجتماعية لغربي آسيا (يونيسكوا أو إسكوا) عام 1973، وقد أسسها المجلس الاقتصادي والاجتماعي التابع للأمم المتحدة بقرار 1818 (LV) كبديل لمكتب الأمم المتحدة الاقتصادي والاجتماعي في بيروت (يونيسوب)، وقد تغير الاسم عام 1985، ويعتبر الأمن السيبراني من بين القضايا التي تعالجها اللجنة ضمن تقاريرها ومؤتمراتها والأبحاث والدراسات التي تشرف عليها، يمكن إعطاء أمثلة بسيطة كالتالي:

لقد عقدت اللجنة ورشة عمل حول تحفيز الأمان في الفضاء السيبراني في المنطقة العربية يومي 8 و9 ديسمبر 2014 في مسقط بعمان، بالتعاون مع المركز الإقليمي للأمن السيبراني للاتحاد الدولي للاتصالات وهيئة تقنية المعلومات في عمان وبرعاية وزارة المالية العمانية، كانت الورشة تهدف إلى بناء القدرات الوطنية في المنطقة العربية في مجال الأطر التنظيمية والمؤسساتية من أجل تعزيز الأمن السيبراني ومواجهة الجرائم السيبرانية، وقد حضر ورشة العمل أكثر 80 مشاركا من أثني عشرة بلدا عربيا (تقرير الإسكوا، 2015).

وفي ديسمبر 2018 استضافت الإسكوا حواراً إقليمياً واجتماعاً للخبراء بشأن حوكمة الإنترنيت والأمن السيبراني تمحور حول تعزيز الثقة في الفضاء السيبراني، ونُظّم بالشراكة مع جامعة الدول العربية في إطار التحضير للمنتدى العربي الخامس لحوكمة الإنترنت، وقام نحو 50 مشاركاً من 14 بلداً عربياً بتقديم توصيات بشأن مسائل الثقة والسلامة والأمن على الإنترنت تتسق مع خريطة الطريق الثانية التي وضعتها الإسكوا وجامعة الدول العربية لحوكمة الإنترنت (تقرير الإسكوا السنوي، 2018).

3.2. جامعة الدول العربية:

كثيرا ما تضع جامعة الدول العربية محور الأمن السيبري ضمن أجنداتها، سواء تعلق الأمر بالاجتماعات التي تعقدها دوريا، أو بالمؤتمرات والندوات التي تنظمها، وأهم ما صدر عنها **قانون الإمارات العربي الاسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها**، حيث اعتمده مجلس وزراء العدل العرب في دورته التاسعة عشرة سنة 2003 (القرار رقم 495-د19-2003/10/8)، ومجلس وزراء الداخلية العرب في دورته الحادية والعشرين سنة 2004 (القرار رقم 417-د21-2004)، وتم تكليف الأمانة الفنية للجامعة بتعميم المشروع على الدول العربية للاسترشاد به، على أن تقدم كل دولة بعد عامين تقريرا حول مدى استفادتها من القانون الاسترشادي وملاحظاتها بهذا الشأن.

4.2. الاتحاد الدولي للاتصالات

قام الاتحاد الدولي للاتصالات بالكثير من المبادرات لمواجهة الجريمة السيبرية، حيث أنشأ بوابة الأمن السيبراني في 2009، وقام بتطويرها تدريجيا بهدف تحسين إمكانية النفاذ إلى المعلومات ونشرها، وكذلك لتحسين التعاون على الخط بين الجهات صاحبة المصلحة العاملة في مجال الأمن السيبراني (https://www.itu.int).

كما أطلق الاتحاد الدولي للاتصالات في إطار البرنامج العالمي للأمن السيبراني، وبالتعاون مع وكالات الأمم المتحدة الأخرى والشركاء الآخرين، مبادرة حماية الأطفال على الخط COP في نوفمبر 2008، بوصفها مبادرة تعاونية دولية للعمل على تعزيز حماية الأطفال على الخط في العالم، وقد انبثق عن هذه المبادرة العديد من الأنشطة والمؤتمرات والمساهمات المشتركة تهدف جميعها إلى حماية فئة الأطفال من المخاطر في الفضاء السيبري (تقرير الاتحاد الدولي للاتصالات، 2019/2018)، وقد جاء ضمن التقرير المرحلي السنوي للاتحاد إستراتيجية تبناها الاتحاد ملخصها أنه ينبغي تحسين التأهب في مجال الأمن السيبراني بنسبة 40 % بحلول 2020، (تقرير الاتحاد الدولي للاتصالات، 2018-2019)،

5.2. شراكة دولية متعددة الأطراف لمكافحة التهديدات الالكترونية [IMPACT]

هي شراكة عالمية بين القطاعين العام والخاص، أسست في مارس 2009، تهدف إلى محاربة التهديدات الإلكترونية، وهي تساعد البلدان الشريكة، وبخاصة الأمم المتحدة، على اعتماد أساليب تعزيز الأمن الإلكتروني، حيث تعمل كل الجهات المشاركة على العناية بالبرنامج العالمي للأمن السيبراني (GCA) ويقع مقرها الرئيسي في سيبرجايا، في ماليزيا (http://gssd.mit.edu)، وفي أوت 2010 وافقت أكثر من 50 دولة من الدول الأعضاء رسميا على الاشتراك في الخدمات التي تقدمها شراكة IMPACT (كتاب أخبار الإتحاد،2010) .

خاتمة

أصبحت التكنولوجيا في العصر الحالي تتدخل في جميع مجالات الحياة، فهناك توجه استراتيجي للحكومات نحو تكريس المدن الذكية والحكومات الإلكترونية، ثم أن التسويق والتجارة وحتى التعليم والصحة والسياسة والبنوك وغيرها يتم إنجاز نشاطاتها عبر الشبكة العنكبوتية، لذلك فإن أي خطر أو خلل يتهددها قد يشلّ مجال حيوي يرتبط بشكل مباشر بمصلحة إستراتيجية للفرد والدولة والمنظمات والجماعات بشكل عام، لذلك فإن هناك الكثير من الجهود الوطنية والإقليمية والدولية التي تبذل في سبيل التصدي للمخاطر التي يتعرض لها الفضاء السيبري من اختراقات وتخريب الكتروني وعمليات سطو إلكترونية، وتشكيل عصابات وجماعات إرهابية، واختطاف للنساء والأطفال والاتجار بالبشر وترويج المخدرات وغيرها عبر المواقع الإلكترونية.

وما يشهده الفضاء السيبري من جرائم إلكترونية وتطوير لأساليب القرصنة والاختراق كل يوم يقابله في الجانب الآخر جهود دولية وإقليمية للتصدي، وابتكار تقنيات حماية متطورة للأنظمة، لكن ذلك غير كافي،

خاصة بالنسبة للدول العربية التي لم تبلغ فيها التقنية التطور الكافي الذي يمكّنها من مجابهة كل خطر يتهدد فضاءها السيبري، ثم أن الخلل يبرز من خلال ضعف التعاون بين هذه الدول في جميع المجالات بما فيها المعلوماتية، وعدم وجود اتحاد للقوى في سبيل تحقيق الأمن القومي بما فيها الأمن السيبري، لكن ذلك لا يمنع من وجود بعض المبادرات التي تقودها جامعة الدول العربية والإسكوا وغيرها.

وبالتالي ومن خلال هذه الدراسة تم التوصل إلى مجموعة نتائج كالتالي:

أولا: كلما تطورت التكنولوجيا وأصبحت متاحة لعدد أكبر من المستخدمين، كلما زادت معها الجريمة السيبرية من حيث عددها وقوتها وتنوعها، وهو ما يثير المخاوف حول المستقبل الذي تسعى فيه الحكومات والمنظمات لجعل التكنولوجيا متاحة بنسب أكثر في المستقبل، والذي يعد أمرا إيجابيا نظرا للحاجة الملحة للتكنولوجيا في الوقت الحالي، لكنه بالمقابل يخلق بيئة خصبة لصناعة الجريمة السيبرية والإبداع والابتكار لوسائل اختراق وتخريب جديدة ومتطورة.

ثانيا: تأسيس العديد من المنظمات والمراكز واللجان ذات الطابع العالمي التي تُعنى بالجريمة السيبرية سواء بشكل متخصص أو كأحد اختصاصاتها، لكن ذلك لم يكن كافيا، خاصة أن حلقة الربط بين الجهود الفردية للدول وجهودها كتكتلات داخل المنظمات تعد ضعيفة.

ثالثا: هناك تباين بين الدول في ما يخص مستوى التطور في استخدام التكنولوجيا، فالوضع في أوروبا وأمريكا واستراليا مثلا يختلف عن الوضع في دول أفريقيا ودول العالم الثالث في قارة آسيا، في حين الجريمة السيبرية تتخذ طابعا عالميا، وهو ما يخلق تباين في كيفية التصدي لها وتوفير أنظمة حماية عالية التقنية.

رابعا: هناك ضعف في التعاون بين الدول العربية، مما يعوق إمكانية ابتكار نظام حماية تعاوني بينها، وخلق شراكات، وتوحيد الجهود العربية، بالمقارنة مع الدول الأوروبية مثلا، والتي كثيرا ما تنجح في التغلب على هجمات سيبرية نتيجة تكاثف جهود حكومات الإتحاد وأنظمتها.

ومن خلال ما سبق تسنى اقتراح **التوصيات** التالية:

أولا: الاتفاق على خطة عالمية في شكل قانون يتبناه الإتحاد الدولي للاتصالات، حيث يتم مراقبة أي تطبيق جديد أو أي إصدار تقني جديد وإخضاعه للدراسة، لتحديد الاحتمالات الممكنة لاختراقه والإضرار بمستخدميه، ثم إصداره مرفقا بتحذيرات ونصائح للمستخدمين، مع خلق دعاية له تتخللها توعية للمستخدمين، ويصبح هذا الإجراء شرطا قانونيا ملزما لكل من له علاقة بصناعة التقنية.

ثانيا: تعزيز التعاون الدولي أكثر وأكثر من خلال تنظيم مؤتمرات عالمية مكثفة، لدراسة ومناقشة مشاكل الفضاء السيبراني، وجعله من أولويات أعرق المنظمات خاصة الأمم المتحدة على المستوى الدولي، اليونسكو وغيرها، على أساس أن التكنولوجيا هي مستقبل البشرية، فالجدير تعزيز الحماية لضمان أمن سيبري مستقبلي.

ثالثا: تعزيز التعاون بين الدول العربية، من خلال تكثيف المؤتمرات المتخصصة في مجال التكنولوجيا، ومناقشة مشاكل الفضاء السيبري في الوطن العربي، خاصة وأن الجرائم السيبرية في الإقليم العربي تأخذ منحى أخطر يرتبط بشكل مباشر بالأمن القومي وسلامة الأقليات وأنشطة الشبكات الإرهابية والمخابرات والخطر الأجنبي.

رابعا: ضرورة تكوين أفراد الشرطة الوطنية خاصة لدى الدول العربية بخصوص متابعة الجريمة السيبرية والتحقيق فيها والكشف عنها، لأنه لا يمكن لمن لا يفقه في الجانب التقني والمعلوماتي العمل على تتبع جنائي وشرطي لجريمة عالية التقنية مرتكبة في فضاء افتراضي عالي التقنية (الفضاء السيبري)، وذلك من خلال دورات تدريبية، وتعاون دولي في ما يخص تخريج خلايا شرطية متخصصة في مجابهة الجريمة السيبرية عالية التقنية.

خامسا: ضرورة التفاعل الشرطي لكل الدول المنضوية تحت منظمة الإنتربول، من خلال توحيد الجهود الوطنية مع جهود المنظمة وخلق جسر تعاون دائم غير متقطع، وذلك بهدف اكتساب خبرات تمكّن الشرطة الوطنية من التكفل بأكبر قدر من هذه الجرائم، على الأقل تلك التي يمكن تحديد حدودها الجغرافية.

قائمة المصادر والمراجع

أولا: الوثائق الرسمية

1- القرار رقم 495-د19-2003/10/8. مجلس وزراء العدل العرب الدورة التاسعة عشرة سنة 2003.

2- القرار رقم 417-د2004/21، مجلس وزراء الداخلية العرب، الدورة الحادية والعشرين سنة 2004.

3- إعلان سلفادور بشأن الاستراتيجيات الشاملة لمواجهة التحديات العالمية، المرافق لقرار الجمعية العامة للأمم المتحدة 230/65، A/Res/65/230 بشأن مؤتمر الأمم المتحدة الثاني عشر لمنع الجريمة والعدالة الجنائية، بتاريخ 01 أفريل 2011.

4- التقرير السنوي للإنتربول لعام 2012.

5- تقرير حول ورشة عمل حول تحفيز الأمان في الفضاء السيبراني في المنطقة العربية، بتاريخ 08 و 09 ديسمبر 2014 بمسقط، عمان، الوثيقة رقم E/ESCWA/TDD/2015/WG.1/ Report المؤرخة في 25 فيفري 2015

6- التقرير السنوي للإنتربول لعام 2016.

7- التقرير السنوي للإنتربول 2017.

8- التقرير السنوي للانتربول 2018.

9- تقرير الإسكوا السنوي، لعام 2018 .

10- تقرير عن تنفيذ الخطة الإستراتيجية للاتحاد وعن أنشطة الاتحاد للفترة 2018-2019 (التقرير المرحلي السنوي للاتحاد)، الوثيقة C19/35-A بتاريخ 18 أفريل 2019.

11- تقرير الاجتماع الثامن للمتخصصين بأمن وسلامة الفضاء السيبراني أيام 1- 3 جويلية 2019، بتاريخ: 2020/01/01 على الساعة 20:00 مساءا، موقع المركز العربي للبحوث القانونية والقضائية http://carjj.org .

ثانيا: المؤلفات

1- أيمن عبد الله فكري، الجرائم المعلوماتية – دراسة مقارنة في التشريعات العربية والأجنبية، طبعة 2017 مكتبة القانون والاقتصاد، الرياض السعودية.

2- نهلا عبد القادر مومني، الجرائم المعلوماتية، الطبعة الثانية 2010، المكتبة الوطنية، المملكة الأردنية الهاشمية.

ثالثا: الأبحاث والدراسات الصادرة عن الهيئات

1- دراسة حول: الجريمة الالكترونية في المجتمع الخليجي وكيفية مواجهتها، بحث فائز بجائزة الأمير نايف بن عبد العزيز للبحوث الأمنية لعام 2015، من إعداد فريق بحث مجمع البحوث والدراسات، أكاديمية السلطان قابوس لعلوم الشرطة، نزوى، سلطنة عمان.

2- دراسة شاملة عن الجريمة السيبرانية، مكتب الأمم المتحدة المعني المخدرات والجريمة، فيينا، مسودة فيفري 2013- كتاب أخبار الاتحاد، بناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات، 10 ديسمبر 2010.

رابعا: الرسائل الجامعية

1ـ عزيزة رابحي، الأسرار المعلوماتية وحمايتها الجزائية، أطروحة دكتوراه، تخصص القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، جامعة تلمسان، السنة الجامعية 2018/2017.

2ـ صغير يوسف، الجريمة الإلكترونية عبر الإنترنيت، مذكرة ماجستير، تخصص قانون دولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري ـ تيزي وزو، تاريخ المناقشة 2013/03/06.

3ـ يحي الشريف حنان، تأثير نظام المعلومات على اليقضة في المؤسسات الصغيرة والمتوسطة، رسالة دكتوراه، كلية العلوم الإقتصادية والعلوم التجارية وعلوم التسيير، جامعة فرحات عباس ـ سطيف 1، السنة الجامعية 20118/2017.

خامسا: مقالات منشورة على المواقع الالكترونية

1- حمزة بن دلاج، مقال منشور على موقع: **موقع معرفة** https://www.marefa.org ، بتاريخ 2019/12/18 على الساعة 22:00 مساءا.

2- ٤-https://www.securityartwork.en, Alex Rodriguez, Security and History, The Case of the Security Pacific National Bank, 21 de december 2009, date de navigation 28/04/2019, h 16:30.

سادسا: المواقع الالكترونية

1_ موقع النظام العالمي للتنمية المستدامة http://gssd.mit.edu

2_ موقع منظمة الشرطة الجنائية الدولية https://interpol.int

4_ موقع الاتحاد الدولي للاتصالات https://itu.int

5_ موقع ناشيونال جيوغرافيك http://natgeo.com

6_ موقع جامعة الدول العربية http://lasportal.org

7_ موقع المركز العربي للبحوث القانونية والقضائية http://carjj.org .