تأثير الجرائم الالكترونية على البنى السوسيو اقتصادية

Cybercrime Effect on Socioeconomic Structures

ط.د.علاء الدين فرحات، قسم العلوم السياسية، كلية العلوم السياسية، المدرسة الوطنية العليا للعلوم السياسية

ملخص الدراسة:

معظم بلدان العالم صارت تعي أن ثمة نوعا آخر من العولمة "عولمة التهديدات الناجمة عن الجرائم الالكترونية" التي صاحبت موجة التطور التقني، والتي استهدفت أمن الدولة من كل النواحي الحيوية الاجتماعية منها والاقتصادية، خاصة وأن الاقتصاد أصبح يدار الكترونيا (الاقتصاد الإلكتروني)، فالمنافسة انتقلت في هذا العالم المعولم من قضايا الأمن القومي إلى قضايا الاقتصاد القومي، فمست الجرائم الالكترونية كل الجوانب الاقتصادية كسرقة الأسرار والتجسس الصناعي، غسيل الأموال والتلاعبات بالبورصات العالمية، إضافة إلى نتائج الجرائم الالكترونية على البنى الاجتماعية كنشر الأفكار المتطرفة، الجرائم الجنسية وكل ما يمس قضايا أمن الأسرة.

الكلمات المفتاحية: الجرائم الالكترونية- الاقتصاد- المجتمع- الأمن السيبراني

Abstract:

Most countries of the world have become aware that there is another kind of globalization, the globalization of threats posed by the electronic crimes that accompanied the wave of technical development, which targeted the state security of all vital aspects social, and economic especially since the economy is managed electronically **(Electronic Economy)**, the competition has moved in this globalized world from the national Security issues to the national economy issues, Cybercrime touched all the economic aspects such as stealing secrets and industrial espionage, money and manipulations of global stock markets laundering, in addition to the results of cybercrime on social infrastructure such as spreading extremist ideas, sexual offenses and all that affects the family security issues.

Keywords: Electronic Crimes -Economy - Society - Cybersecurity

مقدمة:

إن ثورة المعلومات الجديدة التي عكست نفسها على العالم الكوني، و التي شكلت الاتصالات والمعلومات إحدى ركائزها، دفعت بالدول نحو الانتقال السريع لاستخدام الفضاء الالكتروني لكي يكون العامل الرئيس في دفع الاقتصاديات إلى مستويات جديدة، أخذت التجارة الالكترونية السمة الأبرز فيها، وبدورها أدت التحولات التكنولوجية الحديثة في مجال الأجهزة والبرمجيات إلى بروز أشكال جديدة من التهديدات كالجرائم الالكترونية بحيث استغل بعض المجرمين التقنية لتطوير قدراته الإجرامية وهذا عبر الشبكة المعلوماتية كوسيلة لإلحاق الضرر بالآخرين، وبتنامي أشكال الجريمة الالكترونية وتطور أشكالها وتفاقم تهديداتها على البنى السوسيو-اقتصادية جراء المخاطر التي تستهدف الاعتداء على المعطيات بدلالاتها التقنية الواسعة، في الوقت الذي تحاول فيه وكالات تنفيذ القانون معالجة هذه المشكلة، إلا أنها تنمو باطراد؛ حيث أصبح العديد من الناس ضحايا القرصنة والاحتيال وسرقة الهوية والبرمجيات الخبيثة، كما استهدفت أمن الدولة من كل النواحي الاقتصادية، خاصة وأن الاقتصاد أصبح يدار الكترونيا (الاقتصاد الإلكتروني)، فالمنافسة انتقلت في هذا العالم المعولم من قضايا الأمن القومي إلى قضايا الاقتصاد القومي. الأمر الذي دفع بالدول إلى العمل على الحد من هذه الجرائم المستحدثة من خلال عديد الوسائل التقنية والتشريعية للوقاية من تداعياتها، بحيث بات لزاما أن يواكب التحرك الأمني والتشريعي للدول التطور الحاصل في مجال التقنية الإجرامية، مما سبق فإن مَشْكَلة «Problématisation» هذا الموضوع من هذه الزاوية يمكننا من فهم تداعيات الجريمة الالكترونية على البنى السوسيو اقتصادية، ووفق هذا يأتي تساؤلنا حاملا للإشكال الآتي:

الإشكالية : ما مدى تأثير الجريمة الالكترونية على اقتصاد الدول ومجتمعاتها ؟

وللإجابة على الإشكالية المطروحة وتماشيا مع العنوان المقترح، ارتأينا أن نتبع الخطة التالية لدراسة الموضوع حيث قسمناه إلى ثلاثة محاور، وسم المحور الأول بـ: الجرائم الالكترونية: الأصول والخصائص مبرزين فيه التعريف والنشأة والخصائص وكذا البرمجيات المستخدمة في الجرائم الالكترونية، الأسباب الرئيسية للجرائم الالكترونية، وفي محور ثان؛ الجرائم الالكترونية: الآثار الاقتصادية والمجتمعية تطرقنا فيه إلى الاقتصاد الالكتروني وكذا الجرائم الاقتصادية في عصر العولمة. ومن ثم اشرنا في جزئية أخرى إلى تأثيرات الجرائم الالكترونية على المجتمعات، وفي محور ثالث : الاتجاهات المستقبلية في تقانة الجرائم الالكترونية على المستويين الاقتصادي والاجتماعي وأنماط مكافحتها، تم التطرق إلى الأمن السيبراني، الاستعلام وكذا سبل المكافحة ومنه الى الإجراءات المتخذة على المستوى العربي والعالمي لمكافحة جرائم الالكترونية. سبق كل هذا مقدمة شارحة وخاتمة تشمل النتائج المتوصل إليها و التوصيات.

1- الجرائم الالكترونية: الأصول والخصائص

1-1: تعريف الجريمة الالكترونية :

بداية يجب أن نشير إلى أنه لا يوجد مصطلح قانوني موحد للدلالة على الجرائم الناشئة عن استغلال تقنية المعلومات واستخدامها ففي هدا الإطار آثر المشرع الانجليزي في قانون إساءة استخدام الحاسوب عام 1990 عدم وضع تعريف محدد لجرائم الحاسوب بغية عدم حصر القاعدة التجريمية في إطار أفعال معينة تحسبا للتطور العلمي والتقني في المستقبل.

في إطار تعريف الفقه للجريمة الالكترونية نجد أن الاتجاهات تباينت في هدا السياق بين موسع لمفهوم الجريمة المعلوماتية وبين مضيق لها، ومن التعريفات المضيقة تعرف على أنها "كل فعل غير مشرع يكون العلم بتكنولوجيا الحاسبات الآلية بقدر كبير لازما لارتكابه من ناحية لملاحقته وتحقيقه من ناحية أخرى.

وفي نفس السياق يرى الأستاذ **Tredman أن** : "الجريمة الالكترونية تشمل أي جريمة ضد المال مرتبطة بالاستخدام المعالجة الآلية للمعلومات"

ويرى الأستاذ Mass أن المقصود بالجريمة الالكترونية:" الاعتداءات القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق ربح[1].

كما يعرفها البعض الآخر بأنها: تصرف غير مشروع يؤثر في الأجهزة والمعلومات الموجودة عليها[2].

- نلاحظ أن هده التعريفات ضيقت من مفهوم الجريمة الالكترونية إذ يخرج من نطاقها العديد من الأفعال غير المشروعة يستخدم الحاسب كأداة لارتكابها.

وفق هذا يمكن القول أن الجرائم الالكترونية تتضمن تلك العمليات التي يمكن بواسطتها الدخول إلى معلومات وبيانات الآخرين سواء كانوا أفرادا أو مؤسسات أو دول والحصول عليها بدون إذن منهم بقصد استغلالها لغايات وأهداف غير مشروعة من خلال اختراق مواقعهم الخاصة، وكذالك تتضمن كل العمليات المخالفة للقانون(كالتزوير، التحريض، نشر الأفكار الإرهابية، ونشر الطرق والأساليب الإجرامية التي تؤدي إلى الذعر والخوف والترهيب ... الخ) ، والتي يستخدم فيها الحاسوب وكل التطبيقات المرافقة له.[3]

كما يمكننا القول أن الجرائم الالكترونية هي: كل فعل وكل سلوك غير مشروع أو غير أخلاقي أو غير مسموح به صادر عن إرادة جنائية يقوم به شخص ما لديه دراية ومعرفة بتكنولوجيا المعلومات المختلفة(تكنولوجيا التخزين والاسترجاع وتكنولوجيا الاتصالات الحديثة) ويوجه ضد المصلحة العامة والخاصة عبر وسط الكتروني.[4]

1-2: نشأة الهجمات السيبرانية.

جرائم المستقبل كيف ستكون؟ مصادر أمريكية كالكاتب (ألفين توفلر) مؤلف كتاب (الحروب ومناهضوها)، يجيب أنها عبارة عن كومبيوتر ضد الأقمار الصناعية وفكر وأعصاب البشر، وهي لا تتطلب أية أسلحة تقليدية بل تتطلب معلومات دقيقة وبرامج كمبيوتر، ويقول خلال 5-10 سنوات سيكون بإمكاننا أن نخاطب الدول المعادية الكترونيا وتقنيا ودون قتل نفس واحدة[5].

وكشرح لتطور الظاهرة، يمكننا ربطها مباشرة بحدثين مهمين: **الأول** باستحداث أجهزة الكمبيوتر في منتصف الخمسينيات من القرن المنصرم كأداة لمعالجة وحفظ المعلومات رقميا (Digital) رافقه تضافر جهود عدد من الشركات الخاصة والعامة، توج بتطور وحدة المعالجة المركزية(CPU) وذلك لتسهيل المهام الموكلة له، وقد تطور ذلك بصورة جذرية في العقود اللاحقة، حتى أصبح جهاز الكمبيوتر، أساسا في عمل الكثير من المؤسسات الخاصة والعامة، فضلا عن الحياة اليومية للأفراد.

أما الحدث **الثاني** فهو بظهور الشبكة العنكبوتية والذي أحدث انقلابا مثيرا في حياة البشرية من خلال التواصل ونقل المعلومات بسرعة فائقة عن طريق سيل البيانات المرسلة عبر الأثير.

وفي سياق متصل، يصف البعض أن نشور الثورة المعلوماتية الحالية، هو بمثابة الجيل الثالث للثورات التقنية التي غيرت في أسلوب الحياة وإمكانيات البشرية، وبعبارة أخرى الثورتان الزراعية والصناعية وأخيرا الثورة المعلوماتية.

لقد سارعت الدول في وتيرة استخدام الكمبيوتر لتحقيق قفزات نوعية في المجال الأمني والعسكري، وذلك في مطلع التسعينيات من القرن المنصرم حتى أطلق البعض عليها مصطلح الحرب السيبرانية الباردة(Cyber Cold War) أو سباق التسلح السيبراني (Cyber Arms Race) .

وفي بادئ الأمر لم يكن للهجمات السيبرانية صدى على المستوى الدولي، اذ نشأت الجريمة السيبرانية أولا على هيئة جرائم طالت المؤسسات المالية والمصرفية، فضلا عن الشركات المتخصصة ببرمجة نظم الاتصالات، وقد دأبت الدول على اتخاذ تدابير تشريعية لتجريمها وتحديد عقوبات لها.[6]

1-3: خصائص الجريمة الالكترونية

تتميز الجريمة الالكترونية بخصائص تميزها عن الجرائم التقليدية ولعل من أهمها ما يلي:

- **الجريمة الالكترونية جريمة عابرة للحدود:** الجريمة الالكترونية تتسم غالبا بطابع دولي ذلك لأن الطابع العالمي لشبكة الانترنت وما يرتبه من جعل معظم دول العالم في حالة اتصال دائم على الخط On Line ، فالجريمة الالكترونية لا تعترف بالحدود بين الدول والقارات فهي تعتبر شكل جديدا من أشكال الجرائم العابرة للحدود الإقليمية بين دول العالم كافة، اذ يمكن ومن خلال النظام المعلوماتي ارتكاب العديد من الجرائم مثل: جرائم التعدي على قواعد البيانات، وتزوير وإتلاف المستندات الالكترونية، الاحتيال المعلوماتي، وسرقة بطاقات الائتمان، القرصنة، وغسيل الأموال.

- **صعوبة إثبات الجريمة الالكترونية:** فالجرائم المعلوماتية تتصف بالخفاء، أي عدم وجود آثار مادية يمكن متابعتها، وهي خطيرة وصعبة الاكتشاف، أو هي صعبة في تحديد مكان وقوعها ومكان التعامل معها بسبب اتساع نطاقها المكاني وضخامة البيانات، وترجع صعوبة إثبات الجريمة الالكترونية إلى عدة أمور أهمها:[7]

✓ تقع في بيئة الكترونية يتم فيها نقل المعلومات وتداولها بالنبضات الالكترونية غير المرئية وبدون مستندات ورقية (لا تترك آثار مادية)

✓ صعوبة الاحتفاظ الفني بدليل الجريمة المعلوماتية.

✓ تحتاج الى خبرة فنية والذكاء في ارتكابها، ويصعب على المحقق التقليدي التعامل معها.

✓ تعتمد على الخداع في ارتكابها والتضليل في التعرف على مرتكبيها، وما يساعد من ازدياد عدم التعرف على مرتكبي الجرائم الالكترونية إحجام البنوك والشركات ومؤسسات الأعمال عن الإبلاغ عما يرتكب من جرائم معلوماتية تجنبا للإساءة لسمعتها وهز ثقة العملاء فيها، وكذلك إخفاء أسلوب ارتكاب الجريمة خوفا من قيام آخرين بتقليد هذا الأسلوب.

- **عدم وجود مفهوم مشترك للجريمة المعلوماتية:** من خصائص الجريمة الالكترونية عدم وجود مفهوم مشترك لماهية الجريمة الالكترونية، وكذلك عدم وجود تعريف قانوني موحد لها ولعل السبب في ذلك يرجع إلى عدم وجود تنسيق دولي في مجال الجريمة المعلوماتية، ويرجع ذلك إلى عدم وجود معاهدات دولية ثنائية أو جماعية لمواجهة الجريمة الالكترونية، أو لاختلاف مفهوم الجريمة تبعا لاختلاف النظم القانونية.
- **وقوع الجريمة المعلوماتية أثناء المعالجة الآلية للبيانات:** ويمثل هذا الشرط الأساسي الذي يتعين توافره حتى يمكن البحث في قيام أو عدم قيام أركان الجريمة الالكترونية الخاصة بالتعدي على نظام معالجة البيانات، ذلك أنه في حالة تخلف هذا الشرط تنتفي الجريمة الالكترونية.

والجريمة الالكترونية قد تقع أثناء عملية المعالجة الآلية للبيانات في أي مرحلة من المراحل الأساسية لتشغيل نظام المعالجة الآلي للبيانات سواء عند مرحلة إدخال البيانات، أو أثناء مرحلة المعالجة،أو أثناء مرحلة إخراج المعلومات.[8]

- **قلة الإبلاغ عن وقوع الجريمة الالكترونية:** لا يتم – في الغالب الأعم – الإبلاغ عن جرائم الانترنت إما لعدم اكتشاف الضحية لها وإما خشية من التشهير، لذا نجد أن معظم جرائم الانترنت اكتشافها بالمصادفة، بل وبعد وقت طويل من ارتكابها.
- **الجريمة الالكترونية جريمة مستحدثة:** تعتبر الجرائم الالكترونية –سواء التي تتعرض لها أجهزة الكمبيوتر أو التي تسخر تلك الأجهزة في ارتكابها- من الجرائم المستحدثة، فعلى الرغم من المزايا والمنافع

الايجابية المترتبة على العولمة وثورة المجتمع الالكتروني، إلا أنها ساعدت على ظهور وتعزيز أنواع جديدة من الجرائم، من أبرزها جرائم غسيل الأموال، اختراق قطاع الأعمال، سرقة الملكيات الفكرية... الخ

- **عدم كفاية التعاون الدولي في مجال الجرائم الالكترونية:** عدم وجود معاهدات دولية كافية للتسليم أو للمعاونة الثنائية أو الجماعية بين الدول تسمح بالتعاون الدولي، أو عدم كفايتها إن كانت موجودة لمواجهة المتطلبات الخاصة لجرائم الكمبيوتر وديناميةالتحريات فيها وكفالة السرعة بها.[9]

4-1: البرمجيات المستخدمة في الجرائم الالكترونية.

إن الجماعات الإجرامية المنظمة تمارس أنشطتها اللاقانونية التي يتعسر على الأجهزة الأمنية ضبطها، بيد أن هذه الحالة المتعسرة زاد من تعسرها بشكل كبير خاصة عندما طغت وسائلها الاختراقية القنوات الفضائية والالكترونيات والحواسيب والانترنت والتكتلات الاقتصادية والثورة الموسوعية ووسائل الاتصالات الجديدة، حيث استفاد الأفراد والجماعات الإجرامية من هذا الانفتاح الكوني عبر الأجهزة الالكترونية[10]، مستخدمين بذلك عديد البرمجيات التي وبواسطتها يصلون إلى أهدافهم ومن بين هذه البرمجيات يمكننا ذكر:

- ✓ **الفيروسات(Les Virus):** الفيروس الالكتروني هو برنامج يهدف الى تخريب وشطب بيانات من ذاكرة الحاسوب[11]، ويستخدم مضيفه (الكمبيوتر المصاب) لإعادة إنتاج نفسه والانتشار في أجهزة كمبيوتر أخرى، وساهمت ديمقراطية الدخول إلى فضاء الانترنت في تسريع انتشار الفيروسات الأكثر حداثة.
- ✓ **الهجوم العاصفي (Tempest-attack):** منهجية "العاصفة" تعني في الأصل عملية تسمح بالدراسة والمراقبة المناسبة للإشارات الصادرة عن أجهزة معالجة وبث المعلومات مثل الكمبيوتر، والأخيرة يتم اعتراضها قبل أن يتم إرسالها، مع مر الزمان صار معنى الكلمة أجهزة الإعلام الآلي المحمية بفض هذه المنهجية التي تمنع انتشار الإشارات الالكترومغناطيسية خارج مكان العمل.
- ✓ **حصان طروادة:** نعني بـ "حصان طروادة" البرامج التي يجري وضعها في برمجيات (التشفير/ فك التشفير) وتكون قادرة فور ذلك على إرسال المفتاح إلى المصمم عندما يكون فك الشفرة مهيئا، أو إرسال المعلومات المتعلقة بالمستخدم في مرحلة التشفير.[12]
- ✓ **هجوم الحرمان من الخدمة (Denial-of-service attack):** هجوم الحرمان من الخدمة أو هجوم الحرمان من الخدمة الموزعة: هو محاولة من القراصنة جعل جهاز أو شبكة حاسوب غير متوفرة لمستخدميها المستهدفين بمعنى حرمانهم من الخدمة التي تقدمها الشبكة، وعادة ما يستهدف منفذو هجمات الحرمان من الخدمة المواقع الإلكترونية أو الخدمات التي تستضيفها خوادم ويب رفيعة المستوى مثل البنوك وبوابات الدفع ببطاقات الائتمان والشركات.
- ✓ **الاصطياد بالرمح (Spear phishing):** وهو نوع من أنواع هجمات الاصطياد التي تركز على مستخدم واحد أو دائرة داخل منظمة، يتم شنها من خلال انتحال هوية جهة جديرة بالثقة لطلب معلومات

سرية، مثل أسماء تسجيل الدخول وكلمات المرور. وغالبا ما تظهر هذه الهجمات على شكل رسالة إلكترونية من الموارد البشرية للشركة أو أقسام الدعم الفني فيها، وقد تطلب من الموظفين تحديث اسم المستخدم وكلمات المرور الخاصة بهم، وبمجرد حصول المخترق على تلك البيانات فإنه يستطيع الولوج إلى مصادر الشبكة، وهناك نوع آخر من هجمات الاصطياد بالرمح التي تطلب من المستخدمين النقر على رابط، مما يؤدي إلى نشر برمجية تجسس خبيثة يمكنها سرقة البيانات.

- ✓ **بوتنت (Botnet) :** وهي كلمة مركبة من "روبوت" و"نتوورك"، وتعني بالتالي "روبوت الشبكة"، وهي عبارة عن مجموعة من البرامج المتصلة بالإنترنت تتواصل مع برامج أخرى شبيهة بهدف أداء مهام معينة، وقد تكون المهمة عادية مثل التحكم بقناة الدردشة على الإنترنت "آي آر سي" IRC))، أو خبيثة مثل استخدامها لإرسال بريد إلكتروني غير مرغوب به (سبام) أو المشاركة في هجمات الحرمان من الخدمة الموزعة "دي دي أو إس" (DDoS)، لكنها عادة ما ترمز إلى الجانب الخبيث.
- ✓ **دودة الحاسوب** (Computer Worm): وهي برامج حاسوب خبيثة صغيرة قائمة بذاتها قادرة على استنساخ برمجيتها من أجل الانتشار إلى حواسيب أخرى، وعادة تستخدم شبكة حاسوب لنشر نفسها معتمدة على أخطاء أمنية في الحاسوب المستهدف للوصول إليه وعلى عكس فيروس الحاسوب لا تحتاج الدودة إلى أن ترفق نفسها ببرنامج موجود كي تنتشر، وهي تسبب عادة بعض الضرر للشبكة حتى لو كان ذلك باستهلاك عرض النطاق الترددي، في حين أن الفيروسات تعمل دائما تقريبا على إفساد أو تعديل الملفات المستهدفة[13] .

وقد تستغل الدودة للقيام بأعمار تخريبية أو لسرقة بيانات خاصة ببعض المستخدمين أثناء تصفحهم الإنترنت أو إلحاق الضرر بهم أو بالمتصلين بهم، وعادة يصعب التخلص منها نظرا لسرعة انتشارها وقدرتها على التلون والتناسخ والمراوغ.

ومن البرمجيات الخبيثة أيضا:

"رانسوم وير "وهي برمجية خبيثة تقيد الوصول إلى نظام الحاسوب الذي تصيبه، وتطالب بـ"فدية" تدفع لصانع البرمجية لإزالة هذا القيد.

"آدوير "وهي برمجية خبيثة تولد إعلانات بشكل تلقائي على جهاز المستخدم أثناء تصفح الإنترنت من أجل تحقيق ربح مادي لصانعها.

" سبايوير "وهي برمجية خبيثة تساعد على جمع معلومات عن شخص أو منظمة دون علمهما، وترسل تلك المعلومات إلى طرف آخر دون موافقة المستخدم أو تؤكد سيطرتها على جهاز حاسوب دون علم صاحبه[14] .

1-5: الأسباب الرئيسية للجرائم الالكترونية

يمكن حصر الأسباب التي تدفع للقيام بالجرائم الالكترونية بما يأتي:

الدافع المادي: فمعظم عمليات الاحتيال التي تكون عبر شبكة الانترنت هدفها مادي، مثل سرقة أرقام البطاقات الائتمانية أو اختراق أنظمة بنكية ومراكز الصرافة[15]، فكما هو الحال مع العديد من الجرائم التي ترتكب خارج الإنترنت ، فإن المال هو الدافع الرئيسي لكثير من مجرمي الإنترنت. خاصة وأن مخاطر الإجرام أقل وضوحا في الشبكة العنكبوتية، إن إدراك المخاطر المنخفض جدا إضافة إلى المكافأة المالية المرتفعة يدفع العديد من مجرمي الإنترنت إلى الانخراط في استعمال البرامج الضارة بغرض سرقة الهوية ، والهجمات الاحتيالية لطلب المال. يقدر بيزنس ويك Businessweek أن الجرائم السيبرانية التي تستهدف الحسابات المصرفية عبر الإنترنت وحدها - على سبيل المثال - تقدر بحوالي 700 مليون دولار سنوياً على مستوى العالم[16].

الدافع المعنوي: بعض الأشخاص يقومون بعملية الاحتيال من اجل المتعة واثبات قدراتهم في العالم الافتراضي، عن طريق إلحاق الضرر بالآخرين، أو بدافع الانتقام.

الدافع السياسي والعنصري: تمارس بعض الطوائف عمليات الهجوم الالكتروني على طوائف اخرى أو جماعات أخرى لأهداف معينة(انتقام-تهديد-تشويش-زعزعة الأمن-الابتزاز)، كما تقوم بعض الحكومات بالتجسس والحصول على معلومات خاصة بالعدو[17].

الدافع الأيديولوجي والاخلاقي للجريمة السيبرانية: بعد أن رفضت شركات مالية مثل فيزا Visa وماستركارد MasterCardوباي بال PayPal السماح للحسابات وأصحاب البطاقات بالمساهمة في ويكيليكس غير الربحية المثيرة للجدل ، قامت مجموعة "hacktivist Anonymous" بتنسيق سلسلة من هجمات الروبوت على خوادم الشركات ، مما جعلها غير قابلة للوصول إلى مستخدمي الإنترنت. يتم تنفيذ هذه الأنواع من الهجمات لأسباب أخلاقية أو أيديولوجية أو اثنيه، حيث تضر أو تعطل أجهزة الكمبيوتر والشبكات للتعبير عن المظالم ضد الأفراد أو الشركات أو المنظمات أو حتى الحكومات الوطنية.

الأسباب البنيوية: وإلى جانب الأسباب السابقة الذكر التي تحفز المجرمين، فإن البيئة التي ترتكب فيها الجريمة السيبرانية تعمل أيضًا على تفسير انتشار الظاهرة. في حين يتم تخزين المزيد والمزيد من المعلومات الشخصية والحساسة عبر الإنترنت - زيادة المكافآت المحتملة للمجرمين السيبرانيين - لم يتحسن أمن الكمبيوتر ولا التطبيقات مثل فلاتر البريد الإلكتروني بشكل كبير من حيث التغطية. ووفقًا للشركة المصنعة لـ Norton المضاد للفيروسات - على سبيل المثال - فإن ما يصل إلى 41 بالمائة من أجهزة الكمبيوتر لم يكن لديها حماية أمنية محدثة في عام 2012[18].

2- الجرائم الالكترونية: الآثار الاقتصادية والمجتمعية

2-1: الاقتصاد الالكتروني

يعتمد الاقتصاد الحالي على المعلومات وأدواتها من حاسب آلي الى وسائل اتصال الى برمجيات، في هذا الشأن قال نائب الرئيس الأمريكي السابق "آل جور Gore في ديسمبر العام 1993 في كلمة نادي الصحافة الوطني: "اليوم تناسب التجارة ليس على الطرق الإسفلتية ولكن على الطرق السريعة المعلوماتية... فكر في البناء التحتي المعلوماتي الوطني كشبكة من الخطوط السريعة... هذه الخطوط السريعة تحمل المعلومات بدلا من الناس والبضائع.[19]

في ظل الاقتصاد الالكتروني يتجاوز إنتاج السلع المعلوماتية إنتاج السلع المادية بالنظر إلى قيمتها الاقتصادية الإجمالية، وسيتحول النظام الاقتصادي من نظام تنافسي يقوم على السعي إلى الربح إلى نظام تأليفي ذي طابع اجتماعي يسهم فيه الجميع.[20]

2-2: الجرائم الاقتصادية في عصر العولمة.

من المتوقع أن يزداد نشاط الجريمة الاقتصادية في عصر العولمة لأسباب عدة منها أن من أهم مظاهر العولمة زوال الحواجز الاقتصادية بين الدول، وشيوع النشاط الاقتصادي العابر للحدود الوطنية مما يجعل سوق الجريمة عامة معولم، وخاصة سوق الجريمة الالكترونية، والتي تستفيد من التطورات في مجال التقنيات والاتصالات عامة حتى غدت غالبية هذه الجرائم الكترونية أو فضائيةCyber ، والجريمة السيبرانية Cyber crime أصبحت تحديا لصانعي السياسات الأمنية، ذلك أن التحقيق فيها بالغ الصعوبة ويحتاج إلى خبرات فنية،كما أن الأدلة الرقمية (Digital Eudence مرد هذا النشاط الإجرامي الالكتروني وغيره من النشاط المستحدث هو تحول البنى الاجتماعية والاقتصادية إلى عالمية، والى معلوماتية والكترونية، هذا وتعد الجريمة الالكترونية الاقتصادية من النوعيات الحديثة التي تشكلت مع معطيات العولمة وبالذات في عصر التقدم التقني في الاتصالات والمعلومات ، حيث أصبحت الجرائم الالكترونية التي تمس اقتصادياتها عابرة للدول بفضل التقنيات الحديثة مما يجعل أثرها في أكثر من دولة واحدة، لذلك فهي ظاهرة دولية الملامح والشكل.

- ومن أهم تلك **الظواهر الإجرامية المستحدثة الاقتصادية الشكل** كنماذج مايلي:
  - تزويد نطاق الائتمان والاحتيال المالي الالكتروني
  - غسيل الأموال الناتجة عن الجرائم
  - الاحتيال في الملكية الفكرية
  - ابتزاز المصارف والمؤسسات المالية عن طريق التهديد بتدمير برامج الحاسب الآلي الخاصة بهم.

- القرصنة في البرامج والأقراص واستخراج نسخ منها للبيع.[21]
- التلاعب بالبيانات الاقتصادية والمالية وتزييفها أو مسحها من أجهزة الحواسيب.[22]

فنظرا لتلازم النمو الاقتصادي للدول بتوفر الأمن في المجتمع، فإن هذا لا يختلف كثيرا في حالة الاقتصاد الرقمي، خاصة مع زيادة حجم الاقتصاد الرقمي، فعلى سبيل المثال، يشير تقرير صادر عن شركة(Emarketer) إلى أن حجم التجارة الالكترونية بلغ 1.5 تريليون دولار في عام 2014 بزيادة نسبتها 20% مقارنة بعام 2013 الذي بلغ فيه 1.2 تريليون دولار، ونظرا لارتفاع معدل الجرائم السيبيرية المنظمة والخطيرة، فإن ذلك يمثل تهديدا لنو الاقتصاد الرقمي، ما لم تقد الدول بتعظيم معايير الأمن السيبيري بما يضمن الحد من هذه الجرائم.[23]

من جهة أخرى وفي في تقرير صدر حديثاً بعنوان «بيان التهديدات في قطاع الأمن السيبراني الصناعي»، قامت "**بوز ألن هاملتون**" الشركة العالمية للاستشارات والتكنولوجيا، بإلقاء الضوء على أبرز المخاطر التي تهدد أنظمة التحكّم الصناعي في العامين 2016 و2017، وعلى الإجراءات الأكثر فعالية لمواجهتها. تراقب هذه الأنظمة وتسيّر أجزاء كبيرة من حياتنا التي باتت متّصلة بعالم الانترنت اليوم، وتؤثر على الصناعات كقطاع التصنيع والأدوية والنقل والطاقة والبتروكيماويات والكثير غيرها.

وفي استفتاء أجري في العام 2015 وشمل 314 منظمة تعتمد أنظمة التحكّم الصناعي حول العالم، يعمل 20 بالمائة منها في الشرق الأوسط، أشارت 100 جهة من المعنيين بالاستفتاء إلى أن أنظمة التحكّم لديها تعرّضت للخرق أكثر من مرتين خلال الأشهر الإثني عشر الماضية.

وقال الدكتور ماهر نايفه نائب الرئيس الأول لدى بوز ألن هاملتون Booz Allen Hamilton : «**تتحقق مسيرة النجاح من خلال ضمان مقاربة متكاملة تتيح للمعنيين في القطاع التعاون في مواجهة المشاكل السيبرانية المشتركة المتعددة الأبعاد. هذا وتحتاج عملية التخفيف من الخطر لأكثر من مجرد ضبط لجدران الحماية وتحديث الأنظمة، فهي تحتاج للاستثمار في الموارد البشرية وتدريبها على السياسات والإجراءات**[24].

كما ينبغي الأخذ بعين الاعتبار كل أوجه الموقع السيبراني: التكنولوجيا والمعايير، السياسة والحوكمة، القيادة والثقافة، التخطيط والعمليات والإدارة والميزانية.

وأكد التقرير أن القطاعات الصناعية كالطاقة والتصنيع والخدمات والنقل هي الأكثر عرضة لمخاطر الهجمات السيبرانية. وكان فريق الاستجابة للطوارئ والحوادث السيبرانية في أنظمة التحكّم الصناعي قد أبلغ عن أكثر من 800 حادث أمني سيبراني على مستوى العالم منذ العام 2011، حيث وقعت غالبية تلك الحوادث في قطاع الطاقة.

وينذر تقرير «بيان التهديدات في قطاع الأمن السيبراني الصناعي» ببيئة سيبرانية باتت خطيرة أكثر من السابق بالنسبة لمشغّلي أنظمة التحكّم الصناعي[25]..

وفي هذا الصدد يكتب المدير السابق لجهاز الاستخبارات الفرنسية **"بيار ماريون"** ملخصا لسلوك الدول التي تمارس الجوسسة الاقتصادية مع حلفائها العسكريين والسياسيين" **نحن حلفاء، هذا صحيح، لكن في مجال الاقتصاد والتكنولوجيا نحن متنافسون"** . من جانبه يضيف في نفس السياق وبكثير من التفاصيل "ستانفيلد تونر" مدير الاستعلام(1977-1981) تحت إدارة الرئيس جيمي كارتر Jimmy Carter : "إذا كان يجب الاعتراف بالقوة الاقتصادية كعنصر مهم من الأمن القومي، لا يختلف عن القوة العسكرية، فلماذا إذن يجب على الولايات المتحدة الأمريكية أن تخشى سرقة واستخدام الأسرار الاقتصادية".

في جوان 1994 لاحظ "فلاديمير تسخانوف" رئيس المديرية العامة لمكافحة التجسس الاقتصادي الروسي: "فعلا، انه منذ نهاية الحرب الباردة تزايدت أنشطة أجهزة الاستخبارات الأجنبية الموجهة ضد الاقتصاد الروسي بما في ذلك بلدان المعسكر الشرقي سابقا والبلطيق، انتقلت الأولويات على ما يبدو من المواجهة العسكرية إلى المواجهة الاقتصادية.." صار العالم مجالا للتبادلات بدون إنصاف.

ففي العام 1996 مثلا، نجحن كاميرات تعمل بالأشعة تحت الحمراء في جمع معلومات استعلامية حول ابتكارات تكنولوجية ونماذج من شركة فولسفاغن، حيث ظلت الكاميرات مدسوسة داخل مراكز وحلبات الاختبار وكانت تسير عبر الحاسب لتنقل الصور عن طريق الموجات الهرتزية ومرت الحادثة دون اكتشاف أمر فاعليها.[26]

3-2: تأثيرات الجرائم الالكترونية على المجتمعات

إن التطور التكنولوجي اوجد ما يسمى بعالمية الثقافة التي أزالت الحواجز بين الشعوب وأثبت عدم فاعلية وسائل المنع أو مقص الرقيب ،[27]حيث لا يتوقف تأثير الجرائم المتصلة بالكمبيوتر عند الأثر المادي الناجم عنها وإنما يتعدى ذلك ليهدد نظام القيم والنظام الأخلاقي خاصة في المجتمعات المحافظة والمغلقة (التلوث الثقافي) .[28]

وللحديث عن دور الانترنت هنا يكفي أن نعلم أن شبكة الإنترنت تتضمن حوالي مليون صورة ورواية أو وصف له علاقة مباشرة وواضحة بالجنس[29]. وقد تضاعف هذا الرقم عشرات المرات خلال فترة قصيرة .

كما كشفت دراسة لمؤسسة مراقبة الانترنيت المملكة المتحدة وحدها تشهد جريمة إلكترونية جديدة كل عشر ثوان حيث شهدت البلاد ارتكاب أكثر من ثلاثة ملايين جريمة إلكترونية خلال العام الماضي. وتوصل التقرير إلى أن جرائم الإنترنت التي تتراوح بين الحصول على معلومات شخصية حول مستخدمي الإنترنت،

والتحرش الجنسي بهم، وممارسة الاحتيال عبر شبكة المعلومات الدولية يتم ارتكابها في بريطانيا بمعدل جريمة واحدة كل عشر ثوان .

وحسب إحصاءات قدمتها «مؤسسة مراقبة الإنترانت » ، كان عدد المواقع الإباحية للقاصرين، سنة 2004، يصل إلى 3433 موقع. وسيقفز هذا الرقم إلى 10656 موقع سنة 2006. وتتواجد 54 في المائة من المواقع الإباحية للقاصرين بالولايات المتحد الأمريكية وأن عدد الجرائم الجنسية بلغ نحو 850 ألف حالة، فيما بلغت عمليات سرقة الهوية 92 ألف حالة، بينما وصل عدد جرائم الاحتيال للحصول على الأموال نحو 207 آلاف عملية، بزيادة 30 في المائة عن العام السابق، في حين تمت نحو 145 ألف عملية اختراق للحاسبات عبر الإنترنت .

ويرى الخبراء ان هذا الوضع نشأ لأنه لا يوجد حاليا تعريف واضح و موحد للجرائم الالكترونية بالرغم من المحاولات العديدة التي قامت بها الدول المتقدمة و على رأسها أمريكا و هيئات الأمم المتحدة و مجموعة الدول الأوروبية، وهذا دون شك سيحتاج إلى زمن طويل و مثابرة جادة و تكاتف دولي لان هذه الجرائم لا تعرف الحدود الجغرافية أو السياسية[30] .

- **هناك أنواع أخرى من جرائم الإنترنت التي تمس المجتمع نذكر منها ما يلي:**

✓ التهديدات: تهديد سلامة الأشخاص من خلال استخدام شبكة الكمبيوتر.

✓ المواد الإباحية المتعلقة بالأطفال، والتي تشمل إنشاء وتوزيع أو الوصول إلى المواد التي تستغل الأطفال جنسيا دون السن القانونية.

✓ التهريب: نقل مواد غير الشرعية عبر الإنترنت.

✓ تبييض الأموال(غسيل الأموال)، الذي يعني نقل عائدات النشاط الإجرامي بقصد إخفاء مصدر الأموال ووجهتها.

✓ البلطجة الإلكترونية: والتي تتضمن المطاردة، وإرسال رسائل تهديد، وتغيير الصور ثم توزيعها بقصد المضايقة أو التخويف.

✓ الإرهاب الالكتروني، وهو العنف الذي يكون له دوافع سياسية، ترتكب ضد السكان المدنيين من خلال استخدام تكنولوجيا الحاسوب.

✓ الاتجار بالبشر عندما يكون من إما التماس أو الإعلان على الإنترنت سهلت استغلالهم في البغاء

✓ لعب القمار على الانترنت، الذي يعتبر غير قانوني حاليا في الولايات المتحدة على سبيل المثال.

✓ القرصنة، وهو الوصول غير المشروع لموارد الكمبيوتر أو الشبكة دون ترخيص

✓ الأذى الجنائي، الذي يتضمن بيانات ضارة أو تدمير أو المعلومات الموجودة على الشبكة بقصد حرمان مالكي ومستخدمي المعلومات. هذا ويمكن أن تشمل تركيب الرموز الخبيثة مثل الفيروسات وأحصنة طروادة، والديدان.[31]

- ✓ الابتزاز والاحتيال وسرقة الهوية واستغلال الأطفال
- ✓ حقوق الطبع والنشر أو التعدي على العلامة التجارية: فسرقة الملكية الفكرية تهدد القدرة التنافسية الوطنية والابتكار الذي يدفعها.

تتجاوز هذه التحديات الحدود الوطنية. يمكن أن يؤدي انخفاض تكاليف الدخول إلى الفضاء السيبراني والقدرة على إنشاء وجود افتراضي مجهول إلى "ملاذات آمنة" للمجرمين[32].

- تأثيرات الجريمة الالكترونية على الأشخاص الطبيعيون:

يعتبر الأشخاص الطبيعيون أكثر ضحايا الجرائم المرتكبة عبر الانترنت، وذلك راجع إلى التزايد المستمر والكبير في أعداد المشتركين من خلال الشبة العالمية للانترنت، فلم تعد الجرائم المرتكبة عبر الانترنت مقتصرة على القطاعات المالية والعسكرية، وبالتالي فإن كثيرا من الأشخاص يتعرضون لجرائم النصب والسرقة والإتلاف ومن الطبيعي أن تكون شبكة الانترنت المجال الخصب لارتكاب تلك الجرائم، حيث أصبحت ملايين الأسرار المتعلقة بالناس سواء كانوا فراد عاديين أو في مراكز معينة في متناول كل من يستطيع اختراق شبكة المعلومات التي تنطوي على كل هذه الأسرار.[33]

تعتبر جرائم الإتلاف عن طريق الفيروسات من أكثر الجرائم التي يتعرض لها الأشخاص الطبيعيون عبر البريد الالكتروني الذي يعتبر من أهم البوابات التي يقفز منها القراصنة إلى أجهزة الأشخاص وتعتبر من أكثر الجرائم التي يتعرض لها الأشخاص أيضا سرقة أرقام بطاقات الائتمان.

يتعرض كذلك الأشخاص لجرائم النصب على شبكة الانترنت وخير مثال على ذلك وقوع الكثير ن الشعب الأمريكي ضحية لجريمة النصب من قبل أشخاص مستغلين الحادث الإرهابي الذي حدث في الولايات المتحدة الأمريكية في 9/11 حيث قامت العديد من الجهات بإنشاء عدة مواقع على شبكة الانترنت بغرض جمع التبرعات للضحايا، وعلى هذا الأساس قامت حكومة الولايا المتحدة الأمريكية بتحذير رعاياها من الوقوع ضحايا لتلك العمليات الإجرامية.

زيادة على هذا هناك العديد من الجرائم التي تتعلق بالاطلاع الغير المشروع على البيانات الشخصية وانتهاك الحياة الخاصة للأشخاص واستغلالها .

تتمة لما سبق يشير تقرير مؤسسة « We are social» إلى أن نحو 2.5 مليار نسمة أي ما يعادل 35% من سكان العالم يستخدمون الانترنت في عام 2014، وذلك بزيادة تقدر بـ 135 مليون مستخدم عن العام السابق، ولا شك في أن هناك دور للانترنت في تعبير المواطن عن تطلعاته في المجالات المختلفة سواء سياسية أو علمية أو اقتصادية أو ثقافية . الخ، وبعض من المواد المنشورة مفيدة وتؤثر بالإيجاب على أخلاقيات المجتمع، والبعض الآخر يمثل تهديدا له، كالمواد الإباحية، والإرهاب، ونشر الفكر المتطرف، ومحاولة تجنيد الشباب، والترويج للاتجار بالممنوعات ... الخ، بالإضافة إلى جعل المواطنين أكثر انكشافا على الثقافات الأخرى، من ثم تعرض القوميات والهويات لعمليات اختراق خارجي، قد تؤثر على الأفكار

والتوجهات والعادات، خاصة أنها قد تخرج عن النسق العام للدولة، وتتسبب في تهديد السلم الاجتماعي، وعليه فإنه لا بد من العمل على توعية المواطنين بتلك النوعية من المخاطر لتحقيق الأمن السيبيري في بعده المجتمعي.[34]

3- الاتجاهات المستقبلية في تقانة الجرائم الالكترونية على المستويين الاقتصادي والاجتماعي وأنماط مكافحتها

3-1: الأمن السيبراني:

نعني بالأمن السيبراني مجموع الوسائل التقنية والتنظيمية والإدارية المتخذة لمنع الاستخدام غير المصرح به، سوء استغلال المعلومات الالكترونية ونظم الاتصالات والمعلومات التي تحتويها، وذلك بهدف ضمان تيسر واستمرارية عمل نظم المعلومات وتعزيز حماية وسرية وخصوصية البيانات الشخصية واتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين من المخاطر في الفضاء السيبراني.

وواجبات الأمن السيبراني هي:

- يشمل الأمن السيبراني مجموع الأطر القانونية والتنظيمية وإجراءات سير العمل بالإضافة إلى الوسائل التقنية والتكنولوجية، وهي تمثل الجهود المشتركة للقطاعين الخاص والعام الهادفة الى حماية الفضاء السيبراني الوطني.
- التركيز على ضمان تأمين أنظمة المعلومات وتقوية الخصوصية.
- حماية سرية المعلومات الشخصية.
- اتخاذ جميع الإجراءات الضرورية لحماية المواطنين والمستهلكين من مخاطر الفضاء السيبراني.
- يسعى الأمن السيبراني إلى تحقيق خصائص أمن أصول المؤسسات والمستخدمين والحفاظ عليها وحمايتها من المخاطر الأمنية ذات الصلة في البيئة السيبرانية[35]

الأمن السيبراني يعتمد على مزيج مركب من التحديات التقنية، السياسية، الاجتماعية والثقافية حسب توصيات الاتحاد الدولي للاتصالات، إن صلاحية الأمن السيبراني الوطني تعتمد على **الركائز الخمسة الآتية:** تطوير إستراتيجية وطنية للأمن السيبراني وحماية البنية التحتية للمعلومات الحساسة والسعي لتعاون وطني بناء بين الحكومة وشركات الاتصالات والمعلومات وردع الجريمة السيبرانية وخلق قدرات وطنية لإدارة حوادث الحاسب الآلي، والسعي لبناء ثقافة وطنية فيما يتعلق بالأمن السيبراني.

إن الأمن السيبراني يشكل مجموع الأطر القانونية والتنظيمية، الهياكل التنظيمية، إجراءات سير العمل بالإضافة إلى الوسائل التقنية والتكنولوجية والتي تمثل الجهود المشتركة للقطاعين الخاص والعام، المحلية والدولية والتي تهدف إلى حماية الفضاء السيبراني الوطني، مع التركيز على ضمان توافر أنظمة المعلومات

وتمتين الخصوصية وحماية سرية المعلومات الشخصية واتخاذ جميع الإجراءات الضرورية لحماية المواطنين والمستهلكين من مخاطر الفضاء السيبراني .

تبيّن توصيات الاتحاد الدولي للاتصالات وأفضل الممارسات الدولية أن الأمن السيبراني يعتمد على مزيج مركب من التحديات التقنية، السياسية، الاجتماعية والثقافية .

وبشكل أدق فإن صلاحية الأمن السيبراني الوطني تعتمد على الركائز الخمسة التالية:

1. تطوير إستراتجية وطنية للأمن السيبراني وحماية البنية التحتية للمعلومات الحساسة.
2. إنشاء تعاون وطني بين الحكومة ومجتمع صناعة الاتصالات والمعلومات.
3. ردع الجريمة السيبرانية.
4. خلق قدرات وطنية لإدارة حوادث الحاسب الآلي.
5. تحفيز ثقافة وطنية للأمن السيبراني.

ان نقطة انطلاق الأمن السيبراني الوطني تبدأ بتطوير سياسة وطنية لرفع الوعي حول قضايا الأمن السيبراني والحاجة لإجراءات وطنية والى التعاون الدولي. أما الخطوة الثانية فتتمثل بتطوير المخطط الوطني لتحفيز الأمن السيبراني بهدف تقليص مخاطر وأثار التهديدات السيبرانية وتتضمن المشاركة في الجهود الدولية والإقليمية لتحفيز الوقاية الوطنية من،و التحضير لـ، والاستجابة إلى و التعافي من الحوادث السيبرانية[36] .

2-3: الاستعلام كآلية مواجهة

يعد الاستعلام الاقتصادي حاليا السلاح المناسب لضبط استراتيجيات المنافسة في سوق تتطور باستمرار، ومع ذلك تبقى مساهمة الجوسسة حاسمة، فالأخيرة، الموجهة نحو البحث عن العوامل التنافسية وغزو الأسواق الخارجية، تسمح للجهات الراعية لها بتقليص نفقاتهم والرفع من أدائهم وزيادة حصصهم في السوق على حساب منافسيهم، تملي الآثار المحتملة لهذه التصرفات على سوق العمل وبالتالي على السلم الاجتماعي، على الحكومات والمؤسسات تصور وتنفيذ الاستراتيجيات التجارية وبرامج التحسيس، في هذا السياق تجد المصالح الخاصة نفسها مدعوة للكشف عن التهديدات التي قد تؤثر على المصالح الاقتصادية والتجارية لبلدانهم، ورصد فرص خدمة هذه المصالح.37

3-3: سبل المكافحةّ:

لم يتم الاقتصار على عملية الاهتمام بالأمن الالكتروني على البعد التقني وحسب بل تجاوزه إلى أبعاد أخري أصبحت ذات علاقة في تفسير القضية مثل الإبعاد الثقافية والاجتماعية والاقتصادية والعسكرية وغيرها ، والتي دفعت إلى أهمية أن تكون مرتكزات لتعزيز الأمن الالكتروني ،وهو ما عمل على دعم حقيقة

ان الاستخدام غير السلمي للفضاء الإلكتروني يؤثر على كل من الرخاء الاقتصادي والاستقرار الاجتماعي لجميع الدول التي أصبحت تعتمد على البنية التحتية الكونية لمعلومات[38] ، فعملت الدول إلى إنشاء قاعدة تقنية وكذا قانونية لمجابهة هذا التهديد، إلا أن القانون يواجه صعوبة في التكيف مع الجريمة السيبرانية. و بالتالي، من الصعب مكافحة الجرائم الإلكترونية باستخدام الأساليب والمنظمات التقليدية. على سبيل المثال ، عادة ما تعتمد وكالات إنفاذ القانون الهرمية والساكنة على قوانين وأنظمة وإجراءات داخلية محددة للعمل بفعالية ضد المجرمين. الأدوات الفعالة بالنسبة للجهات الموكلة بإنفاذ القانون تجد نفسها غير فعالة في المجال الافتراضي. يمكن لتكنولوجيا وتكتيكات المجرمين الإلكترونيين أن تتغير بشكل أسرع من قدرة القانون على التكيف معها[39].

هذا و يرى البعض أنه وفي سبيل مكافحة الجريمة الالكترونية يجب أن تتحرك الدول المختلفة في محورين، الأول: داخلي بحيث تتماشى قوانينها الداخلية من هذا الشكل الجديد من الجرائم، والثاني: دولي عن طريق عقد الاتفاقيات الدولية، وهذا بالطبع يقتضي التنسيق بين قوانين الدون المختلفة لضمان تحقق مبدأ ازدواجية التجريم، وحتى لا يستفاد مجرمو المعلوماتية من عجز التشريعات الداخلية من جهة، وغياب المعاهدات الدولية التي تعالج سبل مواجهة هذه الجرائم من جهة أخرى.[40]

حيث أن انتشار الجريمة الالكترونية قد يؤدي إلى خلل عام قد يهدد المجتمع كله في اقتصاده وسيادته وأمنه القومي بما يتطلب حماية المواقع المهمة والإستراتيجية من خلال استخدام التقنيات المتطورة ووسائل الكشف المبكر عن عمليات الاختراق[41].

3-4: الإجراءات المتخذة على المستوى العربي والعالمي لمكافحة جرائم الالكترونية.

سنت عدد من الدول الأوربية قوانين خاصة بجرائم الانترنت والحاسوب مثل بريطانيا وهولندا وفرنسا والدنمارك والمجر وبولندا واليابان وكندا. كما اهتمت البلدان الغربية بإنشاء أقسام خاصة بمكافحة جرائم الإنترنت، بل إنها خطت خطوة إلى الأمام وذلك بإنشاء مراكز لاستقبال ضحايا تلك الجرائم.

حيث لا يقف دور القانون علي مجرد تنظيم العلاقات المترتبة علي التقدم التكنولوجي بل إنه يجب أن يحمي القيم التي تحيط باستخدام التكنولوجيا، ويحدد المسار الصحيح الذي يجب أن يسلكه التقدم التكنولوجي حتى لا يتخذه المجرمون أداة لتطوير وسائل إجرامهم، بل يكون علي العكس من ذلك وسيلة لمحاربة هذا الإجرام، وهو ما يوجب على القانون أن تمتد نصوصه إلي الأنشطة الجديدة التي تفرزها

التكنولوجيا حتى تحدد الجريمة في نصوص منضبطة واضحة، ولا يترك بحثها إلي نصوص قانون العقوبات التقليدي، التي قد تتسم بعدم اليقين القانوني أو لا تتسع لملاحقة الأنماط الجديدة من الإجرام.

وقد تتجاوز نتائج هذه الجرائم إلى وقوع جرائم أخرى تهدد الحق في الحياة والسلامة البدنية، إذا ما أدي العبث في المعلومات إلى تغيير طريق العلاج أو تركيبة الدواء.

و قد تؤثر على نطاق الخدمات الإلكترونية وقطاعات التنمية الاقتصادية، وتكنولوجيا المعلومات، الأمر الذي يتطلب إعادة هيكلة قطاع الاتصال، وتدعيم دور الدولة في حماية المستخدمين تكنولوجيا الاتصالات، من خلال إجراءات تتميز بالشفافية الكاملة، خاصة أننا نواجه تحديات جديدة بما يعرف بالجريمة الإلكترونية، التي يجب مكافحتها، لتشجيع الاستثمار وحماية حقوق الملكية الفكرية، الأمر الذي يستلزم ألا يتم بمعزل عن الثوابت التشريعية والقانونية، فالتقدم التكنولوجي أفرز أنماطا جديدة من الجريمة، وكذا من المجرمين، فكان للتقدم في العلوم المختلفة أثره على نوعية الجرائم، واستغل المجرم ثمرات هذه العلوم في تطويع المخترعات العلمية الحديثة لخدمة أهدافه الإجرامية، فالمشكلة الرئيسية لا تكمن في استغلال المجرمين الإنترنت، وإنما في عجز أجهزة العدالة عن ملاحقتهم، وعدم ملاحقة القانون لهم ومسايرة التكنولوجيا الجديدة لتشريعاته.[42]

وعلى مستوى الدول العربية يعتبر انعدام وجود إستراتيجية عربية لمواجهة جرائم الحاسب الآلي سيفضي في السنوات القليلة القادمة الى فشل هذه التقنية وتعرضها للكثير من النهب المنظم من قبل المجرمين.

لهذا يجب وضع إستراتيجية في العالم العربي عن طريق تطوير القوانين والأنظمة التشريعية الحالية لمواجهة ظاهرة الجريمة الالكترونية التي تتطور مع مرور الوقت وهذا من خلال:

- توفير البيئة المناسبة لتطوير القدرات الفنية البشرية لمكافحة جرائم التقنية.
- تحقيق التعاون والتكامل بين الأجهزة الأمنية في العالم العربي من جانب والقطاع الخاص من جانب أخر.
- دعم البحوث الخاصة في هذا المجال والمدعمة بالإحصائيات الدقيقة حول هذه الظاهرة.
- نشر الوعي الأمني على المستوى الشعبي.

- تطوير البنية التحتية الفنية اللازمة لمراقبة أنشطة المعلومات. وإنشاء معاهد خاصة في مجال جناية التقنية مهمتها تطوير القدرات العربية في مجال معالجة وحفز وتبويب الأدلة الجنائية والأبحاث.
- تطوير المناهج في كليات الشرطة في العالم العربي كي تتماشى مع تطور هذه الظاهرة.
- أخيرا يجب ربط هذه النشاطات والآليات بعضها ببعض لوصول الى درجة عالية من الجدوى والتنسيق.

هذه الأسس تعتبر مطلبا ملحا في الوقت الراهن وذلك نتيجة للقصور الواضح في البنية الأساسية لمكافحة الجرائم الالكترونية في العالم العربي، هذا القصور ، في تصوري نابع من الآتي[43]:

- عدم وجود التجهيزات الفنية المتطورة، وعدم توفر الربط الشبكي اللازم بين إدارات الأمن الجنائي لتبادل المعلومات والخبرات
- قلة الكوادر البشرية المتخصصة في مجال التقنية، وقلة الدعم المادي والمعنوي لتطويرها.
- قلة التشريعات اللازمة للحد من هذه الظاهرة.

خاتمة:

كما سبق وأن ثبت أن للجرائم الالكترونية تأثير بليغ على الاقتصاد وكذا على المجتمع، والاستخدام غير السلمي للفضاء الإلكتروني يؤثر على كل من الرخاء الاقتصادي والاستقرار الاجتماعي لجميع الدول التي أصبحت تعتمد على البنية التحتية الكونية لمعلومات، و على الدولة العمل على تأمين المستخدم النهائي (المستهلكين والشركات والوكالات الحكومية) ، في المقام الأول من خلال تبادل المعلومات ، وتشجيع اعتماد المعايير التقنية، والاستثمار في الأمن السيبراني، ومواكبة هذا التزاوج بين الجريمة والتطور الالكتروني ، واتخاذ أفضل الممارسات القانونية، التقنية وكذا الردعية تجاه هذا النوع من الجرائم. في حين أن تحسين الأمن لدى المستخدم النهائي هو جزء هام من المشكلة، والعمل أيضا على تحسين أمن منتجات تكنولوجيا المعلومات التجارية وتعطيل عناصر تمكين الجريمة السيبرانية في السوق السوداء التي يمكن أن يكون له تأثير يغير قواعد اللعبة على وضع الأمن السيبراني لدينا.

الهوامش:

---

[1] نهلا عبد القادر المومني، **الجرائم المعلوماتية**،ط1(عمان: دار الثقافة، 2008)،ص ص.46-48.

[2] عبد الفتاح بيومي حجازي، **الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت**، (مصر: دار الكتب القانونية، 2006)، ص2.

[3] هايل عبد المولى طشطوش، **الإرهاب حقيقته ومعناه، دراسة تحليلية للإرهاب من حيث المعنى، الخلفية التاريخية، الدوافع والأسباب، الأشكال والأنواع**، الإرهاب المعاصر، ط1،(الأردن: دار الكندي للنشر والتوزيع، 2008)،ص ص 208-209.

[4] جعفر حسين جاسم، **حرب المعلومات بين ارث الماضي وديناميكية المستقبل**(عمان- الأردن: دار البداية،2010).ص 64.

[5] عبد القادر المخادمي، **الحرب الناعمة هل تكون بديلا لحروب المستقبل**؟(الجزائر: ديوان المطبوعات الجامعية، 1015) ، ص 153.

[6] أحمد عبيس نعمة الفتلاوي،"الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر"، (بحث منشور في كلية القانون بجامعة الكوفة- العراق، 2015)، ص ص 9- 11 .

[7] خالد ممدوح إبراهيم، **الجرائم الالكترونية، ط 1**، (الإسكندرية: دار الفكر الجامعي،)2008،ص ص 87-89.

[8] خالد ممدوح إبراهيم، المرجع نفسه، ص ص 83-85.

[9] المرجع نفسه، ص ص 86-87.

[10] معن خليل العمر، **الجريمة المنظمة والإرهاب**،ط 1، عمان-الأردن: دار الشروق للنشر والتوزيع،2013، ص 183.

[11] بسام عبد الرحمن المشاقبة، **الأمن الإعلامي**،ط 1،(عمان، الأردن:دار أسامة للنشر والتوزيع2012)، ص165. .

[12] محمد خلفاوي، **الاستعلام رهان حرب صامتة**، ط 2، (درارية-الجزائر، 2016) ، ص. 231.

[13] القرصنة الالكترونية سلاح العصر الرقمي، مقال في موقع الجزيرة للدراسات ، تم تصفح الموقع يوم 02-05-2018. https://goo.gl/t74o8z

[14] المرجع السابق.

[15] أسامة سمير حسين، **الاحتيال الالكتروني الوجه القبيح للتكنولوجيا**،ط1 (عمان: الجنادرية للنشر والتوزيع، 2011)، ص 95.

[16] *Edward Mercer, "*Causes of Cyber Crime", **itstillworks web cite**, available from *https://goo.gl/JY3tYj.*

[17] أسامة سمير حسين، ص 96

[18] Edward Mercer , Op.cit.

[19] عباس ابو شامة عبد المحمود، عولمة الجريمة الاقتصادية، **مركز الدراسات والبحوث لجامعة نايف العربية السعودية**، 2007، ص 47.

[20] السيد ياسين، **المعلوماتية وحضارة العولمة: رؤية نقدية عربية**،ط 3،(القاهرة: نهضة مصر للطباعة والنشر والتوزيع، 2006)، ص 13.

[21] عباس ابو شامة عبد المحمود، المرجع نفسه، ص ص 45-46.

[22] إيهاب خليفة، القوة السيبرانية نمط جديد لممارسة التأثيرات غير التقليدية في العلاقات الدولية، **مفاهيم المستقبل ملحق شهري صادر عن مجلة اتجاهات الأحداث**، العدد 6(جانفي 2015): 2.

[23] محمد مختار، هل يمكن أن تتجنب الدول مخاطر الهجمات الالكترونية؟، **اتجاهات الأحداث**، العدد 6، (2015): 6.

[24] المؤسسات الصناعية تواجه خطر الهجمات السيبرانية، مقال من موقع البيان، تم تصفح الموقع يوم 14-02-2017. https://goo.gl/Ehbonz

[25] المرجع نفسه.

[26] محمد خلفاوي، مرجع سابق، ص ص 183-184.

[27] عبد الرزاق محمد الدليمي، الإعلام والعولمة،ط 1(الأردن: دار مكتبة الرائد العلمية، 2004) ص17.

[28] عبد العالي الديربي، "الجريمة المعلوماتية، تعريفها، أسبابها وخصائصها"، **دوريات المركز العربي لأبحاث الفضاء الالكتروني**، تم تصفح الموقع يوم 10-05- 2018 https://goo.gl/hePsVK

[29] حسنين المحمدي بوادي، إرهاب الانترنت الخطر القادم، (الإسكندرية: دار الفكر الجامعي، 2002)، ص 65.

[30] رجاء كامل، الجرائم الالكترونية.. الخطر داخل البيوت،الموقع الرسمي لوزارة الدفاع لدولة السودان، تم تصفح الموقع يوم 15-02-2017. https://goo.gl/vup3ob

[31] Cyber crime , "National Crime Prevention Council Report" , USA.2012. p 2

[32] International Stratrgy For CyberSpace, Prosperity, Security and Openness in a Networked Word, May 2011. Book online. https://goo.gl/3T9MnZ

[33] صغير يوسف،" الجريمة المرتكبة عبر الانترنت"،(مذكرة لنيل شهادة الماجستير في القانون، تخصص القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية بجامعة مولود معمري تيزي وزو، الجزائر، 20013)، ص 23.

[34] محمد مختار، مرجع سابق، ص ص 6-7.

[35] حمزة صيوان عطية الفتلاوي، "الأمن السيبراني والحروب السيبرانية"، **جريدة خيمة العراق الصادرة عن وزارة الدفاع العراقية** ، 357، 4 مارس 2015، ص 10.

[36] د.ذ.ك، "محة عامة حول الأمن السيبراني"، موقع الهيئة المنظمة للاتصالات في الجمهورية اللبنانية ، تم تصفح الموقع يوم 05-05-2018. https://goo.gl/k3drZh

[37] محمد خلفاوي، مرجع سابق، ص ص 183-184

[38] عادل عبد الصادق، "خطر الحروب السيبرانية عبر الفضاء الالكتروني"، مقال في موقع لغة العصر، تم تصفح الموقع يوم 12-05-2018 . https://goo.gl/e3Nm3q

[39] David Alfredo, "Causes of Cyber Crime", techwalla web cite, available from https://goo.gl/cPucR4 retrieved 10-05-2018

[40] خالد ممدوح إبراهيم، **الجرائم الالكترونية**، ط 1(الإسكندرية: دار الفكر الجامعي، 2008)، ص ص 83-84

[41] رجاء كامل، مرجع سابق.

[42] سمير سعدون مصطفى وآخرون، الجريمة الالكترونية عبر الانترنت أثرها وسبل مواجهتها، **منشورات المعهد التقني كركوك** (2010): 6.

[43] مصطفى يوسف كافي، **جرائم الفساد-غسيل الأموال-السياحة- الإرهاب الالكتروني-والمعلوماتية**، ط1(عمان: مكتبة المجتمع العربي للنشر والتوزيع، 2014)، ص ص 153-156.