واقع جرائم تكنولوجيا الإعلام والاتصال في العالم و آليات مكافحتها

د. زبيدي البشير جامعة الوادي – الجزائر-

أ.حفوظة الأمير عبد القادر جامعة تلمسان – الجزائر-

ملخص:

إن التطور الحاصل في تكنولوجيا الإعلام والاتصال، وظهور شبكة الانترنت بكل ما حملته من تقدم وخدمات لم يمر على العالم بسلام، لأنه بقدر ما أحدث آثار ايجابية وغير نمط حياة المجتمعات وساهم في التطور والرقي في جميع المجالات ولاسيما المعاملات الالكترونية، بقدر ما كان له أثر سلبي على حياة الناس ومصالح الدول، كل هذا تجلى في تطويع الانترنت والوسائل الالكترونية لتكون عالما من عوالم الجريمة، وهكذا ظهرت إلى الوجود الجرائم الالكترونية بشتى أنواعها، وسنحاول في بحثنا هذا التطرق إلى عرض مجهودات الدول العربية في مواجهة ومكافحة هاته الجرائم.

Abstract :

The evolution in the information and communication technology, and the emergence of the Internet with all what it carried as progress and services, this is not passed peacefully on the world, because as much as it affected positive issues and it changed in communities life style and contributed to the development and progress in all fields, particularly electronic transactions, as much as it had a negative impact on people's lives and interests of the states, all of this was reflected in the adaptation of the internet and electronic means to be a world from the worlds of crime, and so came into being the electronic crimes of various kinds, and we will try in our research that address the development of electronic transactions and the definition of what the cyber-crime and what the mechanisms to ensure combating it.

مقدمة:

في ظل التطور الهائل الذي شهده مجال الإعلام والاتصال والذي رافقه التطور الكبير في تكنولوجيات الحواسيب والأجهزة الذكية، أدى ذلك إلى ظهور أدوات واختراعات وخدمات جديدة نتج عنها نوع جديد من المعاملات يسمى بالمعاملات الالكترونية والذي يقصد بها كل المعاملات التي تتم عبر أجهزة الكترونية مثل الحاسوب، شبكة الانترنيت، الهاتف المحمول(الهواتف الذكية)، و نتيجة التطور الكبير والسريع لهذه الأجهزة وضعف القدرة على المرافقة و المراقبة والتحكم، ظهر نوع جديد من الجرائم يسمى بالجريمة الالكترونية أو المعلوماتية أو التقنية، والتي هي عبارة عن نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي أو الهواتف الذكية الموصولة بشبكة الانترنيت بطريقة مباشرة أو غير مباشرة لتنفيذ الفعل الإجرامي وأصبحت هذه الجرائم في وقتنا الراهن تهدد أمن وسلامة الأفراد أو المؤسسات أو حتى الحكومات، وهو ما يقتضي الإسراع في اتخاذ الإجراءات اللازمة والتي من شأنها التقليل من حدة هذا النوع من الجرائم.

من خلال مما سبق تبرز الإشكالية الرئيسية لهذه الورقة البحثية، والمتمثلة في:

- **ما هو واقع جرائم تكنولوجيا الإعلام والاتصال في العالم؟ و ما هي سبل مواجهتها ومكافحتها؟**

أهمية الموضوع:

ترجع أهمية موضوع جرائم تكنولوجيا الإعلام والاتصال في الانتشار الواسع لهذا النوع من الجرائم والذي رافق الاستخدام الواسع للمعاملات الالكترونية على الصعيد الدولي والإقليمي والوطني هذا من جهة، ومن جهة أخرى فقد أصبحت جرائم تكنولوجيا الإعلام والاتصال مُتلازمة مع التطور السريع والهائل في مجال تكنولوجيا الاتصالات والمعلومات، فنتيجة للتقدم الكبير في استخدامات الشبكة العنكبوتية (الإنترنت)، طفت الجرائم الالكترونية بصورها المُختلفة، وأصبحت تهدد الأمن المعلوماتي للأفراد، المؤسسات والحكومات.

منهج البحث المتبع :من أجل الإجابة على التساؤل المطروح وبغية اختبار الفرضيات اعتمدنا في البحث على المنهج الوصفي التحليلي والذي يتناسب مع موضوع الدراسة من خلال وصف جرائم تكنولوجيا الإعلام والاتصال وتحليلها لتحديد أنواعها و مسبباتها ومحاولة إيجاد الآليات الكفيلة للتصدي لها.

ولتحقيق أهداف البحث، فقد تم تضمين البحث معالجة المحاور التالية:

1- ماهية جرائم تكنولوجيا الإعلام والاتصال.
2- سبل مواجهة جرائم تكنولوجيا الإعلام والاتصال

1- ماهية جرائم تكنولوجيا الإعلام والاتصال.

1-1-مفهوم جرائم تكنولوجيا الإعلام والاتصال: جرائم تكنولوجيا الإعلام والاتصال لها عدة مسميات فمنهم من ينعتها بجرائم الحاسوب أو الانترنيت، أو جرائم التقنية العالية أو جرائم الياقات البيضاء، ومع تعدد المسميات تتعدد التعاريف فمنهم من يعرفها من جانب فني (تقني)، أما التعاريف الأخرى فيطغى عليها الجانب القانوني.

فمنهم من يعرف جرائم تكنولوجيا الإعلام والاتصال على أنها فعل ضار يستخدم الفاعل، الذي يفترض أن لديه معرفة بتقنية الحاسوب، نظاماً حاسوبياً أو شبكةً حاسوبيةً للوصول إلى البيانات والبرامج بغية نسخها أو تغييرها أو حذفها أو تزويرها أو تخريبها أو جعلها غير صالحة أو حيازتها أو توزيعها بصورة غير مشروعة[1]، ويعرفها أحمد صياني بأنها تصرف غير مشروع يؤثر في الأجهزة و المعلومات الموجودة عليها وهذا التعريف يعتبر جامع مانع من الناحية الفنية لجرائم تكنولوجيا الإعلام والاتصال حيث انه لارتكاب الجريمة يتطلب وجود أجهزة كمبيوتر زيادة على ربطها بشبكة معلوماتية ضخمة[2] ، ويعرفها آخرون على أنها جريمة ذات طابع مادي , تتمثل في كل فعل أو سلوك غير مشروع، من خلال استعمال الوسائط الإلكترونية , حيث تتسبب في تحميل أو إمكانية تحميل المجني عليه خسارة , وحصول أو إمكانية حصول مرتكبه على أي مكسب، وتهدف هذه الجرائم إلى الوصول غير المشروع لبيانات سرية غير مسموح بالاطلاع عليها ونقلها ونسخها أو حذفها , أو تهديد وابتزاز الأشخاص والجهات المعنية بتلك المعلومات، أو تدمير بيانات وحواسيب الغير بواسطة فيروسات[1]

والبعض الآخر يعرفها بأنها "الجرائم التي ترتكب ضد أفراد أو مجموعات مع وجود دافع إجرامي لإلحاق الضرر عمدا بسمعة الضحية، أو التسبب بالأذى الجسدي أو النفسي للضحية بشكل مباشر أو غير مباشر، باستخدام شبكات الاتصال الحديثة مثل الإنترنت (غرف الدردشة، البريد الإلكتروني..)، والهواتف الجوالة (الرسائل النصية القصيرة ورسائل الوسائط المتعددة)، وتشمل جرائم تكنولوجيا الإعلام والاتصال أي فعل إجرامي يتم من خلال الحواسيب أو الشبكات كعمليات الاختراق والقرصنة، كما تضم أيضا أشكال الجرائم التقليدية التي يتم تنفيذها عبر الإنترنت[1]، ولقد عرفها الدكتور عبد الفتاح مراد على أنها :" جميع الأفعال المخالفة للقانون والشريعة والتي ترتكب بواسطة الحاسب الآلي من خلال شبكة الانترنت وهي تتطلب إلمام خاص بتقنيات الحاسب الآلي و نظم المعلومات سواء لارتكابها أو للتحقيق فيها ويقصد بها أيضا أي نشاط غير مشروع ناشئ في مكون أو أكثر من مكونات الانترنت مثل مواقع الانترنت وغرف المحادثة أو البريد الالكتروني كما تسمى كذلك في هذا الإطار بالجرائم السيبيرية أو السيبرانية لتعلقها بالعالم الافتراضي"، وهناك من يسميها أيضا بجرائم التقنية العالية أو جرائم أصحاب الياقات البيضاء[1]. وعرفتها منظمة التعاون الاقتصادي والتنمية (OCDE) بأنها: كل سلوك غير مشروع، أو غير أخلاقي أو غير مصرح به، يتعلق بالمعالجة الآلية للبيانات أو بنقلها[2].

و قد اصطلح المشرع الجزائري على تسمية الجرائم الالكترونية بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وعرفها بموجب المادة 02 من القانون 09-04 المؤرخ في 05 غشت 2009، على أنها جرائم المساس بأنظمة المعالجة الآلية للمعطيات الآلية المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية .[3]

1-2- خصائص جرائم تكنولوجيا الإعلام والاتصال: تتميز جرائم تكنولوجيا الإعلام والاتصال بخصائص وصفات تميزها عن غيرها من الجرائم الأخرى ومن بين أهم هذه الخصائص ما يلي[4]:

1 - مرتكب جرائم تكنولوجيا الإعلام والاتصال في الغالب شخص يتميز بالذكاء والدهاء ذو مهارات تقنية عالية ودراية بالأسلوب المستخدم في مجال أنظمة الحاسب الآلي وكيفية تشغيله وكيفية تخزين المعلومات والحصول عليها ، في حين أن مرتكب الجريمة التقليدية في – الغالب - شخص أمي بسيط ، متوسط التعليم .

2- مرتكب جرائم تكنولوجيا الإعلام والاتصال – في الغالب – يكون متكيفا اجتماعيا وقادرا ماديا ، باعثه من ارتكاب جريمته الرغبة في قهر النظام أكثر من الرغبة في الحصول على الربح أو النفع المادي، في حين أن مرتكب الجريمة التقليدية – غالبا – ما يكون غير متكيف اجتماعيا وباعثه هو النفع المادي السريع.

3- تقع جرائم تكنولوجيا الإعلام والاتصال في مجال المعالجة الآلية للمعلومات وتستهدف المعنويات والماديات

4- جرائم تكنولوجيا الإعلام والاتصال ذات بعد دولي، أي أنها عابرة للحدود، فهي قد تتجاوز الحدود الجغرافية باعتبار أن تنفيذها يتم عبر الشبكة المعلوماتية وهو ما يثير في كثير من الأحيان تحديات قانونية إدارية فنية، بل وسياسية بشأن مواجهتها لاسيما فيما يتعلق بإجراءات الملاحقة الجنائية.

5- هي جريمة ناعمة، تنفذ بسرعة وهي صعبة الإثبات: ناعمة أي أنها لا تتطلب لارتكابها العنف ولا استعمال الأدوات الخطيرة كالأسلحة وغيرها، فنقل بيانات ممنوعة أو التلاعب بأرصدة البنوك مثلا لا تحتاج إلا إلى لمسات أزرار، تنفذ بسرعة أي أنها تتميز بإمكانية تنفيذها بسرعة فأغلب الجرائم المعلوماتية ترتكب في وقت قصير جداً قد لا يتجاوز الثانية الواحدة، وفي المقابل فهي صعبة الإثبات لعدم وجود الآثار المادية التقليدية(

مثل بقع الدم، تكسير، خلع...الخ .)وهذا ما جعل وسائل الإثبات التقليدية غير كافية، مما أدى إلى البحث عن أدلة فعالة لإثباتها، كاستخراج البصمات الصوتية أو استعمال شبكية العين ومضاهاتها باستخدام وسائل آلية سريعة.[5]

6- الجاذبية: نظرا لما تمثله سوق الكمبيوتر والإنترنت من ثروة كبيرة للمجرمين أو الأجرام المنظم، فقد غدت أكثر جذبا لاستثمار الأموال وغسلها وتوظيف الكثير منها في تطوير تقنيات وأساليب تمكن الدخول إلى الشبكات وسرقة المعلومات وبيعها أو سرقة البنوك أو اعتراض العمليات المالية وتحويلا مسارها أو استخدام أرقام البطاقات...الخ.[6]

7- امتناع المجني عليهم عن التبليغ: لا يتم في غالب الأحيان الإبلاغ عن جرائم الانترنيت إما لعدم اكتشاف الضحية لها و إما خشية من التشهير، لذا نجد أن معظم جرائم الانترنيت تم اكتشافها بالمصادفة، بل وبعد وقت طويل من ارتكابها.[7]

8- سرعة محو الدليل وتوفر وسائل تقنية تعرقل الوصول إليه: يسهل محو الدليل من شاشة الكمبيوتر في زمن قياسي باستعمال البرامج المخصصة لذلك، إذ يتم عادة في لمح البصر وبمجرد لمسة خاطفة على لوحة المفاتيح بجهاز الحاسوب على اعتبار أن الجريمة تتم في صورة أوامر تصدر إلى الجهاز[8].

1-3- أصناف جرائم تكنولوجيا الإعلام والاتصال: لم يستقر الفقهاء على معيار واحد لتصنيف الجرائم الالكترونية وذلك راجع إلى تشعب هذه الجرائم، وسرعة تطورها، فمنهم من يصنفها بالرجوع إلى وسيلة ارتكاب الجريمة، أو دافع المجرم، أو على أساس محل الجريمة، و على هذا الأساس يمكن تقسيمها إلى:[9]

1-3-1- الجرائم الواقعة على الأموال: في ظل التحول من المعاملات التجارية التقليدية إلى المعاملات التجارية الالكترونية، وما انجر عنه من تطور في وسائل الدفع والوفاء، وفي خضم التداول المالي عبر الانترنيت، أصبحت هذه المعاملات عرضة لشتى أنواع الجرائم.

1-3-2- الجرائم الواقعة على الأشخاص: مع تطور شبكة الانترنيت أصبحت المعلومات المتعلقة بالأفراد متداولة بكثرة عبرها، مما جعلها عرضة للانتهاك من طرف هؤلاء المجرمين وجعلت سمعة الأفراد مستباحة.

1-3-3- الجرائم الواقعة على أمن الدولة: من أهم الجرائم الالكترونية التي تهدد أمن الدول وهي ما يلي:

أ- الجماعات الإرهابية: استغلت الكثير من الجماعات المتطرفة الطبيعة الاتصالية للأنترنيت من أجل بث معتقداتها وأفكارها، بل تعداه الأمر إلى ممارسات تهدد أمن الدولة المعتدى عليها.

ب- الجريمة المنظمة: استغلت عصابات الجريمة المنظمة الإمكانيات المتاحة في وسائل الاتصال والانترنيت في تخطيط وتمرير وتوجيه المخططات الإجرامية وتنفيذ العمليات الإجرامية بيسر وسهولة[10] .

ج- الجرائم الماسة بالأمن الفكري: يبقى الأمن الفكري من بين أخطر الجرائم المرتكبة عبر الانترنيت، حيث تعطي الانترنيت فرصا للتأثير على معتقدات وتقاليد مجتمعات بأكملها مما يجعلها عرضة للهزيمة الفكرية وهو ما يسهل خلق الفوضى.

د- جريمة التجسس الالكتروني: سهلت شبكة الانترنيت الأعمال التجسسية بشكل كبير حيث يقوم المجرمون بالتجسس على الأشخاص أو الدول أو المؤسسات الدولية أو الوطنية، وتستهدف عملية التجسس في عصر المعلوماتية ثلاث أهداف رئيسية وهي: التجسس العسكري، والتجسس السياسي، والتجسس الاقتصادي.[11]

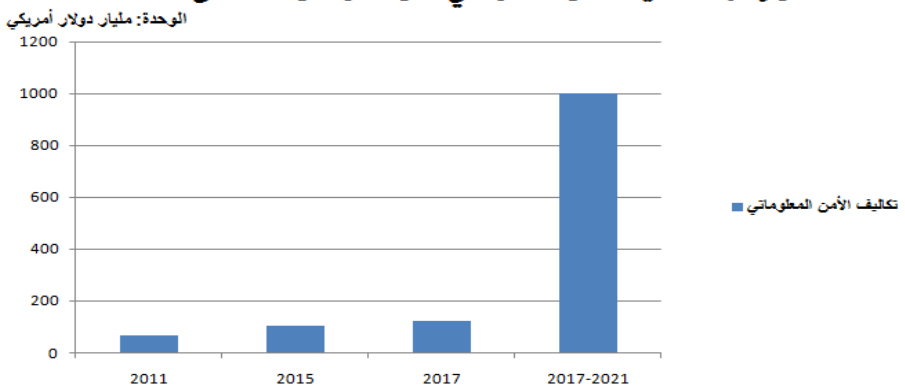
1-4- واقع جرائم تكنولوجيا الإعلام والاتصال في العالم:

1-4-1- جرائم تكنولوجيا الإعلام والاتصال حقائق وأرقام: مع شيوع استخدام الكمبيوتر أواخر سبعينات القرن الماضي برزت ظاهرة القرصنة الإلكترونية، وسرعان ما تحول السلوك الذي بدا في بدايته انحرافا لمراهقين شغوفين بالتكنولوجيا، حربا تشن بين الدول، وهي تهدد منشئات حيوية كالمفاعلات النووية ومحطات الكهرباء كما تدمر المخزونات النقدية لبنوك ودول وتهتك أسرارا لا يراد لها الخروج إلى العلن[12] ، وكشفت أرقام وبيانات عالمية، تزايد جرائم تكنولوجيا الإعلام والاتصال في مختلف أنحاء العالم، مع التوسع المتزايد لاستخدام الانترنت والأجهزة الذكية، وأظهرت دراسة لموقع "أرقام ديجتال" أن عدد ضحايا الهجمات والجرائم الالكترونية، يبلغ555 مليون مستخدم سنويا، وأكثر من 1.5 مليون ضحية يوميا، في حين تقع ضحية كل ثانية لهذه الهجمات، وأكثر أنواع الجرائم سرقة هويات وعددها 224 مليون سرقة، وأظهرت الدراسة أن مواقع التواصل الاجتماعي هي الأكثر اختراقا، إذ بينت أن أكثر من 600 ألف حساب فيسبوك يتم اختراقها يوميا وبينت الدراسة أن الكلفة السنوية المخصصة للأمن المعلوماتي قدرت بـ 100 مليار دولار، بعدما كانت في حدود 63,1 مليار دولار سنة 2011، ومن المتوقع أن تتجاوز 120 مليار دولار بحلول سنة 2017 [13]، وحسب تقرير نشرته شركة مشاريع الأمن السيبراني(CYBERSECURITY VENTURES) بعنوان: Cyber Security Economy predictions 2017-2021، فإن العالم سينفق ما قيمته 1 تريليون دولار خلال الفترة التي

تمتد من 2017 الى غاية 2021 على منتجات وخدمات الأمن السيبراني لمكافحة الجريمة الالكترونية و في هذا الإطار فقد سجل فتح حوالي مليون وظيفة خاصة بالأمن السيبراني خلال سنة 2016، ومن المتوقع أن يكون هناك عجز بحوالي 1,5 مليون وظيفة خلال عام 2019[14].

والشكل الموالي يوضح تطور تكاليف الأمن السيبراني أو المعلوماتي خلال الفترة الممتدة من 2011 والى غاية 2021.

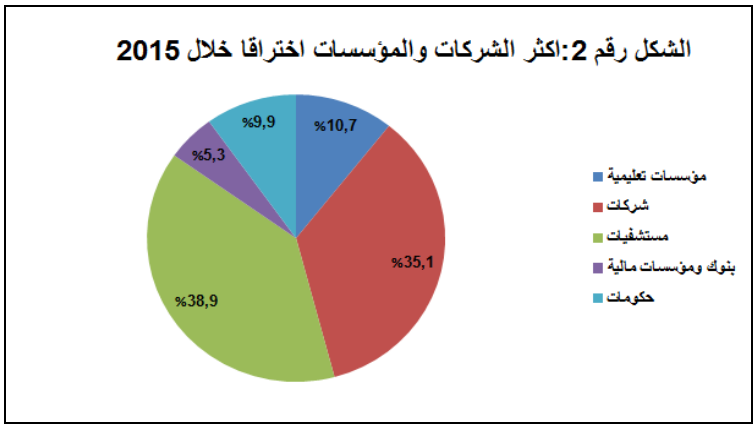
الشكل رقم 1: تكاليف الأمن المعلوماتي خلال الفترة من 2011 الى 2021



المصدر: من إعداد الباحثين اعتمادا على معطيات موقع أرقام ديجيتال و cybersecurity ventures .

والشكل الموالي يبين أكثر المؤسسات أو الشركات تعرضا للاختراق خلال سنة 2015.

الشكل رقم 2:اكثر الشركات والمؤسسات اختراقا خلال 2015

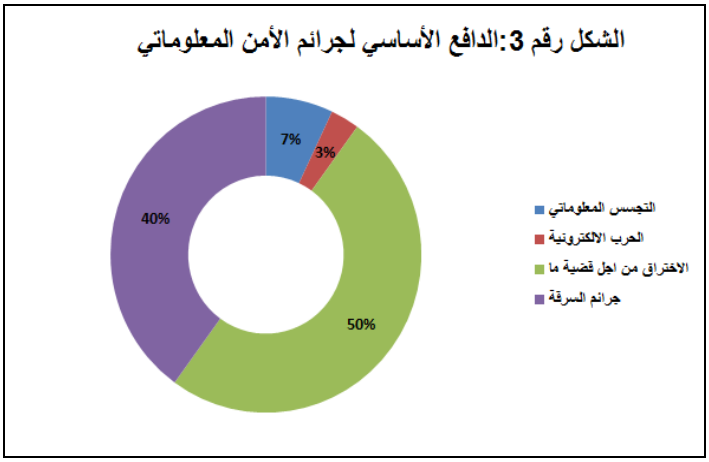


المصدر :من اعداد الباحثين اعتمادا على دراسة لموقع ارقام ديجيتال على الموقع التالي:

http://digital.argaam.com/article/detail/112326

أما بالنسبة للدوافع الأساسية للإجرام المعلوماتي فقد تباينت ما بين جرائم من اجل السرقة، بدافع التجسس المعلوماتي، الحرب الالكترونية أو الاختراق من أجل قضية ما، والشكل الموالي يوضح النسب المئوية المقابلة لذلك.

الشكل رقم 3:الدافع الأساسي لجرائم الأمن المعلوماتي

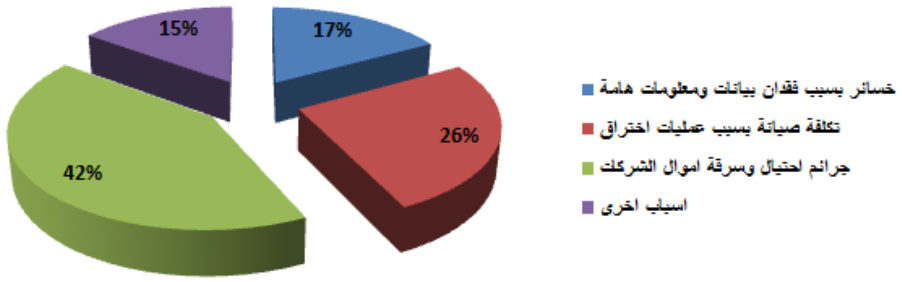


المصدر :من اعداد الباحثين اعتمادا على دراسة لموقع ارقام ديجيتال على الموقع التالي

:http://digital.argaam.com/article/detail/112326

ومن المتوقع أن تكبد الجرائم الالكترونية الاقتصاد العالمي حوالي 6 تريليون دولار بحلول سنة 2021 وهي ضعف الخسائر المسجلة سنة 2015 والمقدرة بحوالي 3 تريليون دولار[15] ، وأكثر الخسائر تحدث إما بسبب فقدان بيانات ومعلومات هامة أو نتيجة لتكلفة صيانة عمليات الاختراق أو بسبب احتيال وسرقة أموال من الشركات، والشكل الموالي يوضح ذلك :

الشكل رقم 4:اسباب خسائر الجرائم الالكترونية



المصدر :من اعداد الباحثين اعتمادا على دراسة لموقع ارقام ديجيتال على الموقع التالي:
http://digital.argaam.com/article/detail/112326

ولقد عايشنا خلال سنتي 2015 و 2016 العديد من حوادث الاختراق والقرصنة ولعل أهمها مايلي:

1- في سبتمبر من سنة 2016، كشفت شركة ياهوو(yahoo) عن أكبر عمليات قرصنة وسرقة لقاعدة بيانات مستخدميها، هذه العملية تُعتبر من أكبر عمليات القرصنة في التاريخ لشركة تقنية، حيث حصل القراصنة على بيانات أكثر 500 مليون مستخدم ، و في ديسمبر من نفس السنة تعرضت الشركة نفسها، لصدمة أخرى حيث أعلنت بأن بيانات أكثر من مليار مستخدم قد تم الاستيلاء عليها وأصبحت معروضة للبيع ، منها كلمات السر وأسئلة الأمان وأرقام هواتف وتواريخ ميلاد، هذه الحوادث خفضت من أسهم الشركة الأمريكية اقتصاديا وإعلامياً بشكل ملحوظ[16].

2- لقد واجه مستخدمو الإنترنت حول العالم يوم 2016/10/21، صعوبات في دخول المواقع الالكترونية الرئيسية، وهذه المشكلة تسببت في سقوط أهم مواقع العالم، مع تردد أنباء عن أن سبب المشكلة هجمات إلكترونية، وبحسب موقع Business Insider ، فقد تعرضت أهم مواقع العالم لهجوم الحرمان من الخدمة (DDOS) والذي يعتبر أكثر الهجمات الإلكترونية شيوعاً في عالم الإنترنت و الذي يستهدف DNS، وهي أهم فقرة في منظومة الانترنت، إذ تعمل على ترجمة عنوان الموقع إلى عنوان IP، وأبرز المواقع الرئيسية التي تعرضت للسقوط هي Amazon ، Twitter، Github ,Etsy ,Spotify[17].

3- كشف محققون عما يعتقدون أنه أكبر جريمة إلكترونية في التاريخ، سرق خلالها قراصنة روس من العديد من بنوك دول العالم (شملت مصارف في اليابان والصين والولايات المتحدة، مروراً بمصارف في الدول الأوروبية)، ما يصل إلى مليار دولار، وهي العملية التي وصفت بأنها "ثورة في عالم الجريمة الإلكترونية" ، وهذه السرقة تشكل علامة فارقة على بداية مرحلة جديدة في ثورة النشاط الإجرامي الإلكتروني، حيث يسرق المستخدمون الأموال مباشرة من البنوك ويتجنبون المستخدمين العاديين.[18]

1-2-4- واقع جرائم تكنولوجيا الإعلام والاتصال في الوطن العربي:

لقد أصبحت الهجمات الإلكترونية مصدر تهديد حقيقيا لاقتصاديات الدول، ولم تعد هذه الجرائم تقتصر على سرقة أموال البنوك أو الأفراد، بل اجتاحت قطاعات جديدة على غرار أمن الموانئ، التي قد تتعرض لهجمات خطيرة من عصابات الجريمة المنظمة أو الإرهابيين أو حتى الدول المعادية، وذكر بعض الخبراء أن الأرباح الضخمة التي تحققها الجرائم الإلكترونية تجاوزت أرباح تجارة المخدرات، وذكر الخبراء أيضا أن الجرائم الإلكترونية أصبحت اليوم واقعاً في دولة الإمارات، بوقوع نحو مليوني شخص من سكان الدولة ضحية للجرائم الإلكترونية خلال سنة 2015.[19]

وكشف موقع «جوبال ريسك إنسايتس» أن المملكة العربية السعودية هي البلد الأكثر استهدافا بالهجمات الإلكترونية في الشرق الأوسط، وأن إيران أكثر من يستهدفها إلكترونيا، ونوه التقرير إلى أن الهجمات الإلكترونية على المملكة وصلت عام 2015 إلى 160 ألف محاولة هجوم يوميا، ويشير نفس التقرير إلى أن الإمكانيات الرقمية والالكترونية الكبيرة للسعودية تجعلها هدفا مميزا للهجمات الالكترونية حيث تمتلك المملكة أكبر عدد من المشتركين في خدمة الإنترنت في العالم العربي[20]. و حسب تقارير دولية مستقلة، فإن الإمارات سجلت أفضل

أداء في صد الهجمات الإلكترونية في منطقة الشرق الأوسط خلال النصف الأول من سنة 2016، في الوقت الذي أكدت هيئة تنظيم الاتصالات على فعالية منظومة الحماية الإلكترونية في الدولة[21].

و منذ عام 2014، ارتفعت معدلات ما يُطلق عليه قانوناً اسم الجريمة الإلكترونية في لبنان، ما وضع المعنيين في المصارف والمؤسسات المالية والأجهزة الأمنية أمام سباق مع القراصنة القادرين على تطوير أدواتهم وتكتيكاتهم بموازاة تطور وسائل المكافحة، حيث بلغ عدد عمليات القرصنة الإلكترونية التي تعرضت لها المصارف اللبنانية حصراً منذ عام 2011 حتى الفصل الثالث من سنة 2016، وفق أرقام هيئة التحقيق الخاصة لدى مصرف لبنان، 233 عملية، وصلت فيها قيمة الأموال التي تعرضت للقرصنة إلى نحو 26 مليوناً ونصف مليون دولار، من ضمنها 15 مليون دولار بين عامي 2015 و2016 طالت القطاع المصرفي بشكل مباشر، وفق رئيسة مكتب مكافحة الجرائم المعلوماتية وحماية الملكية الفكرية، المقدم سوزان الحاج. وتعكس هذه الأرقام الحد الأدنى، إذ إن القيمة الفعلية للغنائم وعدد العمليات الإلكترونية، باعتراف هيئة التحقيق ومكتب مكافحة الجرائم المعلوماتية، أكبر بالتأكيد، لأن هناك حالات لم يتم الإبلاغ عنها إما بدافع الحفاظ على السمعة أو يقيناً باستحالة استعادة تلك الأموال.[22]

والجزائر كغيرها من الدول لم تسلم هي الأخرى من ما يسمى الجريمة الالكترونية، حيث لم تسلم مواقع التواصل الاجتماعي وفضاءات تبادل المعلومات، من عملية السطو على الصور والبيانات الشخصية، واستعمالها كوسيلة للابتزاز والمساومة و التشهير، ناهيك عن استغلال بيانات الحسابات الشخصية بالإضافة إلى الاعتداء على أنظمة المعلومات، وحسب مصدر عليم لجريدة الفجر، فقد تم تسجيل أكثر من 500 جريمة إلكترونية في الجزائر خلال سنة 2016، علما أن هذا يخص عدد الحالات التي قامت بعملية التبليغ فقط، والأكيد أن البعض يرفض إيداع شكوى لاعتبارات اجتماعية وثقافية، وهو الأمر الذي جعل مصالح الدرك الوطني تتجند لحماية مستعملي الانترنت مثل مستخدمي مواقع التواصل الاجتماعي الذين يشكلون حيزا كبيرا من طبيعة استعمال هذه التكنولوجيا، كما تمت معالجة 385 جريمة الكترونية من قبل الفرق المتخصصة في مكافحة الجريمة الالكترونية التابعة للأمن الوطني، إلى جانب تسجيل 57 قضية في مجال جرائم الاعتداء على سلامة الأنظمة المعلوماتية.[23]

2- سبل مواجهة جرائم تكنولوجيا الإعلام والاتصال:

2-1- الإجراءات المتخذة على المستوى العربي والعالمي لمكافحة جرائم تكنولوجيا الإعلام والاتصال:

أ- الشق التشريعي: 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.[24]

أما على مستوى الدول العربية فقد قامت الدول العربية بالتوقيع على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات وذلك بتاريخ 2010/12/21، كما أدت هذه الاتفاقية كذلك لميلاد قوانين عديدة لمكافحة ما يسمى بالجرائم الإلكترونية في السعودية والأردن وقطر والإمارات والعراق وسلطنة عمان. وصارت الاتفاقية سارية المفعول بعد تصديق الرئيس المصري عليها سنة 2015 ليكتمل نصاب الدول السبع المطلوبة لسريانها.[25]

ب- الشق الأمني: إن مواجهة مخاطر الجرائم المعلوماتية تعتمد بشكل كبير على تبني استراتيجية أمنية- مجتمعية متكاملة، والتي تعمل فيها أجهزة مكافحة الجريمة الرسمية في الدولة جنباً إلى جنب مع أفراد المجتمع ومؤسسات القطاع الخاص، هو ما يمكن من خلاله مكافحة الأنشطة الإجرامية في الفضاء الإليكتروني والتقليل من مخاطرها والحد من انتشارها، وهذه الرؤية تتسق مع نتائج الدراسات التي أجريت في بلدان مختلفة من العالم حول التعامل مع جرائم الإنترنت، والتي أوضحت أهمية مشاركة العديد من المصادر والمؤسسات الخاصة في تحمل جزءًا من المسؤولية فيما يتعلق بمكافحة هذه الجرائم والسيطرة عليها وتلك المصادر تتمثل في[26]:

1- مزودو خدمة الإنترنت الذين يملكون القدرة على تحديد ما يعرف ب (IP) (Internet Protocol) للمشتركين، ما يتيح إمكانية مراقبة الأنشطة الخطرة على الإنترنت وتقييد اشتراك المستخدمين المنخرطين في تلك الأنشطة.

2- المواطن العادي بدوره كذلك يمكن أن يساهم من خلال تحمل مسؤولية حماية نفسه من الوقوع ضحية لجرائم الإنترنت باقتنائه برمجيات الحماية من الفيروسات.

3-المصارف التجارية وشركات البطاقات الائتمانية عليها أيضاً مسؤولية كبيرة في حماية عملائها من خلال تطبيق إجراءات وقائية ضد الاحتيال، وكذلك تنصيب برمجيات مراقبة خاصة على خوادمها لتعقب النشاطات غير المعتادة على حسابات العملاء ووضع أنظمة لتنبيه العميل على كل عملية تتم على حسابه.

4- المحققين الخاصين الذين يعملون بالتنسيق مع أجهزة العدالة الجنائية يمكن أن يلعبوا دوراً مهماً في مكافحة جرائم الإنترنت.

وقد قدمت شركة « فاير آي FireEye » المتخصصة في مجال التصدي للهجمات الالكترونية المتقدمة 8 إجراءات مهمة لتفادي مخاطر تزايد الهجمات الالكترونية التي تستهدف دول الخليج العربي، بعدما كشفت عن جملة من التصورات والرؤى التحليلية بشأن مشهد

الهجمات الالكترونية في مناطق أوروبا والشرق الأوسط وأفريقيا، وعلى وجه الخصوص في دول مجلس التعاون الخليجي، وتمثلت هذه الإجراءات في ما يلي[27]:

- ☒ التوقع الدائم بأن تكون تلك الشركات مستهدفة.
- ☒ أنه من الممكن تخطي حدود الضوابط الأمنية المتوفرة لديها.
- ☒ التأكد دائما من أن ليس هناك أي كيان تجاري بمنأى عن الهجمات.
- ☒ وضع إطار عمل خاص بالمخاطر ذات الصلة بالأنترنت.
- ☒ الحصول على منصة استخبارات التهديدات الأنسب لتحسين قدرات الكشف عن الهجمات المحتملة.
- ☒ إنشاء خدمة الاستجابة للحوادث الطارئة وإدارتها، والتي من شأنها تمكين الشركات من اكتشافها والتفاعل مع هجمات APT بالسرعة الممكنة.
- ☒ وضع خطة استجابة واضحة والعمل على تحضيرها استعدادا للتعامل مع أي حالة اختراق.

2-2- التجربة العملية لدولة استونيا لمواجهة جرائم تكنولوجيا الإعلام والاتصال: كتجربة عملية في مجال التصدي للإجرام الالكتروني نذكر على سبيل المثال « استراتيجية الأمن السيبراني (الأمن المعلوماتي) للفترة الممتدة من 2014- 2017 »، التي تبنتها دولة استونيا، وهي استراتيجية تقوم بتحديد المخاطر التي تهدد الأمن المعلوماتي لدولة استونيا وتقدم التدابير اللازمة لإدارة هذه المخاطر، وتتولى وزارة الشؤون الاقتصادية والاتصالات مهمة توجيه سياسة أمن الانترنيت و أيضا التنسيق ما بين الأطراف المعنية بتنفيذ بهذه الاستراتيجية والمتمثلة في وزارة الدفاع الوطني، وزارة العدل، وزارة الداخلية، وزارة الخارجية، مصالح الأمن والشرطة، الجهاز المسؤول على نظام المعلومات، وزارة التعليم والبحث، ومنظمات أصحاب العمل، وتضمنت هذه الاستراتيجية مايلي[28]:

أولا- مبادئ ضمان الأمن السيبراني (الأمن المعلوماتي): اشتملت هذه الاستراتيجية على المبادئ الأساسية التالية:

- الأمن الالكتروني هو جزء لا يتجزأ من الأمن القومي، فهو يدعم سير العمل في الدولة والمجتمع، ويعزز القدرة التنافسية للاقتصاد والابتكار.
- الأمن الالكتروني مكفول من خلال احترام الحقوق والحريات الأساسية، وكذلك من خلال حماية الحريات الفردية والمعلومات الشخصية.
- يتم ضمان الأمن الالكتروني بطريقة منسقة من خلال التعاون بين القطاعين العام والخاص، مع مراعاة الترابط المتبادل بين البنية التحتية القائمة والخدمات في مجال التجارة الالكترونية.
- يبدأ الأمن الالكتروني انطلاقا من المسؤولية الفردية عن استخدام أدوات تكنولوجيات المعلومات والاتصال.
- الأولوية القصوى لضمان الأمن السيبراني هو استباق ومنع التهديدات المحتملة والتصدي بفعالية للتهديدات التي تتحقق.
- يتم دعم الأمن الالكتروني عن طريق البحث والتطوير المكثف والقادر على المنافسة دوليا.
- يُكفل الأمن الالكتروني عبر التعاون الدولي مع الحلفاء والشركاء.

ثانيا- الهدف العام من الاستراتيجية: الهدف العام من هذه الاستراتيجية هو زيادة قدرات الأمن السيبراني ، وتوعية السكان حول كيفية التعامل مع التهديدات السيبرانية، وبالتالي ضمان استمرار الثقة في الفضاء الالكتروني.

ثالثا- الأهداف الفرعية: تشتمل استراتيجية الأمن المعلوماتي على الأهداف الفرعية التالية:

1- ضمان حماية نظم المعلومات الأساسية للخدمات الهامة: ويتم تحقيق هذا الهدف عن طريق الإجراءات التالية:

- ☒ تأمين أو ضمان حلول بديلة للخدمات الهامة.
- ☒ ضمان أمن البنية التحتية وخدمات تكنولوجيات المعلومات والاتصال.
- ☒ إدارة التهديدات السيبرانية على القطاع العام والخاص.
- ☒ تأسيس نظام وطني لرصد أمن المعلومات .
- ☒ ضمان الاستمرارية الرقمية للدولة.
- ☒ تعزيز التعاون الدولي في مجال حماية البنية التحتية الحيوية للمعلومات.

2- تعزيز مكافحة الجرائم الالكترونية: وذلك من خلال:

2-1- تعزيز الكشف عن الجرائم الالكترونية.

2-2- رفع مستوى الوعي العام اتجاه مخاطر الانترنيت.

2-3- تعزيز التعاون الدولي لمكافحة الجريمة الالكترونية.

3- تطوير قدرات الدفاع السيبراني الوطني: عن طريق

3-1- مزامنة التخطيط العسكري والاستعداد لحالات الطوارئ المدنية.

3-2- تطوير الدفاع السيبراني الجماعي و التعاون الدولي.

3-3- تطوير قدرات الدفاع السيبراني العسكري.

3-4- ضمان مستوى عال من الوعي بشأن دور الأمن السيبراني في الدفاع الوطني.

4- تطوير قدرات استونيا في مجال إدارة التهديدات الأمنية الالكترونية: من خلال:

4-1-تكوين وتأطير جيل قادم من المتخصصين في مجال الأمن المعلوماتي.

4-2-المساهمة في البحوث المتعلقة بالأمن السيبراني لإيجاد الحلول الآمنة.

4-3- دعم وتنمية المؤسسات التي توفر الأمن السيبراني وتقدم حلول الأمن المعلوماتي الوطني.

5- استونيا تطور الأنشطة المشتركة بين القطاعات: عن طريق:

5-1- وضع إطار قانوني لدعم الأمن الالكتروني.

5-2- تعزيز سياسة الأمن السيبراني الدولية.

5-3- التعاون الوثيق مع الحلفاء والشركاء.

5-4- تعزيز قدرة الاتحاد الأوربي.

2-3- تجربة الجزائر لمواجهة جرائم تكنولوجيا الإعلام والاتصال: كخطوة أولى للحكومة الجزائرية لمواجهة ما يعرف بجرائم تكنولوجيا الإعلام والاتصال ، صدر سنة 2009 القانون رقم 09-04 المؤرخ في 05 غشت 2009، والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، إلا أن تجسيد بنوده على أرض الواقع ضعيف إلى حد الساعة، بعدما أهملت الجوانب التقنية الكفيلة بتصنيف هذه الجرائم وتحديد العقوبة المناسبة في حق مرتكبيها، واقتصرت العقوبات في أغلب الأحيان على الغرامة المالي. و يتضمن القانون 19 مادة موزعة على 6 فصول، أعده نخبة من رجال القانون بمشاركة خبراء ومهنيين مختصين في مجال الإعلام الإلكتروني من كافة القطاعات المعنية، يتضمن القانون أحكاما خاصة بمجال التطبيق وأخرى خاصة بمراقبة الاتصالات الإلكترونية وعددت الحالات التي تسمح باللجوء إلى المراقبة الالكترونية، بالإضافة إلى القواعد الإجرائية المتضمنة تفتيش المنظومات المعلوماتية وكذا حجز المعطيات المعلوماتية التي تكون مفيدة للكشف عن الجرائم الالكترونية، و نص القانون في فصله الخامس على إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، تتولى تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ، ومساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن هذه الجرائم، وتتكفل أيضا بتبادل المعلومات مع نظيراتها في الخارج، قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم الالكترونية وتحديد مكان تواجدهم، كما أن هذا القانون أكد في فصله الأخير على مبدأ التعاون والمساعدة القضائية الدولية من إطار مبدأ المعاملة بالمثل.[29]

وفي نفس السياق، قال رئيس الكتلة البرلمانية لجبهة العدالة والتنمية لخضر بن خلاف، في تصريح خص به «يومية السلام اليوم » أن «مشكلتنا في قوانين سنّتها الحكومة فيما يخص الجريمة الإلكترونية ولم تطبّقها»، مضيفا أن هناك مراسيم متعلقة بهذا القانون المصادق عليه سنة 2009، لم تصدر لحد الساعة ولأسباب مجهولة، ما جعل حسبه، معالجة القضايا من هذا الشأن تصطدم بشبه فراغ قانوني، ما أدى في عديد الحالات إلى استصدار أحكام وعقوبات تقريبية لا سند لها، كما دعا نفس المتحدث، الحكومة إلى ضرورة مراجعة موقفها تجاه هذا القانون، وقال: لا بد من إيلائه أهمية أكبر في ظل دخول الشارع الجزائري نفق الإدمان، والاعتماد الرهيب على شبكة الإنترنت وما يصاحبها من آليات وخدمات إلكترونية، فضلا عن فتح مجال السمعي البصري، الذي يمكن أن يصطدم بمثل هذه الجرائم مستقبلا، مشددا في السياق ذاته على ضرورة تشريع قوانين جديدة تكرّس العقاب الصارم لكبح مثل هذه الجرائم التي وصفها بالخطيرة والمدمّرة.[30]

الخاتمة:

إن التطورات الهائلة التي عرفتها التكنولوجيات الحديثة للإعلام والاتصال، ورغم ما وفرته من تسهيلا في أمور حياتنا، إلا أنها في المقابل فتحت الباب على مصراعيها لتطور أدوات ووسائل وسبل تنفيذ الجرائم الالكترونية، وجعلتها أكثر تعقيدا وصارت مكافحتها تبدو صعبة المنال إذا لم تتضافر جهود جميع الأطراف الفاعلة في الساحة المعلوماتية، وأمام هذا الوضع بات لزاما على حكومات الدول الإسراع في اتخاذ الإجراءات اللازمة لتطوير آليات التصدي لمثل هذه الجرائم وتعزيز التعاون الدولي في هذا المجال.

التوصيات:

من الرغم من الاجتهادات والمبادرات التي انتهجتها دول العالم في معالجة الظاهرة إلا أنه مزال نقائص وثغرات على عدة مستويات، وعلى أثر هذا ومن خلال بحثنا المتواضعة فإننا نوصي بالنقاط التالية:

- ☒ تعزيز التعاون الدولي في مجال مواجهة القرصنة والإجرام الالكتروني من خلال رسم سياسات تهدف إلى تشديد العقوبات على مرتكبي هذا النوع من الجرائم.
- ☒ تحديث وتطوير التقنيات باستمرار للتمكن من التصدي لهذه الجرائم في أقل وقت ممكن.
- ☒ تنظيم حملات توعية لمستعملي الوسائط الالكترونية (الحاسوب، الانترنيت، الهواتف الذكية ...)، وتعريفهم بحجم الخطورة التي تترصدهم في حالة عدم اتخاذ الاحتياطات الوقائية اللازمة.
- ☒ تعزيز وتدعيم التعاون العربي في مجال مكافحة الجريمة الالكترونية عن طريق مصادقة جميع الدول الأعضاء في جامعة الدول العربية على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، وذلك من أجل درء أخطار هذه الجرائم وحفاظا على الأمن المعلوماتي للدول العربية.
- ☒ اتخاذ تدابير من شأنها الحفاظ على سرية المعلومات الخاصة بالحسابات البنكية وبطاقات الائتمان وغيرها من وسائل تبادل المعلومات.
- ☒ التحديث المستمر لبرامج حماية الحواسيب من الفيروسات .
- ☒ التدريب والتكوين المستمر للكوادر البشرية العاملة في مجال مكافحة الجرائم الالكترونية، واستحداث شهادات عليا متخصصة في المجالات التقنية والقانونية المتعلقة بمكافحة الجرائم المعلوماتية، وحث الجامعات والمراكز البحثية على تسليط الضوء أكثر على مثل هذه الجرائم، من خلال تكثيف الندوات والملتقيات و الأيام الدراسية حول هذا الموضوع.

المراجع:

1- كامل فريد السالك، الجريمة الالكترونية، محاضرة ألقيت في ندوة التنمية ومجتمع المعلوماتية 21-23 أكتوبر 2000، الجمعية السورية للمعلوماتية، حلب، سورية.

2- إسراء جبريل رشاد مرعي، الجرائم الالكترونية- الأهداف-الأسباب-طرق الجرائم ومعالجتها، مقال منشور على الموقع الالكتروني للمركز الديمقراطي العربي للدراسات الإستراتيجية والسياسية والاقتصادية، قسم الدراسات المتخصصة، على الرابط: http://democraticac.de/?p=35426 تاريخ الاطلاع 2017/02/13.

3- منى شاكر فراج العسبلي، تأثير الجريمة الالكترونية على النواحي الاقتصادية، مقال منشور على موقع كنانة أونلاين على الرابط: http://kenanaonline.com/users/ahmedkordy/posts/320920 تاريخ الاطلاع:2017/02/13.

4- رماح الدلقموني، الجرائم الالكترونية.. عندما تصبح التقنية وسيلة للإجرام، مقال منشور على موقع الجزيرة الإخبارية الالكتروني، قسم علوم وتكنولوجيا، بتاريخ 2015/04/06 على الرابط: http://www.aljazeera.net/news/scienceandtechnology/2015/4/6 تاريخ الاطلاع 2017/02/13.

5- إسراء جبريل رشاد مرعي، مرجع سبق ذكره.

6- يونس عرب، صور الجرائم الالكترونية واتجاهات تبويبها، ورشة عمل تطوير التشريعات في مجال مكافحة الجرائم الالكترونية، مسقط، سلطنة عمان،2-4 ابريل 2006، ص 7.

7- القانون رقم 09-04 المؤرخ في 05 غشت 2009، والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية رقم 47، ص 5.

8- مفتاح بوبكر المطردي، الجريمة الالكترونية والتغلب على تحدياتها، ورقة مقدمة إلى المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية بالسودان المنعقد في 23-2012/9/25، ص 16.

9- كامل فريد السالك، مرجع سبق ذكره.

10- عبد العال الديربي، الجريمة المعلوماتية.تعريفها..أسبابها..خصائصها،دوريات مفاهيم إستراتيجية، المركز العربي لأبحاث الفضاء الالكتروني، مقال منشور بتاريخ 2013/01/13 على الرابط: http://accronline.com/article_detail.aspx?id=7509 تاريخ الاطلاع 2017/02/13.

11- محمد صالح العادلي، الجرائم المعلوماتية (ماهيتها وصورها)، ورشة العمل الإقليمية حول تطوير التشريعات في مجال مكافحة الجرائم الالكترونية، سلطنة عمان،2-4 أفريل 2006، ص 7.

12- موسى مسعود أرحومة، الإشكاليات الإجرامية التي تثيرها الجريمة المعلوماتية عبر الوطن، المؤتمر المغاربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس، 2009، ص3.

13- صغير يوسف، الجريمة المرتكبة عبر الانترنيت، رسالة ماجستير في القانون، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2013، ص 43-58.

14- سامي علي حامد عياد، الجريمة المعلوماتية وإجرام الانترنيت، دار الفكر الجامعي، الإسكندرية 2007، ص 83.

15- علي عدنان الفيل، الإجرام الالكتروني، منشورات زين الحقوقية، الطبعة الأولى 2011، ص 96-97.

16- القرصنة الالكترونية سلاح العصر الرقمي، مقال منشور على موقع قناة الجزيرة الالكتروني بتاريخ:2015/01/05،

17- القرصنة_الالكترونية_سلاح_ العصر_الرقمي /http://www.aljazeera.net/knowledgegate/newscoverage/2015/1/5 ، تاريخ الاطلاع 2017/02/10.

18- احصائيات صادمة وغريبة عن جرائم الأمن المعلوماتي، دراسة مقدمة من طرف موقع أرقام ديجيتال بتاريخ 2015/10/25 متوفرة على موقع : http://digital.argaam.com/article/detail/112326 ، تاريخ الاطلاع : 2017/02/11.

19- cyber security economy predictions 2017-2021,cybersecurity ventures 2016 .

20- cyber security economy predictions 2017-2021, Op. Cit.

21- مدثر النور أحمد، أكبر حوادث الاختراق حجمًا وتأثيرًا في العالم للعام 2016!، مقال منشور:2016/12/25، على موقع: http://www.arageek.com/tech/2016/12/25/2016-hacking-operations.html ، تاريخ الاطلاع 2017/02/11.

22- الانترنيت ينهار.. والطائر الأزرق يكف عن التغريد، مقال منشور بتاريخ 2016/10/22، على موقع:http://bab.com/Node/275623 تاريخ الاطلاع: 2017/02/11.

23- أكبر سرقة بالتاريخ.. متسللون سرقوا مليار دولار، مقال منشور على موقع« عربية SKY NEWS »، بتاريخ 2015/02/16 على الرابط: http://www.skynewsarabia.com/web/article/724420 تاريخ الاطلاع: 2017/02/11.

24- الجرائم الإلكترونية.. أرباح تفوق ما تجنيه تجارة المخدرات، مقال منشور على الموقع الالكتروني لجريدة الاتحاد بتاريخ:2016/02/05، http://www.alittihad.ae/details.php?id=5035&y=2016&article=full ، تاريخ الاطلاع 2017/02/10.

25- محمد خالد، السعودية الأكثر تعرضا للهجمات الإلكترونية في الشرق الأوسط، مقال منشور على موقع الخليج الجديد بتاريخ:2016/08/01، http://thenewkhalij.org/ar/node/43159 ، تاريخ الاطلاع 2017/02/11.

26- يوسف العربي، الهجمات الإلكترونية تزداد شراسة على الإمارات ومنظومة حماية متكاملة في المواجهة ، مقال منشور على الموقع الالكتروني لجريدة الاتحاد بتاريخ:2016/11/27، http://www.alittihad.ae/details.php?id=60105&y=2016 ، تاريخ الاطلاع 2017/02/11.

27- الاستيلاء على 26.5 مليون دولار: مصارف لبنان تتعرّض لـ7 أنواع من الهجمات الإلكترونية!، مقال منشور على موقع (ghadi news) بتاريخ:2016/12/01، http://ghadinews.net/Newsdet.aspx?id=27361 ، تاريخ الاطلاع 2017/02/11.

28- أزيد من 500 جريمة إلكترونية في الجزائر سنة 2016، مقال منشور على الموقع الالكتروني لجريدة الفجر بتاريخ:2017/02/10، http://www.al-fadjr.com/ar/realite/352178.html ، تاريخ الاطلاع 2017/02/11.

29- سمير سعدون مصطفى، محمود خضر سلمان، حسن كريم عبد الرحمن، الجريمة الالكترونية عبر الانترنيت أثرها وسبل مواجهتها، مجلة التقني، المجلد 24، الإصدار 9، 2011، ص 49.

30- عزة مغازي، قانون الجريمة الإلكترونية.. التورنت يحملك إلى طرة، مقال منشور على موقع المنصة بتاريخ 2016/02/04 على الرابط: https://almanassa.com/ar/story/1019 ، تاريخ الاطلاع 2016/02/12.

31- عبدالله بن فازع القرني، مواجهة جرائم الإنترنت: نحو إستراتيجية أمنية - مجتمعية متكاملة، مقال منشور على موقع جريدة الرياض بتاريخ 2014/02/21 على الرابط : http://www.alriyadh.com/912032 تاريخ الاطلاع: 2017/02/12.

32- إجراءات لتفادي مخاطر تزايد الهجمات الالكترونية التي تستهدف دول الخليج العربي، مقال منشور على موقع جريدة مكة، تاريخ النشر 2016/06/01 على الرابط: http://makkahnewspaper.com/article/147871 ، تاريخ الاطلاع: 2017/02/12.

33- Estonia Cyber Security Strategy 2014-2017, Ministry of Economic Affairs and Communication, Estonia 2014, p 7-12.

34- القانون رقم 09-04 المؤرخ في 05 غشت 2009، مرجع سبق ذكره، ص 5- 8.

35- قاسمي.أ، 160 مليار دولار سنويا مكاسب عصابات الجريمة المنظمة عبر الإنترنت، مقال منشور على موقع يومية السلام اليوم، بتاريخ 2014/01/25، على الرابط: http://essalamonline.com/ara/permalink/32212.html، تاريخ الاطلاع 2017/02/12.