حماية خصوصية المَوَاقِع الالكترُونية من الإختراق

Protectingwebsiteprivacyfrom hacking

بوجمعة محمد* أستاذ محاضر أ
جامعة الجزائر 1 كلية الحقوق - الجزائر
m.boudjemaa@univ-alger.dz

تاريخ الارسال: 2025/04/22	تاريخ القبول: 2025/05/28	تاريخ النشر: 2025/06/03

ملخص :

بعد أن سادت الأنماط التقليدية في أنظمة التخطيط والإدارة وكذا التجريم والعقاب، تحولت الأوضاع والظروف فصرنا ضمن نماذج جديدة نعيشها ونحياها بين الحين والآخر وأضحينا أمام الحوكمة الالكترُونية، التعليم الالكتروني، الإرهاب الالكترُوني، والجَرِيمَة الالكترُونية والأَمن الالكترُوني والحرب الالكترُونية وغيرها، هذا ما جعل الدول النامية تسعى لتدارك ما قد فاتها من هذا التطور المعلوماتي الرهيب، بعد أن أصبح العالم قرية الكترُونية تتحكم في دواليبها الدول الغربية.

لغاية وصول الأمر إلى الفكر الالكترُوني والأَمن الالكترُوني، الذي وجب أن يكون كل فرد من مجتمعاتنا على علم ودراية بمقتضياته، كما يجب على الحكومات وخاصة حكومات الدول العربية أن تُطور من منظومتها المعلوماتية، فهي جد متأخرة في ذلك، خاصة أن ثمانين بالمائة من مَوَاقِعها الالكترُوني محل اختراق وقرصنة لعدم حدوث الحماية المتوافرة لمَوَاقِعنا الالكترُوني وأنظمتها المعلوماتية، وإذا كان اختراق وقرصنة الآلاف من المَوَاقِع الالكترُونية أمرا خطرا فالأخطر من هذا اختراق المَوَاقِع الالكترُونية الأَمنية التي تعكس استراتيجيات وتوجهات الأنظمة الوطنية.

الكلمات المفتاحية : حماية ؛ الجريمة الالكترونية ؛ المواقع الالكترونية ؛ اختراق

*المؤلف المرسل : بوجمعة محمد

Abstract:

After the spread of traditional models of management, administration, and control systems, as well as criminalization and punishment, conditions and circumstances changed, and we found ourselves in new patterns that we live and experience from time to time. We are nowfaced with e-governance, e-learning, e-terrorism, e-crime, e-security, e-warfare, and others. This has prompted developing countries to strive to make up for what they have missed in this terrifying information development, after the world has become an electronic village whose wheels are controlled by the Western world. Until the matter reached the electronic thought and electronic security, which every individual in our societies must be aware of and knowledgeable of its requirements, and governments, especially the governments of Arab countries, must develop their information system, as they are very late in that, especially since eighty percent of their websites are subject to hacking and piracy due to the lack of protection available to our websites and their information systems. If hacking and piracy of thousands of Arab websites is a dangerous matter, then what is more dangerous than this is hacking the security websites that reflect the strategies and directions of national systems.

Keywords: Protection ; cybercrime ; Electronic websites ; hacking.

مقدمة:

بعد أن سادت الأنماط التقليدية في أنظمة الإدارة والتسيير والضبط وكذا التجريم والعقاب، تغيرت الأوضاع والظروف فأصبحنا في أنماط جديدة نعيشها ونحياها بين الفينة والأخرى وصرنا أمام الحوكمة الالكترُونية، التعليم الالكترُوني، الإرهاب الالكترُوني، والجَرِيمَة الالكترُوني والأَمن الالكترُوني والحرب الالكترُونية وغيرها، هذا ما جعل الدول النامية تسعى جاهدة لتدارك ما قد فاتها من هذا التطور المعلوماتي الرهيب، بعد أن أصبح العالم قرية الكترُوني يتحكم في دواليبها العالم الغربي .

إلى أن وصل الأمر إلى الفكر الالكترُوني والأَمن الالكترُوني، الذي يجب أن يكون كل فرد من مجتمعاتنا على علم ودراية بمقتضياته، كما يجب على الحكومات وخاصة حكومات الدول العربية أن تُطور من منظومتها المعلوماتية، فهي جد متأخرة في ذلك،خاصة أن ثمانين بالمائة

من مَوَاقِعها الالكترُوني محل اختراق وقرصنة لعدم حدوث الحماية المتوافرة لمَوَاقِعنا الالكترُوني وأنظمتها المعلوماتية، وإذا كان اختراق وقرصنة الآلاف من المَوَاقِع الالكترُونية العربية أمرا خطرا فالأخطر من هذا اختراق المَوَاقِع الالكترُونية الأَمنية التي تعكس استراتيجيات وتوجهات الحكومات العربية،وبالتالي فإن من أولويات الجهات المختصة بها أن تجعل من أولوياتها حماية مَوَاقِعها الالكترُونية، وتبني أحدث التقنيات التي تعتمد على السواعد والأدمغة المحلية الوطنية، لأن التخطيط الأَمني الاستراتيجي يجعلنا لا نثق في كل ما يُستَجلب إلينا من تقنيات وتجهيزات مستوردة من الدول الغربية، هذه التقنيات والتجهيزات والمستقبلات والبرامج التي تكون آلية من آليات الرقابة أو الاختراق والإتلاف والتصنت وكل العمليات التي قد تضعف من المنظومة الأَمنية العربية.

وقد كان من الجهود العربية في هذا الصدد القانون الاسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها الذي اعتمده مجلس وزراء العدل العرب في دورته التاسعة عشرة بالقرار رقم 495-د19- 2003/10/8، واعتمده مجلس وزراء الداخلية العرب في دورته الحادية والعشرين بالقرار رقم 417- د- 2004/21، إذ وسع من مفهوم الجرائم الالكترُوني لتشمل تلك الجرائم التقليدية المرتكبة عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها، وخصوصا تلك الجرائم الخطيرة التي تمس أَمن الدولة، أو المؤسسات العسكرية أو الاقتصادية[1].

أهمية الدراسة: توضح هذه الدراسة أهمية وأولوية الحماية الواجب توفيرها للمَوَاقِع الالكترُوني الأَمنية للدول العربية، وتبرز الخطر الداهم الذي يترصد المنظومة الأَمنية العربية، من خلال الاطلاع على برامجها وقواعدها البيانية، كما تبرز أهمية الدراسة في إجلاء الرؤى لأهم السبل الكفيلة لحماية مَوَاقِعنا الالكترُونية الأَمنية تحقيقا للأَمن المعلوماتي بمختلف جوانبه.

أهداف الدراسة: تهدف هذه الدراسة لتحيق أمرين اثنين:

- الأمر الأول: توضيح ما يقوم به أعداء هذه الأمة من ترصد وتجسس على ما تحويه البرامج المعلوماتية والمَوَاقِع الالكترُونية والآثار المترتبة عن ذلك.

- الأمر الثاني: ضرورة توحيد جهود الحكومات العربية في تبادل المعارف وما تم التوصل إليه؛ لمجابهة ما تترصدنا به أعين الجهات والأجهزة النظامية وغير النظامية الغربية، والاستفادة من

خبرات بعض النوابغ الذين تزخر بهم الدول العربية والذين تمكنوا من ابتداع وتطوير أنظمة الحماية وكذا أنظمة التظليل الالكترُوني.

إشكالية الدراسة: تتمحور إشكالية الدراسة حول حقيقة الإرهاب الالكترُوني والحروب الالكترُوني الموجهة ضد المَوَاقِع الالكترُونية الأَمنية وكذا حقيقة وأهداف اختراق وإتلاف المَوَاقِع الالكترُونية، وسبل التصدي لها وأيضا مدى تحقيق الأَمن المعلوماتي لمَوَاقعنا الالكترُونية الأَمنية؟

خطة الدراسة:

أولا: الإختراق أهم مقوضات أَمن المَوَاقِع الالكترُونية الأَمنية

1- الارهاب الالكترُوني

2- مظاهر الحرب الالكترونية

أ-إختراق المَوَاقِع الالكترُونية

ب- نشر الفيروسات

ج-التجسس الالكترُوني

د- الحرب الاعلامية

3-الجَرِيمَة الالكترُونية وفحواها

ثانيا: اختراق واتلاف المَوَاقِع الالكترُونية بين المسببات والآثار

1- مواطن الضعف في شبكة الإنترنيت
2- مفهوم الاختراق وآثاره المترتبة عنه
3 - التصدي لاختراق وإتلاف المَوَاقِع الالكترُونية الأَمنية

ثالثا : أَمن المعلومات أولوية هامة لحماية المَوَاقِع الالكترُونية الأَمنية

1- عناصر أَمن المعلومات لدى أجهزة الأَمن المختلفة

2- مخاطر تهديدات أَمن المعلومات

خاتمة.

أولا: الإختراق الالكترُوني والحروب الالكترُونية:

لما كان التحول إلى مجتمع معرفي معلوماتي من الأولويات الملحة والغايات المنشودة تحقيقا للتنمية المستدامة بكل معانيها كان لزاما أيضا حماية المعلومات من شتى صور العدوان وما أضحى يسمى بالإرهاب الالكترُوني أو الحروب الالكترُونية المُعلنة على البيئة المعلوماتية في شكل اختراق أو إتلاف أو تخريب أو سرقة و تشويش أو تجسس أو إعادة إرسال؛ وأضحى الإعتداء على البيئة المعلوماتية إعتداءً على الأَمن الوطني وأحد أبرز مقوضاته الرئيسية[2].

1/ الإرهاب الالكترُوني :

كان إجتماع عناصر الشبكات الإرهابية أمرا عسيرا أو مستحيلا في بعض الأحيان، لكن هذه الصعوبة اضمحلت اليوم وأضحى ذلك من اليُسر بمكان من خلال استخدامهم للتقنيات الحديثة وللرسائل الرقمية؛ حيث أصبح بالإمكان الاجتماع والتحاور والحصول على كل ما يُرَوجون له من أفكار ومبادئ عبر مَوَاقِع الإنترنت ومنتديات الحوار وأنظمة البالتوك وغيرها، إلى أن تحول بهم الأمر من موضع الدفاع إلى موضع الهجوم والعدوان[3].

وأصبح من الأهداف المعلنة للإرهاب الالكترُوني إيقاع أقصى ما يمكن من خسائر ممكنة لدى الطرف الآخر والمعادي في نظرهم، وكذا شن حرب نفسية بالإضافة إلى محاولات تطوير الأجهزة والتقنيات الفايروسية التي تعمل على تخريب المَوَاقِع الالكترُونية أو التسلل إليها والتصنت لها أو السطو على محتوياتها، وأصبحت بذلك الحرب المعلوماتية ذات أهمية لا تقل عن الحرب المعلنة ضد الدول[4].

وقد إنتبه الغرب إلى خطورة الإرهاب الالكترُوني في فترة مبكرة، حيث شكل الرئيس الأمريكي الأسبق بيل كلينتون لجنة خاصة (www.nipc.gov) مهمتها حماية البيئة التحتية الحساسة في أمريكا، واتبع ذلك إنشاء مراكز خاصة بكل ولاية على حدث للتعامل مع إحتمالات أي هجمات إرهابية الكترُوني، وغير بعيد عن ذلك قامت الإستخبارات المركزية بإنشاء مركز حروب المعلوماتية ووظفت بها ألفا من خبراء أَمن المعلومات، كما شكلت قوة ضاربة لمواجهة الإرهاب على مدار الساعة[5].

2/ مظاهر الحرب الالكترُونية:

ترتبط في بعض الأحيان الحرب الالكترُونية بوجود خلاف أو نزاع دولي؛ ومن مظاهر هذه الحرب:

أ-اختراق المَوَاقِع الالكترُونية:

يعد الاختراق أبرز صور الحروب الالكترُونية– كما سنفصل فيه لاحقا– إذ يقوم شخص أو أكثر باختراق موضع ما لتعديل أو الاستحواذ على معلومات سرية موجودة به،أو إتلاف الموقع وشله عن العمل؛ ويتم الإعلان عن ذلك بوضع شارات أو رسائل تُنبئ عن احتلال الموقع بصورة مشابهة لرفع أعلام الإحتلال زمن النزاعات المسلحة.

ب- نشر الفيروسات:

وهي بمثابة برامج يتم تمريرها بسرعة كبيرة جدا من خلال شبكة الإنترنت جراء تبادل الملفات والبرامج بين مستخدمي الشبكة، وينتج عن هذه الفيروسات تخريب للمَوَاقِع برمتها أو لبعض محتوياتها أو تعطيلها عن العمل لفترة من الزمن؛ ومن ذلك المبرمج التايواني الذي طور فيروس تشيرنوبيل Chrnobyl الذي اعتبر من أبرز الفيروسات المدمرة، إذ بقي الفيروس خامدا داخل أجهزة الحاسب المصابة، حتى حلول الذكرى 13 لكارثة المفاعل النووي السوفياتي (تشيرنوبيل) في يوم 26 إبريل 1999 حيث نشط في هذا اليوم ليصيب ما يزيد عن 60 مليون جهاز على مستوى العالم، ولم تسلم من ذلك حتى الدول العربية.

ج-التجسس الالكترُوني:

عهدت الكثير من حكومات الدول إلى تكثيف وتطوير جهودها للتجسس على العديد من العمليات التي تتم عبر شبكة الإنترنت، وكانت في ذلك الولايات المتحدة الأمريكية وبواسطة أجهزتها الأَمنية، قد نشطت من حركات التجسس على من أسمتهم بالجماعات الإرهابية وكان من صلاحيات هذه الأجهزة التجسس على مستخدمي الإنترنت أثناء تصفحهم أو تبادلهم للرسائل الالكترُوني؛ ولم تكن إسرائيل بعيدة عن إستغلال التجسس الالكترُوني، حيث كان لها باع كبير في ذلك حيث أقامت قسما خاصا في هيئة أركانها للتجسس على شبكة الإنترنت، ليس هذا فحسب بل وأقامت صفقة مع شركة مايكروسوفت الأمريكية لشراء برامج للتصنت على الاتصالات من خلال شبكة الإنترنت قدرت بـ: 217 مليون دولار[6].

د - الحرب الإعلامية:

أضحت الإنترنت أداة هامة للتأثير على الرأي العام، حيث صار بالإمكان تأسيس مَوَاقِع من قبل أفراد أو منظمات للحصول على الدعم المادي والمعنوي لقضاياهم، ومن ذلك ما قامت به حركات شيشانية بتأسيس مَوَاقِع لبيان المذابح التي يتعرضون لها من طرف القوات الروسية، وهذا ما لم تكن وسائل الإعلام التقليدية تتمكن من فعله آنذاك، وأصبحت هذه المَوَاقِع مصدرا لمعلومات الكثير من وكالات الأنباء[7].

بيد أن هذه المَوَاقِع لم تسلم من الاختراق من طرف منظمات حاولت إخضاعها والحيلولة دونها؛ صورة أخرى من صور الحرب الإعلامية على الإنترنت تتمثل في التصويت على حملات استطلاع الرأي التي تستضيفها بعض المَوَاقِع، كقضية الطفل الفلسطيني الشهيد محمد الدرة حيث تم التصويت على أن تكون صورته هي صورة العام ولكن اليهود قاموا باختراق الموقع وثم شن حملة للتصويت لصالح صورة كلب.

ثم إن الحرب المعلوماتية على وجه الخصوص تتمثل في كل ما يمكن أن تتعرض له شبكات الكمبيوتر من هجمات تستهدف تعطيل أو تخريب أو تدمير أنظمة تخزين ونقل المعلومات على أجهزة الكمبيوتر وشبكاته أو استهداف الأجهزة والشبكات في حد ذاتها خاصة إذا كان الأمر متعلقا بالأجهزة الأَمنية والاستخباراتية، وتعرف الوسائل والأساليب المستعملة في ذلك بأنها أنظمة معلوماتية بالأساس مصممة من أجل التأثير بشكل خاص على البنية التحتية المعلوماتية[8] دون تدميرها مباشرة بالشكل المادي المعروف[9].

3 / الجَرِيمَة الالكترُونية وفحواها:

هذه الأعمال المذكورة آنفا والتي تستخدم فيها التقنية الحديثة وأنظمة الحاسوب أصبحت تسمى بالجَرِيمَة الالكترُوني، وهي من أبرز وأخطر جرائم القرن الجديد المسايرة للتطور الباهر في تكنولوجيا المعلومات والاتصال حيث تعد شبكة الإنترنت أكبر شبكة في تاريخ البشرية[10]، وهي أبرز أدوات العالم لربط ما يفوق عن 500 مليون جهاز كمبيوتر في أكثر من 200 دولة، ويستخدمها اليوم أكثر من مليار مشترك عبر العالم ولم يعد اليوم السطو على أموال مؤسسة أو بنك ما يتطلب أسلحة بقدر ما يحتاج إلى تحكم في تقنيات التعامل البنكي الالكترُوني .

ورغم حداثة هذا النوع من الجرائم نسبيا[11] إلا أنها لاقت اهتماما واسعا لدى المختصين[12] وقد أوضحت منظمة Busieness Software Alliance في الشرق الأوسط وجود تباين بين دول

منظمة الشرق الأوسط في حجم خسائر الحاسب الآلي حيث وصلت إلى 30مليون دولار أمريكي بالمملكة العربية السعودية والإمارات العربية المتحدة؛ وقدرت الولايات المتحدة الأمريكية خسائرها من جرائم الحاسب الآلي مابين 03و05 بلايين دولار سنويا[13] ، وبالتالي فإن جرائم الحاسب الآلي من أكثر الجرائم ترتيبا للخسائر ويكون الإختراق والإتلاف وزرع الفيروسات أعلى ما يُترتب من الأضرار، فعلى سبيل المثال وصلت خسائر فيروس كود رد 02 مليار دولار أمريكي، في حين وصلت الأضرار المادية لفيروس الحب الشهير 8.7 مليون دولار[14] ، وتكمن صعوبة الجرائم الالكترُونية والحاسب الآلي في صعوبة الاحتفاظ بأثرها، وصعوبة التحقيق فيها والكشف عن القائمين بها واعتمادها على الخدع والتحايل وتحتاج لقدر كبير من الدهاء، وقد تم تصنيف القائمين بهذه الجرائم إلى أصناف متعددة أهمها:

أ- ذوو القبعات البيضاء: وهم من يتولوا تنفيذ أوامر السلطات التابعين لها إذ يقوموا بشأن هجماتهم على المَوَاقِع أو الأنظمة المطلوبة.

ب- ذوو القبعات الرمادية: أحيانا يقومون بهذه المهمة القراصنة أشرار وأحيانا من مُنطلق أن المعلومة ملك للجميع ومن حقهم الحصول عليها.

ج- ذوو القبعات السوداء: وهم يقومون بأعمال القرصنة بهدف الحصول على معلومات وأسرار أَمنية أو تحصيل مكاسب مادية أو تخريب مَوَاقِع معينة.

ثانيا: سبل اختراق وإتلاف المَوَاقِع الالكترُونية بين المسببات والآثار:

ما من شك في أن الوصول إلى المَوَاقِع الالكترُونية وتحديدا الأَمنية منها يعد مهددا كبيرا للأَمن الوطني، فاختراق موقع لفرد ما أو لشركة خاصة يمكن أن يبرر ويتم تجاوز أضراره بكيفية ما، ولكن المَوَاقِع الالكترُونية الأَمنية التابعة لأجهزة الاستخبارات والدفاع والأَمن أمر هام وبالغ الخطورة، حيث أن هذه الهيئات هي التي تكفل الحماية وتحقيق الأَمن والحيلولة دون الإرهاب الالكترُوني والجرائم الالكترُوني وغيرها من صور الجرام التقليدية والحديثة، وبالتالي إذا كانت هي من تعرض للعدوان يعني المخاطر المنصبة على مَوَاقِع أخرى سيكون احتلالها والإضرار بها من باب أيسر وأسهل.

والواضح أن أجهزة الكمبيوتر العربية أكثر تعرضا للإختراق والتجسس كما أن الدول العربية أقل اهتماما بالمسائل الأَمنية في الشبكة، عدا البعض منها التي أولت للموضوع أهمية

قصوى حيث تحتل المملكة العربية السعودية الصدارة في توفير أنظمة الحماية الالكترُوني تحقيقا للأَمن المعلوماتي.

1/ مواطن الضعف في شبكة الإنترنت:

تعتري شبكة الإنترنت العديد من العيوب والكثير من الضعف في أنظمة الدفاع، ولعل الضعف ناجم عن الأخطاء والبرمجة والعيوب في تصميم النظام، وبعض نقاط الضعف الأخرى مرتبطة بالإدخال الخاطئ للمعلومات والبيانات، وقد يفشل المبرمج أحيانا في التحقق من حجم البيانات التي تم تخزينها مما يؤدي إلى فيض وتدفق في البيانات مما قد يسبب فساد المكدس أو إلى خلل في الذاكرة[15].

وفي حال حصول أخطاء برمجية أو إعدادات فاشلة في خادم الويب فإن ذلك قد يسمح بدخول المستخدمين عن بعد غير المصرح لهم إلى الوثائق السرية المحتوية على معلومات شخصية أو الحصول على معلومات حول الجهاز المضيف للخادم مما يسمح بحدوث اختراق للنظام كما يتيح للكثير في تنفيذ أوامرهم على الجهاز بتعديل في النظام أو إطلاق لهجمات إغراقية وصولا في الأخير لتعطيل مَوَاقِع أو شلها عن العمل[16].

2 / مفهوم الاختراق وآثاره المترتبة عنه:

أ / مفهوم الاختراق:

الاختراق أو ما يسمى بالإنجليزية The Haking هو بصورة عامة القدرة على الوصول إلى هدف معين بطريقة غير مشروعة من خلال ثغرات في نظام الحماية الخاص بالهدف المرجو اختراقه، وبطبيعة الحال هو سمة سيئة يتصف بها المخترق Hakers بقدرته على دخول حواسيب الآخرين ودون إذن منهم؛ والهاكر هو الشخص الذي يقوم باختراق التطبيقات والحواسيب أو الشبكات أو يقوم بالتحايل للحصول على معلومات سرية، أو الحصول على معلومات تخص البطاقات الائتمانية أو حسابات بنكية أو للحصول على الأرقام السرية لبعض الأنظمة أو كلمات المرور للبريد الالكترُوني لشخص ما، وهناك أيضا ما يُسمى بـ الكراكر أو المقتحم وهو شخص يقوم بالتسلل إلى نظم الحاسوب للاطلاع على المعلومات المخزنة فيها أو لإلحاق الضرر أو العبث بها أو سرقتها[17].

والأصل أن الهاكر يطلق على كل شخص يمتلك قدرات خارقة في مجال البرمجة والتطوير وله قدرات خارقة في مجال البرمجة والتطوير وله باع في التفكير الرياضي والمنطقي، وهؤلاء المخترقون قد يكونوا محترفين أو هواة ومن أمثلة ذلك اختراق مراهقة في سن 15سنة لموقع لقاعدة سرية للغواصات الحربية بسنغافورة، كما قام أحد المراهقين بالتسلل إلى نظام مراقبة حركة الملاحة الجوية في مطار ماشيتيوشش MASSACHUSETTS مما انجر عنه تعطيل نظام الملاحة الجوية لمدة 6ساعات كاملة ولم تكن نتائج ذلك بالهينة[18]

وعادة ما تكون الخطوات الأولى للهاكر المبتدئ الولوج إلى أجهزة شخصية إذا كان الجهاز مصاب ببرنامج يفتح بابا خلفيا Back door يجعل من دخول الهاكر إلى الجهاز أمرا مُتيسرا، ويسمى البرنامج الذي تفتح به أبواب خلفية حصان طروادة Trojan Horse، ووظيفتها بالتحديد فتح منفذ Port في الجهاز يستخدمه الهاكر عن طريق برنامج اختراق جاهز ومعد بشكل مسبق للإختراق، ويتمكن الهاكر المحترف بعد ذلك من تتبع حركات كل حرف تكتبه، وذلك بشرط أن تكون موصولا بالإنترنت ويمكنه قراءة كل حرف تكتبه على لوحة المفاتيح، ويمكنه سحب كافة كلمات المرور المخزنة في الذاكرة مما يؤهله لفتح أي ملف والإطلاع على محتواه، ويمكنه مشاهدة الشخص بالكاميرا، بل وأكثر من هذا يمكنه أن يشاركك في المحادثات التي تجريها مع الغير.

والمنطلق يكون بفتح ملف مرسل إليك بواسطة البريد الالكترُوني[19]، حيث أن (أحصنة طروادة) مثلا تكون مضمنة داخل خلفية شاشة أو صورة، لعبة، أو برنامج صوتي أو غيرها، وبمجرد تشغيل أو فتح ذلك تكون قد فتحت بابا خلفيا Back door للهاكر، وسيكون بمقدوره اختراق جهازك والعبث به، وكل ما يحتاجه هو الآي بي (I.B) الخاص بك عند اتصالك وهذا سهل جدا للحصول عليه بحيل وطرق بسيطة[20]

ولأجل هذا ينبغي الحذر بعدم فتح أي ملف أو برنامج يصلك من خلال بريدك الالكترُوني، وتأكد من تحديث المضاد للفيروسات وملفات التجسس في جهازك الشخصي بصفة دورية كما يجب التيقن من اعتماد جهاز حماية Fire wall جيد لبرنامج زون ألارم Zone Alarm لحماية منافذ الجهاز وإغلاق المنافذ المشهورة[21].

ب/ الهاكرواختراق المَوَاقِع :

من الطبيعي أن من يملك موقعا ما ستكون بياناته متاحة للملايين من المتصفحين للشبكة، وما يفصلهم عن الموقع سوى (اسم المستخدم وكلمة المرور). فسمة الهاكر هو

الحصول على هذين البيانين، وقد يُستغنى أحيانا عنهما، حيث يمكن للهاكر استغلال أحد ثغرات نظام التشغيل في سيرفر الشركة المستضيفة لموقعك أو استغلال ثغرة من ثغرات التطبيقات التي تقوم بتركيبها في موقعك كالمنتديات أو المجلات الالكترُونية أو ما شابه ذلك.

وفي ذلك يتم الاعتماد على العديد من الآليات مثل حقن لغة الاستعلام Cross Site Scripting و SQL Injection أو ما يسمى بسلاح الدمار الشامل ضد المَوَاقِع، واقتحام الجلسات Session Hijacking ونظام CRLF Injection والـ Directory Traversal أي التجول في المجلدات وآلية التلاعب بالمتغيرات Parameters Manipulation وكذا رسائل الإحتيال Phishing Scan التي تصل إلى البريد الالكترُوني للحصول على بياناتك الخاصة واستغلالها وأيضا الرسائل المضللة، والتصنت على الشبكات[22] Sniffing، ويتم الاختراق وفق العديد من الطرق كالاختراق بالثغرات أو الاختراق العشوائي أواليونيكود.

ج/ مساعدات الاختراق:

وعن مساعدات الاختراق فهي تتمثل في وجود ملف باتش Patch أو تروجان Trojan، حيث أنه لا يمكن للهاكر الدخول إلا من خلالها ويمكن للهاكر الدخول لجهازك الشخصي والقيام بالتجسس أو الإتلاف، ويجب أن يكون هناك اتصال بشبكة الإنترنت و تتم عملية الاختراق بتفخيخ بعض المَوَاقِع المشبوهة كالمَوَاقِع الإباحية. وبالتالي صفحات الموقع بإعطاء أوامر بتنزيل ملف التجسس في جهازك.

وأهم البرامج الحديثة التي يستعين بها الهاكرز:

-Hackers Utility: يمكن من كسر الكلمات السرية للملفات وفك تشفير الملفات السرية.

-Back orifice: وهو برنامج فيروسي واسع الانتشار.

-Deep throat 2.0:يقوم هذا البرنامج بمسح الملف واستبداله بالسيرفر الخاص به، ومن خلاله يتم التحكم في المَوَاقِع التي يزورها الضحية وتوجيهه لأي وجهة.

-Ultra Scan-15.exe: أسرع البرامج لعمل Sca على جهاز الضحية لمعرفة المنافذ المفتوحة التي تمكن الهاكر الدخول من خلالها.

Zip Cracker: برنامج مصغر من خلاله يتم كسر الثغرات وكلمة السر.

د/ أنواع الاختراق:

1/ اختراق المزودات أو الأجهزة الرئيسية للشركات والمؤسسات أو الجهات الحكومية، وذلك باختراق الجدران النارية التي عادة توضع لحمايتها وغالبا ما يتم ذلك باستخدام المحاكاة Spoofing وهو مصطلح يطلق على عملية انتحال شخصية للدخول على النظام :

2/ اختراق الأجهزة الشخصية والعبث بما تحتويه من معلومات.

3/ التعرض للبيانات أثناء انتقالها والتعرف على ثغرتها إن كانت مشفرة وهذه الطريقة تستخدم في كشف أرقام بطاقات الائتمانية وكشف الأرقام السرية للبطاقات البنكية ATM .

هـ- آثار الاختراق:

-تغيير الصفحة الرئيسية لموقع الويب كما حصل لموقع فلسطيني مختص بالقدس حيث غير شباب إسرائيليون الصور الخاصة بالقدس إلى صور تتعلق بالديانة اليهودية بعد عملية اختراق مخطط لها.
-السطو بقصد الكسب المادي كتحويل حسابات بنكية أو مكاسب مالية كأرقام بطاقات الائتمان مثلا .

و- تشويه مَوَاقِع الإنترنت:

وذلك ما هو إلا تغيير للصفحة الرئيسية للموقع بصفحة أخرى يعلن فيها المخترق انتصاره على النظام المزود والإجراءات الأَمنية للشبكة[23].

وتقتصر الأضرار التي تسببها عمليات التشويه على الإضرار بالجهة المالكة للموقع، حيث أن المحتويات تبقى سليمة كما هي .

وهذا ما يتضح عند تصفحك لموقع ما وتأتيك الصفحة الرئيسية برسم بذئ أو محتويات مغايرة لما كانت عليه هذه الصفحة أو بإشارة إلى أن الوصول إلى هذا الموقع غير ممكن، وهذا ما سيكون له أثر كبير على الموقع وسمعته[24]

أسباب هذه الهجمات:

1/ التسلل إلى النظام

2/ أسباب سياسية متعددة

3/ أسباب إقتصادية واجتماعية ونفسية متعددة

4/ دوافع الانتقام من الرئيس الاداري مثلا

5/ الطبيعة التخريبية لبعض الأشخاص

ز- برامج Net Bus:

تم تطوير هذا البرنامج في نسخ عديدة وهو برنامج يسمح لأي شخص السيطرة على الجهاز الضحية عن بعد وذلك بـ:

- عرض صورة مفاجئة على شاشة الضحية

- إنزال أي ملف من المخترق إلى جهاز الضحية

- فتح وغلق باب CD ROM تلقائيا دون إذن المستخدم

- التحكم في الصوت

- وضع مؤشر الماوس في مكان ما دون إمكانية تحريكه

- سماع كل ما يقوله الضحية في حال ارتباطه بالميكروفون

- عرض رسالة قصيرة مع عدم إمكانية حذفها - إغلاق أي نافذة مفتوحة بالشاشة

- التجسس على المستخدم ومراقبة كل ما يقوم به

- تغيير أو حذف كلمات السر الخاصة بالضحية واستبدالها

- عرض محتويات القرص الصلب بالكامل عن بعد

بالإضافة إلى ما سبق نجد أيضا:

ح- انتحال شخصية المَوَاقِع:

وهو من أحد الأساليب وأشهرها خطورة حيث يمكن تنفيذ هذا حتى مع المَوَاقِع التي يتصل بها من خلال نظام الاتصال الأَمني Secured Server حيث يمكن اختراق هذا الحاجز الأَمني، ويتم شن هجوم على الموقع للسيطرة عليه، وبالتالي يتم توجيه أي شخص إلى موقعه بمجرد كتابة اسم الموقع الأصلي[25]

ط- الإغراق بالرسائل:

وذلك بإرسال المئات أو الآلاف من الرسائل إلى البريد الالكترُوني لشخص ما بقصد الإضرار به حيث يؤدي ذلك إلى تعطل الشبكة وعدم إمكانية استقبال أي رسائل فضلا عن إمكانية انقطاع الخدمة، وخاصة إذا كانت الجهة المتضررة من ذلك هي مقدمة خدمة الإنترنت مثلا، حيث يتم ملء منافذ الاتصال وكذا قوائم الانتظار ومما يؤدي إلى انقطاع الخدمة، لذا عمدت بعض الشركات إلى تطوير برامج باستقبال جزء محدود من الرسائل في حال التدفق الكبير لها.

3 / التصدي لاختراق وإتلاف المَوَاقِع الالكترُونية الأَمنية:

يتمثل التحدي الحقيقي للحروب الالكترُوني في مدى القدرة على اكتشاف وقوع وشن هذه الحروب وسرعة مواجهتها، إذ أنه في أثناء كثيرة لا يمكن اكتشاف وجود تجسس أو تصنت أو اختراق إلا بعد مدة طويلة وهذا ما يكون مهددا لأَمن المَوَاقِع الالكترُونية الأَمنية والإطلاع على أسرارها وخطط عملها وبرامجها في مكافحة الإرهاب مثلا أمر أو التصدي لآفة المخدرات وغيرها، وسيكون من أهم سبل الوقاية من الاختراق والإتلاف ما يلي:

1. بث الوعي بين مستخدمي الحاسب والإنترنت بطبيعة الحرب الالكترُونية وتدريبهم على إتخاذ إجراءات وتدابير احترازية لمنعها، وضرورة اعتماد التدريب الأَمني المعاصر الذي بات ضرورة قصوى لتحقيق أَمن المجتمعات .
2. مراقبة شبكات الحاسب باستمرار للكشف عن حالات الاختراق وسد الثغرات الأَمنية في الشبكة المراقبة.
3. تأهيل مديري الشبكات وحثهم على الاطلاع عن كل جديد في مجالات اختصاصهم.
4. بيان أن حماية المَوَاقِع الالكترُونية الأَمنية مسؤولية الجميع وليس رجال الأَمن فقط.
5. التحكم في البرامج الأَمنية كالجدران النارية ومجابهة الفيروسات وتحديثها باستمرار .
6. القيام بنسخ المعلومات المخزنة حتى لا يتم إتلافها كليا في حال اختراق الموقع.

7. الاعتماد على الطاقات الوطنية من الشباب المؤهلين الذين أثبتوا كفاءاتهم الخارقة في اختراق المَوَاقِع لسد الثغرات الأَمنية التي يلج من خلالها المخترقون .
8. تكثيف الطبقات الأَمنية وطبقات أَمن الوصول بفرض قيود أَمنية زمانية ومكانية.
9. اعتماد سياسة الحلول الأَمنية التي تعد بمثابة خدمة من الخدمات المقدمة من مؤسسة حلول التصميم.

والمشرفون على هذه الخدمات هم شباب يمتازوون بمؤهلات عالية في مجال أَمن المعلومات ويتولى تقديم خدمة الحارس الشخصي الذي يتولى تقديم المعلومة الأَمنية والمشورة والتحليل الأَمني ويتولى تقديم خدمة العين الساهرة وهي أحد خدمات الحلول الأَمنية الهادفة إلى الإطلاع الدائم على حالة الموقع الفنية ويتولى نظام العين الساهرة إبلاغ المعني بأي حالة بطؤ أو توقف أو اختراق

10/ عدم الدخول إلى المَوَاقِع المشبوهة التي قد يستخدمها المحترفون في إدخال ملفات التجسس، وعدم فتح أي رسالة الكترُوني يكون مصدرها مجهولا .

11/ محاولة تغيير كلمة السر بصورة دورية حيث أنها قابلة للإختراق بصفة دورية[26] وضرورة تكوينها لحروف وأرقام دوريا.

12/ ضرورة تطهير حواسيب الهيئات الأَمنية من التروجان الذي يتيح للمخترق التحكم الكامل في الجهاز مع ضرورة تحديث برامج مكافحة الفيروسات بصفة دورية .

ثالثا : أَمن المعلومات أولوية هامة لحماية المَوَاقِع الالكترُونية الأَمنية :

إن الحديث عن المَوَاقِع الالكترُونية الأَمنية يعكس جانبا هاما من المنظومة الأَمنية العربية، حيث أن اختراق أو إتلاف هذه المَوَاقِع، يعكس مدى هشاشة هذه المنظومة وإذا ما تم الوصول إلى هذه المَوَاقِع المذكورة فإن ذلك حتما سيتيح للجماعات الإِرهابية ولوكالات التجسس الإطلاع على كل المعلومات الإستراتيجية، وهذا ما يشكل مقوضا رئيسيا ومعولا من معاول هد الأَمن الوطني .

وأَمن المَوَاقِع الالكترُونية يتبع بالضرورة مواجهة الجرائم الواقعة عليها ومتابعة تطوراتها وهذا ما أضحى ظاهرة اجتماعية خاضعة للتطور الاجتماعي حيث أنه في كل جماعة المجرم

والجَرِيمَة أمران متلازمان فلا وجود لجَرِيمَة دون مجرم ولا لمجرم من غير جَرِيمَة، وإن كان حال الجَرِيمَة في تطور فهذا حال المجرم أيضا[27].

ونتيجة للتطور التقني الحاصل اليوم لم يعد المجرم اليوم أو الشبكات الإجرامية متغافلة عن تتبع الوسائل العلمية التي تعتمدها الشرطة أو أجهزة الحد من الجَرِيمَة بل قد تتجاوز قدراتهم في بعض الأحيان[28].

ولكن ما يجب التنويه إليه أن المجرم في الغالب يكتشف ولا يبتكر أي أن مدى التطور في العلم يجاوز عادة قدرة المجرمين على الاستفادة من العلم،أي أن ما يتم ابتكاره من تقنيات حديثة يظل على الأقل لفترة من الزمن خفيا عن المجرمين ليتم اكتشافه لاحقا والتصدي له[29]

ولا يعني دائما أن الوسائل العلمية لمكافحة الجَرِيمَة تفقد جوهرها بمجرد ما أن يتصدى لها المجرمون ولكن الواجب مع ذلك هو ضرورة تطوير هذه الوسائل العلمية أو تطوير كيفية استخدامها، حتى لا يلحقها ركب المجرمين، وإذا لم تكن هذه التقنيات في تطور فهي حتما في تدهور من منطق أنه من لم يكن في زيادة فهو في نقصان.

وفي هذا كان من الواجب أن تكون أبرز سمات الأجهزة الأَمنية سمة العلمية، بالإضافة إلى مبدأ الإلزامية ومبدأ الواقعية[30].

وفوق هذا يكون من الضرورة بمكان وضع معايير وأسس وضوابط لانتقاء رجال الأَمن وتدريبهم التدريب الأكمل جراء تعدد شبكات الإجرام إلى أن أضحى هنالك ما يسمى بالجَرِيمَة المنظمة التي تعتمد هي الأخرى على أسس وتقنيات فاعلة جدا، وعلى مجرمين محترفين ولأجل التصدي للإرهاب الالكترُوني المعاصر[31].

1/ عناصر أَمن المعلومات لدى أجهزة الأَمن المختلفة:

إن أَمن المعلومات عُرف بأنه العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الإعتداء عليها ، هذا من الناحية الأكاديمية أما من الناحية التقنية فهو الآليات والوسائل والإجراءات اللازمة لضمان حماية المعلومات من الأخطار الداخلية والخارجية، ومن الناحية القانونية التشريعية فإن أَمن المعلومات هو كل دراسات وتدابير حماية سرية وسلامة محتوى توافر المعلومات ومكافحة أنشطة الإعتداء عليها أو إستغلال نظمها في ارتكاب الجَرِيمَة، وهذا هو الغاية المرجوة من تشريعات حماية المعلومات

من الأنشطة غير المشروعة وتكون بطبيعة الحال الظروف مشددة في تسليط العقاب إذا كان المحل المستهدف هو مقومات الأَمن الوطني.

أما من الناحية الأَمنية فإن أَمن المعلومات يسعى إلى فرض طوق صارم من الفواصل والحواجز الأَمنية العلمية وتجنيد كل الطاقات المؤهلة علميا وتجديد البحوث والدراسات واعتماد كل الأساليب العلمية في ذلك وعن عناصر أَمن المعلومات في المجال الأَمني فهي تتمثل أساسا في:

أ/ السرية والوثوق:

وتعني التأكد من أن المعلومات لا يمكن أن يطلع عليها أو يستكشف فحواها أحد من غير المخولين بذلك، خاصة وأن قواعد البيانات والمعلومات المتواجدة لدى أجهزة الأَمن والاستخبارات والأَمن العسكري تتطلب السرية التامة والتكاملية القصوى أكثر من أي جهاز أو مؤسسة أخرى، كما يمكن لهذه الأجهزة الأَمنية أن تعتمد على أسلوب التظليل في بعض الأحيان للتيقن من وجود اختراق أو تجسس أو تنصت وما شابه ذلك.

ب/ التكاملية وسلامة المحتوى:

كما أنه من الواجب على القائمين على الأنظمة المعلوماتية لدى أجهزة الأَمن أن يتيقنوا من أن محتوى المعلومات صحيح ولم يتم تعديله أو العبث به وبشكل خاص لم يتم تدمير المحتوى أو تغييره أو العبث به في أي مرحلة من مراحل المراجعة أو التبادل سواء في مرحلة التعامل الداخلي مع المعلومات أو عن طريق تدخل غير مشروع.

ج/ إستمرارية توافر المعلومة أو الخدمة وتحديثها:

إذ لا بد وأن يكون هنالك تدفق عال للتقنية الحديثة، بل لابد وأن يكون هنالك إستمرارية وعدم انقطاع لها بالإضافة إلى تحديث وتجديد هذه التقنيات.

2/ مخاطر تهديد أَمن المعلومات:

تصنف المخاطر المتصلة بعمليات الحماية إلى طوائف ثلاث:

- طائفة المخاطر التي تتعرض لها المعلومات في مرحلة خلق واسترجاع وتعديل وإبقاء المعلومات وجامعها وجود المعلومات داخل النظام.

Read.Create ,modify ,Delete refers to information (data and software) in side the computer system.

- طائفة المخاطر التي تتعرض لها المعلومات في مرحلة النقل، أي التبادل بين أنظمة الحاسوب

Transport refers to information (data and software) transported via net work or on media

- طائفة المخاطر التي تتعرض لها المعلومات في مرحلة التخزين على وسائط خارج النظام .

Store refers to information (data and software) when it is stared on computer media and taken out of the computer system (I. E. Back up tapes/diskets)

وإزاء هذه الطوائف من المخاطر سيكون على أجهزة الأَمن والاستخبارات إعتماد كل البرمجيات والأساليب التقنية لمكافحة ظاهرة اختراق الأنظمة والمَوَاقِع الالكترُونية باعتماد تقنيات مقاومة الفيروسات مثلا وتقنية الجدران النارية FIRE WALL والشبكات الافتراضية الخاصة VERTUAL PRIVATE NET WORKS، وبات من الضرورة أيضا تبني إستراتيجية قوية لأَمن المعلومات securite policy والتي تتمثل في مجموعة الأسس والقواعد التي يطبقها الأشخاص لدى التعامل مع التقنية ومع المعلومة داخل المنشأة، وتتصل بشؤون الدخول إلى المعلومات والعمل على نظمها وإدارتها

واستراتيجيات أَمن المعومات لدى أجهزة الأَمن تهدف إلى تعريف المستخدمين والإداريين لديها بالواجبات الملقاة على عاتقهم لحماية أنظمة حواسيبهم التي يشتغلون عليها والشبكات التي يتواصلون من خلالها، في كل مراحل الإدخال والمعالجة والخزن والنقل وإعادة الاسترجاع، لأن خطأ بسيطا سيكلف الكثير ولأن المعلومات المتعامل بها لا تخص الجانب الشخصي للمتعامل بل إنها تتعلق بأَمن أمة برمتها .

الخاتمة:

مما سبق ذكره اتضح أن التقنيات الحديثة واستخدامها بات ضروريا كضرورة الماء والهواء، ولكن هذه التقنيات إما نتحكم في دواليبها فتصبح سلاحا بأيدينا أو أن نتهاون في تطويرها واعتمادها فتكن وبالا علينا كالدواء الذي يُستخدم للاستطباب فإذا تجاوز تاريخ الصلاحية أضحى سُما قاتلا، نفس الشيء بالنسبة للتقنية الحديثة .

ثم إن التطرق تحديدا للمَوَاقِع الالكترُوني الأَمنية كان نتيجة للرصيد المعلوماتي الذي تحويه والكم الاتصالي الذي تتعامل بموجبه فإذا كان اختراق موقع لشركة أو مؤسسة أو مركز ما يكلف أموالا فإن اختراق المَوَاقِع الأَمنية يكلف الأموال والمقومات والأرواح، والتهاون في حمايتها برهة من الزمن يكلف الكثير ولمدة أطول

خاصة وأن الغرب يسعى لمعرفة كيف يفكر العرب والمسلمون، وكيفية التفكير لا يتم البحث عنها في موقع شركة أو موقع ألعاب أو نوادي التسوق وإنما في المَوَاقِع الالكترُونية الأَمنية، فهاهي وكالة التجسس الأمريكية NSA تقيم لها أكبر محطة في بريطانيا تعمل على رصد كل المراسلات والاتصالات الجارية بين العالم العربي والغرب خاصة ما كان عن طريق الانترنيت، وهذا بعد أن أدرك الغرب أن من يملك المعلومة يملك القوة

وبالتالي أضحى واجبا على الأجهزة الأَمنية والعاملين لديها– والمسؤولية ملقاة أيضا على الأفراد لأن الأمر جلل يخص أفراد الأمة كلهم– أن تكون اليقظة سمتهم والتفوق ميزتهم، لأن هذه التقنيات إن لم تكن لنا فهي ضدنا، فإما أن نتحكم في دواليبها وإلا كانت من الأمور السلبية علينا

وفي هذا وصلنا إلى العديد من النتائج التي تراءى لنا وجوب إتباعها لتحقيق أَمن المَوَاقِع الالكترُونية الأَمنية ومنها:

1/ ضرورة إخضاع التعاملات الخاصة بتقنيات الحاسوب كغيرها من المعاملات الأخرى لأحكام الشريعة الإسلامية، وتسليط أشد العقوبات إذا ما كان الاختراق أو الإتلاف أو التجسس واقعا على مَوَاقِع مؤسسات الدولة، لما في ذلك من تهديد لمقومات الوطن

2/ الامتناع عن تعريض الشبكات الداخلية للخطر من خلال فتح ثغرات أَمنية عليها، كما يجب صب المعلومات الواردة والصادرة عبر الخط الخارجي للإنترنيت والمتنافية مع ديننا الحنيف ومع الأنظمة المعمول بها، هذه المَوَاقِع التي في الغالب ما تكون محملة بما يهدد منظومتنا الالكترُونية

3/ ضرورة إيجاد البنية التحتية للمفاتيح العمومية PKI لتوفير البيئة الأَمنة التي تضمن أَمن وسرية التعاملات وإثبات هوية المتعاملين وتكامل وسلامة الرسائل المتداولة بينه

4/ تحديد متطلبات أَمن المعلومات عموما و أَمن معلومات الأجهزة الحكومية وخاصة الأَمنية منها. وحماية الخصوصية والوثوق والسرية للبيانات الأَمنية واعتماد كل تقنيات الحد من الفيروسات ومحاربة الاختراق والتجسس والإتلاف والتظليل وغيرها

5/ ضرورة التكامل بين أجهزة الأَمن والدفاع والاستخبارات مع دور الجامعات في ذلك، حيث أنها أهم منابع المعرفة وأهم مؤسسات الإنتاج الفكري العربي، مع ضرورة إنشاء هيئة عربية عليا للعلوم والتكنولوجيا والمعلوماتية تعتمد على قدرات النوابغ في هذا المجال، وضرورة إطلاق مشروع عربي لسد الفجوة العلمية والتكنولوجية والمعلوماتية

6/ إنشاء مركز عربي لمكافحة الإرهاب المعلوماتي والحد من الحروب الالكترُونية المعلنة على العالم العربي والإسلامي، واستخدام مراكز بحث مختصة في الحروب الالكترُونية على غرار ما هو موجود لدى العديد من دول العالم الغربي

7/ دعم العمل مع الأنتربول والمؤسسات الدولية لأن هذه الجرائم في الغالب تتجاوز الحدود، وضرورة سن اتفاقية دولية بهذا الشأن لتوحيد الجهود الدولية في هذا

8/ ضرورة تدخل المؤسسات التشريعية بسن النصوص المواكبة لتجريم حالات التجسس والاختراق والإتلاف خاصة إذا كانت موجهة لأجهزة الأَمن ومؤسسات الدولة، وعدم الاكتفاء في ذلك بعناصر التجريم التقليدية حيث أن المشتركين في الجَرِيمَة الالكترُونية قد يكونوا من جنسيات أخرى، وأن شرط التوافق الزماني والمكاني قد يكون غير متوافر بين الجاني والضحية

9/ تحليل ودراسة الأحداث الأَمنية وحالات العدوان على المَوَاقِع الالكترُونية الأَمنية بدقة لاستنباط واستقراء ما تحويه هذه الجرائم المستجدة والأهداف التي يريد الوصول إليها من هم وراء هذه الاعتداءات.

الهوامش:

[1] إبراهيم بلبالي، الجريمة الالكترُونية بين وضوح معالم وأهداف التجريم وصعوبة التصنيف والتطبيق، ورقة بحث مقدمة ضمن المؤتمر الدولي للجريمة الالكترُونية وقانون الانترنيت بكلية الحقوق والعلوم السياسية، جامعة الجلفة، الجزائر 2009/05/04.

[2] مجلة خالد العسكرية، التقنية والأمن بتاريخ 01/ 06/ 2005 الدورة الثانية 18،2005/04/17 على موقع www.kkmag.gov.sa/detail. بتاريخ 2009/08/01.

[3] ممدوح عبد الحميد عبد المطلب، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنيت، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، سنة 2000م.

[4] صباح حسن الزبيدي، دور الجامعات العربية في بناء مجتمع المعرفة في ضوء الإرهاب المعلوماتي، مؤتمر الإرهاب في العصر الرقمي، جامعة الحسين بن طلال الدولي، 10، 2008/07/13.

[5] موقع: www.minshawi.com/old/internet.

[6] نفس الموقع.

[7] ممدوح عبد الفتاح، دور وسائل الإعلام كأداة في الصراع، دراسة تطبيقية على حرب الخليج، كلية الإعلام، جامعة القاهرة، 1996.

[8] B. **TCHIKAYA.**, <<Les infractions internationales relatives à l'informatique et aux télécommunications>>, *in* Droit international pénal, (sous la direction de Hervé ASCENSIO, Emmanuel DECAUX, Alain PELLET), Edition A.PEDONE, paris, 2000, pp.595, 596.

[9] Michael **N.SCHMITT**, <<Wired warfare: Computer network attack and *jus in bello*>>, I.R.R.C, I.C.R.C, Vol. 84, No 846, June 2002, p. 366-367.

ساعد العقون، الحرب المعلوماتية زمن النزاعات المسلحة والقانون الدولي الإنساني، ورقة عمل ضمن الملتقى الدولي للجريمة الالكترُونية، بكلية الحقوق، جامعة الجلفة الجزائر 05/04 ماي 2009.

[10] ممدوح عبد الحميد عبد المطلب، المرجع السابق.

[11] محمد محمود مندورة ، جرائم الحاسب الآلي، دورة فيروس الحاسب الآلي، مكتب الآفات المتحدة، الرياض.

عن موقع : www.minshawi.com/old/internet

[12] ذياب البداينة، جرائم الحاسب والإنترنيت، أبحاث الندوة العلمية لدراسة الظواهر الإجرامية المستحدثة وسبل مواجهتها، أكاديمية نايف العربية للعلوم الأمنية،

عن نفس الموقع

[13] نفس المرجع

[14] عن موقع: http://ajeeb.com.8/8/2001

[15] عن موقع: .www.dzsecurity.net/vb/archive/index بتاريخ 2009/07/30

[16] تدابير مكافحة الجرائم المتصلة بالحواسيب مؤتمر الأمم المتحدة لمنع الجريمة وللعدالة الجنائية: المنعقد في بانكوك في18-25/04/2005 وثيقة رقم 203/14 1/conf على الموقع الالكترُوني: htt://www.un.org/arabic/events/conferences/crime-html

[17] Bouchaib RAMAIL: la criminalité informatique, criminalité a double dimension: internationale, thèse pour l'obtention du grade de ducteur en droit privé-option: des affaires, faculté des sciences juridiques, économiques et sociales- fés, 2005, p:82.

بلبالي ابراهيم، المرجع السابق.

[18] عن موقع: .www.dzsecurity.net/vb/archive/index بتاريخ 2009/07/30

[19] رمضان قنفود، المسائل القانونية المتعلقة بالبريد الالكترُوني ، ورقة بحث مقدمة للملتقى الدولي حول الجريمة الالكترُونية وقانون الإنترنيت، كية الحقوق والعلوم السياسية جامعة الجلفة، الجزائر 05/04/ماي 2009.

عبد الهادي فوزي العوضي، الجوانب القانونية للبريد الالكترُوني، ط1، دار النهضة العربية، جمهورية مصر العربية، 2005، ص12.

[20] عن موقع : www.derhall.com/articles/23بتاريخ 2009/08/01

[21] نفس المرجع

[22] نفس المرجع

[23] عن موقع :http://ahlalhadeeth.com/vb attachment.

[24] نفس المرجع

[25] نفس المرجع

[26] عن موقع : .http:// forum.sh3bwah.maktoob.com/t76695

[27] نيازي حتاتة، مجرم العصر الحديث، مجلة الأمن العام المصرية، 44، ص 44.

[28] لطفي جمعة، دور الشرطة في حفظ السكينة والنظام، مجلة الأمن العام المصرية، العدد 24، ص 05.

[29] قزران مصطفى، الجهود الدولية لمكافحة الجريمة الالكترونية، ورقة بحث ضمن الملتقى الدولي للجريمة الالكترونية وقانون الأنترنيت، كلية الحقوق والعلوم السياسية، جامعة الجلفة، الجزائر، 2009/05/04.

[30] التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي"، قرار الجمعية العامة للأمم المتحدة في الدورة الثالثة والخمسون بتاريخ 04 جانفي 1999، رقم الوثيقة (A/RES/53/70).

[31] إبراهيم عيد نايل، جرائم الإرهاب السياسية الجنائية في مواجهة الإرهاب في القانونين الفرنسي والمصري، دار النهضة العربية، ص 05.