نجاح مشروع الحكومة الإلكترونية اجتناب الفشل من خلال إدراك المخاطر الالكترونية

أ.د حديد نوفيل *

بوزيد هجيرة سومية **

Résumé :

Les perpétuelles changements spectaculaires à tous les niveaux, notamment le développement rapide des technologies de l'information et de la communication, a rendu le monde d'aujourd'hui non traditionnel, où tout est virtuel, en particulier dans le domaine économique où les États ne manquent pas ces grands avantages découlant de l'utilisation des technologies nouvelles de l'information et de la communication à la prestation des ces services gouvernementaux. Mais malgré cela, cette utilisation a apporté beaucoup de cyber-risques qui pourraient conduire à des cyber-attaques ou des cyber-crimes, qui peuvent empêcher le fonctionnement de ce gouvernement électronique.

الملخص: التغيرات الهائلة على كافة الأصعدة ومختلف المستويات خاصة التطورات المتلاحقة في تكنولوجيات المعلومات والاتصال، جعلت من العالم اليوم بيئة غير تقليدية؛ افتراضية، كل شيء فيها الكتروني لا سيما في المجال الاقتصادي. والدول لم تفوت الايجابيات الكبيرة الناتجة عن استخدام التكنولوجيات الحديثة للمعلومات والاتصال لتقديم خدماتها الحكومية. لكن رغم هذا صاحب هذا الاستعمال الكثير من المخاطر الالكترونية التي قد تؤدي إلى اعتداءات أو جرائم الكترونية تصل حد تعطيل وفشل الحكومة الالكترونية في تأدية مهامها.

* أستاذ، مخبر إدارة التغيير في المؤسسة الجزائرية-الجامعة الجزائر 3.

** أستاذة مساعدة أ، جامعة الجزائر 3.

مقدمة:

استجد على العالم خلال فترة تاريخية لا تتعدى العقدين من الزمن تغيرات وتطورات هائلة على كافة الأصعدة والمستويات. ولعل الطفرات والانجازات العلمية والتكنولوجية غير المسبوقة أهم هذه التطورات التي أدخلت العالم بأسره؛ أفراد، مؤسسات، وحتى حكومات في عصر تكنولوجيات المعلومات والاتصالات. التي ومنذ ظهورها وهي تؤدي إلى ظهور خدمات جديدة لتداول المعلومات ونقلها بطريقة رقمية[1] يتضاءل فيها دور العامل البشري فأخذتنا شيئا فشيئا إلى الافتراضية[2]. فمؤسسات اليوم بلا عمال؛ التعليم بلا معلمين؛ التجوال بلا ترحال؛ الأفلام بلا ممثلين....جعلت التكنولوجيا عامة والانترنت خاصة من العالم بيئة غير تقليدية تقع خارج الإطار الواقعي الملموس، إنه الفضاء الافتراضي[3].

عالمية بطابعها، فتحت الانترنت خاصة والتكنولوجيا عامة مجالات عديدة للاستفادة منها، لا سيما في المجال الاقتصادي: الأعمال الالكترونية[4]، الإدارة الالكترونية للأعمال[5]، التجارة الالكترونية[6]. والحكومات بدورها لم تفوت الايجابيات الكبيرة – من ناحية الإنتاجية والسرعة في الأداء، التكلفة، الشفافية ...- المتأتية من تطويع التكنولوجيات الحديثة للمعلومات والاتصالات في الإدارات العمومية، واستغلالها لخدمة المواطنين ومؤسسات الأعمال في إطار ما يُسمى بالحكومة الالكترونية والتي لا تقتصر فقط على الادارات العمومية وإنما تشمل المؤسسات الاقتصادية المنطوية تحت هذه الحكومة من جهة والأفراد أي المواطنين المتعاملين معها من جهة أخرى.

لكن، رغم أن التكنولوجيات الحديثة للمعلومات والاتصالات غيرت جذريا من شكل الحكومة التقليدي الكلاسيكي وأضافت بعدا مشرقا، إلا أنه لا يُمكن إنكار أن هذا الأثر الايجابي حمل معه الكثير من المخاطر المرتبطة باستخدام هذه التكنولوجيات؛ والتي قد تؤدي إلى اعتداءات أو جرائم الكترونية[7] تُؤثر على سير تقديم الخدمات الحكومية الكترونياً وقد تصل حد تعطيلها تماماً.

([1]): Digital.
([2]): Cyber.
([3]): Cyber Espace. Voir également l'annexe N°1.
([4]): e-Business.
([5]): e-Management.
([6]): e-Commerce
([7]): Cyber-crime.

وفقا لهذا، إن التوجه اللافت نحو تبني مشروع الحكومة الالكترونية في كثير من الدول على غرار الجزائر يجب أن يصاحبه إدراك ووعي بهذه المخاطر الالكترونية التي تعتبر من أهم التحديات التي تواجه هذا المشروع وقد تُعرِضه للفشل. فماهي هذه المخاطر؟ ومن يُسببها ؟ وماهي أدوات تنفيذها ؟

لأجل فهم هذا الموضوع؛ سنحاول في هذه الورقة إلقاء الضوء على المخاطر الإلكترونية التي تواجه الحكومة الالكترونية من خلال الجوانب التالية:

1- الحكومة الإلكترونية: التكنولوجيا في خدمة المواطن، المؤسسة وأعوان الدولة

2- الجريمة في الفضاء الافتراضي

3- الجريمة الإلكترونية من Robert Tappan Morris إلى Russian Business Network

4- الجريمة الإلكترونية استغلال الحاسوب كهدف، كوسيلة وكمحل للاعتداء

5- الجريمة بسلاح الكتروني

6- تجنب المخاطر الالكترونية من خلال الأمن الالكتروني

1- الحكومة الإلكترونية: التكنولوجيا في خدمة المواطن، المؤسسة وأعوان الدولة.

لا تعد الحكومة الالكترونية نظام حكم شائع في بلدان العالم، رغم أن فكرتها قديمة نسبيا. بل أن تطبيقها سبق ظهور هذا المصطلح(*) الذي يحمل معه تشعبا في المفاهيم المرتبطة بها واختلافا في الغرض من استخدامها.

سبق ظهور مصطلح الحكومة الالكترونية، استخدام تكنولوجيا المعلومات والاتصال لتأدية بعض الأعمال الإدارية في الإدارات العمومية. لكن هل الحكومة الالكترونية مجرد تألية لوضائف الحكومة التقليدية أم أنها وسيلة للإصلاح الإداري من شأنها تحقيق فعالية وفاعلية الحكومة كلها؟.

(*): كانت الحكومة الالكترونية قيل ثلاثة عقود محصورة في استخدام ما كان متاح آنذاك من أجهزة وبرامج الكترونية في الأعمال الادارية المكتبية e-Administration. ثم تعدى ذلك إلى تقديم خدمات الحكومة على الخط Administration en ligne، إلى أن وصلت إلى شكلها الحالي كأداة للتواصل بين أعوان الحكومة فيما بينهم، وبينها وبين مؤسسات الأعمال ومواطنيها e-gouvernement.

يشير مصطلح الحكومة الالكترونية حسب منظمة التعاون والتنمية الاقتصادية، إلى استخدام تكنولوجيا المعلومات والاتصال كأداة أفضل للإدارة. وبالتالي وحسب نفس الجهة، لا يتم تصميم الحكومة الالكترونية بناءا على شكل الحكومة الحالي وإنما يجب السعي لاستخدام تكنولوجيا المعلومات والاتصال لتحويل الهياكل، والعمليات والأهم ثقافة الإدارة[1] .

يدعم BRADIER هذا بتعريفه للحكومة الالكترونية على أنها : استخدام تكنولوجيا المعلومات والاتصال دون اغفال تأهيل الموظفين، ليس فقط لتحسين الخدمات العامة ولكن أيضا لتعزيز الديمقراطية ودعم السياسة العامة[2].

في نفس السياق سجلنا من خلال بحثنا رأياً مشابهاً لما سبق؛ يعتبر الحكومة الالكترونية استخدام لخدمات الانترنت من أجل تعزيز الحصول على المعلومات وإيصالها من قبل الحكومة الالكترونية ومختلف أعوانها، وتحسين أدائها عن طريق زيادة فعالية وجودة الخدمات الحكومية المقدمة[3].

إذن لا ينحصر مفهوم الحكومة الالكترونية في تلك الزاوية الضيقة، فهي ليست مجرد برامج وأجهزة ومواقع إلكترونية. بل هي شكل جديد يحمل معه طريقة عمل واتصال[**] وتشارك وثقافة مغايرة في تعاملات الحكومة. أي أنها:

" تطويع واستغلال تكنولوجيا المعلومات والاتصال وخاصة الانترنت لتقديم الخدمات الحكومية بفعالية وفاعلية في الأداء ينجم عنه تحسين لجودة الخدمة وتعزيز الاتصال بين أعوان الحكومة فيما بينهم من جهة و بين الحكومة ومؤسسات الأعمال والمواطنين من جهة أخرى.

([1]) : Lau Edwin, «Principaux enjeux de l'administration électronique dans les pays membres de l'OCDE», Revue française d'administration publique, 2004/2 no110, P: 225.

([2]) : Bradier Agnès, «Le gouvernement électronique : une priorité européenne», Revue française d'administration publique, 2004/2 no110, P: 337.

([3]) : Benyekhlef Karim, «L'administration publique en ligne au Canada : précisions terminologiques et état de la réflexion», Revue française d'administration publique, 2004/2 no110, P: 271.

[**]: يتم تصنيف الأطراف المتعاملة مع الحكومة الالكترونية كالتالي:

1- G to G : للدلالة على الخدمات المتبادلة بين أعوان الحكومة بين بعضهم البعض.

2- G to B : للدلالة على الخدمات المتبادلة بين الحكومة والمؤسسات الاقتصادية.

3- G to C : للدلالة على الخدمات المتبادلة بين الحكومة والمواطنين.

تنبع أهمية اللجوء إلى الحكومة الالكترونية إلى ما يُمكن أن تحققه من مزايا جمة. لكن ينبغي التنويه إلى أنها ليست الحل السحري لتحقيق ما سبق الإشارة له، وإنما الانتقال نحوها محفوف بالكثير من المخاطر التي يجب الوعي بها. ولأنها أي الحكومة الإلكترونية افتراضية فالمخاطر المصاحبة لها ذات طابع خاص يجعل منها عائقا للانتقال السليم.

2- الجريمة في الفضاء الافتراضي.

لحداثة موضوع الجرائم الالكترونية[8] نسبياً، حداثة تكنولوجيا المعلومات والاتصال، تباينت الآراء وما زالت متضاربة حول توحيد تسمية لهذا النوع من الجرائم: جرائم معلوماتية، جرائم الحاسوب والانترنت. وقد تبقى متضاربة حول تبني مفهوم مشترك لها.

فأحيانا يتم التركيز على تكنولوجيا المعلومات والاتصال كوسيلة لارتكاب هذه الجرائم، وأحيانا أخرى على المعلومات المتداولة باستخدام تكنولوجيا المعلومات والاتصال كهدف لهذه الجرائم.

حسب La Rousse، الجريمة الالكترونية هي: "الجرائم الجنائية المرتكبة في شبكات الاتصال خاصة الإنترنت.[9]

حسب المشرع الجزائري، وفي المادة " 2 / آ " من القانون المتضمن قواعد الوقاية من الجرائم الإلكترونية في مفهوم هذا القانون بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال : جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية[10].

([8]): جريمة إلكترونية، اعتداء الكتروني Cyber-Attaque؛ تهديد الكتروني Cyber-Menace، أم مخاطر الكترونية Cyber-Risque. ارتأينا قبل التفصيل في موضوع الجرائم الالكترونية توضيح الفروق بين هذه المصطلحات التي لها علاقة بالموضوع المدروس،عموما، أية حالات لا يُراد حدوثها لأنها تسبب ضرراً تعتبر أخطارا Dangers، إذا أمكن حدوثها تصبح مخاطر أي أخطار محتملة الوقوع. كلما اشتد هذا الاحتمال تصبح تهديدات. وإذا حدثت فعلا تصبح اعتداءات التي تسمى لطابعها غير الشرعي جرائم، ولأنها واقعية سنركز عليها بالدراسة والتحليل في هذه الورقة.

([9]):http://www.larousse.fr/dictionnaires/francais/cybercriminalit%C3%A9 Consulté le : [21/03/2013].

([10]): الأزرق بن عبد الله، أحمد عمراني، "نظام المعلوماتية في القانون الجزائري: واقع وآفاق"، ورقة عمل ضمن المؤتمر السنوي السادس لجمعية المعلومات والمكتبات السعودية، حول بيئة المعلومات الآمنة: المفاهيم والتشريعات والتطبيقات، الرياض، 6-7 ماي 2010، ص: 06.

ونحن بدورنا نفضل مصطلح الجريمة الالكترونية للدلالة على: "كل سلوك أو فعل غير مشروع يتم بموجبه استهداف الحاسوب أو استعماله كوسيلة أو كمحل لإلحاق الضرر به أو بالمعلومات المخزنة داخله أو ما تمثل هذه المعلومات باستخدام تكنولوجيات المعلومات والاتصالات".

ارتباط الجريمة الالكترونية بالتكنولوجيات الحديثة للمعلومات والاتصال أضفى عليها سمات مميزة جعلها تختلف اختلافا جذريا عن الجريمة العادية.

ناهيك عن السرعة، الإشكاليات التشريعية والملاحقة القضائية. الجريمة الالكترونية بطبعها متغيرة، مستحدثة، متضاعفة، هادئة لا تحتاج إلى عنف؛ بل كل ما تتطلبه القدرة على استغلال الوسائل التكنولوجية.هي جريمة عابرة للحدود ترتكب من مسافات متباعدة، افتراضية لا تترك غالبا أثراً مرئياً بل يُمكن وفي لحظة إتلاف الدلائل فيها.

هذا الاختلاف الجذري بين الجريمة العادية والجريمة الالكترونية جعل من الضرر الناتج عن هذه الأخيرة لا يُقارن مع الأولى. خاصة في الدول التي تعتمد على الحكومة الإلكترونية فحسب دراسة لمؤسسة Symantec سنة 2014، تستهدف الاعتداءات الالكترونية القطاعات الحكومية بالمرتبة الأولى وبنسبة 16 %[11]. أما عن الضحايا فتم تسجيل 378 مليون ضحية لاعتداء الكتروني في نفس السنة[12]، مقابل 556 مليون ضحية سنة 2012[13]. ومع مرور الوقت وتطور مظاهرها أصبحت الجريمة الالكترونية نشاطاً مربحاً ومغرياً حتى أصبحت تفوق في تكلفتها تجارة المخدرات بشتى أنواعها مجتمعة. وعلى سبيل المثال في الولايات المتحدة الأمريكية تضاعفت تكلفة الجريمة الالكترونية في ثلاث سنوات." البنوك الأمريكية وحدها خسرت 12 مليار دولار أمريكي جراء هذه الجرائم مقابل 900 مليون دولار أمريكي من جرائم سرقة عادية"[14].

([11]) :http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf P :19. Consulté le : [10/06/2014].

([12]) : http://go.symantec.com/norton-report-2013/ Consulté le : [10/06/2014].

([13]) :http://ebookbrowse.com/2012-norton-cybercrime-report-master-final-050912-pdf-d398339874 P: 6. Consulté le : [10/06/2014]

([14]) : La cybercriminalité coûte plus cher que les trafics de cocaïne, héroïne et marijuana, Article publié le 08/05/2012, Journal Le Monde, Disponible sur : http://www.lemonde.fr/technologies/article/2012/05/08/la-cybercriminalite-coute-plus-cher-que-les-trafics-de-cocaine-heroine-et-marijuana_1698207_651865.html Consulté le : [12/09/2012].

لأجل هذا، تفوقت اليوم الجريمة الالكترونية على كل أشكال الجرائم الأخرى من ناحية الطبيعة، المظهر، والأضرار. ليس هذا فقط بل حتى الفاعل الذي يقترف هكذا جرائم[15] يتسم بدوره بخصائص معينة تُميزه عن المجرم العادي. كذلك، الدوافع التي تحركه على ارتكابها مختلفة.

3- الجريمة الإلكترونية من Robert Tappan Morris[16] إلى Russian Business Network[17]

تعتبر المؤسسات المالية أكثر القطاعات استهدافا بالاعتداءات الالكترونية. فالرغبة في الثراء المالي المحرك الأكثر دفعا لارتكاب هكذا أفعال، لكنه ليس الوحيد فالجريمة الالكترونية يمكن أن يوجه لها عدة دوافع أخرى نذكرها كالتالي:

- **الدوافع الشخصية:** وهي، الدوافع المادية: لكسب المال. والدوافع العاطفية: لعدم الرضا أو الانتقام. والدوافع الفكرية: للتسلية واللهو والعبث، أو للتعلم وإرضاء الفضول الفكري، أو للتحدي والشعور بالفخر واثبات المهارات التكنولوجية.
- **الدوافع التجارية:** لأغراض التنافس بين المؤسسات الاقتصادية.
- **الدوافع السياسية:** لنشر الأفكار الدينية، العرقية والإيديولوجية.

إن أوائل الجرائم الالكترونية ارتكبها أطفال صغار مفتونون بالتكنولوجيا[18] يستخدمون النصوص أو البرامج الخبيثة المتوفرة عبر الانترنت للاعتداء على أنظمة ضعيفة بها ثغرات كثيرة. فعلى سبيل المثال، تم في العام 2003 إلقاء القبض على شاب يبلغ من العمر 17 سنة للاعتداء ولدوافع سياسية على 2000 موقع الكتروني حكومي أغلبها في الولايات المتحدة الأمريكية[19]. إذن المجرم الالكتروني ليس دوما

([15]) يُسمى بالمجرم الالكتروني أو Cyber-Criminel.

([16]): سنة 1988 قام Robert Tappan Morris 23 سنة، طالب في جامعة Cornell الأمريكية بالخطأ بإطلاق برنامج خبيث عطل آنذاك حوالي 6000 حاسوب وكلف الحكومة الأمريكية حوالي 100 مليون دولار أمريكي.

([17]): منذ سنة 2007 إلى يومنا هذا تعتبر هذه الشبكة عصابة منظمة متخصصة في أنشطة الجريمة الإلكترونية تستخدم مختلف أشكالها للاعتداء على المنظمات الحكومية الدبلوماسية المدنية والعسكرية بما فيها قطاع الطاقة والصناعة النووية.

([18]) : Script Kiddies.

([19]) :GUILLEMIN Christophe, « Le "script-kiddie" le plus recherché de France est sous contrôle judiciaire », Article publié le 10/07/2003, Disponible sur : http://www.zdnet.fr/actualites/le-script-kiddie-le-plus-recherche-de-france-est-sous-controle-judiciaire-2137368.htm Consulté le : [11/05/2012].

محترف، متخصص، يملك القدرة والمهارة والمعرفة العالية الوافية بالتكنولوجيات الحديثة للمعلومات والاتصال.

بل اليوم وبنقرة زر واحدة يُمكن لأي أحد تحميل برنامج يُمكِنه من الاعتداء على من يشاء؛ أفراد، مؤسسات أو حكومات. فالمجرم الالكتروني ليس بالضرورة خبير تكنولوجي بل يُمكن أن يكون هاوي كالمراهق الباحث عن التسلية، والمريض النفسي المهووس، والفضولي الراغب في الإطلاع، والتقني المتطلع للتعلم. لكن الخطر الذي يواجه هذه الفئة إمكانية استغلالها من أطراف أخرى وتحولها من الإجرام الفردي إلى جماعات منظمة. فحسب صريح لمدير الـ Interpol 80% من الجرائم الالكترونية ترتكبها عصابات منظمة يتواجد أفرادها في مناطق متباعدة من العالم[20].

هاوي كان أم محترف، يمكن أن يهدف المعتدي من خلال هذا السلوك الإجرامي إلى الاختراق[21] أي التسلل غير المشروع للحصول على المعلومات السرية المتواجدة بالحاسوب. أما إذا تعدى ذلك إلى تدميرها وإفسادها يعتبر هذا قرصنة[22] معلوماتية.

4- الجريمة الالكترونية: استغلال الحاسوب كهدف، كوسيلة وكمحل للاعتداء

سبق ومن خلال تقديم تعريف للجريمة الالكترونية اعتبارها كل سلوك يستهدف و يستخدم الحاسوب لأغراض غير شرعية وعليه يُمكن تصنيف هذه الجريمة حسب مجالها إلى:

4-1: الجريمة الالكترونية المعلوماتية:

وهي التي تهدف للحصول وبطريقة غير شرعية على المعلومات المتواجدة بالحاسوب والشبكات وقد تصل إلى حد تدميرها وتخريبها أو تحريفها. وفي الوقت المعاصر تعتبر الانترنت ذاكرة جماعية كونية لاسيما في الفترة الأخيرة مع توسع شبكات التواصل الاجتماعي، والمنتديات، و الـ Blogs ...أي مواقع الـ web2.0 عامة التي أخذت شهرة ورواج مقارنة بمواقع الـ web الأخرى.

(20) : La cybercriminalité coûte plus cher que les trafics de cocaïne, héroïne et marijuana, Article publié le 08/05/2012, Journal Le Monde, Disponible sur : http://www.lemonde.fr/technologies/article/2012/05/08/la-cybercriminalite-coute-plus-cher-que-les-trafics-de-cocaine-heroine-et-marijuana_1698207_651865.html Consulté le : [12/09/2012].

(21) : Hacking ou Intrusion.

(22) : Cracking ou Piratage informatique.

هذه المواقع أصبحت الوسائط المفضلة للأشكال المختلفة للاعتداءات الالكترونية نظراً للثغرات المتواجدة بها التي تهدد المعلومات المخزنة فيها وبالدرجة الأولى المعلومات الشخصية للأفراد[23].

4-2: الجريمة الالكترونية المالية:

وهي التي تستهدف ما تمثله المعلومات من أموال وأصول؛ كجرائم الاحتيال وسرقة بيانات الدفع الالكتروني. وجرائم التزوير المرتبطة بالغش في السجلات الالكترونية[24]وتزوير الهوية والغش في نقل الأموال الكترونيا إضافة إلى الغش في المزادات الالكترونية مثلا.

4-3: الجريمة الالكترونية الثقافية:

وهي التي تعتبر الحاسوب بيئة لها. ويدخل في هذا الصنف الجرائم المرتبطة بالملكية الفكرية للمؤلفات العلمية والأدبية ونسخها بالطرق التكنولوجية، أو استخدامها دون ترخيص كالتعدي على القنوات الفضائية المشفرة وإتاحتها عبر الانترنت. وجرائم المحتوى غير المشروع لنشر مواد مخلة بالحياء والآداب العامة أو إرسال رسائل تهديد وابتزاز.[25]

([23]): نشرت في 2011/10/24 جريدة Le Monde الفرنسية مقالا عن رفع طالب قانون نمساوي دعاوى ضد موقع التواصل الاجتماعي Facebook بداعي حفظ معلومات شخصية عنه، وفوجئ بملف من 1200 صفحة بها كم فلكي من المعلومات الشخصية المخزنة (الرسائل التي أرسلها واستقبلها وحذفها، الصور التي نشرها، الـ Likes التي قام بها...).

المصدر:

Facebook accusé de conserver des données effacées et de créer des "profils fantômes", Journal Le Monde, Disponible sur :
http://www.lemonde.fr/technologies/article/2011/10/24/facebook-accuse-de-conserver-des-donnees-effacees-et-de-creer-des-profils-fantomes_1592814_651865.html

تاريخ الإطلاع [12/09/2012].

([24]) : Cyber-Fraude.

([25]): حسب ممثل لمركز الوقاية ومكافحة الجرائم المعلوماتية والجرائم الالكترونية التابع لمصالح الدرك الوطني الجزائري. الشتائم ورسائل التهديد المرسلة عبر الانترنت تمثل 55% من الحالات التي تمت معالجتها من قبل هذه المصالح في مجال مكافحة الجرائم الالكترونية. بينما سجلت 3 حالات تسرب معلومات في إطار التجسس الصناعي من مؤسسات عمومية إلى أطراف أخرى.

Source : Mohamed.B, « Cybercriminalité en Algérie Les insultes et menaces par mails prolifèrent », Journal Algérie news, 2 février 2013, p :06.

4-4: الجريمة الالكترونية السياسية:

وهي التي تهدف لتعطيل الأعمال الحكومية الحساسة المدنية والعسكرية؛ وكل أنشطة الإرهاب الالكتروني[26]. فالإنترنت اليوم تؤمن للجماعات الإرهابية وسيلة اتصال فعالة للتنسيق سواء على الصعيد المحلي أو العالمي، وكذلك يُمكن استغلالها لجمع الأموال، وللدعاية ونشر الأفكار الإرهابية، وتجنيد الشباب للقيام بها بل وأصبح من الممكن استخدام الخدمات الجديدة للانترنت لمحاكاة اعتداء إرهابي قبل تنفيذه في العالم الحقيقي. لكم الأخطر أن يتم استخدام الانترنت لشن اعتداءات الكترونية على القطاعات الحيوية للحكومة (البنوك، الصحة، التعليم، الطاقة...).

كما حدث العام 2007 في دولة استونيا التابعة سابقا للاتحاد السوفيتي. - التي كانت من رواد الحكومة الالكترونية –، حيث تعرضت وبالتزامن مع قرار نقل نصب تذكاري "الجندي البرونزي" من عاصمة الدولة إلى مكان آخر، الأمر الذي اعتبرته روسيا إهانة كبرى للجنود الذين حاربوا النازية خلال الحرب العالمية الثانية، تعرضت لوابل من الاعتداءات الالكترونية ضد موقع الرئاسة، البرلمان، الوزارات، المؤسسات الحكومية، مواقع الأحزاب السياسية، كبار البنوك، ومؤسسات الاتصالات. ما أدى إلى شل البلاد بأكملها وإجبارها على قطع كافة الاتصالات الخارجية.

هدفاً كان أم وسيلة، يُعتبر الحاسوب والإنترنت من الوسائل التكنولوجيات الحديثة للمعلومات والاتصالات الأكثر استعمالا لارتكاب الجريمة الالكترونية.

5- الجريمة بسلاح الكتروني[27]

الجريمة الالكترونية تضم أشكالا لا يُمكن حصرها لأننا نشهد تطورات متلاحقة قد تكون أبدية، نظراً لارتباطها الارتباط الوثيق بالتكنولوجيا. ويُمكن أن نصنف أشكال الاعتداءات الالكترونية في أربع فئات رئيسية وهي:

5-1: الاعتداء باستخدام البرامج الخبيثة[28]:

يُسمى برنامج خبيث كل برنامج معلوماتي قادر على إلحاق الضرر بالحاسوب كتعطيله، أو بالشبكات كتدمير المواقع الالكترونية. إضافة إلى سرقة المعلومات المتداولة فيها.ويُشاع استخدام لفظ

(26) :Cyber-Terrorisme.
(27) : Cyber-Arme.
(28) : Malware ou Programme Malveillant.

فيروس للدلالة على نفس معنى البرامج الخبيثة، إلا أن هذه الأخيرة تمثل الفيروسات وبرامج أخرى مغايرة. ويُقسم FLIOL Eric البرامج الخبيثة إلى برامج خبيثة بسيطة، وبرامج خبيثة متكاثرة ذاتيا[29].

5-1-1: البرامج الخبيثة البسيطة:

وهي البرامج الخبيثة التي تتميز بالسكون، أي تظهر في شكل نسخة واحدة فقط. تكون وظيفتها غير معلنة، أي الإجراءات المحتواة فيها خفية. تنطلق في العمل عند تنفيذ البرنامج.

إذا كانت هذه الإجراءات متمثلة في الهجوم على الحاسوب والشبكات لإلحاق الضرر بها عند حدث معين: تاريخ معين، فعل معين (استخدام لنظام استغلال الحاسوب)، إدخال بيانات خاصة (سلسلة حروف معينة)، يسمى عندها البرنامج الخبيث **بالقنبلة المنطقية**[30]. أما إذا تمثلت هذه الإجراءات في استغلال الحاسوب والتحكم به، بواسطة فتح ثغرة على شكل باب خلفي[31] من قبل المعتدي لتوجيهه للقيام بأعمال ضارة كسرقة كلمات المرور وغيرها من المعلومات السرية، إيقاف وتشغيل الحاسوب والانترنت، تحميل ملفات منها وإرسال رسائل عبرها. وهذا دون علم أو موافقة المستخدم. يسمى عندها البرنامج الخبيث **بحصان طروادة**[32].

5-1-2: البرامج الخبيثة المتكاثرة ذاتيا:

وهي البرامج الخبيثة التي لها نفس ضرر البرامج الخبيثة البسيطة، مع القدرة على التضاعف أي نسخ نفسها بنفسها، والانتقال من برنامج إلى آخر ومن حاسوب إلى آخر بصفة ذاتية.

إذا كان هذا الانتقال أو الانتشار يتم بواسطة تبادل المعلومات الرقمية. يسمى هذا البرنامج الخبيث **بالفيروس المعلوماتي** الذي يُشبه في طبيعته الفيروس العضوي. أما إذا كان هذا الانتقال يتم فقط عبر الشبكة فيسمى هذا البرنامج الخبيث **بالدودة المعلوماتية** [33].

(29) : FILIOL Eric, « Les Virus Informatiques : théorie, pratique et application », 2ème édition, Springer, Paris, 2009, P :111.
(30) : Bombe Logique.
(31) : Backdoor ou Porte Dérobée.
(32) : Trojan ou Cheval de Troie
(33) : Worm ou Ver informatique.

الإصابة بالبرامج الخبيثة تكون عبر التحميل العشوائي لبرامج مجانية[34] عبر الانترنت تبدو كبرامج مفيدة كتلك التي تحسن من أداء الحاسوب، أو مسلية كالألعاب الالكترونية[35].

ونشير هنا إلي وجود العديد من البرامج التنفيذية تحت اسم برمجيات Downloaders، تعمل على تحميل أحد البرامج الخبيثة من أحد الخوادم المتواجدة بالانترنت بمجرد تنفيذها بالحاسب. ووجود برمجيات تنفيذية أخرى تحت اسم برمجيات Droppers تعمل على شحن أحد البرامج الخبيثة بذاكرة الحاسب المصاب بمجرد تنفيذها، ولا يستلزم أن يكون الحاسب المعني مرتبط بالانترنت وعادة ما تكون برمجيات كل من النوعين الأول والثاني من نوع البرمجيات المجانية[36].

تتراوح المخاطر المتأتية من البرامج الخبيثة[37] من مجرد الإزعاج بتكرار إظهار نافذة معينة، إلى التعطيل الكامل لتشغيل الحاسوب. كما فعل الفيروس Tchernobyl العام 1998، والذي جعل القرص الصلب للحواسيب المصابة غير قادر على الإقلاع. وحذَف نظام الـ Bios بها، فأجبر المستخدمين على إعادة تنصيبه من جديد الأمر الذي كان مستعصياً على غير المحترفين. فأجبرهم على تغيير أجهزتهم أو تغيير البطاقة الأم بها.

([34]) : Freeware.

([35]) : حسب مؤسسة Kaspersky Lab 71% من عينة متكونة من 3300 مؤسسة صغيرة، متوسطة، وحكومية في عدة دول من العالم، يَحضرون تحميل الألعاب الالكترونية مجانا عبر الانترنت. المصدر:
http://www.kaspersky.com/downloads/pdf/kaspersky_global_it-security-risks-survey_report_eng_final.pdf P:15. Consulté le : [21/03/2013].

([36]) : حديد نوفيل، " تكنولوجيا الإنترنت وتأهيل المؤسسة للاندماج في الاقتصاد العالمي "، أطروحة دكتوراه، كلية العلوم الاقتصادية وعلوم التسيير، جامعة الجزائر، 2006-2007، ص: 176.

([37]) : وصل حسب مؤسسة Bitdefender عدد البرامج الخبيثة سنة 2012 إلى 90 مليون برنامج خبيث، بارتفاع 23% عن سنة 2011. المصدر:
http://www.bitdefender.fr/blog/Une-augmentation-de-23-des-malwares-en-2012-1129.html Consulté le : [26/03/2013].

كما سجل موقع Globmeter المقدم لاحصائيات آنية 888 952 فيروس منذ بداية العام الحالي فقط. المصدر:
http://globometer.com/internet.php. Consulté le : [15/06/2014].

5-2: الاعتداء باستخدام برامج الجوسسة[38]:

عكس البرامج الخبيثة لا تقوم برامج الجوسسة بالتخريب وإنما الاعتداء بالتصنت على المعلومات المخزنة بالحاسوب، مثل المعلومات الشخصية[39] وبيانات الدفع الالكتروني. وكذلك تلك التي يستعملها المستخدم أثناء إبحاره في الانترنت والتجسس على المواقع التي يتصفحها، الكلمات التي يبحث عنها في محركات البحث، وغيرها.

عادة ما تكون برامج الجوسسة محتواة في برامج إعلانية[40].ونذكر في هذا المقام أشهر برمجيات الجوسسة: "البرمجيات المسجلة لنقرات لوحة المفاتيح"[41]، التي تقوم وكما يدل اسمها تقوم بتسجيل وتخزين كل البيانات التي يكتبها المستخدم على لوحة مفاتيح الحاسوب، ثم إرسالها إلى المعتدي.

5-3: الاعتداء بانتحال عنوان الـ IP وتزوير اسم النطاق[42]:

يتم هذا الاعتداء عن طريق الاحتيال، بتصميم المعتدي لمواقع انترنت مزيفة يتم فيها تعويض عنوان الـ IP الخاص بها أو اسم نطاقها DNS بآخر مزور. ومحاكية للمواقع الأصلية، ثم اصطياد الضحية اصطيادا الكترونيا[43] بطريقة غير مباشرة؛ عن طريق إرسال طعم في شكل رسالة بريد الكتروني مزعجة، وغير مرغوب فيها[44]، تبدو للمستخدم مغرية كربحه جائزة مالية معتبرة، أو جذابة كإسهامه في عمل خيري. هذا بغرض توجيهه إلى تلك المواقع الوهمية وسرقة بياناته الشخصية السرية وخاصة المالية.

---

(38) : Spyware ou Logiciel Espion.

(39) يكاد الفرد اليوم وبطريقة شرعية أن يُقايض بياناته الشخصية للحصول على خدمات الانترنت. فلإنشاء بريد الكتروني مثلا، يُجبر على تقديم كمٍ من البيانات المتعلقة بحياته الشخصية. ويندرج هذا الأمر في إطار تشكيل ما يسمى بالهوية الرقمية للأفراد Profiling .

(40) : Adware.

(41) : Keyloggers ou Enregistreurs de touches.

(42) : IP Spoofing ou Usurpation de l'adresse IP/ DNS Spoofing ou Usurpation du DNS.

(43) : Phishing ou Filoutage.

(44) : Spam ou Pourriel/Courrier indésirable.

تعد الهند بـ 28.8% من أوائل الدول التي تصدر منها رسائل البريد الالكتروني المزعجة في 2014. أنظر الملحق رقم 2. كما أحصت مؤسسة Symantec العام 2013، 29 بليون رسالة Spam يوميا. المصدر:

http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf P:81. Consulté le : [10/06/2014].

4-5: الاعتداء بمنع تقديم الخدمة[45]:

يتم هذا الاعتداء بإغراق خادم الشبكة بفيضان من الرسائل الالكترونية دفعة واحدة من حاسوب واحد فقط أو بالاستعانة بعدد من حواسيب مستخدمي الانترنت دون علمهم أو إرادتهم. باستخدام برمجيات تُدعى Flooders مثل UDF Flooders و SYN Flooders ويعجز بهذا على تلبية هذه الطلبات، فيشل ويتوقف عن أداء عمله.

من خلال دراستنا لموضوع الجريمة الالكترونية استنتجنا أنه مفهوم معقد. تعقده ناتج عن تغير هوية مرتكبيه واستحداث مجالاته وأسلحته سابقة الذكر التي لا تستعمل بصورة منفردة وإنما بدرجة عالية من الاعتمادية. وهذا ما يجعل منها ؛ أي من الجريمة الالكترونية لا يستهان بها كعائق يحد من نجاح الحكومة الالكترونية.

6- تجنب المخاطر الالكترونية من خلال الأمن الالكتروني

إدراك الحكومة لهذه المخاطر الالكترونية يتطلب اعتماد سياسة أمنية فعالة كعامل أساسي لنجاحها. من خلال إتباع مجموعة من الاجراءات التنظيمية واستخدام الوسائل البشرية والتقنية لحماية تعاملات الحكومة الالكترونيةوهذا ما يُعرف بالأمن الالكتروني(*) الذي يرتكز بالدرجة الأولى على حماية المعلومات المتداولة بين أركان الحكومة الإلكترونية اعتماداًعلى ثلاثة معايير أساسية توفرها يجعل من الحكومة الالكترونية نظاماً آمناً، وهي:

6-1: السرية " عدم افشاء المعلومة": أي لا يجب أن يتحصل على المعلومة إلا من له التصريح بذلك.

6-2: السلامة " عدم تعديل المعلومة": أي لا يجب أن يغير من شكل أو معنى المعلومة إلا المخول بذلك.

6-3: التوافر "عدم انقطاع خدمة الحكومة": أي يجب ضمان استمرارية تأدية الحكومة الالكترونية لوضائفها في كل الظروف.

([45]) : Denial of Service ou Dénie de Service.

(*): سوف نكتفي بالإشارة فقط إلى الأمن الالكتروني كحل لتجنب المخاطر الالكترونية لأنه موضوع يحتاج لمقال لوحده.

لهذا الغرض، وفضلا عن التوعية والتأهيل لمستخدمي الحكومة الالكترونية. يُمكن استخدام عدة وسائل تقنية ومنها: البطاقات الذكية، الجدران المقاومة للنار، تقنيات التشفير والتوقيع الإلكتروني وكذلك وسائل الحماية البيومترية التي أصبحت تأخذ الحيز الأكبر من الاهتمام في الآونة الأخيرة.

ونشير أيضا في هذا المجال إلى وجود مجموعة من القواعد والشروط والمتطلبات يستعملها أصحاب القرار في الحكومة الالكترونية كمرجعيات للحماية من المخاطر الالكترونية ومنها عائلة ISO 27000 المعترف بها على نطاق عالمي واسع وأهمها: ISO 27002الذي يُوفر مجموعة من المبادئ التوجيهية للمعايير التنظيمية المتعلقة بأمن المعلومة خاصة وممارسات الإدارة الفعالة لأمن المعلومات. فهو يحتوي على 15فصلا توجيهيا لتحقيق الحماية سواءاً في الجوانب الاستراتيجية أو التشغيلية. من ناحية تحديد مسؤولية تصميم وتنفيذ والحفاظ على أمن المعلومات. واختيار واستخدام الأساليب المناسبة لتحليل المخاطر الالكترونية. وخاصة وصفه لمجموعة من التدابير والخطوات لبلورة إطار عام لضمان التشغيل الفعال لوسائل الأمن، إضافة إلى جملة من التوصيات للحد من المخاطر الالكترونية والتوعية لها.

خاتمة:

لآثارها السلبية وربما الكارثية على الحكومة الالكترونية والفاعلين فيها: أفراد؛ مؤسسات؛ وإدارات عمومية، يُعد اجتناب حدوث الاعتداءات الالكترونية رهاناً رئيسياً لنجاح مشروع الحكومة الالكترونية. ولمواجهة المخاطر الالكترونية ينبغي التيقظ لها الكترونيا[46]. وهذا بالاستعداد من خلال الجمع النظامي لكافة المعلومات حولها والثغرات الموجودة في نظام الحكومة الالكترونية. وبالحماية منها بالتنبؤ بها واستشرافها قبل حدوثها من خلال إدراك الدوافع التي تحرك لتنفيذ الجرائم الالكترونية والوعي بالوسائل المحتمل استعمالها.

لذا نقترح على أصحاب القرار في الحكومات ضرورة اعتماد سياسية أمنية فعالة متراصفة مع سياسة إنشاء مشروع الحكومة الالكترونية وتدعيمها بتشريعات قانونية، ووسائل تكنولوجية. ولأن مواجهة المخاطر الالكترونية ليست مسألة وسائل تشريعية وتكنولوجية فحسب، ينبغي الاستثمار في توعية المستخدمين وتأهيلهم للتعامل مع التكنولوجيات الحديثة للمعلومات والاتصالات. وهذا من خلال انشاء خلية أو جهة مكلفة بالاهتمام بموضوع الأمن الالكتروني لتجنب فشل الحكومة الالكترونية وهي مجرد مشروع عند التعرض لهكذا نوع من المخاطر.

([46]) : Cyber-Veille.

قائمة المراجع:

- الأزرق بن عبد الله، أحمد عمراني، "نظام المعلوماتية في القانون الجزائري: واقع وآفاق"، ورقة عمل ضمن المؤتمر السنوي السادس لجمعية المعلومات والمكتبات السعودية، حول بيئة المعلومات الآمنة: المفاهيم والتشريعات والتطبيقات، الرياض، 6-7 ماي 2010.

- حديد. ن، " تكنولوجيا الإنترنت وتأهيل المؤسسة للاندماج في الاقتصاد العالمي "، أطروحة دكتوراه، كلية العلوم الاقتصادية وعلوم التسيير، جامعة الجزائر، 2006-2007.

- Benyekhlef Karim, « L'administration publique en ligne au Canada : précisions terminologiques et état de la réflexion », Revue française d'administration publique, 2004/2 no110.

- Bradier Agnès, « Le gouvernement électronique : une priorité européenne »,Revue française d'administration publique, 2004/2 no110.

- FILIOL Eric, « Les Virus Informatiques : théorie, pratique et application », 2ème édition, Springer, Paris, 2009.

- GUILLEMIN Christophe, « Le "script-kiddie" le plus recherché de France est sous contrôle judiciaire », Article publié le 10/07/2003, Disponible sur :

- http://ebookbrowse.com/2012-norton-cybercrime-report-master-final-050912-pdf-d398339874

- http://globometer.com/internet.php

- http://go.symantec.com/norton-report-2013/

- http://www.bitdefender.fr/blog/Une-augmentation-de-23-des-malwares-en-2012-1129.html

- http://www.kaspersky.com/downloads/pdf/kaspersky_global_it-security-risks-survey_report_eng_final.pdf

- http://www.larousse.fr/dictionnaires/francais/cybercriminalit%C3%A9

- http://www.lemonde.fr/technologies/article/2011/10/24/facebook-accuse-de-conserver-des-donnees-effacees-et-de-creer-des-profils-fantomes_1592814_651865.html.

- http://www.lemonde.fr/technologies/article/2012/05/08/la-cybercriminalite-coute-plus-cher-que-les-trafics-de-cocaine-heroine-et-marijuana_1698207_651865.html

- http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_appendices_v19_221284438.en-us.pdf

- http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf

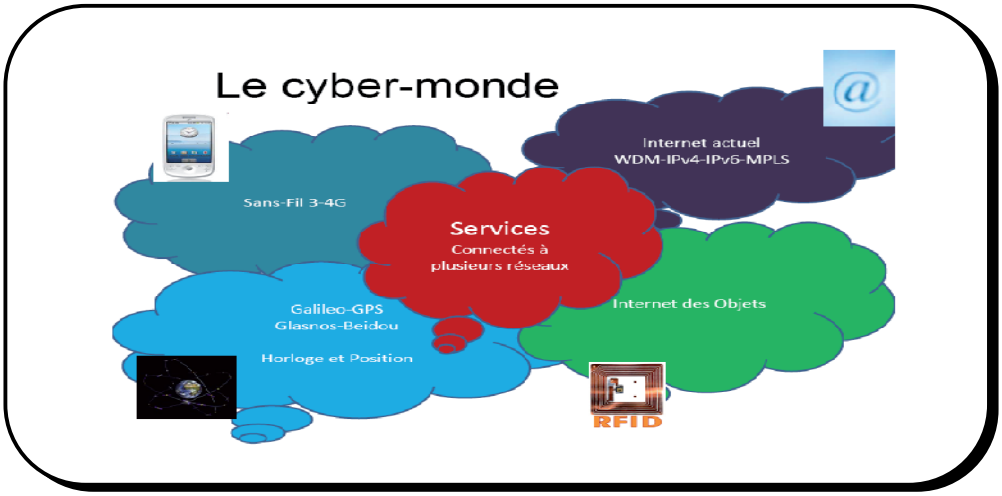
- http://www.zdnet.fr/actualites/le-script-kiddie-le-plus-recherche-de-france-est-sous-controle-judiciaire-2137368.htm

- Lau Edwin, « Principaux enjeux de l'administration électronique dans les pays membres de l'OCDE », Revue française d'administration publique, 2004/2 no110.

- Mohamed.B, « Cybercriminalité en Algérie Les insultes et menaces par mails prolifèrent », Journal Algérie news, 2 février 2013.
- Mohamed.B, « Cybercriminalité en Algérie Les insultes et menaces par mails prolifèrent », Journal Algérie news, 2 février 2013.
- WOLF Philippe & VALLÉE Luc, « La Criminalité en France », Rapport de l'Observatoire national de la délinquance et des réponses pénales, CNRS éditions, Novembre 2011, P :793. Disponible sur : http://www.inhesj.fr/sites/default/files/rapport_2011_0.pdf

الملاحق:

الملحق رقم (01): مكونات الفضاء الافتراضي.



Source: WOLF Philippe & VALLÉE Luc, « La Criminalité en France », Rapport de l'Observatoire national de la délinquance et des réponses pénales, CNRS éditions, Novembre 2011, P :793. Disponible sur : http://www.inhesj.fr/sites/default/files/rapport_2011_0.pdf , Consulté le [26/03/2013].

الملحق رقم (02): مصادر الـ Spam عالميا.

Fig. A.3

Malicious Activity by Source: Spam Zombies, 2012–2013

Source: Symantec

Country/Region	2013 Spam Rank	2013 Spam Percentage	2012 Spam Rank	2012 Spam Percentage	Change
India	1	9.8%	1	17.1%	-7.4%
Netherlands	2	8.2%	3	6.5%	1.7%
Russia	3	6.6%	10	2.7%	3.8%
Taiwan	4	5.5%	17	2.2%	3.2%
Iran	5	5.3%	18	1.5%	3.7%
China	6	5.1%	9	3.1%	2.0%
Vietnam	7	5.0%	13	2.5%	2.5%
Peru	8	4.5%	12	2.6%	1.9%
United States	9	4.3%	5	4.2%	0.1%
Italy	10	3.2%	20	1.5%	1.8%

Source :http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_appendices_v19_221284438.en-us.pdf P:9 Consulté le: [10/05/2014].