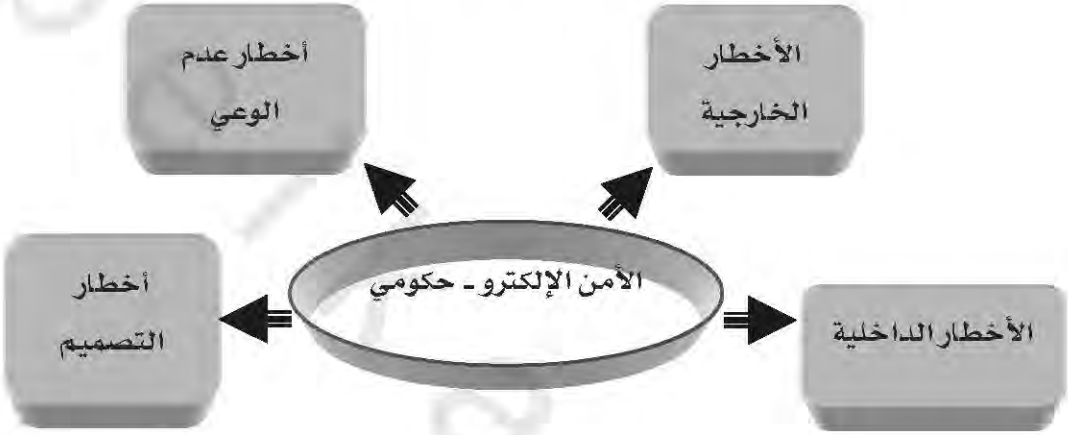
الفصل الثالث عشر

****

أدوات الأمن المعلوماتي
في الحكومة الإلكترونية

قبل أن نحاول طرح أدوات الأمن المعلوماتي في الحكومة الإلكترونية[31] يتوجب علينا تحليل المخاطر التي قد تنجم من جراء عدم الاهتمام بموضوع أمن وسرية المعلومات ويشمل تحليل المخاطر جوانب عديدة منها: الواقع والنوايا ومصادر الخطر بالإضافة إلى وسائل الهجوم الإلكتروني وكيفية تجنبها باعتماد إجراءات الوقاية والدفاع الإلكتروني وما ينتج عنه من كلفة اقتصادية إضافية، ومن المهم أن لا نغفل عن تحديد أصول الحكومة الإلكترونية التي تحتاج إلى جهاز حماية فعّال.



شكل(١) المخاطر المحيطة بالأمن الإلكترو - حكومي

- مصادر الخطر المحتملة:

تعمل أجهزة الحكومة الإلكترونية في فضاء مفتوح يتداخل فيه جمهورها الخارجي (مواطنون، مؤسسات، حكومات أخرى) مع جمهورها الداخلي(وزراء، موظفين..) وتصبح فيه أجهزة تلك الحكومة عرضة للعديد من أنواع الهجوم تحت دوافع مختلفة، ومن الممكن أن تتم مهاجمة أنظمة الحكومة الإلكترونية من داخلها وعبر أحد الموظفين الغاضبين أو من الخارج عبر مجموعات الهاكرز أو

31- عباس بدران، الحكومة الإلكترونية، مرجع سبق ذكره، ص١٩٩ وما بعدها..

أجهزة الاستخبارات في بلدان عدوة وصولاً إلى المؤسسات التجارية الساعية إلى الحصول على معلومات تجارية تنافسية.

- خطر المستخدم الشرعي:

المستخدم الشرعي هو المواطن أو صاحب المؤسسة الحاصل على إجازة من الحكومة في سبيل استعمال خدماتها الإلكترونية، وتكون الإجازة في معظم الأحوال عبارة عن تأكيد هوية المستخدم إلكترونياً عبر شبكة الحكومة بعد أن يكون قد تم تسجيله سابقاً، وقد يحاول هذا المستخدم أن يوظف إمكانية دخوله إلى شبكة الحكومة من أجل تخريب الخدمات المتاحة في نطاق إجازته، وقد يحصل في بعض الأحيان يتمكن هذا المستخدم من الحصول على معلومات لا تخصه في حال وجود عيوب فنية في تصميم الخدمة الإلكترونية المتاحة له. من ناحية أخرى، من الممكن لهذا المستخدم أن ينكر قيامه بخدمات معينة في حين تؤكد أنظمة الحكومة قيامه بها.

- خطر موظفي الحكومة الإلكترونية:

وتشكل هذه المجموعة خطراً كبيراً على أنظمة الحكومة في حال أرادت ذلك، ونظراً لما يملكه بعض الموظفين في الحكومة الإلكترونية من حقوق دخول إلى الشبكة واطلاع على الأنظمة فمن الممكن لهم أن يقوموا بأعمال تخريبية تؤدي إلى إيقاف الخدمة الإلكترونية وقد يكون هؤلاء الأشخاص مدفوعين بدوافع مادية أو نفسية أو لمجرد عدم الرضا عن وضعهم الوظيفي داخل الحكومة.

- خطر أجهزة المخابرات الخارجية:

من الممكن أن تعتمد أجهزة المخابرات الصديقة أو العدوة على حد سواء على الحصول على معلومات عن أشخاص أو مؤسسات أو حتى أجندات الحكومة الداخلية عبر تنفيذ هجمات إلكترونية بهدف اختراق النظام الأمني المعلوماتي للحكومة والدخول إلى مختلف الأنظمة فيها وقد توظف أجهزة المخابرات في هذه

العملية كفاءات تقنية عالية وقادرة في كثير من الأحيان على اختراق أنظمة الحكومة الهدف.

- خطر المؤسسات التجارية:

تسعى المؤسسات التجارية دوماً إلى تحقيق السبق الاقتصادي والإعلامي والتجاري على منافساتها من المؤسسات وقد تحاول هذه المؤسسات أن تخترق أنظمة الحكومة الإلكترونية من أجل الحصول على معلومات عن منافسيها في السوق وقد تلعب أقسام المخابرات التجارية (Business Intelligence Departments) في المؤسسات الكبيرة دوراً خطيراً في هذا المجال وذلك في محاولة منها لإرضاء الإدارة العليا عبر معلومات تجارية تنافسية تملكها الحكومة ولم يتم نشرها.

- خطر المنظمات الإرهابية:

قد تحاول بعض المنظمات الإرهابية فرض أجنداتها السياسية على الحكومة عبر وسائل إرهابية عدة ومنها الحرب الإلكترونية، وربما تسعى إلى تعطيل خدمات الحكومة الإلكترونية بعد الحصول على مبتغاها منها من خلال هجوم إلكتروني مكثف قد يحدث في فترة زمنية قصيرة نسبياً، ويكمن خطر المنظمات الإرهابية في هذا المجال بكونها تتحرك من منطلقات تدميرية تكون فيها مصلحة البلاد العليا نقطة هامشية أمام تحقيق أهدافها.

- خطر مزودي البرمجيات والعتاد:

يمتلك مزودو البرمجيات القدرة على التلاعب بالشفرة البرمجية بحيث يتركون وراءهم أبواباً مفتوحة للأنظمة (Door Back) مما يمكنهم لاحقاً من الدخول إلى تلك الأنظمة بطريقة غير شرعية وتجاوز بوابات الأمن المتاحة للجمهور، وعلى حد سواء يستطيع مزودو العتاد أن يتركوا عيوباً في أجهزة الكمبيوتر والشبكات وغيرها عن قصد بحيث يسهل عليهم تجاوز الإجراءات الأمنية الإلكترونية للحكومة.

- خطر الكوارث الطبيعية:

كما تؤثر الكوارث الطبيعية من زلازل وهزات أرضية وصواعق في الحركة العامة لأجهزة الحكومة ومستوى توافر خدماتها، فقد تلحق تلك الكوارث أضراراً كبيرة بأنظمة الحكومة الإلكترونية وقد تؤدي في بعض الأحيان إلى شل الخدمات الإلكترونية للحكومة في حال أصابت مواقع تشغيل تلك الخدمات.

- خطر عيوب التصميم والتشغيل:

وتشمل عيوب التصميم والتشغيل في مختلف مكونات الحكومة الإلكترونية من الشبكات وطريقة تصميمها إلى البرمجيات المستخدمة وخوارزميات التشفير ومستوياتها وصولاً إلى أساليب وطرق التثبيت كالهوية الإلكترونية، وتقاس قوة جدار الأمن الإلكتروني الواقي بقوة الحلقة الأضعف في هذه المكونات بحيث يؤدي كسر تلك الحلقة الضعيفة إلى اختراق الجدار مهما كانت قوة مكوناته الأخرى. إن طريقة تصميم البنية التحتية لخدمات الحكومة الإلكترونية من الممكن أن يشكّل فارقاً مهماً في مستويات الأمن والسرية لتلك الخدمات، كما تعتمد الخدمات الإلكترونية على مبدأ " التوافر"(Availability) الذي يقول بضرورة توفر الخدمة من خلال بدائل شبيهة في حال تم تدمير الخدمة الأصلية وفي حال لم يؤخذ هذا المبدأ بعين الاعتبار عند تصميم الخدمة فسوف تكون عرضة للانقطاع لاحقاً.

- خطر التناثرية الأمنية:

في كثير من البلدان التي لا تملك مخططاً توجيهياً عاماً (E-Government Master Plan) لتطبيقات الحكومة الإلكترونية على مستوى كافة الإدارات الرسمية والوزارات، تعمد إدارات تلك البلدان إلى تطبيق مفهومها الخاص بالأمن والسرية الإلكترونية بدون الأخذ بعين الاعتبار أية معايير أو مقاييس تضمن كفاءة وفعالية تطبيقاتها، ويؤدي هذا الأمر بالتالي إلى نوع من تناثر وتنوع تطبيق مفاهيم الأمن والسرية عبر الإدارات وقد يشكل ضعف تطبيق إدارة أو وزارة واحدة

لمبدأ الحماية والأمن الحلقة الضعيفة في الجدار الواقي مما ينتج بالنهاية اختراق هذا الجدار.

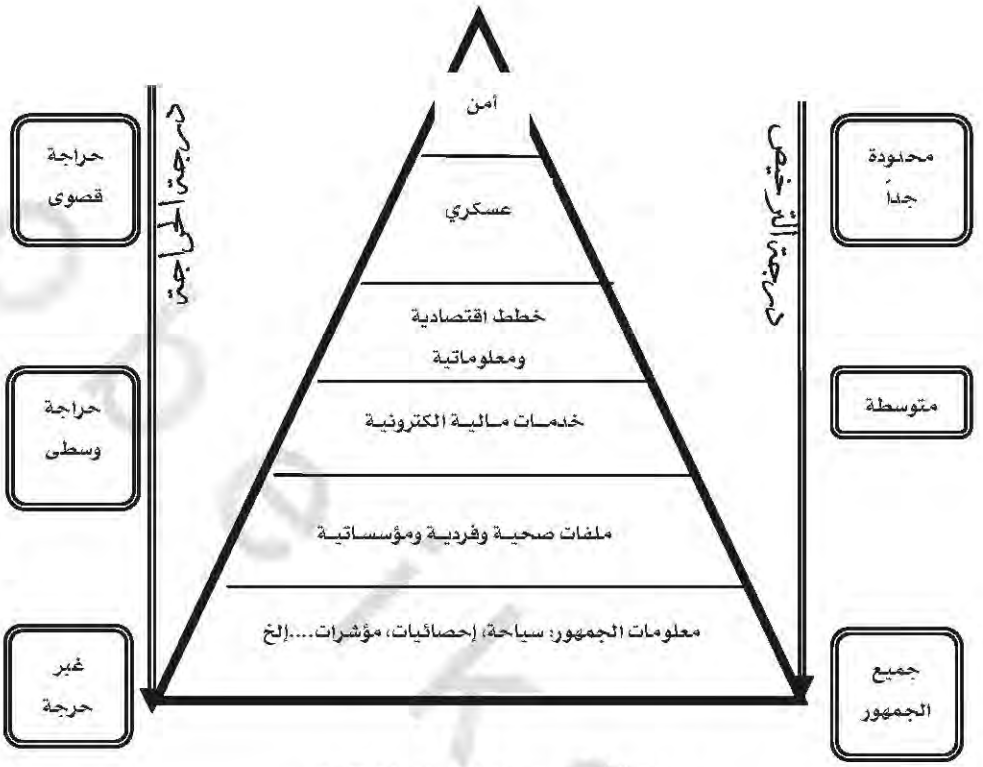
- خطر عدم الوعي بالمخاطر:

يمثل عدم وعي مدراء القمة وموظفيهم في الحكومة الإلكترونية بالمخاطر المذكورة أعلاه الخطر الأعظم على النموذج الإلكترو ـ حكومي فالذي لا يعي المخاطر لا يمكن أن يضع خطط الدفاع والطوارئ.

لا يمكن لأي مشروع حكومة إلكترونية أن يزدهر وينجح بدون معالجة الأخطار المطروحة والجوانب المحيطة بها، وربما من الأفضل للحكومة البقاء في فضائها المادي/الواقعي وعدم الشروع بدخول الفضاء الإلكترو ـ حكومي في حال لم تتسلح بأدوات الدفاع الإلكتروني المناسبة.

□ الأصول الحكومية المعلوماتية الحرجة:

تشتمل أنظمة الحكومة الإلكترونية على كميات ضخمة من المعلومات منها ما هو العام والمتاح للجمهور ومنها ما هو الخاص بالحكومة وحدها، ومنها ما هو خاص بالمواطن الواحد أو المؤسسة الواحدة، تتدرج الحراجة الأمنية لتلك المعلومات عبر مستويات عدة تبدأ بمستوى "دون الحرج" إلى مستوى "الحراجة القصوى" وينبغي اتخاذ التدابير الاحترازية حسب مستويات الحراجة وعدم المبالغة في حماية الأصول العامة الخاصة بالجمهور وبالتالي فقدان الشفافية الحكومية وعدم الاستهتار بالأصول الحرجة وتعريض أمن البلاد الإلكتروني للخطر، وفيما يلي هرم حراجة المعلومات في الحكومة الإلكترونية:



صورة (٢) هرم حراجة المعلومات الحكومية

ونستطيع أن نسرد بعض الأصول المعلوماتية الحرجة فيما يلي:

- خطط الدولة وملفاتها الأمنية والمخابراتية.
- تشكيلات الدولة العسكرية وكيفية تسليح جيشها.
- الملفات القضائية والجنائية.
- أجندات الحكومة السياسية ومخابر اجتماعاتها.
- ملفات المواطنين الصحية، القضائية، الأمنية، .....، الخ.
- ملفات المؤسسات التجارية وبياناتها المالية والاقتصادية.
- قواعد بيانات الهوية الرقمية وكلمات السر وأذونات الدخول.
- قواعد البيانات المالية والاقتصادية.

من الواضح أن الحكومة الإلكترونية يجب أن توازن بين درجة حراجة المعلومات وكلفة تشغيل أنظمة حماية متطورة، فمن غير الضروري على سبيل المثال اعتماد نفس المعايير الأمنية لحماية ملفات مخابراتية في فخ الهستيريا الأمنية المعلوماتية بحيث ينسفون مبدأ الشفافية الحكومية كما ذكرنا سابقاً، وعلى هذا الأساس، من الممكن أن يتم تصنيف وتجميع كافة البيانات والمعلومات والإجراءات الإلكترو ـ حكومية ضمن طبقات الهرم السابق واعتماد معايير مقبولة من كافة الأطراف.

□ تقنيات الهجوم المحتملة:

من الممكن أن يتم الهجوم على خدمات ومعلومات الحكومة الإلكترونية من قبل مصادر الخطر المذكورة سابقاً وبوسائل وتقنيات متعددة، وكلما تطورت وسائل الدفاع تطورت معها وسائل الهجوم وهذا ما يحتم على مدراء الحكومة الإلكترونية اعتماد وسائل حماية ديناميكية للأمن المعلوماتي تتطور بتطور الظروف المحيطة ومن التقنيات المحتملة للهجوم الإلكتروني:

□ التنصت على المعلومات:

تطورت تقنيات التنصت على المعلومات مع تطور وسائل نقل المعلومات وكلما ظهرت وسيلة جديدة لنقل المعلومات من طرف إلى آخر ظهرت معها وسيلة للتنصت على هذه المعلومات خلال طريقها من المصدر إلى الهدف وعلى سبيل المثال يمكن التنصت على مكالمات الهاتف والفاكس وأخيراً وليس آخراً شبكات المعلومات ومنها الإنترنت. إذ يستطيع المهاجمون أن يتنصتوا على سيل المعلومات المتدفق بين المواطن والحكومة أو مؤسسات الأعمال والحكومة وحتى بين إدارات الحكومة فيما بينها، ومن الممكن الحصول على معلومات أمنية وخصوصية جداً في حال لم يتم تشفيرها على الطريق بين المستقبل والمرسل، وإذا حصل المهاجمون على معلومات الدخول إلى أنظمة الحكومة الإلكترونية من خلال هذه الطريقة فإن تلك الأنظمة وبياناتها سوف تكون تحت رحمة أولئك الأشخاص.

□ نشر الفيروسات الإلكترونية :

الفيروسات الإلكترونية هي عبارة عن برامج صغيرة تستطيع أن تنقل نفسها من جهاز إلى آخر وعبر شبكات الكمبيوتر ومن ضمنها شبكة الإنترنت، وعادة ما تكون هذه البرامج الميكروية غير مرئية للمستخدم العادي وتحتاج إلى شخص خبير لتحليلها ومعرفة الأضرار التي تنتج عنها، ولتبيان مخاطر الفيروسات الإلكترونية يكفي أن نذكر بعض الأمثلة مما حصل في السنوات الأخيرة الماضية على هذا الصعيد، ففي أيار من عام ٢٠٠٠ ظهر فيروس "أنا أحبّك" (I love you) واستطاع أن يصيب ملايين أجهزة الكمبيوتر حول العالم بالضرر وقد قدرت الأوساط العالمية الخسائر الناتجة عن هذا الفيروس بملايين الدولارات. من ناحية أخرى، قد تلعب هذه الفيروسات دور "حصان طروادة" في أنظمة الحكومة الإلكترونية فمن الممكن أن تتخذ مكاناً لها داخل تلك الأنظمة وتبدأ بالتقاط المعلومات الداخلية وبثها إلى جهات معينة خارجية ومن الممكن في مرحلة لاحقة أن تحدث الضرر الفادح بالأنظمة المعلوماتية في الحكومة الإلكترونية.

كما تأتي هذه الفيروسات بنكهات مختلفة فمنها ما هو الخبيث ويحدث إرباكاً في سعة الشبكة Network Bandwidth وتسمى بالدودة الإلكترونية مثل NIMDA التي تسببت بأعطال كبيرة وخسائر مادية قاربت الخمسمائة مليون دولار حول العالم ،ومنها من يغير شكله عبر إضافات عشوائية على جسمه بحيث يصعب تعقبه ومنها ما يقال عنه الفيروسات الحميدة والتي تهدف إلى تنفيذ أعمال مفيدة.

- **مهاجمة الواجهة : شلّ خوادم الويب**

تعتبر خوادم الويب (Web Servers) الواجهة الرئيسية المفتوحة في الحكومة الإلكترونية ويأتي قبلها تقنيات الحماية عبر إنشاء جدار النار(Firewall) وما شابه ، ونظراً لوجود هذه الخوادم في المقدمة فإنه من البديهي أن يتم الهجوم عليها في المقام الأول وتعتمد تقنية الهجوم في هذه الحالة على إرسال بيانات كبيرة الحجم ، عشوائية وغير مترابطة إلى تلك الخوادم التي سوف تحاول معالجتها بدون

فائدة ونظراً لمواصلة الهجوم في نفس الفترة فقد تصل تلك الخوادم إلى مرحلة لن تستطيع فيها مواردها الفيزيائية (ذاكرة وسعة الشبكة) من تحمل المزيد وبالتالي تتوقف الخدمة الإلكترونية وتصاب خوادم الويب في تلك الحالة بالشلل التام مما يستدعي إيقافها ثم إعادة تشغيلها.

- **توليد كلمات السر و أذونات الدخول :**

يعتمد هذا النوع من الهجوم على إمكانية توليد كلمات السر أوتوماتيكياً عبر برامج خاصة تأخذ على عاتقها مسؤولية تجربة كلمات سر عشوائية وبطريقة مكثفة جداً من أجل الحصول على كلمة السر الحقيقية الخاصة بالمستخدم وفي أغلب الأحيان تعتمد هذه البرامج على كلمات مفتاحية وقد يكون استخدامها شائعاً بين الناس بحيث تبدأ بتجربة الكلمات المتداولة ومن ثم تنتقل إلى العشوائية المطلقة في انتقاء الحروف والرموز من أجل تركيب كلمات سر من المحتمل أن يطابق إحداها الكلمات الحقيقية، وعموماً يحتاج هذا النوع من الهجوم إلى فترة زمنية طويلة في حال كانت كلمات السر الأصلية طويلة ومعقدة.

- **تقنية الاعتراض والتغيير:**

ويكون هذا الهجوم ذا طابع غير تدميري بقدر ما يحمل طابع التلاعب بالمعلومات لصالح الجهة التي تقوم بهذا الهجوم، وفي هذا السيناريو يتخذ المهاجمون موقعاً لهم بين الحكومة الإلكترونية والمواطن أو صاحب العمل بحيث يعترضون المعلومات المرسلة ويبدلونها ثم يرسلونها إلى الطرف الهدف.ولتبيان مدى خطورة هذه التقنية، نأخذ مثالاً وهو الانتخابات الإلكترونية حيث يقوم المواطن بالاقتراع عبر شبكة الإنترنت فمن الممكن أن يعترضه المهاجمون ويقومون بسرقة صوته وتجييره لصالح أطراف أخرى عبر تغيير البيانات قبل أن تصل إلى الحكومة الإلكترونية.

- **استخدام الوسائل الإشعاعية:**

تعتبر التقنيات الإشعاعية من الوسائل المتقدمة في مجال الهجوم على الأدوات الإلكترونية ومنها أنظمة وأجهزة الحكومة الإلكترونية، وتمثل الومضات الكهرومغناطيسية (Bomb, Pulse Weapon Electromagnetic) خطراً كبيراً على رقائق السيليكون الخاصة بتلك الأجهزة وفي حال تمكن المهاجمون من الحصول على تلك الوسائل وتوجيهها بطريقة أو بأخرى إلى أجهزة الحكومة الإلكترونية فمن الممكن أن تذوب مكونات تلك الأجهزة تحت تأثير الإشعاع كما يذوب الثلج تحت أشعة الشمس. من وجهة نظر الحكومة، فإن الجانب الإيجابي في هذا النوع من الهجوم هو أن الحصول على معداته وأدواته ليس بالأمر السهل ولكنه ليس بالمستحيل، والجانب السلبي يكمن في إمكانية نقل تلك الأدوات عبر سيارات أو شاحنات صغيرة وركنها قرب مباني الحكومة الإلكترونية وتشغيلها لكي تقوم بعملها التدميري في نطاق تأثيرها.

- **انتحال الشخصية الإلكترونية:**

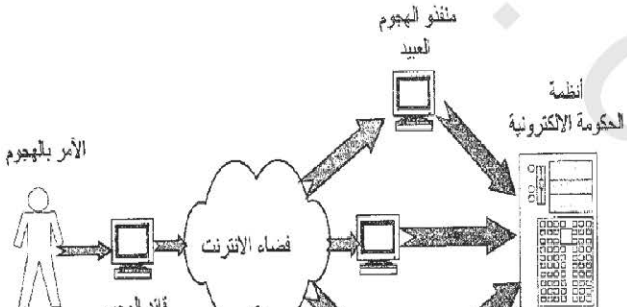
يتشكل جمهور الحكومة الإلكترونية من مختلف طبقات المجتمع وفيهم من يكون عالماً بخفايا التكنولوجيا وآخرون تقتصر معرفتهم على كيفية الاستفادة من خدمات الحكومة عبر الإنترنت من خلال الدخول إلى مواقع تلك الخدمات وطباعة كلمة الدخول ومن بعدها القيام بملء الاستمارات الإلكترونية الخاصة بالخدمة التي ينوي استخدامها. يعتمد المهاجم الإلكتروني في بعض الحالات على انتحال شخصية الحكومة الإلكترونية عبر إنشاء مواقع شبيهة جداً بمواقع خدمات الحكومية الإلكترونية والإيهام للمواطنين بأنها مواقع حكومية حقيقية وبعد أن ينتهي من نصب الفخ الإلكتروني للمواطن يبقى على المهاجم أن يجلب المواطنين إلى ذلك الفخ عبر وسائل عدة ومنها على سبيل المثال إرسال رسائل بريد إلكتروني إلى مجموعات من المواطنين تسألهم فيها أن يقوموا بالتصويت أو إبداء آرائهم أو أية عملية تحتاج إلى اسم دخول وكلمة سر وتوفر لهم تلك الرسائل الرابط الإلكتروني للمواقع المزيفة وحين يدخل المواطن إلى تلك المواقع يكون قد

وقع في الفخ من دون أن يدري وتصبح معلوماته وخصوصياته مكشوفة للمهاجمين الإلكترونيين.

- **هجوم السيد/العبيد:**

ويقوم هذا النوع من الهجوم الإلكتروني على مبدأ توزيع الأدوار بين البرنامج قائد الهجوم (MasterAttacker) والبرامج المنفذة للهجوم (SlaveAttackers)، ويقوم الشخص الآمر بالهجوم بإعداد برنامج رئيسي يرسل إشارة الهجوم لبرامج فرعية موجودة على العديد من الأنظمة المربوطة بالإنترنت بحيث يظهر لوحدات الأمن الإلكتروني في الدولة بأن الهجوم صادر من نقاط تواجد الأنظمة الفرعية في حين أن الهجوم الإلكتروني الفعلي يكون قد تم عبر البرنامج الرئيس وبإشارة من الشخص المسؤول ولسوء الحظ لن تتمكن أجهزة الأمن الإلكتروني من تعقب المهاجم الفعلي الذي يكون قد قام بعملية تضليل إلكترونية توقع الحكومة الإلكترونية في فخ اتهام أشخاص غير معنيين كلياً بالهجوم بل كانوا أيضاً جزءاً من الضحية.

وعلى سبيل المثال فقد يعتمد إرهابيو المعلومات على زرع أنظمة الهجوم الفرعية (العبيد) في مقاهي الإنترنت في الدولة ويقومون بإيقاظها من أمكنة جغرافية متباعدة كلياً وحين يتم تعقب مصادر الهجوم فسوف تصل أجهزة الأمن إلى تلك المقاهي وتنقطع الحلقة تماماً.



- **الاستفادة من ثغرات الأنظمة:**

عادةً ما يقوم مرتكبو الهجوم الإلكتروني بعملية مسح شامل للأنظمة المعروفة والمستخدمة من أجل معرفة نقاط ضعفها الأمنية، وفي الوقت الذي ينشر فيه مزودو البرامج وأنظمة التشغيل معلومات تفصيلية عن تلك الثغرات الأمنية في منتجاتهم من أجل تمكين عملائهم من اتخاذ التدابير الاحترازية يغتنم المهاجمون الإلكترونيون الفرصة بشكل موازٍ من أجل اختراق الأنظمة قبل أن يتم سد ثغراتها الأمنية.

- **تجنيد الأشخاص:**

يعتبر تجنيد الأشخاص أو العمالة المزدوجة من أحد مشاكل الأمن المادي الفعلي وقد كان معروفاً منذ بدء البشرية فقد كانت الأمم تعتمد على عناصر بشرية داخلية في صفوف أعدائها من أجل معرفة خطط وأسرار أولئك الأعداء. وتكمن خطورة هذا الموقف بالنسبة للحكومة الإلكترونية بأن مرتكبي الهجوم الإلكتروني الخارجي قد يحصلون على معلومات حساسة وحرجة جداً عن تركيبات الأنظمة الحكومية وكيفية تجاوز بوابات السرية والأمان من قبل أشخاص داخليين مدفوعين بانتماءات غير وطنية أو من أجل الحصول على المال وأسباب عديدة غيرها. وفي حالة هذا الهجوم فإن أقوى برامج الشيفرة والسرية وجدران الحماية الخارجية سوف تفقد مفعولها كلياً فالعدو الإلكتروني سوف يظهر لتلك الأنظمة بأنه صديق موثوق وتسمح له بالدخول حيث يعيث فساداً وتخريباً ويقوم بسرقة المعلومات الحرجة.

ويجب أن تكون الحكومة الإلكترونية حذرة جداً من مغبة الوقوع في هذا الفخ لأن المهاجمين قد يستفيدوا من سرقة المعلومات لفترات طويلة من الزمن وبدون أن يتركوا آثاراً تبعث الريبة والشك قبل أن يقرروا تحطيم الأنظمة وإتلاف معلوماتها.

□ الهجوم المادي على الحكومة الإلكترونية:

من المحتمل أن تقوم الجهات العدوة بعمليات هجوم حربية تقليدية على منشآت الحكومة الإلكترونية من أجل تدمير بنيتها المعلوماتية وبالتالي شلّ قدرتها على اتخاذ القرارات الصائبة المطلوبة في الأزمنة الحرجة والتي ترتكز بشكل أساسي على معلومات وبيانات مخزونة في أنظمة تلك الحكومة، وقد تلجأ الجهات العدوة إلى هذا الخيار في حال استنفذت الخيارات التقنية الأخرى أو في حال لم تمتلك الجهات القدرة التقنية والخبرات الهجومية الإلكترونية أصلاً. وقد يشمل هذا الهجوم الاعتداء على شبكات الاتصال ومكاتب الحكومة الإلكترونية ومراكز تواجد الخوادم المركزية(Hosting Locations) وصولاً إلى الاعتداء على الأشخاص المولجين بمسؤولية الأمن والسرية في تلك الحكومة.

لقد حاولنا مما تقدم تسليط الضوء على بعض تقنيات وأدوات الهجوم على الحكومة الإلكترونية ومحاولة تحطيم أمن البلاد الإلكتروني ومن المهم أن نعرف أن المهاجمين المحتملين يعملون على تطوير أدواتهم ووسائلهم التخريبية بشكل دائم ولا يتوقفون عند حدود ما تم ذكره.

□ استراتيجيات الدفاع والوقاية:

يقوم أحد مبادئ الدفاع العسكري على نظرية مفادها أن أفضل طريقة للدفاع هي الهجوم، وقد ينطبق هذا المبدأ على الدفاع الإلكتروني لولا أنه في غالب الأحيان يصعب تحديد مكان العدو الإلكتروني في زمن الهجوم الفعلي، ولو قدر للحكومة تحديد المكان فمن الممكن أن تعمد إلى إجراءات أمنية للقبض على مهاجمي الشبكة إن كانوا تحت سيطرتها الأمنية، وإن كانوا في دول أخرى فمن الممكن أن تدخل الحكومة في اتفاقات أمنية إلكترونية مع حلفائها من الدول الخارجية بحيث تطلب من حكومات تلك الدول تعقب المهاجمين المفترضين من أراضيها، هذا النوع من الدفاع هو ما يسمى بـ (الهجوم المضاد المادي) والذي يعتمد على عناصر الأمن والمخابرات وضرورة توفر المعلومات عن أمكنة وتواجد المهاجمين وتكون المعادلة هنا: ((هجوم إلكتروني<- > دفاع مادي بشري))

وعلى صعيد آخر، قد تلجأ وحدة الأمن الإلكتروني في الحكومة (في حال كانت موجودة في تشكيلات الأمن في الدولة) إلى البدء بعملية ((هجوم إلكتروني مضاد)) يهدف إلى شلّ أجهزة وأنظمة العدو وبالتالي قدرته الآنية على مواصلة الهجوم لحين رفع درجة الإجراءات الأمنية الإلكترونية كإقفال الشبكة لفترة معينة والتحقق من الخسائر المحتملة والمعادلة تكون هنا : ((هجوم إلكتروني <- > دفاع / هجوم مضاد إلكتروني))

يتبين لنا من خلال ما تقدم أن عمليات الهجوم والدفاع الإلكتروني هي من العمليات المعقدة والتي تتطلب جهوزية تامة في لحظة وقوع الهجوم الإلكتروني بالإضافة إلى كفاءات تقنية عالية على الأرجح أن لا تكون متوفرة لدى الحكومة وبناءً عليه يبقى على الحكومة الإلكترونية أن تتخذ كافة إجراءات الوقاية للحيلولة دون اختراق أنظمتها وتدمير خدماتها ونذكر من وسائل واستراتيجيات الوقاية :

□ نشر الوعي الأمني المعلوماتي :

لا يمكن تجنب الأخطار المذكورة واعتماد سياسات دفاع إلكترونية من دون وعي كامل وشامل لهذا الموضوع الخطير، وإذا لم يستطع رأس الهرم من رجالات الدولة ومدراء القمة في الحكومة الإلكترونية أن يستوعبوا تلك الحقيقة فمن غير الممكن لمن دونهم من الموظفين أن يأخذوها على محمل الجد ويعطوها الاهتمام الكافي لدرء مخاطرها وبناءً عليه من المهم، بل من الضروري، أن تقوم الحكومة الإلكترونية بحملة توعية عامة حول أمن البلاد الإلكتروني تشمل رأس الدول وصولاً إلى موظفيها وجمهور المواطنين وتشرح لهم المخاطر الأمنية الإلكترونية وكيفية تفاديها وما هي الإجراءات التي قامت بها الحكومة في هذا المجال ومن الممكن إصدار نشرة إعلامية (مجلة – جريدة – تلفزيون، .....) شهرية خاصة بهذا الموضوع.

□ الاستراتيجيات التنظيمية والهيكلية:

بما أن موضوع الأمن الإلكتروني سوف يمس أمن البلاد بشكل عام، فمن المهم أن تقوم الحكومة بإجراءات وقائية تتناسب مع ذلك الموضوع ومنها ما هو على المستوى التنظيمي والهيكلي، إذ لا يجوز إعطاء مسؤولية الأمن الإلكتروني لمجموعة من الأشخاص داخل الدولة كجزء إضافي من مهامهم ولا بد من إنشاء تشكيلات خاصة بالأمن الإلكتروني قد تكون تابعة لأجهزة الدولة الأمنية بحيث يكون تطوير الأمن الإلكتروني ورسم سياسات الدفاع والهجوم الإلكتروني في صلب مهامها وقد نذكر على سبيل المثال وحدة الأمن الإلكتروني ووحدة الرقابة الأمنية الإلكترونية التي سوف تتأكد من أن جميع إدارات الدولة تقوم بتنفيذ إجراءات الوقاية الأمنية المقررة والمرسومة من قبل الدولة.

□ تطوير الاتفاقات الأمنية الخارجية:

لا يوجد دولة في العالم لا تملك اتفاقات أمنية ثنائية أو جماعية مع الدول الخارجية، ومن المفيد أن يتم تطوير تلك الاتفاقات الأمنية لكي تشمل قضايا ومواضيع الأمن الإلكتروني وأوجه التعاون المحتملة، وعلى سبيل المثال قد تتعاون الحكومة مع حكومات خارجية لمنع الاعتداء الإلكتروني الصادر من أراضي تلك الدول وعبر شبكاتها وفي المقابل من الممكن أن يتم تبادل الخبرات الأمنية الإلكترونية مع تلك الحكومات.

- إستراتيجية الترغيب والترهيب:

ويشمل الترغيب هنا على عدة نقاط ومنها تشجيع المواطنين على الإبلاغ عن محاولات الاعتداء الإلكتروني بدون أن يتم الكشف عن المخبرين ويمكن للدولة أن تعمد إلى تخصيص خط هاتف ساخن(Hotline) من أجل استقبال ملاحظات المواطنين في هذا المجال،من جهة أخرى، ينبغي على الحكومة أن تضع العقوبات الرادعة لمرتكبي الجرائم الإلكترونية بحيث تقوم بإرهابهم قبل أن يفكروا

بمحاولة الاعتداء إلكترونياً عليها، وفي هذا المجال سيأتي الدور الحيوي للهيئات التشريعية في الدولة من أجل سن القوانين الرادعة المناسبة.

اعتماد مفاتيح التشفير:

تعتمد تكنولوجيا التشفير الحديثة على النظرية التالية :تمتلك كل جهة أو فرد مفتاحين لتشفير وفك تشفير البيانات، المفتاح الأول وهو المفتاح الخاص ويكون فقط بحوزة الجهة المخولة، والمفتاح الثاني وهو المفتاح العام ويتم نشره على الإنترنت أو على شبكة الحكومة الإلكترونية من أجل استخدامه من قبل الجهات الأخرى لتشفير الملفات والمعلومات المراد إيصالها إلى الطرف الآخر. وعلى سبيل المثال: من أجل تشفير المعلومات المرسلة من قبل المواطن إلى دائرة الآليات بغية تسجيل سيارته، فإن المواطن يستخدم المفتاح العام الخاص بدائرة الآليات لتشفير المعلومات قبل إرسالها وتستخدم الدائرة مفتاحها الخاص لفك تشفير المعلومات بعد استقبالها، وتدعم هذه التقنية مستويات تشفير عالية تصل إلى ١٢٨ بت (١٢٨ bits) وهو ما أثبت فعاليته ضد محاولات الكسر.

وباستخدام نفس التقنية، سوف يصبح الإمضاء الإلكتروني حقيقة تقنية واقعية، ولكن سوف تحتاج الدوائر وأجهزة الدولة إلى آلية لإصدار وإدارة المفاتيح العامة والخاصة وهذا ما اتفق الجميع على تسميته :"البنية التحتية للمفاتيح العامة Public Key Infrastructure "

الهوية الإلكترونية الموحدة:

موضوع الهوية الإلكترونية ووسائلها من المواضيع الجديدة على ساحة النقاش الإلكتروني الحكومي وهو لم يصل إلى مرحلة النضج الكامل بالرغم من ادعاءات الكثير من مزودي البرامج بوجود حلول مناسبة، ومجمل القصة هي أن الحكومة المادية قادرة على التعرف على مواطنيها من خلال جواز السفر أو الهوية الورقية ولكن كيف ستتمكن الحكومة الإلكترونية من التعرف إلى مواطنيها؟

ببساطة يجب أن تكون هناك هوية رقمية أو إلكترونية قادرة على التعريف بالأشخاص وغير قابلة للنقل من شخص إلى آخر وأمينة وموثوقة.

وتدرس بعض الحكومات إمكانية استخدام مكونات مادية (أجهزة صغيرة) وليس فقط مكونات منطقية (برامج) لمعالجة كل الجوانب المحيطة بالهوية الإلكترونية.

تقنية الترخيص الإلكتروني:

سوف تخدمنا الهوية الإلكترونية للتعريف عن أنفسنا لدى الحكومة الإلكترونية وبالتالي الولوج داخل الحدود الإلكترونية للبلاد ولكن هذا لا يعني أننا سوف نصبح في مقام يسمح لنا بتنفيذ وطلب جميع الخدمات الإلكترونية، فبعض الخدمات سوف تكون مقصورة على الرؤساء وغيرها خاص بالمؤسسات وأخرى خاصة بالأفراد وهكذا وباختلاف الناس ومقاماتهم سوف تختلف درجات الترخيص ونطاقها وعلى سبيل المثال يمكن للحكومة أن تعطي تراخيص البحث عن معلومات تجارية لأصحاب المؤسسات المسجلة لدى الدولة والتي تدفع الضرائب بشكل منتظم ويمكن إصدار الترخيص الإلكتروني الخاص باستخدام أجهزة الأمن والعسكر للأفراد المولجين بهذه المهام.

من ناحية أخرى، فإن تقنية الترخيص الإلكتروني قد تستخدم للمحافظة على خصوصية معلومات المواطن والمؤسسات فمن غير الضروري للشخص الحاصل على رخصة إلكترونية لإجراء خدمة معينة أن يكشف كافة معلوماته الشخصية الموجودة في الهوية فقد يحتاج إلى تقديم معلومات الرخصة والتي عادة ما تحتوي على أدنى حد مقبول من المعلومات.

تشفير المعلومات المنقولة والمحفوظة :

لا يمكن غض النظر عن أمن وسرية المعلومات التي تنتقل من طرف إلى آخر عبر شبكة الإنترنت وتركها عرضة لعيون المتنصتين، ومن الواجب اعتماد تقنيات تشفير عالية بحيث تظهر تلك المعلومات بصورة مبهمة تماماً لكل من يحاول

التنصت عليها عبر الشبكة السلكية أو اللاسلكية وأحد التقنيات المستخدمة في هذا المجال هي تقنية "SSL" المتوفرة عالمياً وفي معظم البرامج والأنظمة الإلكترونية، وينبغي اتخاذ نفس الإجراءات بالنسبة للمعلومات الحساسة المحفوظة في الأجهزة بحيث يتم حفظها وهي مشفرة.

تسجيل الأثر الإلكتروني:

تحتاج الرقابة الإلكترونية اللاحقة إلى معلومات تستند إليها لمعرفة من فعل وماذا ومتى من أجل التدقيق في الأعمال المريبة ومساءلة الأشخاص المسؤولين عنها، لذلك يكون من الضروري أن تعمد الحكومة الإلكترونية إلى إنشاء خدمات لتسجيل الأثر الإلكتروني لطالب الخدمة وعلى سبيل المثال يمكن تسجيل معلومات عن اسم المستخدم وتاريخ طلب الخدمة ووقتها وعنوانه على الشبكة والبلد الذي طلب منه الخدمة بالإضافة إلى عدد محاولاته للدخول إلى الشبكة وستكون جميع هذه المعلومات بخدمة قسم الرقابة الإلكترونية لاحقاً.

كلمات مرور معقدة وديناميكية:

لقد تكلمنا سابقاً عن إمكانية توليد كلمات السر إلكترونياً وما هي التقنيات المستخدمة لذلك، ومن أجل تفادي هذا الأمر من الضروري أن تكون كلمات السر تطابق الحد الأدنى لمواصفات الأمن والسرية وطويلة كفاية، ولا تستخدم الكلمات المفتاحية أو أسماء العلم أو الحيوانات أو الكلمات التي يحتمل وجودها في معاجم اللغة، ويمكن زيادة تعقيد هذه الكلمات بجعلها تتغير أوتوماتيكياً مع مرور الوقت عليها.

محاكاة أساليب الهجوم الإلكتروني:

ويسمى هذا الأسلوب في بعض الأحيان بالمناورات الأمنية الإلكترونية وتعمل خلالها أجهزة الأمن الإلكتروني على القيام بهجوم تجريبي غير ضار على أنظمة إدارات الدولة المختلفة للتحقق من صلابتها ومقاومتها وقد يتم هذا الهجوم بدون

سابق إنذار للتأكد من فعالية أجهزة الحماية ومستوى تطبيق الإدارات الحكومية لمعايير الأمن الإلكتروني.

الحماية المادية للأجهزة والأنظمة:

كما في حالة بقية الأجهزة والإدارات الحكومية حيث تخصص الدولة فرق حماية مكونة من عناصر الشرطة والأمن، تحتاج مواقع الحكومة الإلكترونية وأماكن تواجد أنظمتها إلى حماية أمنية للتأكد من عدم تجرؤ أطراف عدوة على العبث والتخريب وتدمير المكونات المادية للحكومة الإلكترونية وقد ينفع من فترة إلى أخرى إجراء مسح راداري لاسلكي للتأكد من عدم وجود أجهزة تنصت إلكترونية في نطاق عمل الحكومة الإلكترونية.

يوجد العديد من تقنيات الدفاع الإلكتروني على المستوى التفصيلي وقد ذكرنا أهمها مع عدم إغفالنا للاستراتيجيات الداعمة لوجود حكومة إلكترونية أمينة وموثوقة.

التخطيط الأمني الإلكتروني:

يعتمد التخطيط الأمني الإلكتروني على أربعة مراحل أساسية تشكل بمجموعها دورة حياة الخطة الأمنية الفرعية في إطار التخطيط الأمني الشامل للبلاد، وينبثق عن كل مرحلة العديد من الإجراءات التي ينبغي القيام بها للتأكد من أن حدود البلاد الإلكترونية محصنة ضد هجمات الأعداء الداخليين والخارجيين، وتبدأ الخطة بمرحلة اتخاذ جميع إجراءات الوقاية الصادرة عن وحدة الأمن الإلكترونية في الدولة ومنها تعميم معايير الأمن والسرية المطلوبتين على كافة إدارات الدولة وتحضير البنية التحتية للحكومة الإلكترونية بطريقة تضمن عدم وجود ثغرات في الجدار الواقي الإلكتروني.

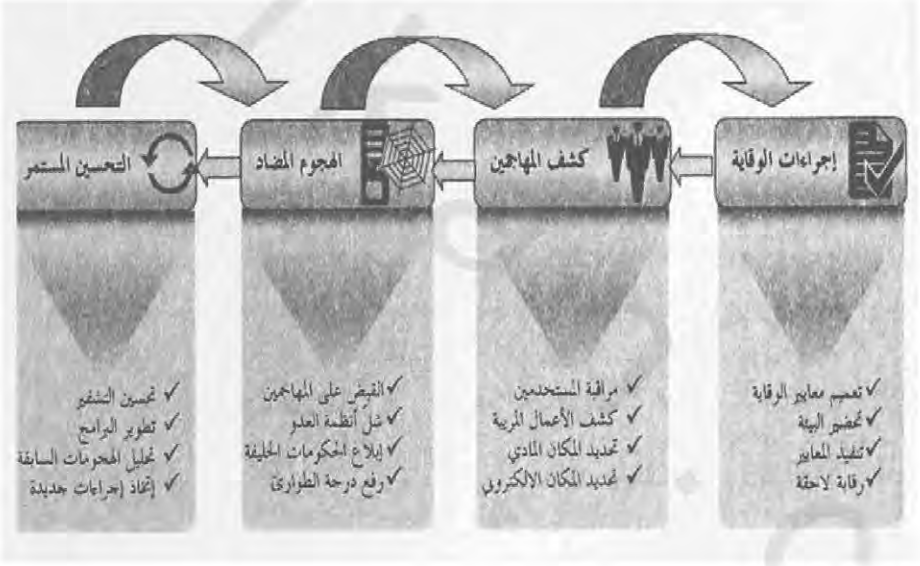
في المرحلة الثانية من الخطة يتم مراقبة الأعمال المريبة التي تحدث في شبكات الحكومة ومنها محاولات دخول متكررة وغير ناجحة ومحاولة إرسال

فيروسات إلى أنظمة الحكومة وإمكانية التلاعب بالبرمجيات والأنظمة من الداخل وبنتيجة هذه التحاليل يصار إلى تحديد أماكن ومصادر التهديد.

المرحلة الثالثة تحتم على وحدة الأمن الإلكتروني القيام بإجراءات دفاعية ومنها التعاون مع أجهزة أمن الدولة للقبض على المهاجمين في حال تم تحديد موقعهم الجغرافي وفي حال لم يتم فإن من الممكن أن تقوم تلك الوحدة بهجوم إلكتروني مباشر وآني على مواقع العدو الإلكترونية لشلّ قدرتها على إلحاق الأذى.

وختاماً ينبغي في المرحلة الأخيرة العمل الدائم على تحسين معايير الأمن والسرية عبر استطلاع التقنيات الجديدة والاستفادة من الأخطاء السابقة.

ويبين لنا النموذج التالي **دورة حياة الخطة الأمنية الإلكترونية**:



كما نلاحظ من خلال الشكل التخطيطي المطروح فمن الضروري عند تنفيذ أية مرحلة من الخطة الرجوع إلى المرحلة التي تسبقها لتعديل الإجراءات وتحسينها حسب ما ينتج عن المرحلة الجاري تنفيذها.