جامعة قاصدي مرباح – ورقلة –

كلية الحقوق و العلوم السياسية

قسم العلوم السياسية

مذكرة مقدمة لنيل شهادة الماستر أكاديمي في العلوم السياسية

التخصص : دراسات أمنية و إستراتيجية

بعنوان :

التخطيط الاستراتيجي الأمريكي لبرنامج الأمن القومي للولايات المتحدة الأمريكية

{ آلية التعامل مع الثغرات الاستخباراتية }

نوقشت بتاريخ : 2017/05/17

أعضاء لجنة المناقشة

د/ بارة سمير ..... رئيسا.

د/ خميس محمد ..... مشرفا و مقررا.

د/ بهاز حسين ..... مناقشا.

- إعداد الطالب :

ايت وعلي وليد

- إشراف الأستاذ:

د / خميس محمد

السنة الجامعية : 2016 / 2017

شكر و تقدير

قال الله عز وجل " ولئن شكرتم لازيدنكم "

{سورة إبراهيم : الآية 7}

لله الحمد والمنة والشكر على توفيقه لي في انجاز هذا العمل المتواضع.

أتوجه بخالص الشكر و التقدير إلى أستاذي و مؤطري، **"الدكتور : خميس محمد "**

للإشراف لهذه المذكرة وعلى توجيهاته ونصائحه القيمة أثناء القيام بهذا العمل.

إلى كافة الأساتذة و إدارة قسم العلوم السياسية بجامعة قاصدي مرباح على ما قدموه لنا طيلة فترة الدراسة.

كما اخص بالذكر رئيس القسم الدكتور : حشود نورالدين.

إلى كل الزملاء في الدراسة **لقسم العلوم السياسية , ماستر دراسات أمنية و إستراتيجية**.

دفعة سنة : 2016 – 2017

الإهداء

إلى

روح والدي العزيز الطاهرة و المغفور له **"ايت وعلي ارزقي "**

وفاءا و عرفانا و اسأل الله له الرحمة

إلى والدتي الحبيبة والعزيزة , حبا و تكريما لهما

وتقديرا لمؤازرتهما و دعمهما

إلى أخي و أختي , و كل أفراد أسرتي

إلى جميع أصدقائي , و كل زملائي في

الدراسة تخصص : دراسات أمنية و إستراتيجية

اهدي لهم هذا العمل المتواضع.

- ايت وعلي وليد

قائمة المحتويات

شكر و تقدير .....

الإهداء .....

قائمة المحتويات .....

مقدمة .....ص 1 - 5.

الفصل الأول :تحليل مفهوم الثغرات الأمنية و الاستخباراتية .....ص6.

المبحث الأول :تعريف الثغرات الأمنية و علاقتها بالمفاهيم الأخرى .....ص7.

المبحث الثاني : خصائص الثغرات الأمنية الجديدة.....ص13.

المبحث الثالث :أنواع و مراحل عملية صنع القرار الأمني.....ص19.

الفصل الثاني :دراسة الحالة حول الثغرة الأمنية/ الاستخباراتية .....ص23.

المبحث الأول :تدخل الاستخبارات الروسية في الانتخابات الرئاسية الأمريكية .....ص24.

المبحث الثاني :التحديات التي تواجهها منظومة الاستخبارات الأمريكية .....ص31.

المبحث الثالث :أشكال عملية استجابة الاستخبارات الأمريكية .....ص36.

الفصل الثالث : تقييم أداء الاستخبارات الأمريكية مع الثغرات الأمنية .....ص 40.

المبحث الأول :نماذج من ثغرات أمنية سابقة.....ص41.

المطلب الأول :تحليل أداء الاستخبارات الأمريكية منذ أحداث 2001/09/11.....ص41.

المطلب الثاني :تحليل أداء الاستخبارات السيبرية .....ص45.

المبحث الثاني :إستراتيجية مواجهة الثغرات الأمنية ذات الطابع المعلوماتي.....ص50.

الخاتمة .....ص57.

قائمة المراجع .....ص61.

مقدمة

لقد شكلت السيادة الوطنية عنصرا مهما من مصادر الصراع بين الدول, و خاصة في مجال الحدود و التدخل في الشؤون الداخلية, فبالإضافة لما تحمله السيادة الوطنية من معاني الهوية و الانتماء و الوجود و الاستقلال, فهي تحمل معاني تتعلق بمكانة الدولة و المجتمع و الهيبة المحلية و الدولية, و تحمل جوهر وجود الدولة و استقلاليتها غير أن السيادة الوطنية قد تميعت في المجتمع المعلوماتي, كما أن زيادة ترابط العالم و زيادة الاعتمادية بين مختلف الدول و المؤسسات و المنظمات و الشعوب قد ولدت أنواعا جديدة من المخاطر الأمنية, فالاعتمادية المتبادلة تقف حاجزا دون ذلك لان في ذلك تهديدا لمصالح الكثير من الأطراف الحكومية و غير الحكومية, فمع زيادة العولمة و الاتصالات, و اختراق الحدود السياسية للدولة تكونت بنية تحتية معلوماتية كونية جعلت مسؤولية الأمن مسؤولية دولية, مما عزز عولمة و عالمية القوانين لحماية البنية التحتية الكونية, و في المجتمع المعلوماتي شكلت المعلومات البنية التحتية للدول و لمؤسساتها, و مع زيادة الاعتماد على تقنيات المعلومات زادت احتمالية التعرض للاختراق أو التخريب مما يهدد الأمن الوطني للمجتمع و الدولة.

إشكالية الدراسة:

و من خلال ما ذكر تمت صياغة الإشكالية على النحو التالي:

- **ما مدى تأثير الثغرات الأمنية في البنية التحتية للأمن القومي الأمريكي ؟ و ما هي متطلبات و آليات التعامل معها ؟**

و تحت هذه الإشكالية نطرح التساؤلات الفرعية التالية:

- ما هي العوامل و الدوافع التي أدت لتدخل جهاز الاستخبارات الروسية في الشؤون الداخلية الأمريكية ؟ و هل لها دور مهم في التأثير على نتائج الانتخابات الأمريكية ؟
- كيف أدى قصور و فشل أجهزة الاستخبارات الأمريكية في حماية و مراقبة تسيير الانتخابات الرئاسية الأمريكية ؟ و ما هي انعكاساتها على البنية التحتية للأمن القومي الأمريكي ؟ و ما هي الإستراتيجية الاستخباراتية المتخذة للحد من عمليات الاختراق و التجسس الالكتروني و مواجهة الثغرات الأمنية ذات الطابع المعلوماتي ؟

فرضيات الدراسة:

- كلما كانت لأجهزة الاستخبارات الأمريكية دور في جمع المعلومات الاستخباراتية الحساسة كانت السياسة الأمنية الأمريكية أكثر نجاحا.
- تشكل المعلومات الحساسة النقطة المركزية و المحورية في دعم الاستجابات و كخطوة أولى لتقدير الخطورة و التحديد الفوري لمدى تأثير الثغرات الأمنية على الأمن القومي الأمريكي.

أسباب اختيار الموضوع:

أسباب موضوعية:

- نوعية و حساسية الموضوع المراد دراسته وأهميته على الساحة الدولية.
- لقد طرحت مجموعة من التساؤلات حول كيفية اختراق البنى التحتية الأمريكية , و خاصة علاقة هذا الاختراق بجهاز الاستخبارات الروسي ودوره في توجيهها.
- نظرا لعدم توفر الكم المعتبر للمعلومات و المراجع , حول تدخل الاستخبارات الروسية في الانتخابات الأمريكية, وذلك راجع لكونها قضية جديدة و حديثة النشأة و هي الحادثة التي لم يتم الاحاطة التامة بجميع حيثياتها من مدخلاتها و مخرجاتها لعدم وجود دلائل ووثائق رسمية بحوزة الباحثين المهتمين بهذه القضية سوى بعض المقالات و التقارير الصحفية و التي اغلبها متوفرة باللغة الأجنبية , كما حاولت التركيز على دراسة هذا الموضوع مما يعطيني دافع اكبر في التحكم أكثر في المعطيات المتوفرة , و تقديمه بشكل مقبول.

أسباب ذاتية:

- ميلي الشخصي واهتمامي الشديد لكل ما يتعلق بعالم وأجهزة الاستخبارات بصفة خاصة نظرا لما تتميز به من طابع الغموض والسرية في مجال عملها.
- رغبة ذاتية في دراسة و اكتشاف العوامل المؤثرة في الانتخابات الرئاسية الأمريكية.
- أن مجال هذه الدراسة تدخل ضمن نطاق و طبيعة تخصصي في الدراسات الأمنية والإستراتيجية.
- هي محاولة للابتعاد عن المواضيع كثيرة التناول حيث إن الدراسات المتعلقة بهذا الموضوع قليلة وله خاصية مميزة و خاص بتدخل عوامل خارجية في الشأن السياسي الداخلي لدولة كبرى هي الولايات المتحدة الأمريكية.

أهمية الدراسة:

يستمد هذا الموضوع أهميته , من كون تعرض الولايات المتحدة الأمريكية للاختراق و التجسس الالكتروني من طرف الاستخبارات الروسية من خلال التدخل المباشر و المساهمة في التأثير على نتائج الانتخابات الرئاسية الأمريكية لحساب مرشح على مرشح أخر, و التي تعد سابقة لا مثيل لها في تاريخ الانتخابات الأمريكية, و أيضا عن فشل الاستخبارات الأمريكية و التي تعد احد الأنظمة أو الأجهزة الأساسية بصفتها الأداة الأولى عن الدفاع ضد شتى التهديدات المحتملة و عن عجزها في احتواء الأزمة الأمنية أو اتخاذها لإجراءات و تدابير استباقية و وقائية ردعية تمكنها من التعرض لهذا النوع من الهجمات (ذات الطابع المعلوماتي) , و خاصة تلك المتعلقة بأمنها القومي , كما تعد الجهة الرسمية و المسؤولة عن تقييم المخاطر و التهديدات الداخلية و الخارجية التي تحيط بالولايات المتحدة الأمريكية , كما يسلط الضوء, عن طبيعة أداء الاستخبارات الأمريكية و إستراتيجيتها المنتهجة لتعزيز و حماية البنى

التحتية المعلوماتية الحساسة من الانكشاف من خلال سد الثغرات, و عن مدى دقة و سرعة استجابة الاستخبارات الأمريكية لمتطلبات و تداعيات هذه الفجوات الأمنية و انعكاسها على البنية التحتية للأمن القومي الأمريكي .

منهج الدراسة :

إن المنهج يعتبر طريق للوصول إلى الدراسة العلمية الصحيحة , و إحدى الوسائل التي لا يقوم البحث بدونها , ونظرا لأهمية هذا البحث , وذلك لتطرقه بشكل خاص حول ماهية الثغرات الأمنية و أهم خصائصها, وأيضا من الناحية الموضوعية من خلال إدراج مختلف المعلومات و المصادر المنوطة بالتدخل الروسي و دور جهازه الاستخباراتي (FSB) , وعن مدى مساهمته في التأثير على صناعة القرار في السياسة الداخلية الأمريكية و المتمثلة بالاختراق و التدخل المباشر للانتخابات الرئاسية الأمريكية, لهذا فقد احتاجت هذه الدراسة من وجهة نظري توظيف نوع من التكامل المنهجي , الذي يقوم على استعمال أكثر من منهج واحد لمحاولة الاقتراب من الموضوع والإشكالية محل الدراسة , ولهذا فقد كانت الحاجة إلى المنهج الوصفي و الذي يتيح من خلاله التقرب لوصف ظواهر التهديدات و الأزمات التي يمكن أن تنبثق من الثغرات الأمنية/ المعلوماتية, كما اعتمدت هذه الدراسة استخدام منهج دراسة الحالة الذي أعادنا إلى مختلف التطورات التي عرفتها الانتخابات الرئاسية الأمريكية كما اعتمدنا أيضا على المنهج التحليلي و ذلك لتحليل كيفية حماية البنية التحتية الأمريكية من الانكشاف عن طريق سد الثغرات الاستخباراتية ذات الطابع المعلوماتي, ومحاولة ربطها على مختلف المستويات لتجاوز مجرد سرد الوقائع و الأحداث في هذه الدراسة , و للإحاطة بكل ملمات و حيثيات هذا الموضوع المراد دراسته.

هيكل الدراسة :

تم تحليل إشكالية التخطيط الاستراتيجي الأمريكي لبرنامج الأمن القومي للولايات المتحدة الأمريكية, و اختبار مدى صحة الفرضيات التي قدمت.

تقوم هذه الدراسة على خطة مقسمة إلى ثلاثة فصول على النحو التالي :

- تناول الفصل الأول بعنوان تحليل مفهوم الثغرات الاستخباراتية و الأمنية , ثلاثة مباحث حيث تعرضنا في المبحث الأول , تعريف الثغرات الأمنية و علاقتها بالمفاهيم الأخرى عن طريق أنواعها و مستوياتها , وعرجنا في المبحث الثاني خصائص الثغرات الأمنية الجديدة , أما المبحث الثالث فقد احتوى على آلية و كيفية صنع القرار الأمني بأنواعه و مراحله .
- الفصل الثاني فخصص للدور الروسي في الانتخابات الرئاسية الأمريكية , فتم تناول هذا الفصل من خلال ثلاثة مباحث , عالج الأول تدخل الاستخبارات الروسية في الانتخابات الأمريكية , أما الثاني فعالج أشكال عملية استجابة الاستخبارات الأمريكية , أما الثالث فيحتوي على أهم التحديات السيبرانية التي تواجهها الاستخبارات الأمريكية .

- وسيكون الفصل الثالث محاولة لتقييم أداء الاستخبارات الأمريكية مع الثغرات الأمنية, حيث تم التعرض في المبحث الأول , نماذج لثغرات أمنية و اقتصادية سابقة أما المبحث الثاني فيتطرق إلى إستراتيجية مواجهة الثغرات الأمنية ذات الطابع المعلوماتي.
- وستكون في الأخير خاتمة تحاول استخلاص النتيجة المتوصل إليها مع اختبار صحة الفرضيات المقترحة.

الفصل الأول

تحليل مفهوم الثغرات الاستخباراتية والأمنية

المبحث الأول : تعريف الثغرات الأمنية وعلاقتها بالمفاهيم الأخرى

المبحث الثاني : خصائص الثغرات الأمنية الجديدة

المبحث الثالث : أنواع ومراحل صنع القرار الأمني

تمهيد:

إن زيادة ترابط العالم Connectivity وزيادة الاعتمادية Dependency بين مختلف الدول و المؤسسات و المنظمات و الشعوب, قد ولدت أنواعا جديدة من المخاطر والتهديدات الأمنية, فالاعتمادية تقف حاجزا دون ذلك لان في ذلك تهديدا لمصالح الكثير من الأطراف الحكومية و غير الحكومية, فمع زيادة العولمة و نظم تقنية الاتصالات و اختراق الحدود السياسية للدولة, تكونت بنية تحتية معلوماتية كونية جعلت مسؤولية حماية الأمن مسؤولية دولية, مما عزز عولمة وعالمية القوانين وحماية البنى التحتية المعلوماتية الكونية مما قد تزيد من احتمالية تعرضها لازمات و لثغرات أمنية محتملة.

المبحث الأول: تعريف الثغرات الأمنية وأنواعها و علاقتها بالمفاهيم الأخرى

يقصد بالثغرات الأمنية في هذه الدراسة الموقف أو الحدث أو مجموعة الأحداث التي تخل بالأمن الوطني, حيث تتسارع الأحداث مما يهدد بتزايد الخسائر المادية والمعنوية, الفعلية أو المحتملة, و مما يستدعي استنفار كافة الأجهزة و السلطات والجهود والإمكانات خصوصا المؤسسات السياسية والأمنية, للسيطرة على الوضع وإنهاء المشكلة في أسرع وقت, وبأقل التكاليف والخسائر.

و من هذا التعريف يمكن الاستنتاج أن من خصائص الأزمات الأمنية الكبرى ما يلي:

- أنها تهدد الأمن القومي أو احد مقوماته, بدرجة أو بأخرى, بطريقة مباشرة أو غير مباشرة.
- أن الخسائر المادية أو المعنوية أو كليهما, الفعلية أو المحتملة هي خسائر كبيرة أو متزايدة.
- أنها تستقطب اهتمام السلطة السياسية و المجتمع و تستدعي المواجهة و استخدام كافة الوسائل, بما فيها الوسائل العنيفة عندما يستدعي الأمر ذلك, لإنهائها في أسرع وقت و بأقل التكاليف[1].

و كل أزمة كبرى هي بدرجة أو بأخرى, أزمة أمنية بطبعها فلكل أزمة أبعاد أمنية لا يمكن تجاهلها أو إغفالها, ويصدق هذا على وجه الخصوص بالنسبة للازمات السياسية و الاقتصادية, و ربما أن البعد الأمني لازمة معينة يشكل أزمة أمنية موازية فرضتها الأزمة الأم, و قد تكون الأزمة الأمنية من النوع المستمر, مثل الأزمات التي تواجهها الدول و المجتمعات في أعقاب الاختلالات الأمنية و الأعمال الإرهابية مثل التفجيرات والاغتيالات و الاعتداء الخارجي والأزمات الإقليمية والدولية ذات الأبعاد الداخلية, بما

[1] الشهراني سعد بن علي, **إدارة عمليات الأزمات الأمنية**, مركز الدراسات و البحوث, جامعة نايف العربية للعلوم الأمنية, الرياض, 2005, ص 25-26.

يجعل الصراع بين القوى الصانعة للازمة والقوى المواجهة لها صراعا مستمرا. و للازمات الأمنية بشكل عام نفس خصائص و مراحل الأزمات الأخرى, إلا أنها تختلف في وسائل المواجهة, فالأزمات الأمنية قد تستدعي استخدام القوة و المواجهة العنيفة.

أما الأزمات الأمنية التي تهمنا هنا هي الأزمات التي تمثل تحديا للسلطة و للشرعية والتي تشكل تهديدا للأمن والنظام العام أو قد يؤدي إلى التأثير سلبا على النواحي الاجتماعية والاقتصادية والسياسية للدولة, وقد تنشا الأزمات الأمنية لأسباب متعددة يأتي في مقدمتها الأسباب السياسية, فقد أصبح من المألوف في الكتابات التي تتناول تعريف الإرهاب أن له صفة سياسية, بمعنى أن أسبابه أو أهدافه كليهما سياسية في الأساس, و انه إحدى أدوات ومظاهر الصراع السياسي الإقليمي والدولي, ولا شك أن الأزمات الإرهابية بشتى أنواعها تمثل النسبة الكبرى من الأزمات الأمنية, فإذا أضفنا الأسباب السياسية للازمات الأمنية تبدو واضحة و لا تحتاج إلى كثير من الجدل, الأزمة السياسية هي دائما أزمة أمنية بدرجة أو بأخرى و أي أزمة أمنية لها أسبابها و دوافعها وآثارها وأبعادها السياسية[1].

أما الأزمات الأمنية الداخلية هي حسب طبيعة الأزمة وقد تستغل هذه الأزمات من قوى أخرى كامنة في المجتمع أو من أطراف خارجية, سواء كانت هذه الأطراف أفرادا أو منظمات أو حكومات, ومن الأفضل التعامل مع هذه الأزمات في مرحلة النشوء والكمون واستباق الأحداث بحلول وقائية وسياسية, وقد تنشا الأزمات الأمنية لأسباب خارجية مثل الأزمات الأمنية المرتبطة بالصراعات والحروب الإقليمية والدولية التي يكون لها انعكاسات داخلية, ومن هنا نشا مفهوم "الجبهة الداخلية" الذي يهدف إلى حماية المجتمع من الآثار السلبية لهذه الانعكاسات, إضافة إلى أن التماسك الداخلي مطلوب لدعم السياسات والاستراتيجيات الخارجية للدولة.

الثغرات Vulnerability:

بصورة عامة تعرف بالحساسية اتجاه الأذى أو الهجوم الجسدي أو النفسي, كما تعني أيضا عدم توفر الحماية اللازمة للممتلكات و الأصول القيمة في امن الشبكات, و يستخدم تعبير الثغرات للإشارة إلى أماكن الضعف في هذه النظم و التي تتيح للمهاجم الاعتداء على سلامة النظام, و قد يتسبب في الثغرات قصور في البرمجيات أو خلل في التصميم, نتيجة لإهمال المبرمج أو المصمم, أو استخدام المهاجم لبرامج خبيثة مثل برامج الفيروسات.

[1] الشهراني سعد بن علي, **مرجع سابق**, ص27-28.

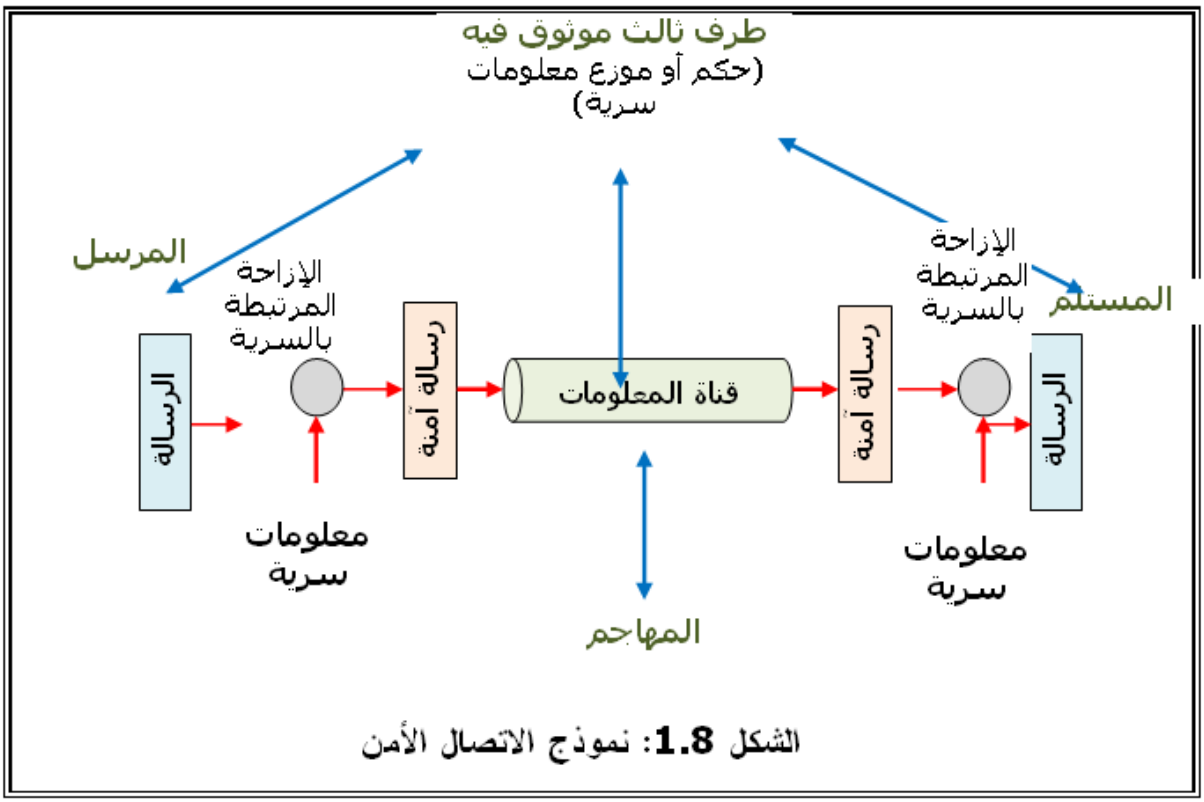
يمكن تصنيف الثغرات في امن الشبكات إلى فئتين :[1]

1. ثغرات فنية : وتكون نتيجة لضعف التحصين الناتج من التقنيات المستخدمة في النظم و الشبكات, في هذه الحالة يعرف الهجوم على الشبكة بالهجوم التقني.
2. ثغرات إدارية : و تكون نتيجة لأسباب غير فنية, و يعرف الهجوم على الشبكة المعلوماتية في هذه الحالة بهجوم الهندسة الاجتماعية Social Engineering Attack .

كما يمكن تقسيم الثغرات من حيث الصعوبة و السهولة إلى فئتين :

أ- ثغرات المستوى الأعلى High Level Vulnerability : و هي ثغرات سهلة الاستغلال, و مثال عليها كتابة شفرة برنامج لاستغلال تلك الثغرة.

ب- ثغرات المستوى الأدنى Low Level Vulnerability : و هذا النوع من الثغرات يصعب استغلاله, و يتطلب الكثير من الجهد و الموارد من قبل المهاجم.

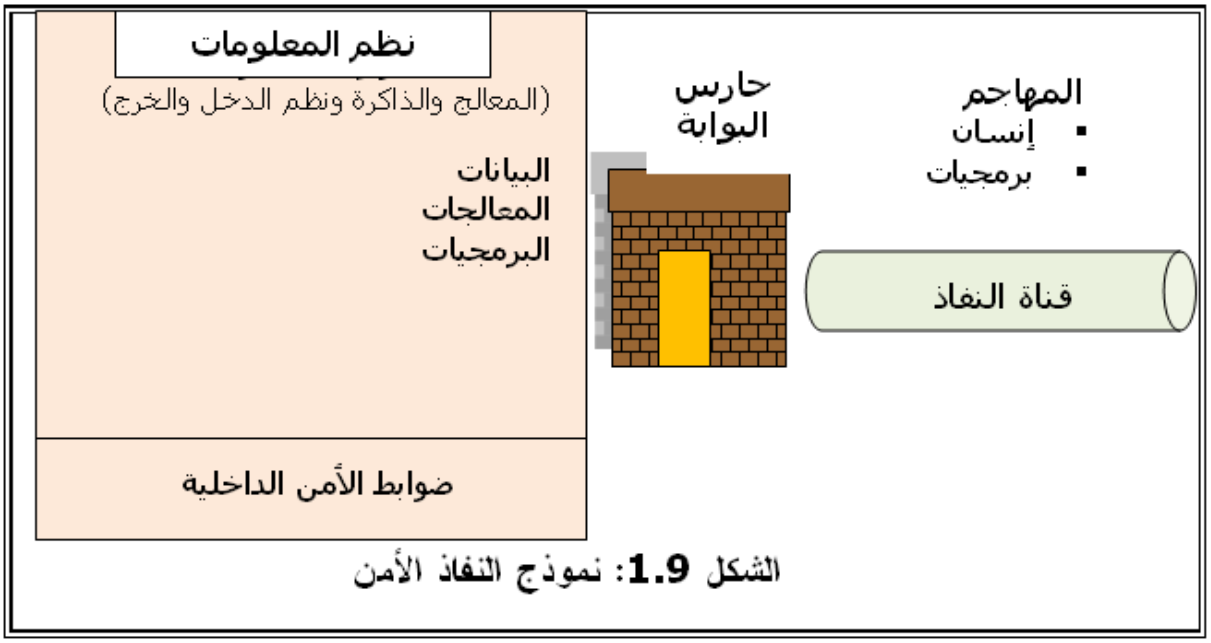


الشكل 1.8: نموذج الاتصال الأمن

الشكل (1-8) : يوضح نماذج انسياب المعلومات على قنوات الاتصال الامنة في حالة تواجد مهاجم محتمل[2].

[1] كمال الدين يوسف يسن, **الثغرات الأمنية في الشبكات اللاسلكية**, ص 20-21, على الموقع التالي : www.google.com/document/pdf, تاريخ الاطلاع : يوم 2017/02/09 على الساعة 20 :42 مساءا .

[2] كمال الدين يوسف يسن, **نفس المرجع**, ص37.



الشكل 1.9: نموذج النفاذ الأمن

الشكل (1-9) : يوضح نموذج نفاذ امن إلى الشبكة حيث يضبط النفاذ إلى المعلومات والموارد في نظم الشبكة في حالة تواجد مهاجم محتمل[1].

الثغرات الأمنية و علاقتها بالمفاهيم الأخرى :

- مفهوم حرب المعلومات : تعني حرب المعلومات **Information Warfare** هو استخدام المعلومات في تحقيق الأهداف والمصالح الوطنية, فالمعلومات مفتاح للقوة الدولية وهي مصدر وطني حيوي يدعم الدبلوماسية والاقتصاد, وتأثير المعلومات هام خاصة في مجالات الأفكار والطريقة التي يتخذ بها القرار والتأثير على القرارات التي يتخذها, وهي أيضا تعنى بتخريب المعلومات أو تدميرها أو سرقتها أو تحريفها أو إساءة استخدامها مع المنع من الوصول إليها, أو تقليل موثوقيتها أو استخدامها ضد أصحابها, إنها باختصار استخدام المعلومات ضد المعلومات إنها سرقة الأسرار إنها حرمان الطرف الأخر من استخدام معلوماته أو منعه من استخدام تقنياته, أنها تحول الطرف المستهدف إلى أعمى معلوماتيا مما يسهل التحكم به والسيطرة عليه, كما جمع المركز الاستراتيجي للدراسات الدولية (CSIS) الأدبيات الخاصة بحرب المعلومات بناء على المصدر والنوع والأهداف, ونظر إلى حرب المعلومات كمزيج من هذه الأبعاد, والخلاصة هي أن حرب المعلومات الهجومية يمكن أن تكون من الداخل أو الخارج و أن أشكال العدوان المعلوماتي تتراوح بين الهجوم على البيانات والبرنامجيات والدخول غير الشرعي والقرصنة والهجمات المادية على مواقع المعلومات, أما الأهداف فيرى المركز أن هناك أربعة أهداف رئيسة

[1] كمال الدين يوسف يسن, **مرجع سابق**, ص 38.

لحرب المعلومات هي : الاستغلال, الخداع, خلق الفوضى, التدمير للمعلومات ونظمها[1], إن الاعتمادية المتزايدة على المعلومات قد جعلت الحاجة ماسة إلى تغير النموذج التقليدي في الأمن والبحث عن نموذج **Paradigm**, لقد أصبحت البنية التحتية المعلوماتية والمعلومات أكثر عرضة للهجمات العدوانية, ويمكن لأي خصم أن يشن حرب معلومات على الطرف الأخر من أي مكان في العالم, وبالتالي فان قدرة الدولة على إدراك الخطورة والدفاع عن المعلومات ضد أي هجوم معلوماتي عنصر حيوي لبقاء الدولة وحفظ الأمن القومي.

- حرب المعلومات الإستراتيجية **Strategic Informational Warefare**: بدا مفهوم حرب المعلومات الإستراتيجية في الظهور في حرب المعلومات[2], ويعني استخدام الدول الحيز الفضائي للتأثير على العمليات العسكرية الإستراتيجية لإيقاع التخريب في البنى التحتية الوطنية, أن حرب المعلومات وما بعد الحرب الباردة قد أدتا إلى إدراك خاص وانتباه للوجه الجديد للحرب. مع تطبيقات في الإستراتيجية العسكرية والإستراتيجية الخاصة بالأمن الوطني.
- حرب الشبكات **Netwars**: وهي المعلومات ذات الصلة بالصراع مع المستوى الكبير بين الأمم أو المجتمعات, وتشمل تعطيل وإرباك وتدمير البنية التحتية المعلوماتية لدى الخصم[3].
- عولمة الأمن: لم يعد تهديد الأمن مشكلة وطنية أو إقليمية بل غدت مشكلة عالمية, و في المجتمع المعلوماتي فان استتباب الأمن ليس قضية محلية أو وطنية وإنما عالمية, مع أن طبيعة السلوكيات الإجرامية ستكون مختلفة في طبيعتها وبالتالي فان عولمة الانحراف سمة من سمات المجتمع المعلوماتي, وبما أن المجتمع الكوني في عصر المعلومات مجتمع كلي فان محصنات الأمن ستكون محط الاهتمام, وان تهديد الاستقرار العالمي ذو تأثيرات سلبية على الجميع, وفي المجتمع المعلوماتي قد لا يكون تحكم الدولة بحدودها أمرا ممكنا بالوسائل التقليدية, ففي وجود أقمار التجسس و الأطباق الفضائية لم تعد السيادة الوطنية ممكنة.
- التجسس **Spying**: تشكل المعلومات ثروة وقوة في المجتمع المعلوماتي, حيث يمكن للشركات والدول إنفاق مبالغ كبيرة في سبيل الحصول على معلومات تقنية عالية او أسرار عسكرية و أمنية أو سياسية أو تجارية, كما وظفت التقنيات الحديثة في عمل التجسس وأعمال الاستخبارات والعملاء بشكل كبير, و يعني الحصول على معلومات هامة من الناحية

[1] Ehlers. V. **Information Warefare and International Security** , 1999, p 155.
[2] البداينة ذياب, **الأمن وحرب المعلومات**, دار الشروق للنشر والتوزيع, ط1, عمان, الأردن, 2006, ص 145.
[3] Arquilla. J. and Ronfeldt , **Cyberwar Is Coming**, Comparative Strategy, volume 12, no 2, 1993, p 141.

الإستراتيجية أو العسكرية أو معلومات ذات طبيعة سرية[1], لقد استخدمت التقنيات في التجسس بشكل أساسي وفي مجال جمع المعلومات.

- الحرب الالكترونية **Electronical Warefare** : وهي استخدام التقنيات الالكترونية المعروفة على اختلاف أنماطها في مواجهة أنظمة السلاح التي يملكها الخصم, وتكون باستخدام أساليب وأجهزة الكترونية متخصصة لرصد وكشف واستطلاع ومراقبة جميع موجات العدو الكهرومغناطيسية المنبعثة من أجهزته اللاسلكية المختلفة, ثم تحليلها ومعرفة محتواها بهدف الوقوف على نوعية معداته وقواته وتحركاته وتشكيلاته وإمكاناته وخططه, فتكون سياسة التعامل معه بعد ذلك طبقا لإجراءات وأساليب مناسبة[2].
- الإرهاب: تتعرض البنية التحتية المعلوماتية للعمليات الإرهابية بكافة أشكالها سواء الإرهاب التقليدي **Conventional Terrorism** والذي يقوم على تدمير البناء التحتي المعلوماتي, أو الإرهاب التكنولوجي **Technological Terrorism** والذي يهدف إلى التأثير على الفضاء باستخدام وسائل مادية مثل تفجير محطات الطاقة والاتصالات مما يؤثر على الفضاء التخيلي **Cyberspace** , أو الإرهاب الفضائي **Cyber Terrorism** والذي يقوم على تدمير البرمجيات وتدمير المعلومات[3], أو الإرهاب المعلوماتي **Informational Terrorism** له طريقتان الأولى عندما تكون تقنية المعلومات هدف أو حيث تشمل هذه الطريقة استهداف الإرهاب لنظم المعلومات و أي بنية تحتية معلوماتية, و الثانية عندما تكون تقنية المعلومات أداة لعملية كبيرة وتشمل هذه الطريقة انتقاء الإرهاب واستغلاله لنظام المعلومات أو سرقة البيانات أو مجبرا للبيانات على أداء مهمة غير شرعية, كما يمكن أن يستخدم الإرهاب الشبكة الكونية في تنظيم اتصالاتهم وعملياتهم و استغلال بعض المواقع لإخفاء معلوماتهم, كما أن استخدام تقنيات الحماية مثل التشفير تزيد عملهم آمنا, ولا يتوقف الخطر عند استخدام الإرهاب للبنية التحتية المعلوماتية الكونية, بل أنها تسهل حصولهم على المعلومات والبرمجيات التي تساعدهم في تنفيذ أعمالهم.
- تحليل التهديدات **Threats Analysis**: وهي تحليل مصادر الخطر ونوعه وحجمه واحتمالاته وآثاره, أن تحليل التهديدات والأخطار يعني تحليل أسباب نشوء الأزمات الأمنية.

---

[1] Davis. I. **Crime and the Net : an Overvew of Criminal Activity on the Internet and the Legal Community's Response**, 1998, on: http://www.Law.ttu.edu/cyberspc/journal.html

[2] البصيلي جاسم محمد, **الحرب الالكترونية – أسسها وأثرها في الحروب**, المؤسسة العربية للدراسات والنشر, ط2, بيروت, 1989, ص30.

[3] Gerard. J.J. M. **Infrastructure Valnerabilities : New Role for DND Department of National Defence, War, Peace and Security**, Canada, 1999, p45.

- الإجراءات الأمنية **Security Measures** : هي الإجراءات الدفاعية والهجومية المتعلقة بحرب المعلومات, أن حفظ المعلومات الإستراتيجية وكلمات السر والعمليات والبرامج خطورة هامة تجعل الحصول على المعلومات عملية صعبة لكن غير مستحيلة, ومن وسائل الحماية كالتشفير وجدران الحماية.
- التحدي **Challenge** : على المستوى الاستراتيجي يقصد بتحدي ذلك الوضع الذي تفرضه عوامل أو قوى معينة ضد كيان معين, بما يهدد مصالح الكيان ويعني الوضع المتأزم الذي يصاحب نشوء الأزمات الأمنية[1].
- الاستجابة **Response** : يقصد برد فعل السلطة للتحديات والأزمات الأمنية ومدى قدرة السلطات على اتخاذ القرارات المناسبة والفعالة في الوقت المناسب, واستغلال القدرات المتاحة للسيطرة على الأوضاع, وعادة ما تربط الاستجابة بالتحدي بما يعني أن النجاح في مواجهة التحدي يعتمد على نوع وحجم قوة الاستجابة.

المبحث الثاني : خصائص الثغرات الأمنية الجديدة

تشكل البنية التحتية المعلوماتية هدفا لعمليات حرب المعلومات الهجومية, ففشل هذه البنية في أداء وظائفها يؤدي إلى إغراق المجتمع مباشرة بتعتيم معلوماتي, ويعاني البناء التحتي المعلوماتي من ثغرات أمنية وانكشافا للعمليات العدوانية فالبنوك والمؤسسات المالية والخدمات الحكومية الأساسية من أكثر المواقع حساسية عند تعرضها لأعمال الاختراق والتطفل, ولقد زاد الاهتمام باستهداف البنية التحتية المعلوماتي الوطنية (NII) مع بداية التسعينيات ومع زيادة الاعتمادية المجتمعية والحكومية على المعلومات, مما دفع إلى تكوين بناء تحتي معلوماتي وطني للدولة, وتشمل التهديدات تخريب وتدمير المنظمات والمؤسسات والشركات والأفراد في قطاع المعلومات عامة, وخاصة البرنامجيات والاتصالات الفضائية ونظم الاتصالات المتصلة بالبنية التحتية المعلوماتية, أما النشاطات العدوانية فتشمل :[2]
الحرمان من الخدمة أو تعطيلها أو استغلالها للمعلومات ونظم التشغيل وخدمات الاتصالات والمراقبة غير المصرح بها, ونظم الاتصالات وقطاع المعلومات والتعديل غير القانوني أو التدمير لرموز وبرامج الشبكات وتحوير المعلومات, والخدمات المتعلقة بالأقمار الصناعية مما يؤدي إلى خسارة كبيرة.

[1] الشهراني سعد بن علي, **مرجع سابق**, ص 39.
[2] البداينة ذياب, **مرجع سابق**, ص 31.

وتتفاقم المشكلة عند الثغرات الأمنية في البناء التحتي المعلوماتي الكوني, حيث لم تعد البنية التحتية المعلوماتية الوطنية هي الهدف بل الكونية كذلك, خاصة مع زيادة الاعتمادية الدولية على هذه البنية في الاتصالات.

لقد أصبح تهديد امن البنية التحتية المعلوماتية عابرة للحدود الوطنية, وذلك بتصريح من مدير مركز حماية البناء التحتي الوطني في (FBI) Micheal Vatis بقوله : " نحن بحاجة إلى الاستعداد للجهات الإرهابية الخطرة على نظم البناء التحتي الحساس, و أن أدوات العدوان (الجريمة الفضائية) معقدة و متوافرة لأي شخص يمكنه الوصول للانترنت"[2].

ولا يتوقف الأمر على الثغرات في البنية التحتية المعلوماتية الوطنية, بل يمكن مهاجمة النظم المعلوماتية الكونية والهدف من ذلك :

1. سرقة المعلومات (Theft of Information) سرقة معلومات خطط الخصم والاستراتيجيات الاقتصادية.
2. تعديل المعلومات (Modification of Information) تغيير المعلومات وزرع معلومات خاطئة أو فيروسات.
3. تدمير المعلومات (Destruction of Information) مسح المعلومات التي تشمل على معلومات مالية أو عسكرية أو حكومية.
4. تدمير معلومات البنى التحتية المعلوماتية (Destruction of The Information Infrastructure) من خلال الفيروسات.

فمثلما شكلت الصواريخ العابرة للقارات نوعا جديدا من التهديدات الأمنية بين الدول, فان تكنولوجيا عصر المعلومات قد قدمت تحديا جديدا للأمن الوطني, حيث نهاية الجغرافيا وغياب المسافات, وان الهجمات على نظم المعلومات حقيقة واقعية في عصر المعلومات ولازالت هذه الهجمات قليلة الخسائر, ولكنها مرشحة للزيادة ولقد قدر بان أكثر من 90% [1], من هذه الهجمات قد نفذت باستخدام المعدات المتوافرة والوسائل المتاحة والتي لا يمكن لأي شخص استخدامها.

[1] Sakkas. P. E, **Espionage and Sabotage in the Computer World, International Journal of Intelligence and Counterintelligence**, Vol 5, No 2, 1995, p 162.

التهديدات (Threats) : من الصعب ربط التهديدات الفضائية بمكان أو زمان, أو جماعة فقد تصدر من محترف أو جماعة إرهابية أو استخبارات أجنبية, ولقد حددت وكالة مشاريع البحوث الدفاعية المتقدمة (DARPA) مهددات البناء التحتي المعلوماتي و صنفتها في خمسة فئات هي[1] :

1. التهديدات الخارجية المحايدة (Exterrnal Passive Attack) مثل التنصت , تحليل الإشارات.
2. التهديدات الخارجية النشطة (External Active Attack) مثل الدخول غير المصرح به.
3. الهجوم على نظام عامل (Running System Attack) .
4. الهجوم الداخلي (Internal Attack) .
5. الهجمات للوصول إلى تعديل النظام مثل خرق حماية الدخول للنظم والانكشاف.

الانكشافات الجديدة (New Vulnerabigities) :

يقول روبرت مارش Robert M. Marsh رئيس اللجنة الرئاسية لحماية البنية التحتية الحساسة في رسالة إلى الرئيس الأمريكي:

" إن هناك قدرة كبيرة لاستغلال الثغرات في البنية التحتية المعلوماتية, و أن المقدرة في تحقيق الأذى من خلال شبكات المعلومات يمثل واقعا فعليا, وانه في زيادة و بمعدلات خطرة, و لدينا القليل للدفاع".

وتقول اللجنة في مقدمة تقريرها أن :

" البنية التحتية الحساسة تقف خلف كل جزء من حياتنا, إنها تشكل الأساس في رفاهيتنا, ومدعمات دفاعنا و الحارس لمستقبلنا, إنها قوة لكل جزء من مجتمعنا و لا توجد أولوية ملحة أكثر من أولوية توفير الأمن, و الاستمرارية, وتوافر البناء التحتي الحساس".

إن أي فوضى في البناء التحتي المعلوماتي ستكون مربكة, ويمكن أن تؤدي إلى نتائج خطيرة على الاقتصاد والأمن, إن الاعتمادية المتبادلة و الترابط المتبادل جعل احتمالية أن تكون المعلومات, والبنية التحتية المعلوماتية منكشفة احتمالية عالية.

لقد دعا رئيس توجيه حماية البنية التحتية المعلوماتية بمجهود وطني لتامين الأمن للبنية التحتية الأمريكية التي أصبحت عالية الانكشاف ومترابطة, و تشمل البنية التحتية المعلوماتية الأمريكية

[1] **Defence Sience Board Report of the Defence Sience Board Task Force on Information Warefare- Defence (IW-D)** : office of the Under Secretary of Defence for Acquisition and Technology, Washington DC, 1996, available online at: http://www.jya.com/iwd.html .

الاتصالات و البنوك والطاقة و الخدمات الحكومية الأساسية, و قال مدير وكالة المخابرات المركزية الأمريكية " لدينا الدليل بان عددا كبيرا من الدول في العالم تطور الخطط و الاستراتيجيات و الأدوات لشن هجمات معلوماتية على الشبكات المتصلة بالجيش الأمريكي".[1]

أما الثغرات الفضائية (Cyber Vulnerabilities) و الناجمة عن زيادة الاعتمادية على الاتصالات والمعلومات فقد زادت احتمالية التعديات على البنية التحتية المعلوماتية, و لقد توصلت اللجنة الرئاسية لحماية البنية التحتية المعلوماتية الحساسة إلى أن حماية البنية التحتية الحساسة يتطلب فهما للثغرات الأمنية, و العمل على خفض و إغلاق هذه الثغرات, ولقد أوصت اللجنة بان لا يكون الانتظار لحدوث كارثة إستراتيجية خطيرة الآن, هو الوقت المناسب لحماية المستقبل.

تتفاوت البنى التحتية المعلوماتية بدرجة انكشافها إلى الكوارث الطبيعية والإهمال البشري و سوء التصرف الإنساني, ولقد حدد التقرير الرئاسي الأمريكي بخصوص حماية البنية التحتية الحساسة, إن ثبات و امن قطاع الاتصالات والمعلومات قد أصبح موضوعا في غاية الأهمية, و أن المهدد الرئيس لثبات الاتصالات والمعلومات هو الكوارث الطبيعية و إخفاقات النظام, أما المهدد الرئيس للأمن فهو التعديات المتعمدة الفيزيقية أو الفضائية على نظم المعلومات والبناء التحتي المعلوماتي, و يعتمد على الاستعدادات الحكومية لمواجهة الكوارث و الأزمات في حماية ثبات توافر خدمات الاتصالات والمعلومات, أما المهدد الثالث هو التعديات المتعمدة واعتمادا على الهدف أو الأهداف من التعدي وقد تكون التعديات بهدف التعديل أو الاستخدام أو التخريب أو التدمير للمعلومات والبيانات المخزنة أو الحرمان من الخدمة, و يشمل المعتدون أجهزة الاستخبارات الوطنية, وناقلات المعلومات والإرهابيين والدخلاء والداخلين غير المنتمين, حيث يشكل الداخليون النسبة الكبيرة المهددة للأمن ولنظم المعلومات التي لا يتم كشفها, ويستخدم المهاجمون وسائل متنوعة ضد البنية التحتية المعلوماتية بما في ذلك تحليل الذروة, والهجمات المشفرة و الفنية و أهم هذه الهجمات وأكثرها خطورة هي الهجمات الفيزيقية والفضائية, لقد ازدادت الثغرات في البناء التحتي المعلوماتي وأصبحت أكثر عرضة للتعديات والهجمات.

[1] PCCIP (President's Commission on Critical Infastructure Protection), **Critical Foundations : Protecting America's Infrastructures**, the Report of the President's Commission on Critical Infrastructure Protection, October 1997, p 15, at: http://www.pccip.gov , PDF File.

الخصائص الأمنية لمجتمع المعلومات :

- امن المعلومات : لقد بدا الحديث عن حماية البناء التحتي المعلوماتي وسميت بعض المكونات الهامة في هذا البناء بالبناء التحتي المعلوماتي الحساس, والذي يؤدي تعطيله أو تدميره إلى وضع المجتمع في حالة فوضى, وقد استدعى هذا اهتمام الحكومات لتوفير السبل الكفيلة بحمايته, وظهرت العديد من الخطط لصيانته وبحث البدائل الدفاعية اللازمة وقت الحرب والسلم, فقد أصبحت الحروب الحالية حروب معلومات, لقد بدا الاهتمام بحماية الاقتصاد الالكتروني والحماية ضد التجسس الالكتروني وضد اختراق الدخلاء لنظم المعلومات, لقد تبدلت المفاهيم الأمنية وحلت مفاهيم أمنية معلوماتية تتماشى مع البناء التحتي المعلوماتي[1], فظهر الإرهاب الالكتروني وجرائم المعلومات والدخلاء والمتسللون, وزاد استخدام العمليات النفسية والاستخبارات.
- الجرائم الفضائية (Cybercrimes) : يعد التحول إلى الانترنت الكونية أو ما يشار إليه أحيانا (I – Way) من البحث الأكاديمي والاتصالات إلى الاتصالات الكونية[2] والبناء التحتي المعلوماتي الكوني (Global Information Insfrastruction) من أهم التطورات في التاريخ الحديث, ومن التغيرات الهامة لهذا العصر في مجال الجريمة والسلوكيات الإجرامية ما نتج عن تكنولوجيا (I – Way) , حيث تقترف الجرائم القديمة بطرق حديثة و جرائم حديثة بطرق قديمة, و جرائم حديثة بطرق حديثة, اتخذت الجريمة أشكالا مستحدثة تتماشى مع البنى الاقتصادية والاجتماعية لمجتمع المعلومات, أما في المجتمع المعلوماتي فقد أصبحت المعلومة أداة وهدفا في آن واحد للسرقة, فالمعلومة المتعلقة بالأداة (برنامج, برامج اختراق, جدران الحماية) أو المتعلقة بهدف الجريمة, أو كهدف للسرقة الأسرار الأمنية والعسكرية, لن تكون الجرائم في مجتمع المعلومات مقتصرة على دولة بعينها, وإنما سيكون العالم كله مسرحا لها, حيث يمكن للفرد أن يرتكب جريمة من أي مكان في العالم, لا وجود للحدود العالمية في الجرائم خاصة مع وجود الانترنت وشبكات الاتصال العالمية, وتزداد الخطورة من أن قادة الجريمة يمكنهم من توظيف طاقات إبداعية في هذه المجالات وتحت نشاطات مقبولة, لكن بقصد توظيف واستثمار أموال الجريمة عامة, وتطوير قدراتهم التقنية الجرمية, لقد اقترح "كون وفلسون" انه لتتم الجريمة لابد من حضور ثلاثة عوامل هي : الضحية Victime , المهاجم Attacker , غياب الحراسة الكلية

[1] البداينة ذياب, **مرجع سابق**, ص101.

[2] Boni. W. C. and Kovacich. G, **I – way Robbery: Crime on the Internet**, Boston: Butterworth-Heinemann, 1999.

No Guardian [1], ولقد استخدم "ريز" ثلاثة متغيرات تصف العوامل التي ذكرها "كون وفلسون" وطبقها في مجال الجريمة المعلوماتية وسماتها : الأرضية Ground , والنتيجة Resolve , والمنفعة Utility , أما الأرضية فقد تكون مادية Physical , أو فضائية Cyber , ويجب أن تكون الأرضية لصالح الحارس وتعيق المهاجم, فشبكة المعلومات المحصنة بجدران الحماية ستعيق الهجوم وتصد القراصنة والدخلاء, أما المنفعة وهي في العالم المادي (قوة) وفي العالم الفضائي (ذكاء), وتكثر الجرائم الالكترونية والجريمة عن بعد والإرهاب الفضائي وسرقة المعدات المتصلة بالمعلومات, وتخريب البيانات والدخول غير القانوني للبيانات, وتحتاج تقنيات المنظمات إلى حماية معلومات شاملة (Comprehesive Information Protection) , وهذا يتطلب برامج وعناصر بشرية مدربة وسياسات وإجراءات وبرامج توعية أمنية, ومع تطور التقنيات فقد مكن التشفير المخترقين من أداة فعالة في تخفية نشاطاتهم, هذا بالإضافة إلى الوسائل الالكترونية المتاحة لهم وإمكانية تخزين البيانات ونقلها من مكان لأخر.

- خصائص حرب المعلومات الإستراتيجية :

1. مدخلات قليلة الكلفة : تمتاز حرب المعلومات الإستراتيجية بأنها لا تتطلب كلفة مادية كبيرة أو دعم حكومي كبير كما هو الحال في الحرب التقليدية[2], المتطلب لحرب المعلومات الإستراتيجية هو خبراء نظم المعلومات وإمكانية الدخول إلى الشبكات المهمة, إن الشبكات المترابطة عرضة للهجوم والتخريب ليس فقط من قبل الدول ولكن من جهات غير الدول بما في ذلك الجماعات والأفراد.
2. حدود تقليدية غير واضحة : لقد تعقد التمييز التقليدي بين كل من الاهتمامات العامة والخاصة, والسلوك المستقيم – المجرم الحدود الجغرافية مثل التي بين الدول, مع التطور في التفاعل داخل البنى التحتية المعلوماتية.
3. الدور المتنامي لإدارة الإدراك : إن تقنيات المعلومات الجديدة ربما تزيد بشكل ملحوظ نشاطات التأثير, وقوة الخداع وانتقاء الصور (Images-Manipulation) كما يؤدي إلى تعقيد جهود الحكومة في بناء دعم سياسي للمشاريع الأمنية ذات العلاقة.

[1] Cohen. L. E. & Felson. M, **Social Change and Crime Rate Trends: Routine activity aporoach**, Americain Sociological review, Vol 44, 1979, p 508-608.

[2] البداينة ذياب, **مرجع سابق**, ص 149.

4. تحدي استخباراتي استراتيجي جديد: إن الفهم الضعيف للثغرات في حرب المعلومات الإستراتيجية والأهداف يؤدي إلى إزالة فاعلية طرق جمع الاستخبارات التقليدية وتحليلها, ولقد تطور حقل جديد في حرب المعلومات الإستراتيجية.
5. مشكلات التحذير التكتيكي وتقدير التعدي: لا يوجد حاليا نظام تحذير تكتيكي مناسب للتمييز بين هجمات حرب المعلومات الإستراتيجية والهجمات الأخرى لنشاط الحيز الفضائي بما في ذلك التجسس أو الحوادث.
6. صعوبة بناء تحالفات دائمة والمحافظة عليها: أن الاعتماد على تحالفات يمكن أن يزيد الثغرات الأمنية لجميع الشركاء إلى هجمات حرب المعلومات الإستراتيجية.
7. انكشافات الأراضي: إن وسائل المعلومات قد لاشت الحدود الجغرافية, أن الأراضي منكشفة للتعديات مثلها مثل الأهداف في المسرح و خاصة مع زيادة الاعتماد على البنى التحتية المعلوماتية.

المبحث الثالث: عملية صنع القرار الأمني

أركان القرار الأمني: و لكي يكتمل القرار الأمني فلا بد من توفر أركانه الخمسة وهي:

- ركن السبب: إذ لا بد وأن تكون هناك حاجة واقعية أو قانونية استدعت تدخل الإدارة وبالتالي اتخاذ القرار[1].

- ركن الشكل: وذلك بأن يُفصح القرار عن إرادة الإدارة في الشكل الذي يتطلبه القانون . بأن يكون كتابياً أو شفهياً , صريحاً أو ضمنياً , برقياً أو هاتفياً .

- ركن الاختصاص: وهو تحديد الجهة ذات الصلاحية المنوط بها إصدار القرارات , وتتوزع الصلاحيات حسب المستويات الوظيفية , وتأهيلها وطبيعة الاختصاص .

- ركن المحل: والمقصود به الأثر القانوني الذي يترتب على القرار فور صدوره , أي يكون له أثر معين وممكن وجائز قانوناً[2].

- ركن الغاية: وهو الغرض أو الباعث على اتخاذ القرار , وما هي النتيجة التي يسعى متخذ القرار إلى تحقيقها .

[1] الردادي محمد بن عودة, **دور القيادات الوسطى في اتخاذ القرارات واثر ذلك على كفاءة الأجهزة الأمنية**, رسالة ماجستير غير منشورة, أكاديمية نايف للعلوم الأمنية, الرياض, 1417 ه, ص41.

[2] الجابري عباد بن عبيد, **اتخاذ القرارات في المنظمات الأمنية**, رسالة ماجستير غير منشورة, المركز العربي للدراسات الأمنية والتدريب, الرياض, 1989, ص34.

أنواع القرارات الأمنية:

تختلف عملية اتخاذ القرارات في الجهاز الأمني عن الأجهزة الإدارية الأخرى , لان طبيعة عمل الأجهزة الأمنية يتعلق بتوفير الأمن للممتلكات في الأوقات العادية والطارئة , وهذا يتطلب اتخاذ قرارات سريعة ونافذة ومحققه للأهداف , كما أن اختلاف طبيعة المنظمات الأمنية وطبيعة المواقف الأمنية تؤدي إلى تنوع القرارات الأمنية المتخذة اعتماد ا على عدة معايير هي:

- أهمية هذه القرارات.
- طبيعة تكوين هذه القرارات.
- مدى هذه القرارات.
- عمومية هذه القرارات.
- قابليتها للإلغاء والتعويض [1].

وحيث أنه في هذه الورقة يهمنا أن نحدد نوع القرار الذي سوف يتخذ لمواجهة كارثة أو أزمة طارئة.

فإنه ومن خلال قراءة العديد من التصنيفات التي يراها خبراء الإدارة أن القرارات الإستراتيجية هي قرارات تتصل بمشكلات هامه وطارئة وذات أبعاد متعددة وعلى جانب كبير من التعقيد والعمق, فهذه المشكلات يصعب مواجهتها بقرار فوري , لذلك تعد هذه القرارات مسبقاً قبل ظهور الحالة الطا رئة لتحديد كيفية وأسلوب مواجهتها , وفي هذا النوع من القرارات, يجب أن يتم تسخير كافة الإمكانات والتخصصات و الإستعانة بخبرات المستشارين والمساعدين وبدراسات العلماء المتخصصين ذوي المعرفة والدراية بمثل هذه المشكلات في سبيل اتخاذ القرارات المناسبة .

خطوات و مراحل اتخاذ القرار الأمني:

مما لا شك فيه أن إتخاذ القرار الأمني في الكوارث والأزمات يعد من أخطر القرارات , لذا فإنه من الضروري إتباع المراحل التي يمر بها القرار الأمني هي:

- تشخيص مشكلة الأزمة:

أن التشخيص الصحيح للمشكلة هو الطريق السليم لحلها , وفي هذا الإطار لا بد من التعرف والذي يعني لدى (Strategic Factor) العامل الاستراتيجي أو الحرج للمشكلة, ذلك العامل الحيوي الذي لا بد من تغييره أو تعديله قبل أي شيء آخر . أيضاً لا بد من التمييز بين أسباب المشكلة وأعراضها . إذ أن التركيز على أعراضها سيبقى المشكلة دون حل, إذ يجب التركيز على الأسباب الحقيقية للمشكلة إذا عزمنا على علاجها , لذا يجدر التنويه في هذه المرحلة إلاّ نبحث فيها عن حلول للمشكلة وإنما تحديدها فقط , ليظل التركيز على التشخيص لا العلاج.

[1] الهذلي سعد بن عليوي, **مهارة القائد الأمني في اتخاذ القرار في الظروف الطارئة**, رسالة ماجستير غير منشورة, أكاديمية نايف العربية للعلوم الأمنية, الرياض, ص39.

أن الأزمة الأمنية قد يسهل رصد حركة تطورها أحياناً . إلا انه وفي حالات كثيرة يصعب التعرف على طبيعتها وأهدافها .. بيد أن التركيز الموضوعي الشديد في مرحلة التشخيص يساعد كثيرا في التعرف عليها بكل دقة [1].

ولذلك فإن تشخيص المشكلة وتحديد أسبابها تتطلب في القيادة حسن الفطنة , وعمق البصيرة , وسعة الأفق , ورجاحة التقدير .

ولكي تنجو القرارات المبتغاة من احتمالات الخطأ في التشخيص نتيجة نقص الخبرة الفنية لدى متخذ القرار , فإنه يجب على مُصدّر القرار الاستعانة بأهل الخبرة الفنية المتخصصة من داخل التنظيم أو من خارجه , حيث تؤدي الاستعانة بهؤلاء إلى كشف الأسباب الحقيقة لهذه المشكلة [2].

أنواع القرارات الأمنية :

هي القرارات المبرمجة والقرارات غير المبرمجة والقرارات التنظيمية والقرارات الديمقراطية والقرارات اليقينية والقرارات الارتجالية والقرارات الإستراتيجية والقرارات التكتيكية والقرارات التنفيذية والقرارات الموضوعية والقرارات الكمية والقرارات التأكيدية.

نظم القرارات الأمنية :

إن تضييق مستوى المشاركة في القرارات، وعدم تفويض الصلاحيات يخلق جوًا من عدم الثقة بين الرؤساء والمرؤوسين. إن قدرة المنظمات على توفير المعلومات الضرورية وبسرعة، يعتبر المطلب الأساسي لترشيد عملية اتخاذ القرارات.إن القرارات التي تتخذ بناء على الجهل أو التخيل، تفتقد للأسس العلمية الصحيحة، وبالتالي، فإنها تؤدي إلى عواقب وخيمة وتكون نتائجها سلبية.

مراحل صنع القرار الأمني : وهي خمس مراحل رئيسية :[3]

- تشخيص الحالة القائمة .
- تحديد المشكلة.
- تحديد البدائل الممكنة.
- الاختيار بين البدائل المتكافئة.
- التنفيذ.

[1] الشعلان فهد احمد, **اتخاذ القرارات أثناء الكوارث والأزمات**, مجلة الفكر الشرطي, المجلد السابع, العدد الرابع, الإمارات العربية المتحدة, الشارقة, يناير 1999, ص 108.

[2] السيد طه سعيد, **عملية صنع واتخاذ القرار الإداري**, مجلة الفكر الشرطي, المجلد السابع, العدد الرابع, الإمارات العربية المتحدة, الشارقة, يناير 1999, ص 73.

[3] عبوي زيد منير, **إدارة الأزمات**, دار كنوز المعرفة للنشر والتوزيع, عمان, 2007, ص21.

القرار الأمني ومهارات اتخاذه :

وله ثلاث سمات :اختيار أفضل البدائل والشمولية ومراعاة الظروف المحيطة بمتخذ القرار.

طبيعة وسمات القرار الأمني :

إن المدخل العقلاني يمكن الاستفادة منه في المجال الأمني عن طريق وضع الجوانب الاقتصادية في الاعتبار عند اتخاذ القرار، أي على القيادة الأمنية أن تضع الاعتبارات الاقتصادية المتعلقة بالمجال الأمني صوب اهتمامها[1]، معتمدًة في ذلك على حسابات المكسب والخسارة عند اتخاذه.

التوصيات المتعلقة بصناعة القرار الأمني:

1. ضرورة توسيع مستوى المشاركة في القرارات، وتفويض الصلاحيات، بحيث تخلق جوًا من الثقة بين الرؤساء والمرؤوسين، وبالتالي رفع الكفاءات والمهارات الإدارية بين العاملين.
2. ضرورة التأكيد على أن قدرة المنظمات لتوفير المعلومات اللازمة بسرعة، تعتبر المطلب الأساسي لترشيد عملية اتخاذ القرارات.
3. أهمية توخي الدقة والحذر عن اتخاذ القرارات الأمنية، لما لها من خصوصية عند كافة المنظمات الأمنية الأخرى.
4. يجب أن يخضع القرار الأمني لضوابط معينة تتمثل في الالتزام بالتعليمات العليا الصادرة عن القيادة، والالتزام بقيم المجتمع.
5. تأكيد الاهتمام بعنصر الوقت، وذلك من خلال إتباع أساليب الجدولة الزمنية والمتابعة الدورية للقرارات الصادرة.

[1] العبد القادر محمد علي, **عملية اتخاذ القرارات**, رسالة ماجستير غير منشورة, المركز العربي للدراسات الأمنية والتدريب, الرياض, 1989, ص63.

الفصل الثاني

دراسة الحالة حول الثغرة الأمنية / الاستخباراتية

المبحث الأول :تدخل الاستخبارات الروسية في الانتخابات الرئاسية الأمريكية

المبحث الثاني : التحديات التي تواجهها منظومة الاستخبارات الأمريكية

المبحث الثالث : أشكال عملية استجابة الاستخبارات الأمريكية

تمهيد :

لم يحدث أن تدخلت دولة أجنبية في الانتخابات الرئاسية الأمريكية كما تفعل روسيا اليوم, و لم يحدث أن كان هناك مرشح لحزب سياسي أساسي متعاطف مع تلك الدولة كما هو الحال الآن مع المرشح الجمهوري دونالد ترامب, فخلال السباق الطويل إلى البيت الأبيضأصر ترامب بمطالبته بتحسين العلاقات مع روسيا و الثناء على الرئيس الروسي فلاديمير بوتين, كما دافع عن روسيا ضد الاتهامات بأنها اخترقت الحسابات الالكترونية للحزب الديمقراطي و غيره من المؤسسات الأمريكية, كما حدث حين تم اختراق البريد الالكتروني لمدير حملة كلينتون, و تسليم الرسائل الالكترونية إلى مؤسسة ويكيليكس التي وزعتها أولا على وسائل الإعلام الروسية التي تمولها الدولة.

على الرغم من أنأجهزة الاستخبارات الأمريكية التي تلتقي دوريا بالمرشحين للرئاسة هيلاري كلينتون و دونالد ترامب, لاطلاعهما على أهم ما يحدث في العالم و خاصة الأخطار المحتملة ضد الولايات المتحدة الأمريكية, قد حذرت و أكدت للمرشحين بعد دراسة شاملة أن الاستخبارات الروسية مسؤولة عن هذه الممارسات[1].

كما كشف مؤخرا أن الاستخبارات الروسية تقوم بين وقت و آخر بتحوير بعض الوثائق, و ضمها إلىآلاف الوثائق الحقيقية التي يتم تسريبها, و عن كيفية وصول مثل هذه الوثائق إلى دونالد ترامب؟.

هذه الحادثة و مواقف دونالد ترامب الأخرى من روسيا تطرح أسئلة محيرة حول علاقة ترامب و حملته بالاستخبارات الروسية, و ما قد يأمل ترامب بتحقيقه من هذه العلاقة ؟, و ما إذا كانت لديه مصالح اقتصادية و عقارات في روسيا أم تلقى قروضا من كبار المسؤولين الروس كما يعتقد البعض.

المبحث الأول :تدخل الاستخبارات الروسية في الانتخابات الرئاسية الأمريكية

إذا كانت أجهزة الاستخبارات العالمية لا تتفق فيما بينها على صعيد العمليات التي تنفذها في سياق الملفات و القضايا التي تتابعها, إلاأنها تبدو متقاربة و متشابهة في العمليات الخارجية التي تقوم بها منذ نشوئها, حيث انه يمكن القول أن العولمة مع ما حملته من تطور كبير على صعيد تكنولوجيا المعلومات, سمحت بابتداع و تحديث أساليب التجسس بشكل يسمح للعدو أن يتخطى حدود الدول الكلاسيكية, و يتمكن من اختراق دفاعات الخصم بما يسمح له بتحقيق نتائج عجزت الوسائل التقليدية

[1] هشام ملحم, **الدور الروسي في الانتخابات الأمريكية**, على الموقع الالكتروني http://www.alarabiya/documents.com:أو على الرابط التالي http://ara.tv/y87r:, تاريخ النشر : 2016/10/12, تاريخ الاطلاع عليه : 2017/02/09 على 08 : 10 مساء.

الاستخباراتية في تحقيقها في الماضي, و هذا ما حصل في الانتخابات الأمريكية بعد إشارة التدخل الروسي فيها الكترونيا.

تكفي هذه المقاربة – المقارنة اليوم لتبيان و معرفة الخلفيات التي سمحت بجعل خطوط التماس مشتعلة استخباراتيا بين الولايات المتحدة الأمريكية و روسيا, على خلفية اتهام أجهزة الاستخبارات الأمريكيةلأجهزة الاستخبارات الروسية بالنجاح في عمليات القرصنة التي تزامنت مع الانتخابات الرئاسية التي جرت في الولايات المتحدة, الأمر الذي اثر في نتائج هذه الانتخابات و هو ما ينفيه الرئيس دونالد ترامب انطلاقا من الواقع المتحكم بالنظم الانتخابية في الولايات المتحدة, و هذا ما لا يتفق حوله معظم الخبراء و الباحثين الأمريكيين, وهو أن مسالة التأثير في الانتخابات لا تعدو كونها عملية غير مباشرة انطلاقا من عوامل عدة نذكر منها :[1]

أولا :إذا كان الرئيس المنتخب يتمسك بموقفه الذي يستبعد فيه تأثير القرصنة الروسية على نتائج الانتخابات, فان هذا الموقف يتفق عليه معظم القادة و المسؤولين الأمريكيين من كلا الحزبين الجمهوري أو الديمقراطي, فلا إمكانية لتزوير على نطاق ضيق أو واسع في أي انتخابات أمريكية طالما أنها انتخابات مباشرة من الطبقة و القاعدة الشعبية, و التصويت الفردي الحر هو الذي يميز نظام الاقتراع في الولايات المتحدة, و أنالآلية الحزبية تترك حرية الاختيار فلا محاسبة أوتأنيب على أي تصرف أو قرار قد يتخذونه في التصويت.

ثانيا :إذا كانت اتهامات أجهزة الاستخبارات الأمريكية لروسيا بقرصنة الحسابات الالكترونية لعدد من قيادات الحزب الديمقراطي, مثبتة بفعل سلسلة تحقيقات قامت بها هذه الأجهزة, فانه إلى جانب تأكيد الاختراق التقني من قبل الاستخبارات الروسية تبقى الاتهامات بالتدخل من اجل التأثير في الانتخابات, اتهامات سياسية بامتياز تفتقر إلى الدليل الحسي حول كيفية تغيير نتائج عملية الاقتراع لصالح الرئيس الحالي دونالد ترامب, لدرجة أن نائب الرئيس الأمريكي جو بايدن الذي ترأس جلسة تثبيت تصويت الكلية الانتخابية و التصديق على انتخاب دونالد ترامب, لم يأخذ باعتراضات عدد من أعضاء الكونغرس الديمقراطيين الذين طالبوا بإلغاء نتائج التصويت في عدد من الولايات, مستندين في اعتراضاتهم إلى مبرر التدخل الروسي.

[1] **أبعاد و خلفيات دور الاستخبارات في الانتخابات و السياسة**, على الموقع الالكتروني http://www.almassira.com/subscribtion/signup/index: , تاريخ الاطلاع يوم : 2017/02/10 على 11: 29 ص.

ثالثا : بعد ثماني سنوات من وجود الحزب الديمقراطي في البيت الأبيض, مع ما تركه من انعكاسات شتى بفعل سلسلة أزمات داخلية و خارجية فان إرادة التغيير هي التي فرضت نفسها على الناخب الأمريكي, و هو بالتأكيدما أظهرته نتائج الاقتراع في عدد لا باس به من الولايات المتحدة التي كان يفترض أن تعود أصواتهاإلى المرشحة الديمقراطية هيلاري كلينتون, لكن النتيجة بكاملها كانت لصالح دونالد ترامب, و أن اكبر دليل على تلك الخسارة هو إقرار الرئيس باراك اوباما خلال اجتماع مغلق لعدد من المسؤولين بان وقوفه و دعمه لهيلاري كلينتون كان خطا, و أن الحزب كان يمكن أن يقود الحملة الانتخابية بشكل أفضل, وعليه في ضوء ذلك لم يكن أيمرشح من أي حزب تتوفر لديه أجواء التغيير لم يكن بحاجة إلى دعم خارجي لكي يحقق الفوز.

قبل كشف تقرير أجهزة الاستخبارات الأمريكية حول التدخل الروسي في الانتخابات, تحرك عدد من قادة الحزبين الجمهوري و الديمقراطي بمطالبة مكتب التحقيقات الفدرالي بفتح تحقيقات بشان علاقة دونالد ترامب بروسيا على اعتبارها جهة أجنبية معادية للولايات المتحدة الأمريكية, و التحقيق في شان تعاملات المدير السابق لحملة ترامب الانتخابية بول مانافورت Paul Manafort مع روسيا, و قد استقال مانافورت من إدارة حملة ترامب بسبب الكشف عن تعاملاته التجارية مع حكومة الرئيس الأوكراني المعزول فيكتور يانوكوفيتش حليف الرئيس الروسي فلاديمير بوتين, وكذلك أن المستشار السابق بحملة ترامب كارتر بايج Carter Page قد قام بزيارات سابقة إلى مسؤولين حكوميين روس.

كما قامت وكالات الاستخبارات الأمريكية بنشر قبل الانتخابات بيانا موحدا أعلنت فيه أن مسؤولين رفيعين في الحكومة الروسية قد أمروا بشن حملة من الهجمات الالكترونية و ذلك للتدخل في سير الانتخابات الرئاسية المقبلة, فان روجر ستون احد مستشاري ترامب كشف انه على تواصل مع ويكيليكس.

أهم مرتكزات الحرب الالكترونية الروسية – الأمريكية :

تعود بداية السبب الدافع للتدخل الروسي المباشر في الشأن السياسي الداخلي الأمريكي نظرا إلى تدخل هيلاري كلينتون و التي كانت على رأس وزارة الخارجية الأمريكية[1], في الانتخابات الرئاسية الروسية وتشجيعها و دعمها للاحتجاجات التي أعقبت الانتخابات الرئاسية الروسية الأخيرة في شهر مارس/آذارمن سنة 2012, و التي أعيد فيها انتخاب فلاديمير بوتين رئيسا لروسيا الاتحادية, فقد كانت

[1] داود عمر داود, **العامل الروسي في فوز ترامب**, على الموقع التالي www.raialyoum.com: , تاريخ النشر يوم : 2017/01/11, تاريخ الاطلاع عليه يوم : 2017/02/09 على 21 :08 مساء.

المعارضة الروسية و المنافسون الأربعة لبوتين قد شككوا في نزاهة العملية الانتخابية, و مع انه حصل على 65% من أصوات الناخبين الروس, إلاأن المعارضة اتهمته بتزوير النتيجة, و ترتب على ذلك مظاهرات حاشدة و واسعة احتجاجا على فوز فلاديمير بوتين, و قيام السلطات الروسية بحملة اعتقالات لقادة المعارضة الروسية مما زاد في وتيرة الاحتجاجات في ظل أجواء سياسية متوترة.

رغم تقبل الغرب عموما لنتيجة الانتخابات الروسية بما فيه البيت الأبيضالأمريكي, إلاأن وزارة الخارجية الأمريكية كانت دائمة التعبير عن قلقها العميق مما يتعرض له قادة المعارضة الروسية, الأمر الذي يوضح للدولة الروسية على انه تشجيع من وزيرة الخارجية الأمريكية هيلاري كلينتون على مزيد من المظاهرات في روسيا, و بالتالي زعزعة الاستقرار السياسي في روسيا الاتحادية.

- في يونيو/ حزيران 2015 قامت مجموعة "Cozy Bear" التي تعرف أيضا باسم "APT 29", و هي مجموعة من المخترقين الروس المحترفين, بحملة اختراق على خوادم الحزب الوطني الديمقراطي "Democratic National Committe", أو ما يعرف اختصارا (DNC) دون أن يكتشف الحزب هذا الاختراق[2].
- تنبه مكتب التحقيقات الفدرالي "Federal Bureau of Investigations (FBI) " إلى وجود هجمات على خوادم الحزب الديمقراطي, لكنه لم يشارك بأية تفاصيل و هو ما دفع بالحزب الديمقراطي بدوره إلى تجاهل هذه التحذيرات, لأنه لم يجد أي دلائل على وجود اختراقات على الخوادم, و بالتالي سار الاختراق و كان شيئا لم يكن[3].
- لسبب أو لأخر لم يذكر مكتب التحقيقات الفدرالي (FBI) احتمالية وقوف روسيا خلف هذا الاختراق, لكنه لو قام بذكر هذه المعلومة للحزب الديمقراطي لكان الأمر مغايرا تماما, أو على الأقل لسرع من التحقيقات في صحة هذه المعلومات التي لم تهمل أبدا, لكن الحزب الديمقراطي انتظر حتى شهر مارس/آذار من سنة 2016 ليكتشف وجود اختراق بالفعل و سرقة للبيانات و هو ما أدى إلى الاستعانة بشركة "CrowdStrike " لتامين الخوادم و حمايتها من مثل هذه الهجمات[4].

[2] **Why Security Experts Think Russia was behind the D.N.C breach,** national Security reports, Washington DC, Dec 2016.
[3] **US officials warned DNC of Hack months before party**, Center of Studies, Chicago, Sept 2016.
[4] **FBI took months to warns Democrats of Suspect Russian**, On the site: www.FBI.com.

- إصرار المخترقين الروس لم يكن له حد خصوصا أنهم مدعومون من قبل الحكومة الروسية (أجهزة الاستخبارات الروسية "FSB ")[5], و بالتالي قامت مجموعة جديدة تعرف باسم " Fancy Bear " أو "APT 28 " باختراق الخوادم الخاصة بالحزب الديمقراطي من جديد, و حملة المرشحة الرئاسية هيلاري كلينتون Hillary Clinton و اختراق و سرقة جميع الرسائل الالكترونية و تحديدا تلك الموجودة في حساب المدير و المسؤول عن الحملة الانتخابية جون بوديستا John Podesta.
- محاولة مكتب التحقيقات الفدرالي (FBI) تحذير الحزب الديمقراطي من هجمات جديدة تمت على الخوادم, لكن عدم ترك أي اثر على الخوادم أدى إلى زيادة الصعوبة و التعقيد من مهمة مكتب التحقيقات الفدرالي (FBI) و الحزب الديمقراطي في إمكانية تحديد طبيعة الاختراق أو حتى التأكد من وجوده بالأساس, لتنخفض أهمية التحذيرات حتى مايو/أيار سنة 2016, حينما أعلن رئيس الاستخبارات الأمريكية(DNI)جيمس كلابر James Clapper رسميا عن وجود اختراق بالفعل[1].
- لم تكن مهمة الحزب الديمقراطي و شركة "CrowdStrike " سهلة, و التي قامت بدورها بالانتهاء من عملية تامين الخوادم بشكل كامل مع منتصف شهر يونيو/ حزيران سنة 2016, و هو التاريخ الذي انتشرت فيه القضية في وسائل الإعلام الأمريكية للمرة الأولى[2].
- الرد الروسي كان قاسيا, فاحد المخترقين باسم "Guccifer 2.0 " قام بتسريب الرسائل الالكترونية من بريد هيلاري كلينتون, إضافة إلى تسريب مستندات خاصة بالحزب الديمقراطي على الانترنت[3], و الملفت للنظر أن الولايات المتحدة الأمريكية لم تتمكن من الاستجابة و مواكبة آخر الأحداث و التطورات بشكل رسمي, خصوصا أن مثل هذا الاختراق يعتبر تهديدا للأمن الوطني بحسب القانون الأمريكي.
- لم يكن الهدف من حملات الاختراق الروسية ضد الحزب الديمقراطي الأمريكي واضحا في البداية, كما أنها لم تكن مثبتة كذلك على أن مصدرها من روسيا بشكل قاطع, و التي أدت إلى حالة الهستيريا و الاحتقان و الفوضى التي ضربت الولايات المتحدة الأمريكية جراء اكتشاف الاختراق, مع عودة التعرض للاختراق من جديد و ذلك بتسريب أكثر من 200 ألف رسالة

[5] **Private Security Says Russia was behind John Podesta's Hack**, Intelligence Community reports, U.S, 2016.
[1] **National Intelligence Director : Hackers have targeted 2016 Presidential Compaigns** , Washington DC, USA, 2016.
[2] **Bears in Midts : Intrusion into the Democratic National Committee**, Party report, USA, 2016.
[3] **Trump, Putin, Russia, DNC/Clinton Hack**, Confidential documents, USA, 2016.

بريدية خاصة بالحزب الديمقراطي, لكن هذه المرة عبر موقع ويكيليكس Wikileaks[4], التسريب صادف يوم إعلان دونالد ترامب Donald Trump ترشحه للرئاسة و هو مرشح عن الحزب الجمهوري, في حين هيلاري كلينتون مرشحة الحزب الديمقراطي, و هو ما يوضح رغبة روسيا في فوز ترامب بشكل أو بأخر.

- بعد حملة التسريبات الجديدة, تأكد خبراء الأمن الرقمي في الولايات المتحدة الأمريكية و بعض المسؤولين فيها إلى جانب مكتب التحقيقات الفدرالي[5], أن روسيا هي من تقف خلف هذه الحملات مصرحين بشكل علني أن ما جرى هو تهديد للأمن الوطني من جهة, و تشويه مقصود لصورة هيلاري كلينتون من جهة أخرى, و ما كان من الحكومة الأمريكية سوى الصمت و التجاهل بعد اكتشاف حملات الاختراق الأولى.
- التقاعس أو العجز في الرد على هجمات روسيا من قبل الرئيس الأمريكي ربط بشكل أو بأخر ببعض الأمور السياسية العالقة, في مقدمتها القضية السورية و الذي يسعى إلى كسب ود الروس فيها للوصول إلى حل يرضي جميع الأطراف, و بالتالي لم يرغب الرئيس الأمريكي باراك اوباما في أن تشوب هذه المحاولات أية شائبة[1], مزيج جمع ما بين تردد الولايات المتحدة الأمريكية و قلقها من تعثر المحادثات بخصوص بعض القضايا السياسية العالقة, جعل روسيا الأمر الناهي في الشأن الداخلي الأمريكي, فهي و خلال سنة 2016 ساهمت بشكل كبير في نشر الدعاية والأخبار المؤيدة للرئيس الأمريكي المنتخب دونالد ترامب, و أخبارا أخرى محرجة و معادية لهيلاري كلينتون دون تجاهل المواقع و الحملات الممنهجة لبسط هذه المفاهيم بين أطياف الشعب الروسي, لإعلان دونالد ترامب حليفا محتملا قبل حتى وصوله إلى الحكم.
- قيام الولايات المتحدة الأمريكية في أكتوبر/ تشرين الأول من سنة 2016, أي قبل شهر من موعد الانتخابات الرئاسية, بالإعلان عبر الرئيس الأمريكي باراك اوباما أن روسيا تقف خلف الاختراقات[2].
- الرد الروسي عبر موقع ويكيليكس ببدء حملة جديدة لتسريب وثائق جديدة من بريد المسؤول عن حملة هيلاري كلينتون[3],حيث نجحت التسريبات التي استمرت بشكل يومي في تشويه صورة

[4] **Released Emails Suggest the D.N.C Derided the Sanders Compaigns**, USA, 2016.
[5] **Clinton compaign also hacked in Attacks**, washington post Press, November 2016.
[1] **U.S Wrestles with how to fight Back Against Cyberattacks, the future of cyberterrorism crime & justice international**, USA, march 2016.
[2] **Spy Agency Consensus Grows that Russia Hacked D.N.C , Protection of personal data in the united states**, New York, USA, 2016.
[3] **The Most revealing Clinton compaign emails in Wikileaks** on : www.wikileaks.org.com

كلينتون في أعين الشعب الأمريكي, و هو ما اضطرهم إلى التصويت فيما بعد لصالح دونالد ترامب.

- إجراء الرئيس الأمريكي في 31 أكتوبر 2016 مكالمة هاتفية مع الرئيس الروسي فلاديمير بوتين Vladimir Putin للحديث حول المشاريع النووية, حيث قام بتنبيه الرئيس الروسي حول الاختراقات و ضرورة عدم تكرارها[4], لكن على ارض الواقع تمكنت روسيا في الفوز بهذه الحرب بكل سهولة, فقد قامت بتسريب وثائق أظهرت هيلاري كلينتون و كأنها العدو الأول للولايات المتحدة الأمريكية من جهة, و بررت تلك الوثائق من جهة أخرى ببعض الأفعال التي قام بها دونالد ترامب في السابق, وهو ما اثر بشكل أو بآخر على سير الانتخابات الأمريكية التي فاجأت نتائجها الجميع, ففي وقت بدت فيه داخليا أن هيلاري كلينتون المرشحة الأوفر حظا, وصل الحزب الجمهوري و مرشحه دونالد ترامب إلى سدة الرئاسة, لتتوقف بشكل فجائي حملة التسريبات و الاختراقات في الولايات المتحدة الأمريكية.

أهداف روسيا من التدخل :

هناك مجموعة من المدارس و التوجهات المختلفة من الأفكار حول طبيعة هذه الاختراقات :

أولا :أن روسيا تسعى إلى إضعاف الولايات المتحدة الأمريكية من خلال إثارة الشكوك.

ثانيا :أن روسيا كانت تهدف فعليا إلى دفع بالمرشح دونالد ترامب إلى سدة الرئاسة الأمريكية.

ثالثا : قيام روسيا بشن حملات مماثلة في جميع أنحاء أوروبا, من خلال هجمات الكترونية و تسريبات انتقائية, مع هدف واضح هو تقويض الوحدة الغربية[1].

رابعا : ترى روسيا أنها واقعة تحت حصار الغرب الراغب في تدميرها و احتوائها, مما أدى إلى دعم القادة العسكريون الروس هذا الجيل الجديد من الحروب من خلال الدعاية و الهجمات على مواقع الانترنت, بهدف زعزعة استقرار الدول و تفكيكها من الداخل.

[4] **White house Confirms Pre-Election Warning to Russia over Hacking**, white house report, December 2016.

[1] فتحي التريكي, **حقيقة الاختراق الروسي للانتخابات الأمريكية**, الخليج الجديد , على الموقع الالكتروني www.newkhaleej.com: , صدور التقرير يوم : 2016/12/13 , تاريخ الاطلاع عليه يوم : 2017/02/09 على الساعة 37: 10 مساء.

ملاحظة : قد لا يتم توجيه كل المفاهيم الخاطئة من قبل روسيا, و لكن شائعات مختلف وسائل الإعلام المحلية و الدولية التي تبالغ في تقدير خطر التدخل الروسي في الانتخابات الأمريكية, تصب في مصلحة روسيا و تخدم هدفها في تقويض ثقة الأمريكيين في شرعية و نزاهة ديمقراطيتهم.

المبحث الثاني : التحديات التي تواجهها منظومة الاستخبارات الأمريكية

إن البنية التحتية الحساسة و الاقتصاد و الحياة الشخصية, و حتى الفهم الأساسي و التفاعل مع العالم أصبح أكثر تشابكا مع الانترنت و التقنيات الرقمية.

في بعض الحالات يستعمل العالم التقنيات الرقمية, بطريقة أسرع من القدرة على فهم العواقب الأمنية و تخفيف المخاطر المحتملة.

يستغل اللاعبون الحكوميون و غير الحكوميون شبكة الانترنت على نحو متزايد لتحقيق أهداف إستراتيجية, إن العديد من الحكومات المتوجسة من الدور الذي لعبته شبكة الانترنت في تقويض الاستقرار السياسي و تغيير الأنظمة تسعى لزيادة سيطرتها على المحتوى في "الفضاء السيبيري".

الاستخدام المتزايد للانترنت من اجل تحقيق الأهداف الإستراتيجية يفوق أيضا مدى تطور الفهم المشترك لقواعد السلوك, ما يؤدي إلى ارتفاع احتمالات القيام بحسابات خاطئة, و أيضا إلى سوء فهم قد يؤدي إلى تصعيد غير مقصود[1].

و مما يفاقم هذه التطورات حالة الشك و عدم اليقين التي تعيشها الولايات المتحدة الأمريكية في مواجهة تهديدات سيبيرية جديدة و غير متوقعة.

أما بالنسبة للاتجاهات و الأحداث التي يشهدها الفضاء الالكتروني, فان الخيارات التي ستتخذها الولايات المتحدة و الفاعلون الآخرون خلال السنوات المقبلة ستصوغ الفضاء الالكتروني لعدة عقود, مع احتمال كبير أن تترك أثارا عميقة على الأمن القومي الأمريكي.

[1] جيمس كلابر, **تقدير موقف التهديدات العالمية من قبل "مجتمع الاستخبارات الأمريكية" للجنة الاستخبارات بمجلس الشيوخ**, السفير للتوزيع و النشر, ترجمة شهاب الإدريسي, 2013, ص 7-8.

- **زيادة المخاطر على البنية التحتية الحساسة للولايات المتحدة الأمريكية :**

خلال العامين المقبلين, تقدر أجهزة الاستخبارات الأمريكية أن هناك احتمالا ضئيلا لوقوع هجوم سيبيري كبير يستهدف الأنظمة الالكترونية للبنية التحتية الحساسة للولايات المتحدة, مستوى الخبرة الفنية و التمرس العملاني اللازم من اجل القيام بهجوم بما في ذلك القدرة على خلق أضرارا مادية, سيكون بعيدا عن متناول معظم الجهات الفاعلة خلال هذا الإطار الزماني, أما الفاعلون السيبيريون المتقدمون مثل الصين و روسيا فمن المرجح أن يطلقوا مثل هذا الهجوم المدمر ضد الولايات المتحدة, خارج صراع عسكري أو أزمة يعتقدون أنها تهدد مصالحهم الحيوية, مع ذلك قد تشن دولة معزولة أو فاعلون غير حكوميون هجمات اقل تطورا, كشكل من أشكال الانتقام أو الاستفزاز, و يمكن لهذه الجهات الفاعلة الأقل تقدما لكن شديدة التحفز أن تصل إلى بعض الشبكات الأمريكية المحمية بشكل سيء من تلك التي تتحكم بالمهام الأساسية.

و على الرغم من قدرتها على بلوغ هذه النقاط الحساسة و التسبب في عواقب وخيمة, فان احتمال قدرتها على إحداث تخريب منهجي يبقى محدودا, في نفس الوقت هناك خطر يتمثل في أن الهجمات غير المتطورة قد تحقق نجاحات كبيرة, بسبب إعدادات و أخطاء النظام غير المتوقعة, أو بسبب الضعف في عقدة واحدة على الشبكة تمتد و تخرب أجزاء أخرى من النظام الشبكي, لقد اخترقت الاستخبارات و الأجهزة الأمنية الأجنبية العديد من شبكات الكمبيوتر الأمريكية العائدة للحكومة و قطاع الأعمال و المؤسسات الأكاديمية و هيئات القطاع الخاص, و قد استهدفت معظم النشاطات التي تم رصدها شبكات غير سرية متصلة بشبكة الانترنت, لكن الفاعلين الأجانب يستهدفون أيضا الشبكات السرية. الأهم من ذلك الكثير من البيانات الحساسة في الولايات المتحدة موضوعة على شبكات حساسة لكنها غير سرية.

أن قطاعات الأعمال المعتمدة بشكل كبير على الشبكات و على تكنولوجيا المعلومات توفر فرصا للاستخبارات و الأجهزة الأمنية الأجنبية, و الجواسيس الموثوقين الكامنين داخلها و المخترقون الذين يستهدفون جمع البيانات الحساسة عن الأمن القومي الأمريكي.

- **التحكم في المعلومات و إدارة الانترنت :**

مراقبة المعلومات على الانترنت قضية أساسية بين الولايات المتحدة و غيرها من الجهات الفاعلة[1].

تقوم بعض الدول و من ضمنها روسيا و الصين و إيران بالتركيز على " التأثير السيبيري", و احتمال أن يسهم المحتوى على شبكة الانترنت في تقويض الاستقرار السياسي و تغيير الأنظمة.

تركز الولايات المتحدة الأمريكية على امن الشبكة و على صلابة و سلامة شبكاتها و أنظمتها المعلوماتية, النموذج الحالي المتمثل في تعدد أصحاب المصالح القائمين على إدارة الانترنت يوفر منتدى للحكومات و القطاع التجاري و الأوساط الأكاديمية و المجتمع المدني, للتداول و الوصول إلى توافق في الآراء بشان تنظيم الانترنت و المعايير التقنية, في المقابل فان أي حركة لإعادة تشكيل إدارة الانترنت نحو نموذج حكومي وطني يتعارض مع العديد من أهداف سياسة الولايات المتحدة, ولا سيما تلك المتعلقة بالتدفق الحر للمعلومات و الخدمات.

شكلت هذه القضايا جزءا أساسيا من النقاشات خلال تفاوض دول العالم على معاهدة عالمية حول الاتصالات و التي عقدت بمدينة دبي بالإمارات العربية المتحدة, النص الجديد المثير للجدل دفع الكثير من الدول بما في ذلك الولايات المتحدة, إلى عدم التوقيع على المعاهدة بسبب اللغة التي اعتمدتها بشان امن شبكة الأمن, و مراقبة البريد الالكتروني و توسيع دور الأمم المتحدة في إدارة الانترنت, أظهرت المفاوضات أن الخلافات حول هذه القضايا ستشكل تحديات طويلة الأمد بوجه التعاقدات الثنائية و المتعددة الأطراف.

إن مراجعة إدارة الانترنت تقوم على نموذج حكومي في الإدارة يمكن أن يؤدي إلىإقرار تشريعات دولية تتحكم في المحتوى الموجود على الانترنت, و يقيد تبادل المعلومات عبر الحدود و يبطئ الابتكار التقني بشكل كبير, و يزيد من الفرص الماثلة في الشبكة الدولية أمام الاستخبارات الأجنبية و عمليات المراقبة في المدى القريب.

[1] جيمس كلابر, **تقدير موقف التهديدات العالمية من قبل "مجتمع الاستخبارات الأمريكية" للجنة الاستخبارات في مجلس الشيوخ**, مرجع سابق, ص 10.

- **دور الفاعلون الآخرون :**

تقوم أجهزة الاستخبارات الأمريكية بتتبع التطورات السيبيرية للفاعلين غير الحكوميين, و من ضمنهم الجماعات الإرهابية و المخترقون أو (الهاكرز) و مجرمو الانترنت, و قد رصدت مؤشرات على أن بعض الإرهابيين رفعوا من مستوى اهتمامهم بتطوير قدرات سيبيرية هجومية, و من المحتمل أنهم مقيدون بالموارد المحدودة و القيود التنظيمية و وضع الأولويات[1].

يستمر الهاكرز في عملية استهداف واسعة تشمل الشركات و المؤسسات عبر الهجمات الرامية إلى إيقاف الخدمة, معظم المخترقون يستخدمون عمليات إيقاف الخدمة لمدة قصيرة, أو ينشرون معلومات متعلقة بهم شخصيا على مواقع الشركات المقرصنة, كشكل من أشكال الاحتجاج السياسي.

و قد تتشكل مجموعة أكثر جذرية من اجل صنع تأثيرات أكثر منهجية مثل تعطيل الشبكات المالية, و قد تدفع بطريق الخطأ إلى عواقب غير مقصودة يمكن أن يساء تفسيرها على أنها هجوم ترعاه دولة ما, أما بالنسبة لمجرمو الانترنت فهم يهددون مصالح الولايات المتحدة الاقتصادية, و ذلك ببيع أدوات من خلال سوق سوداء متنامية, قد تمكن من الوصول إلى أنظمة البنية التحتية الحساسة, و قد تصل إلى لاعبين حكوميين و غير حكوميين, بالإضافة إلى ذلك فان عددا قليلا من الشركات التجارية تبيع لوازم الاختراق في السوق المفتوحة.

و يمكن لهذه الأجهزة و حزم البرمجيات أن تعطي الحكومات و مجرمي الانترنت القدرة على سرقة المعلومات في الأنظمة المستهدفة أو حذفها أو التلاعب بها, بل إن هناك شركات أخرى تطور و تبيع تقنيات ذات جودة احترافية تدعم العمليات السيبيرية, فالحكومات الأجنبية تستخدم بالفعل بعض هذه الأدوات من اجل استهداف أنظمة الولايات المتحدة.

[1] جيمس كلابر, **تقدير موقف التهديدات العالمية من قبل "مجتمع الاستخبارات الأمريكية" للجنة الاستخبارات في مجلس الشيوخ**, مرجع سابق, ص11.

- **مكافحة التجسس:**

تستهدف أجهزة الاستخبارات الأجنبية الحصول على معلومات الأمن القومي الأمريكي و تقويض المزايا الأمنية و الاقتصادية و التكنولوجية, و السعي إلى التأثير على السياسات الوطنية للولايات المتحدة بطريقة سرية جدا[1].

هذه الجهود الاستخباراتية الأجنبية توظف الأساليب التقليدية للتجسس, مع استخدام متزايد للوسائل التقنية المبتكرة.

بين التهديدات الخارجية البارزة, تبقى روسيا و الصين مصدرين للتهديدات الاستخباراتية الأكثر قدرة و ثباتا و الأشد عدوانية في ممارسة التجسس الأمني و الاقتصادي ضد الولايات المتحدة, مواجهة مثل هذه التهديدات الاستخباراتية الخارجية يمثل أولوية قصوى لأجهزة الاستخبارات الأمريكية, كما تشكل نقاط الضعف في امن الشبكات العالمية فرصا للخصوم لاستغلال البنية التحتية الحرجة للولايات المتحدة.

إن الاعتماد على معدات أجنبية مع مجموعة من الموردين المتعاقدين في مجال تكنولوجيا المعلومات و الاتصالات السلكية و اللاسلكية و الطاقة, يخلق فرصا لاستغلال الأنظمة و البنية التحتية الحرجة للولايات المتحدة و زيادة التأثير عليها.

الترابط بين تكنولوجيا المعلومات و تكامل التكنولوجيا الأجنبية ضمن تكنولوجيا المعلومات لدى الولايات المتحدة, سيرفع من احتمال و مدى تأثير الاستخبارات الخارجية و العمليات الأمنية التي يمكن أن تستهدفها, إن التوطيد المرجح استمراره للبنية التحتية و الذي يعني أن الشبكات و البنى التحتية الحرجة ستبنى من مجموعة أكثر محدودية من الخيارات و المعدات, سيزيد أيضا من مدى و تأثير المخاطر المحتملة.

[1] جيمس كلابر, **تقدير موقف التهديدات العالمية من قبل "مجتمع الاستخبارات الأمريكية" للجنة الاستخبارات في مجلس الشيوخ**, مرجع سابق, ص 23.

- **حرب الفضاء:**

نظم الفضاء و البنى التحتية الداعمة لها توفر مجموعة واسعة من الخدمات, بما في ذلك الاتصالات و عمليات تحديد المواقع و الملاحة و التوقيت و العمل الاستخباراتي و المراقبة و الاستطلاع, و هي التي تقوم بتامين المصالح الوطنية الحيوية منها : العسكرية و المدنية و العلمية و الاقتصادية.

تدرك الدول الأخرى هذه الفوائد التي تعود على الولايات المتحدة الأمريكية و هي تسعى لتقويض ميزة التقدم الاستراتيجي للولايات المتحدة, من خلال توظيف إمكانياتها من اجل حرمان أو تدمير قدراتها على الوصول للخدمات الفضائية[1].

إن نسبة زيادة التهديدات الموجهة نحو الخدمات الفضائية الحيوية الأمريكية خلال العقد المقبل, مع تطوير القدرات المضادة التخريبية و الهدامة.

و في مقال صحفي نشر في سنة 2015, تصريح لمسؤول عسكري روسي رفيع المستوى بان روسيا تطور قدراتها في مجال حرب الفضاء.

المبحث الثالث : أشكال استجابة الاستخبارات الأمريكية

صرح زعيم الديمقراطيين في لجنة الاستخبارات بمجلس الشيوخ مارك وارنر " ستقاس ديمقراطية أمريكا جزئيا بالكيفية التي سنرد بها, و الخطوات التي نتخذها لتطوير إستراتيجية الكترونية قوية و استباقية ".

و قال النائب ادم شيف زعيم الديمقراطيين بلجنة الاستخبارات في مجلس النواب " انه يجب على الكونغرس الشروع في تحقيقات شاملة لتحديد ما حدث و كيفية حماية الحكومة الأمريكية ".

بعد صدور تقرير رئيس الاستخبارات الأمريكية حول القرصنة الروسية للانتخابات الأمريكية, قيام الرئيس باراك اوباما بإصدار أوامر بطرد 35 دبلوماسيا روسيا على خلفية علاقتهم و مساهمتهم بالاختراق و التدخل المباشر و التأثير على سير الانتخابات الأمريكية.

[1] جيمس كلابر, **تقدير موقف التهديدات العالمية من قبل "مجتمع الاستخبارات الأمريكية" للجنة الاستخبارات في مجلس الشيوخ**, مرجع سابق, ص 25.

تلتها أيضا سلسلة من الإجراءات الردعية منها فرض عقوبات اقتصادية على روسيا و فرض تقييد السفر على بعض المسؤولين الروس رفيعي المستوى.

تصريح الرئيس دونالد ترامب بعزمه على إعادة هيكلة واسعة النطاق و التي تشمل أجهزة الاستخبارات الأمريكية بما فيها وكالة الاستخبارات الوطنية (DNI) و أيضا وكالة الاستخبارات المركزية (CIA).

و من عجيب المفارقات أن ردع الدول عن استخدام القوة ربما يكون أسهل من ردعها عن تصرفات لا ترقى إلى هذا المستوى, و لعل التهديد بشن هجوم مفاجئ كان مبالغا فيه, صحيح أن البنية الأساسية الحرجة مثل الاتصالات عرضة للخطر, لكن الدول الكبرى من المرجح أن تكون مقيدة بفعل الترابط المتبادل, و قد أوضحت الولايات المتحدة أن الردع لا يقتصر على الانتقام السيبراني و لكنه من الممكن أن يستهدف قطاعات أخرى بأي أدوات تختارها من التشهير و العقوبات الاقتصادية إلى الأسلحة النووية[1].

و قد وافقت الولايات المتحدة الأمريكية و غيرها من الدول, بما في ذلك روسيا على أن القوانين التي تحكم النزاع المسلح تنطبق على الفضاء السيبراني, و تتوقف كيفية التعامل مع العمليات السيبرانية باعتبارها هجوما مسلحا على نتائجه, و ليس على الأدوات المستخدمة.

في سنة 2015 , وافقت مجموعة من الخبراء الحكوميين تابعة للأمم المتحدة ضمت الولايات المتحدة, روسيا, الصين, و اغلب الدول التي تمتلك قدرات سيبرانية كبيرة, على قاعدة تتلخص في عدم استهداف المرافق العامة في زمن السلم, و أقرت دول مجموعة العشرين هذه الاتفاقية في القمة التي استضافتها تركيا في نوفمبر/ تشرين الثاني لسنة 2015 [2].

كما بذلت إدارة الرئيس باراك اوباما الجهود لتصنيف خطورة الهجمات السيبرانية, و في سنة 2016 واجهت إدارة الرئيس اوباما اختبارات صعبة في تقدير الإمكانات التصعيدية للرد بتدابير سيبرانية أو استجابة تؤثر على قطاعات مختلفة مثل العقوبات, و لم تكن الإدارة راغبة في اتخاذ خطوات ربما تؤدي في حد ذاتها إلى عرقلة الانتخابات الأمريكية.

[1] جوزيف ناي, **الكرملين و الانتخابات الأمريكية**, مركز الجزيرة للدراسات, على الموقع الالكتروني: http://www.aljazeera.net/documents/index , تاريخ النشر: 2016/12/11 , تاريخ الاطلاع : 2017/02/21 على 07: 42 مساء

[2] جوزيف ناي, نفس المرجع.

كما أرسلت الولايات المتحدة قبل ثمانية أيام من التصويت تحذيرا إلى روسيا بشان التدخل في الانتخابات عبر خط خاص, أنشئ قبل ثلاث سنوات للتعامل مع أحداث سيبرانية كبرى و الذي يربط بين مراكز الحد من المخاطر النووية لكلا البلدين.

و لان أنشطة الاختراق السيبراني الروسية بدت و كأنها تباطأت و توقفت, اعتبرت الإدارة الأمريكية التحذير ممارسة ناجحة في الردع, لكن بعض المسؤولين أكدوا أن الروس حققوا بالفعل هدفهم.

خاتمة الفصل :

و من خلال ما تم ذكره في هذا الفصل, يمكن القول أن الحرب الالكترونية بين روسيا و الولايات المتحدة الأمريكية لم تنته بفوز الروس, لكنها أدت إلى تقسيم الشعب الأمريكي بشكل كبير و تقويض الإيمان الشعبي بالعملية الديمقراطية و إضعاف ثقته بالنظام الانتخابي الأمريكي, كما أدت إلى ارتباك كبير حول مستوى حماية النظام الرئاسي و السياسي للولايات المتحدة الأمريكية و عن مدى قدرتها على مواجهة حروب من هذا النوع في المستقبل.

و هذا يوضح إستراتيجية روسيا في التدخل المباشر في الدول الأخرى, و التي أصبحت سمة من سمات سياستها, مم يعني أنها ستنطلق خارجيا في تدخلاتها العسكرية كما حصل في سوريا, و تدخلاتها السياسية كما حصل في الانتخابات الأمريكية و كما يحصل الآن في أوروبا و خاصة ألمانيا التي تشكو من تدخل روسيا التي تستهدف زعزعة استقرارها بهجماتها الالكترونية على الأحزاب السياسية الألمانية.

الفصل الثالث

تقييم أداء الاستخبارات الأمريكية مع الثغرات الأمنية

المبحث الأول : نماذج من ثغرات أمنية سابقة

المطلب الأول : تحليل أداء الاستخبارات الأمريكيةمنذأحداث2001/09/11

المطلب الثاني : تحليل أداء الاستخبارات السيبرية

المبحث الثاني : إستراتيجية مواجهة الثغرات الأمنية ذات الطابع المعلوماتي

تمهيد :

يخضع أداء الاستخبارات الأمريكية لجدل عنيف و مكثف للعديد من الأسباب, و ذلك بطلب مراجعة شاملة لاحتياجات الاستخبارات في بيئة تهديد متغيرة, فقد أصبح الوقت متاحا أمام الخبراء و صانعي السياسة لتطوير فهم جديد بشان كيفية جمع المعلومات ذات الصلة باحتياجات صانعي السياسة في القرن الحادي و العشرين و تنظيمها و تحليلها, و لم تؤدي تجربة إعادة التفكير في الأساسيات من التخطيط إلى التقنية إلى الأفراد إلى أي تغييرات مهمة في الاستخبارات, لان توصياتها غالبا ما كانت صعبة التطبيق بسبب وقوع أحداث أيلول/ سبتمبر 2001.

أدت الهجمات الإرهابية على الولايات المتحدة الأمريكية و الشعور المتراكم بوجود أزمة قومية, و فشل التحذير بإمكانية حدوث هجمات إرهابية, إلى خلق بيئة جديدة تماما لمراجعة أداء الاستخبارات الأمريكية و نقاط قوتها و ضعفها, و العديد من الأفكار حول كيفية إصلاح مجموعة الهيئات و الوكالات و المكاتب التي تشكلها أو تغييرها.

و من الجدير بالذكر انه من غير العادي أن تكون القدرة على التحقق من أجهزة استخبارات أي دولة و أدائها بمثل هذه الطريقة من الانفتاح و التفاصيل, إن ذلك في الواقع يشكل مثالا أخر على المنهجية الأمريكية المتميزة, و هي طريقة تطور المؤسسات السياسية الأمريكية و سياستها و ممارساتها كان ذلك للأفضل أو الاسوا بطرق تتسم بالتميز, فالصرامة و النقد للبيروقراطية الاستخباراتية الأمريكية و أدائها الأخير, فهذا يعني كذلك الاعتراف بالشفافية الاستثنائية للنظام الأمريكي[6].

المبحث الأول : نماذج من ثغرات أمنية سابقة

المطلب الأول : تحليل أداء الاستخبارات الأمريكية منذ أحداث 2001/09/11

لقد خلقت ثورة المعلومات ضغوطا جديدة و فرضت الدخول في جدلية مهمة بشان ماهية الاستخبارات و ماهية المعلومات و احتمالية القدرة على القرار ما المطلوب في وضع معين أو عدم القدرة على ذلك.

إن تعقب اللاجئين في مناطق الحروب قد يشكل مهمة معلوماتية يمكن أن تناط بوكالة الاستخبارات أو مؤسسة غير حكومية منافسة, كذلك يمكن تحقيق مراقبة خرق العقوبات بصورة سرية أو بالوسائل

[6] **"Fixing Intelligence"**, Foreign Affairs, vol 81, no 1, (January/February 2002), p44.

الأكثر علانية, فان توافر النفاذ السريع إلى المعلومات الخام عبر شبكة الانترنت و القنوات الفضائية و غيرها من الأجهزة و الوسائل و أدوات عصر المعلومات تجعل الرجوع إلى أساسيات ماهية الاستخبارات, و كيف يمكن أن تقدم الاستخبارات أفضل خدمة ممكنة لصانعي السياسة.

تتطلب قضيتا الاستخبارات و هما التعامل مع التحديات الإرهابية الدائمة, و فهم دور الاستخبارات و في الواقع تمثل الحالتين شكلين مختلفين من التحديات بالنسبة إلى الاستخبارات الأمريكية, فالشكل الأول يتعلق بكيفية تعامل الاستخبارات مع تنامي التهديدات و استمرارها لدى جهات متنقلة غير حكومية و مدمرة, أما الشكل الثاني فهو مشكلة استخباراتية تقليدية, أي تعقب قدرات الخصم العسكرية القائمة في مكان محدد جغرافيا, و بمقارنة الحالتين يمكن الحصول على فرصة التحقق من سلسلة من القضايا الاستخباراتية, كذلك يمكن للمقارنة أن توضح الطريق التي يعتقد الخبراء و السياسيون أنها تستطيع إصلاح الخلل, و أخيرا تقتضي دراسة الحالتين التفكير بالعلاقة الغامضة بين الاستخبارات و السياسة, كما تسلط الضوء على دور المعلومات الاستخباراتية في مجتمع منفتح و غني بالمعلومات.

في تموز/ يوليو 2003 نشرت لجنة مجلس الشيوخ لشؤون الاستخبارات و لجنة الكونغرس الدائمة حول الإرهاب نتائج التحقيق الذي استمر 18 شهرا حول نشاطات قطاع الاستخبارات الأمريكية المتعلقة بهجمات 11 أيلول/ سبتمبر, و يضم التقرير الذي لم ينشر منه جزء بسيط لدواعي السرية إلى أكثر من 800 صفحة[1], و يتضمن معلومات مفصلة عما كان معروفا في أوساط مختلفة داخل الحكومة الأمريكية قبل الهجمات, و كذلك الإخفاقات المنهجية التي أدت إلى عدم المشاركة بالمعلومات بطريقة ايجابية, و التي ربما كان من الممكن أن تمنع وقوع الهجمات أو تضع الحكومة الأمريكية في وضع أفضل لتتهيأ لهذه الهجمات و تخفف من تأثيرها, إن نتائج لجنة التحقيق المشتركة حول أداء الاستخبارات قوية و متزنة, و جاء فيها : " قبل 11 أيلول/ سبتمبر لم يكن قطاع الاستخبارات منظما أو مجهزا بشكل جيد, كما لم يكن متكيفا بصورة مناسبة لمواجهة التحدي الذي شكله الإرهاب العالمي الذي ركز على أهداف داخل الولايات المتحدة الأمريكية[2], لقد كانت هناك ثغرات حقيقية بين التغطية الجماعية التي توفرها القدرات الاستخباراتية الأمريكية الخارجية و الداخلية, و لم تولي وكالات الاستخبارات الخارجية الأمريكية احتمال حدوث هجوم داخلي الاهتمام المناسب, و قد فاقمت هذه المشكلات بصورة كبيرة من

[1] النص الكامل على الموقع التالي www.gpoaccess.gov/serialset/creports/911.html:

[2] أيلين ليبسون, **الاستخبارات الأمريكية بعد الحادي عشر من سبتمبر : سد الثغرات**, مركز الإمارات للدراسات والبحوث الإستراتيجية, ط1, أبو ظبي, 2005, ص 11.

مدى تعرض الأمة إلى تهديد إرهابي دولي خطير و مباشر داخل الولايات المتحدة الأمريكية بصورة متزايدة ".

تتمتع وزارة الأمن الداخلي الجديدة التي انشات لدواعي الضرورات البيروقراطية و السياسية لإصلاح أوجه القصور الحكومي في معالجة مشكلة الإرهاب, بوظيفة استخباراتية جديدة و مسؤولية تحذير الرئيس الأمريكي من تهديدات داخل الأراضي الأمريكية, و يطلق على المديرية التي انيطت بها هذه الوظيفة اسم "مديرية تحليل المعلومات و حماية البنية التحتية IAIP ", و مهمتها فهم نقاط الضعف في مواقع البنية الحساسة في الدولة و التحليل المتكامل للتهديدات الواردة من الاستخبارات و مصادر المعلومات العامة, و تحذير الدولة من حيث مستوى التهديد الذي قد تتعرض له[1].

كما تم إنشاء مركز موحد لمراكز تحليل الإرهاب و يطلق على هذا المركز اسم " المركز الموحد للتهديد المتنقل TTIC ", و يقوم بجمع كل الخبرات المتعلقة بالإرهاب من دوائر الاستخبارات المدنية و العسكرية, و إغلاق أي ثغرة أو فجوة بين المصادر الخارجية و الداخلية للمعلومات حول الإرهاب, أما هدف "المركز الموحد للتهديد المتنقل" هو خدمة مركز القرار في الحكومة الأمريكية حول كافة الأعمال التحليلية المتعلقة بالتهديدات الإرهابية[2], و سوف تثبت هذه التغييرات المؤسسية التي واجهت بعض المعارضة و التشكيك في الكونغرس, أنها مفيدة في استيعاب الطاقة و الأفكار داخل النظام البيروقراطي, كما أن البيروقراطيات الكبيرة لها بيئة دائمة تعيق ذلك النوع من خفة الحركة و التعاون مع الأخر الذي ربما كان سيمنع هجمات 11 أيلول/ سبتمبر, التي تواجه التحديات المؤكدة و الدائمة في محاولتهم إعادة التركيز على الموهبة الاستخباراتية و التقنية بطرق جديدة.

إن استهداف الاستخبارات للإرهاب يتطلب على الأقل أنواعا مختلفة من المهارات و هي الحاجة إلى الاهتمام المتأني و الدقيق بالتفاصيل, و الجزئيات لمواد متداخلة مع مواد غير ذات صلة من الأنماط و الروابط, و الحاجة إلى التفكير بشكل استراتيجي و مفاهيمي نظري لتجاوز الثقافة الخاصة و تخيل عالم من القيم و الأهداف, مختلفا كل الاختلاف من اجل التوقع كيف يستطيع الإرهابي النشيط أن يضرب ضربته التالية؟ و متى؟, و قد وجد أن هاتين المهارتين كانتا مطلوبتين للعمل في الاستخبارات الأمريكية قبل 11 أيلول/ سبتمبر, على الرغم من أن قادة أجهزة الاستخبارات الأمريكية شددوا جدا على الأولوية العالية و القصوى لجمع المعلومات و النشاطات ذات العلاقة بالعمليات الإرهابية, و بذلت جهود كبيرة

[1] **وزارة الأمن الداخلي الأمريكية** على الموقع التالي www.dhs.gov :
[2] **كلمة ونستون ويلي, أمام لجنة الشؤون الحكومية التابعة لمجلس الشيوخ في 26 فبراير 2003** , على الموقع التالي :http://www.cia.gov/cia/public_affairs/speeches/2003/wily_speech_02262003.html

لاستخدام التقنيات الجديدة لمسح كميات هائلة من البيانات و تصويرها لمحاولة تحديد ما هو مهم و إدراكه أو يستوجب التصرف بلغة السياسة و الاستخبارات الخاصة.

يرى معظم صانعي القرار الحكوميين أن الاستخبارات تستند إلى الدليل و أن هذا العمل الفعلي أو التكتيكي المتعلق بالهدف الإرهابي تقرره قواعد و ممارسات رفع التقارير بشان ما هو معروف و التمييز بين الحقائق و التوقعات في الحرب على الإرهاب, و في جانب أخر ثمة ادعاء أن قطاع الاستخبارات الأمريكية لم تقم بواجبها في مجال التنبؤ بالخطوات التالية أو تصور سيناريوهات جديدة للهجمات الإرهابية ضد الولايات المتحدة الأمريكية, و هذا الأمر يتطلب نوعا أخر من العمل التحليلي و يدعى بالتحليل الاستراتيجي, و يستند هذا التحليل إلى منهجية مختلفة تماما لا تعتمد على الدليل التجريبي, و إنما على تكامل البيانات الجزئية مع الخبرة الإقليمية و التفكير المجرد للتنبؤ بالمسارات المستقبلية المحتملة لعمل الخصم غير المفهوم بشكل تام, و تطوير كل هذه المنهجيات و الأساليب لفهم هذا السلوك[1].

قبل 11 أيلول/ سبتمبر كانت هناك وصفة تفيد بان اليد العاملة لاثنتي عشر وكالة تشكل قطاع الاستخبارات الأمريكية بحاجة إلى إعادة تجهيز و تنظيم, و إلى وضع مجموعة جديدة من الأولويات غير أن تحقيق التوافق حول هذه الأولويات لم يحدث حتى الآن, إذ يجب أن يكون التركيز عالمي لقطاع الاستخبارات و أن تكون مستعدة للاستجابة لمطالب صانعي السياسة حول أي موضوع, بدءا من مناطق الصراع التقليدية إلى القضايا المتحولة الجديدة و أن التوصل إلى انتقائية اكبر هو المطلوب, و أن قطاع الاستخبارات يجب أن تركز جهودها على القضايا التي تعتبر سرية بالفعل و أنها الوحيدة الذي يمكنها توفير المعلومات و الرؤية, و أن يتركز اهتمام الاستخبارات بجمع المعلومات و تحليلها بصورة كبرى على البرامج السرية و طبيعة عمل المنظمات الإرهابية و السياسات و السلوك لدى الأعداء أو الدول المعادية, و لأي من هذه المناهج تبعات و نتائج بالنسبة إلى القوة العاملة و كذلك لأي من المهارات و الخلفيات التي يجب تقويمها[2].

[1] أيلين ليبسون, **الاستخبارات الأمريكية بعد الحادي عشر من سبتمبر : سد الثغرات**, مرجع سابق, ص 16.
[2] أيلين ليبسون, **نفس المرجع**, ص 17-18.

المطلب الثاني: تحليل أداء الاستخبارات السيبرية

يرى جوزيف ناي صاحب مفهوم "القوة السيبرية" (Cyber Power) أن الدولة مازالت الفاعل الرئيسي على الساحة الدولية, و لكن هذه الساحة أصبح من الصعب التحكم فيها و ذلك نتيجة التهديدات الأمنية الجديدة الناتجة عن التطورات التكنولوجية المتسارعة[1], و نتيجة لهذه المخاطر ظهر ما يسمى ب" السياسات السيبرية (Cyber Politics) ", سواء في إطار استغلال الفضاء الالكتروني لتحقيق مكاسب سياسية أو اقتصادية أو عسكرية, أو محاولة الدولة في أن تعظم من نفوذها على الساحة الإقليمية و الدولية, أو حتى في إطار تنظيم الفوضى الناتجة عن تخبط المعلومات و تداخل أطراف أخرى غير الدولة للسيطرة عليها و لكن قدرة الدول على تنفيذ هذه السياسات مازالت قيد النقاش.

مفهوم الاستخبارات السيبرية Cyber Intelligence : يعد مفهوم الاستخبارات السيبرية من المفاهيم الغامضة و ذلك لعدم وجود تعريف محدد له و تداخله مع مفاهيم أخرى مرتبطة بالفضاء الالكتروني, لكن يمكن تعريفه بصفة عامة على انه نتاج عملية جمع و معالجة و تكامل و تقييم المعلومات المتاحة على الفضاء الالكتروني و تحليلها و تفسيرها, كما يشمل القوى المعادية المحتملة و مناطق العمليات الفعلية أو المحتملة و المنظمات المنخرطة في هذه الأنشطة, و ذلك بهدف جمع و معالجة و تحليل و استخدام المعلومات لتلبية هدف محدد, أي انه يشمل عدة خطوات تتمثل في عملية جمع المعلومات الاستخباراتية و مكافحة التجسس و التهديد الاستخباراتي عبر الفضاء الالكتروني[2], و يختلف هذا المفهوم عن المفاهيم المرتبطة بجمع المعلومات من المصادر المفتوحة و المتاحة عبر الانترنت, مثل إشارات الاستخبارات(Signals Intelligence : SIGNIT)[3] , أو(Open Source Intelligence : OSINT) .

كما ذهبت اتجاهات أخرى لتعرفه انه " المعرفة المتوفرة عن خصوم الدولة في الفضاء الالكتروني و أدواتهم, بالإضافة إلى المعرفة بالوضع الأمني للمنظمة في مواجهة خصومها و أدواتهم و هو الأمر الذي يمكن للدولة أو المنظمة في النهاية من اتخاذ القرارات و تنفيذها", لكن هذا التعريف عام إذ انه يختلف من منظمة استخباراتية إلى أخرى, وفق لحجمها و مدى التعقيد و التشابك في القرارات التي تتخذ و مجال جمع المعلومات و طبيعة الأعداء, و قدم تعريف أخر للاستخبارات السيبرية هو "امتلاك و تحليل

[1]Joseph S. Nye, **The Reality of Virtual Power**, Moscow Times, February 4, 2012, accessible at : http://www.themoscowtimes.com/opinion/article/the-reality-of-virtual-power/430367.html.
[2] Developing Your Cyber Intelligence Analyst Skills, **The State of Security**, jan 27, 2014, accessible at : http:/www.tripwire.com/state-of-security/security-data-protection/developing-cyber-intelligence-analyst-skills/
[3] Operational Levels of Cyber Intelligence, **Intelligence Levels of Cyber Intelligence, Intelligence and National Security Alliance**, September 2013.

المعلومات لتحديد و تتبع و التنبؤ بقدرات الخصوم في الفضاء الالكتروني, و كذلك الإلمام بنواياهم و أنشطتهم و هو الأمر الذي يساعد على إيجاد خيارات مختلفة للحركة تدعم عملية صنع القرار"[1].

و مع قيام " ادوارد سنودن" الموظف السابق في وكالة الأمن القومي الأمريكية (NSA) بكشف العديد من الوثائق التي تدين الولايات المتحدة و بعض الدول بالقيام بعمليات التجسس و استخبارات السيبرية واسعة النطاق, بدأت تتضح الرؤية حول سعي الدول لتوظيف الأنشطة الاستخباراتية في الفضاء الالكتروني, لتشمل ليس الدول فقط بل و الحركات و الجماعات و الشخصيات المهمة و حتى الأفراد العاديين, و بات الصراع الرئيسي بين الدول ليس من اجل امتلاك الموارد المادية و إنما للحصول على المعلومة التي باتت سلاحا جديدا في مواجهة الدول, خاصة في ظل الكم الهائل من المعلومات[2].

و في هذا الصدد يمكن تحليل أنماط الاستخبارات السيبرية المختلفة وفقا لطبيعة الهدف من عملية جمع المعلومات, فقد تكون عسكرية أو سياسية أو اقتصادية.

أولا : الاستخبارات العسكرية السيبرية :

تزايد الاعتماد في الفترة الماضية على الاستخبارات السيبرية في العديد من الجوانب, و التي تتراوح بين التجسس و حرب المعلومات وصولا إلى الحروب السيبرية لأغراض متعددة منها :

- دعم عمليات عسكرية في الفضاء الالكتروني :

وتتمثل في القيام بهجمات في الفضاء الالكتروني لسرقة معلومات عسكرية عن قواعد البيانات و الخطط و الاستراتيجيات و التوقيتات الخاصة بالخصم, و التي من شانها المساعدة في شن عمليات عسكرية, أو القيام بعمليات عسكرية مباشرة في الفضاء الالكتروني كما حدث مع البرنامج النووي الإيراني من خلال فيروس "ستاكسنت"[3], و في سبيل تعزيز قدرتها العسكرية في الفضاء الالكتروني قامت الولايات المتحدة الأمريكية بإنشاء قيادة عسكرية سيبرية عرفت بقيادة حرب الفضاء الالكتروني مسرحا لعمليات عسكرية ممكنة, و تتنافس روسيا و الصين و الولايات المتحدة في مجال الحرب الالكترونية عبر السعي إلى امتلاك القدرات الهجومية و الدفاعية, حيث تمتلك القدرة على تبني

[1] Strategic Cyber Intelligence, **Intelligence and National Security Alliance : Cyber Intelligence Task Force,** March 2014, accessible at : http://www.insaonline.org/i/d/a/Resources/StrategicCyber.aspx.

[2] عادل عبد الصادق, **الاستخبارات الجديدة : إشكالات التجسس الالكتروني في العلاقات الدولية**, مجلة السياسة الدولية, عدد 195, يناير 2014, على الرابط التالي http://googl/qyU1ru:

[3] **حرب الفضاء الالكتروني : التهديد التالي للأمن القومي و كيفية التعامل معه**, مركز الإمارات للدراسات و البحوث الإستراتيجية, على الرابط التالي http://googl/rQVHjr:

إجراءات يمكن من خلالها ردع أية محاولات للهيمنة على نظم المعلومات الخاصة بكل منها, فضلا عن امتلاك القدرة على شن هجمات سيبرية.

- مراقبة و توجيه الرأي العام :

نتيجة لتزايد مستخدمي الانترنت خاصة الشبكات الاجتماعية مثل فيسبوك و تويتر, قامت بعض الدول بتشكيل وحدات مراقبة و تحليل التفاعلات التي تجري على الساحات الافتراضية و تستخدمها لتوجيه الرأي العام الالكتروني, و هم عملاء يتراوحون بين كونهم موظفين في الدولة أو حتى متعاقدين للقيام بمهام معينة, و قد بدا ذلك منذ هجوم روسيا على جورجيا و استونيا في سنتي 2007-2008 , حينما اعتمدت على قراصنة متطوعين أو متعاقدين لشن هجمات الكترونية على استونيا تسببت لها في خسائر اقتصادية كبيرة, فضلا عن شن هجمات سيبرية على جورجيا ساهمت في دعم العمليات العسكرية الروسية, أما الصين فإجمالي عدد الموظفين الذين يقومون بمراقبة المحتوى المعلوماتي على الانترنت يتراوح بين 30 و 50 ألف موظف, بالإضافة إلى وجود متطوعين لمراقبة الانترنت (Internet Surveillance Volunteers) , و أخيرا عصابة الخمسين سنتا (50 Cent Gang) و هؤلاء يتم توظيفهم لكتابة تعليقات لصالح الحكومة و تحويل نقاشات الرأي العام بما يتماشى مع رؤية النظام السياسي[1].

كما قامت وكالة الأمن القومي الأمريكية(NSA) و وكالة مشاريع البحوث الدفاعية المتطورة (DARPA) بتطوير برامج متقدمة لمراقبة و تحليل مواقع التواصل الاجتماعي, و التأثير على الرأي العام الالكتروني من خلال برامج مثل برنامج " دمية الجورب Sock Puppet " و التي يمكن من خلالها تدشين حسابات الكترونية وهمية, يتم من خلالها بث محتوى معلوماتي بهدف تغيير اتجاهات النقاش على الفضاء الالكتروني[2].

- الردع السيبري Cyber Deterrence :

يتم ذلك من خلال وضع استراتيجيات مضادة يدرك الخصم من خلالها انه إذا قام بشن هجوم عبر الفضاء الالكتروني سيواجه بهجوم أخر مضاد يفوق قدراته, كان يتم استهداف البنية التحتية السيبرية, أو أنظمة الاتصالات و الأنظمة المالية و المصرفية أو قطع خدمات الانترنت لردع الخصم عن

[1] Shirley Hung, **''The Chinese Internet : Control though the Layers''**, Massachusetts Institute of Technology, Harvard University, October 30, 2012, accessible at : http://ecir.mit.edu/images/stories/Hung_Internet-pdf.
[2] Nick Feilding and Ian Cobair, **Revealed : US Spy Operation That Manipulates Social Media,** The Guardian, on 21 March 2014, at : http://www.theguardian.com/technology/2011/mar/17/us-spy-operation-social-networks.

محاولة التفكير في الاعتداء, مثل : انقطاع اتصالات الانترنت في كوريا الشمالية لمدة 10 ساعات, مما أثار تكهنات بان الولايات المتحدة وراء هذا الحدث بسبب اتهام "بيونغ يانغ" بأنها وراء عملية القرصنة التي تعرضت لها شركة " سوني للأفلام", خاصة أن الرئيس الأمريكي باراك اوباما توعد بالرد لردع كوريا الشمالية عن التفكير مرة أخرى في توجيه هجمات سيبرية للولايات المتحدة و تكون نموذج لأي دولة أخرى.

ثانيا : الاستخبارات الاقتصادية السيبرية :

تتنوع الحوادث و الهجمات الالكترونية ذات الطابع الاقتصادي لتشمل سرقة المعلومات و تعطيل الأعمال و غلق الحسابات البنكية أو الاستيلاء عليها, كما تتعدد الجهات المقصودة من هذا الهجوم و اخطر أنواع الجرائم الالكترونية الأكثر كلفة هي التي تسببها الفيروسات و الشيفرات الخبيثة, و قطع الخدمة و الاتصال الشبكي داخل المؤسسات الاقتصادية و خارجها و محاولة السيطرة على الأجهزة المتصلة بالانترنت[1].

و يتركز الهجوم الالكتروني بالأساس على قطاعات و مجالات اقتصادية معينة مثل : الطاقة, الخدمات المالية, تجارة التجزئة و المنتجات الاستهلاكية.

- جمع المعلومات الاقتصادية :

تعاني الكثير من الدول خاصة الولايات المتحدة الأمريكية من اختراق شبكات الشركات الأمريكية عبر الفضاء الالكتروني, بهدف سرقة المعلومات التجارية و براءات الاختراعات و أسرار التكنولوجيا المتقدمة من شبكات و أجهزة الشركات العاملة في هذا المجال, و هو ما يخدم أهداف الدول و الشركات التي تقوم بعملية الاختراق بما يساعد على تطوير منتجاتهم و إضعاف قدرة المنتجات الأمريكية على المنافسة بسبب تقليدها أو حتى سرقتها و تطويرها[2], حيث تعتبر كل من الصين و روسيا ابرز القراصنة الالكترونيين الذين يعملون على جمع معلومات اقتصادية استخباراتية, خاصة من الولايات المتحدة حيث صنف تقرير صادر من مكتب مكافحة التجسس الأمريكي بان الصين أكثر الدول نشاطا و استمرارا في عمليات القرصنة الالكترونية على مستوى العالم, كما تجري أجهزة الاستخبارات الروسية

[1] **''The Economic Impact of Cybercrime and Cyber Espionage''**, Macafee Report, July 2013, accessible at : http://www.mcafee.com/sg/resources/reports/rp-economic-impact-cybercrime-pdf.
[2] **Foreign Spies Stealing US Economic Secrets in Cyberspace**, Office of The National Counterintelligence Executive, October 2011, pi.

العديد من العمليات في الفضاء الالكتروني بهدف جمع معلومات اقتصادية و تكنولوجية أمريكية تخدم المصالح الروسية و تساعد في ازدهار الاقتصاد الروسي و تقدمه تكنولوجيا.

- التجسس على المسؤولين و المؤسسات المالية :

إحدى الأدوات التي يمكن أن تمارس بها الولايات المتحدة الأمريكية قوتها الاقتصادية هي التجسس على المسؤولين الماليين بهدف معرفة مواقف الدول تجاه بعض القرارات و المواقف الاقتصادية, حيث كشفت تسريبات "ادوارد سنودن" عن قيام وكالة الاستخبارات البريطانية (MI5) بمراقبة الاتصالات التي تجريها الشخصيات المشاركة في قمة مجموعة العشرين لسنة 2009 بلندن, كما استخدمت هذه الوكالة برنامجا يتيح لها أن تعرف متى يتواصل أعضاء الوفود فيما بينهم, و قد وضعت تحت مجهر المراقبة أشخاصا بعينهم لا سيما وزير المالية التركي, و قد قامت وكالة الأمن القومي الأمريكية(NSA) بالتنصت على الرئيس الروسي "ديمتري مدفيديف" و هو يجري اتصالا هاتفيا عبر الأقمار الصناعية بموسكو[1], فالحكومات لا تعتمد فقط على تقييم و تحليل الخطابات و المفاوضات و التحركات السياسية الظاهرة من اجل تقدير المواقف السياسية و الاقتصادية لنظرائها من الحكومات, بل تلعب الاستخبارات دورا يساعد على استباق الأحداث, و من ثم اتخاذ السياسات التي تصب في مصلحتها أولا و بشكل أسرع في مواجهة الحكومات الأخرى[2].

أما عن تأثير و تداعيات هجوم الفضاء الالكتروني في المجال الاقتصادي, فيمكن القول أنها تتمثل في الخسائر المادية بالإضافة إلى الجوانب اللوجستية, حيث أوردت بعض التقارير الدولية المختصة بمتابعة الهجمات الالكترونية و تأثيراتها الاقتصادية تداعيات و تكاليف هذه الهجمات, و حددتها فيما يلي :

- تنظيف أو علاج تكاليف أي هجوم الكتروني معين.
- فقدان الإنتاجية أو تعطلها.
- تعطل العمليات المعتادة.
- تلف أو سرقة أصول تكنولوجيا المعلومات أو المنظمات المخترقة.

[1] **وثائق "سنودن" تطارد قمة الثمانية.. و تكشف تجسس بريطانيا على قمة ال20**, جريدة الوطن, 18 يونيه 2013, على الرابط التالي :http://www.elwatannews.com/news/details/203056

[2] كريم خشبة, **تسريبات سنودن : إدارة العلاقات الدولية في عصر التسريبات**, تحليل منشور على موقع المركز الإقليمي للدراسات الإستراتيجية بتاريخ 1 يوليو 2014, على الرابط التالي :http://goo.gl/uuEkd/

المبحث الثاني : إستراتيجية مواجهة الثغرات الأمنية ذات الطابع المعلوماتي

مراقبة الانكشافات Vulnerabilities Monitoring :

تهدف مراقبة الانكشاف إلى تحديد الثغرات الأمنية في نظم المعلومات و تشمل البناء الفيزيقي, الأقفال, جدران الحماية, كلمات الدخول, أن المراقبة التقليدية Surveillance يمكن أن تكشف المواد الدقيقة المهربة من الموقع, و يمكن لإجراءات التعامل مع المعلومات المكتوبة أن تحدد الممارسات الخطيرة مثل اخذ الوثائق الحساسة إلى أماكن مجهولة, أو السماح للزوار التجول في المناطق الحساسة.

أنواع التهديدات :أن نوع التهديدات التي يمكن أن يشكله أي فرد إلى نظام المعلومات يعتمد على عدة عوامل منها[1] :

- نوع الدخول Type of Access .
- مستوى الخبرة Level of Expertise .
- الدافعية Motivation .

إيجاد الثغرات في الشبكات :

في الفضاء المعلوماتي فان مراقبة الانكشاف تبدأ بتثبيت البرنامج, أن تشغيل برنامج النظام مباشرة من الصندوق يؤدي إلى جذب المتطفلين, حيث ترسل الرزمة مع المواصفات الأولية لتثبت ذلك النظام و هي مفتوحة بشكل واسع للتعدي, أن نظام التشغيل المستخدم لدعم خادم الشبكة ربما يأتي بكلمات دخول أولية (Default), إن التأكد من انكشافات البرنامج و مشكلات المواصفات يمكن أن تكشف و تحل قبل تشغيل النظام, و حتى بعد التثبيت فانه من الضروري استمرار تحديث المراقبة و إعادة المواصفات عند إضافة عنصر جديد أو حذف عنصر قديم, إن إضافة خط الوصل بالانترنت أو بواسطة الاتصال عن بعد ذو مضامين أمنية هامة[2], و هناك العديد من البرامج المجانية التي تساعد على تحديد نقاط الضعف و الفجوات مثل : برنامج " Computer Oracle & Password System (CIOS)", و برنامج " Security Analysis Tool for Anditing Networks (SATAN)", كما أجرت وزارة الدفاع الأمريكية تجارب لفحص الثغرات الأمنية في شبكاتها حيث قامت وكالة نظم المعلومات الدفاعية

[1] البداينة ذياب, **مرجع سابق**, ص 323-324.

[2] GAO/AIMD, Report to Congressional Requesters, **Computer Attacks at Department of Defense Pose Increasing Risks**, GAO/AIMD-96-84, 22 may 1996, at: http://www.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=gao&docid=f:ai96084.txt

(DISA) ب38 ألف هجوم على شبكات الوزارة, و نجحت في الدخول و الاختراق في 4,4% من الحالات, كما قامت وكالة الأمن القومي الأمريكية(NSA) بعملية تدريبية لمعرفة الثغرات و الانكشافات في شبكات الجيش الأمريكي, و قد عرفت هذه المناورات ب"المتلقي الشرعي Eligible Receiver", و قد تم استخدام أدوات متاحة على الشبكة في عمليات الاختراق و المراقبة, كما تمكن الدخلاء من الحصول على العديد من النظم العسكرية.

بناء النظم الآمنة :

بدا الاهتمام في الأجهزة الأمنية بشراء الأجهزة و البرمجيات التي تحقق اكبر قدر من الأمن للمعلومات السرية, و قد وضعت ثلاثة معايير لتلبي ثلاثة أهداف هي[1] :

1. تقديم خطوط عامة بخصوص الخصائص الأمنية اللازم بنائها في النظم الحالية و المستقبلية مع الاهتمام الخاص بحماية البيانات السرية و عدم الكشف غير القانوني لها.
2. تقديم مقاييس لتقييم درجة الموثوقية الممكن وضعها في نظم المعلومات للبيانات السرية و المعلومات الحساسة.
3. تقديم أسس لتحديد المتطلبات الأمنية حيث حدد " TCSEC " مجموعة من المتطلبات : الخصائص الأمنية الواجب توافرها و الضمانات اللازم تلبيتها و هي على النحو التالي :

- الحماية الأمنية الحذرة : أن تكون النظم قادرة على ضبط الدخول على أساس الفرد المستخدم و يجب فحصها لتحديد التغيرات في الدخول.
- حماية ضبط الدخول : أن توفر النظم المسؤولية الفردية من خلال إجراءات الدخول و الحركات و أن تشمل اختيارات الانكشاف التغيرات التي تخرق أو تسمح بالدخول غير المصرح به للبيانات و السجلات الخاصة بالمستخدمين.
- حماية امن المعلومات : أن تدعم النظم إعطاء أسماء للبيانات الحساسة للمواضيع و الفاعلين بما في ذلك البيانات المصدرة و توفر إذن الدخول رسميا.
- الحماية الهيكلية (البنائية) : مقاومة النظم للدخول غير المصرح به و تتطلب تحقيق الهوية قوية مع إدارة قوية للمواصفات.
- مجالات الأمن :أن تكون النظم مقاومة بشدة للدخول غير المصرح به و نظم مستوى (B3) يجب أن تدعم المدير الأمني استخدام القوائم و تشمل نظم إجراءات الاسترجاع.

[1] البداينة ذياب, **مرجع سابق**, ص 327.

- الحماية المضمونة (المؤكدة) : يجب على النظم أن توفر ضمانات ضد الدخول غير المصرح به.

إدارة الخطورة Risk Management :

- تحليل الخطورة Risk Analysis :

عند الحديث عن وقاية المعلومات لابد من تحديد الخطورة التي تهدد المعلومات و أنظمتها و معداتها, و تطبيق إجراءات امن متنوعة لحماية هذه النظم, إن عملية امن المعلومات عملية مقايضة فبعض الشركات و المنظمات تنفق ما يناسب حماية أجهزتها ضد الأخطار بعضها بمقدار الخسارة الناجمة عن الحماية, و هناك نوعان من تحليل الخطورة منها :

أ- التقديرات الاحتياطية Proactive Assessment : هذه الإجراءات تنفذ قبل حدوث المشكلة و تحديد أهم المخاطر التي تهدد النظام الذي تنوي حمايته, و ما هي احتمالات تعرضه للاعتداء, و تحديد الإجراءات المضادة لكل من المهددات و احتمالات التعرض.

ب- التقديرات الفورية Reactive Assessment : و يتم تنفيذ هذه المهمة بعد حدوث المشكلة و تحديد ما هي الأسباب التي أدت لوقوع الحادثة و ما هي مجالات التعرض التي أدت لذلك, و ما هي الإجراءات غير المناسبة التي كانت متوافرة و ما هي الإجراءات المطلوب إيجادها[1].

- تقدير الخطورة Risk Assessment :

و تعني العمليات التي تحدد فيما إذا كانت الإجراءات الفعلية الموجودة أو المتوقع إيجادها مناسبة لحماية مصادر المعلومات من التهديدات المحتملة, إنها تشمل تحديد رأس المال الواجب حمايته, التهديدات المحتملة, و احتمالية وقوعها و الانكشافات التي يمكن أن تستغل و الخسارة المتوقعة من أي اعتداء, و الإجراءات الدفاعية التي يمكن تثبيتها و تحليل الكلفة و الفاعلية (Cost – Effective)أيأن الكلفة لحماية المعلومات لا تفوق كلفة المعلومات ذاتها, كما أن هناك أعداء محتملون, متطفلون, منافسون, مجرمون, حكومات أجنبية,,,,الخ, لكل منهم دافعه الخاص به و مهاراته التي لها اثر مختلف على كل هدف و هناك أدوات لتقدير الانكشاف.

[1]Icove, D ; Seger, K, & VonStorch, W, **Computer Crime : A Crimefighters information services The Information Society**, Vol 1, No 4, 1995, p 307-338.

حماية البنية التحتيةالوطنية المعلوماتية :

للحكومة دور في الدفاع المعلوماتي على مستوى مسؤولياتها عن الأمن الوطني و الاقتصادي و الأمن العام.

إن زيادة المشاركة في المعلومات داخل البناء التحتي المعلوماتي الواحد و بين القطاعات المختلفة و بين الحكومة يسهل الجهود في تحديد الثغرات و اكتساب الأدوات اللازمة لحماية المعلومات, و تتطلب حماية البنية التحتية المعلوماتية تكامل جهود الوكالات و الأجهزة الحكومية و الخاصة, و هذا يتطلب تبني سياسات تتأقلم مع الثقافة المتغيرة و التطورات التقنية المتسارعة, و للحكومة دور هام في حماية البنية التحتية المعلوماتية بالتعاون مع الإدارات الحكومية, كما أن للبحث العلمي أهمية خاصة في تطوير الوسائل المناسبة في حماية البنية التحتية المعلوماتية.

- المبادئ العامة لأمن النظم GSSP[1] :
- المحاسبة Accountability .
- الوعي Awareness .
- الأخلاقيات Ethics .
- تعددية الحقول Multidesciplinary .
- التناسب Proportionality .
- التكامل Integration .
- قنوات الوقت Time Lines .
- إعادة التقييم Reassessment .
- الديمقراطية Democracy .

الهيئة الرئاسية لحماية البنية التحتية الحساسة :

لقد نادت اللجنة بإستراتيجية عملية لحماية البنية التحتية من خلال التعاون و تبادل المعلومات و إعادة النظر بالقوانين المتصلة بحماية البنية التحتية, و تطوير برامج البحث و التطوير و قد حددت اللجنة خمسة مجالات و هي :

[1] Denning, D, E, and Baugh, Jr. W. E, **Hiding Crimes in Cyberspace**, 1999, p 397-398, at: http://www.cs.georgetown.edu/denning/

1. تكوين السياسات Policy Formation :و هي تقدير الحكومة للتهديدات الناجمة من الثغرات الأمنية و تقدير الخطورة على المستوى الوطني و الأهداف و الاستراتيجيات و السياسات.
2. الوقاية و التخفيف Prevention & Mitigation : تتم بتفحص الثغرات في النظم و الشبكات و وضع إجراءات حماية و عملية لتحقيق مستويات الضمان, و دعم جهود البحث و التطوير و الوعي و التعليم و تقدير التهديدات و تشجيع القطاع الخاص على تطبيق أفضل الممارسات.
3. تبادل المعلومات و تحليلها Information Sharing & Analysis : عن طريق تقديم المعلومات و تحليلها و تحديد الثغرات و وضع الإجراءات اللازمة لسدها.
4. ردة الفعل Consequences Management : و في هذا السياق يحدد ما يحدث بشكل فجائي في البنية التحتية.
5. الاستجابة و إعادة البناء Response Restoration : أن مسؤولية الاستجابة للحاجات الأساسية الناجمة عن الثغرات تقع على عاتق الدولة[1].

كما اقترحت اللجنة بناء وطني لضمان البنية التحتية تتكون من العناصر الآتية :

- مكتب وطني لضمان البنية التحتية CIAO : بالتنسيق في الدعم لعمليات اتخاذ القرار الموجودة و المخططة في تنفيذ القانون و الأمن الوطني و مواجهة الإرهاب و مجالات الاستخبارات, كما يسهل المكتب الوطني تكوين تامين للبنية التحتية ليشمل تقدير الخطر الوطني و دمج منظور القطاع العام و القطاع الخاص, و تحديد أهداف وطنية لتطوير استراتيجيات تطبيق و تقديم تشريعات و تفعيلات أخرى و تقدير الحاجة للتنظيمات الجديدة.
- مجلس ضمان البنية التحتية NICS : لمناقشة سياسات ضمان البنية التحتية و صياغة التوصيات المناسبة للرئيس.
- مكتب دعم الضمان للبنية التحتية : و يقدم الدعم الوظيفي و إدارة للمنظمات الفيدرالية المشاركة في تامين البنية التحتية, و تقديم مساعدة مباشرة في مشاركة القطاع العام و الخاص و يدعم تكوين السياسة و الوقاية و التخفيف من التهديدات و مساعدة المكتب الوطني في إدارة المشاركة بالمعلومات و مركز التحليل.

[1] PCCIP (President 's Commission on Critical Infastructure Protection), **Critical Foundations : Protecting America's Infrastructures**, The Report of the President's Commission on Critical Infrastructure Protection, October 1997, p 15, at: http://www.pccip.gov , pdf file.

- منسقو القطاعات لتسهيل مشاركة المعلومات : حيث تقود القطاع في تحديد الطريقة المثلى في المشاركة بالمعلومات اللازمة لحماية البنية التحتية من قبل الحكومة.
- مركز التحليل و تبادل المعلومات ISAC : و ذلك بالتركيز على جمع معلومات إستراتيجية تتعلق بمهددات البنية التحتية و التعرض للانكشافات و الممارسات و المصادر التي تمكن من تحليل فعال لفهم أفضل للبنية التحتية.
- المركز الوطني لحماية البنية التحتية NIPC : و ذلك بالتنبؤ الفوري لأي هجوم على البنية التحتية و تتبع مسؤولية المركز لمكتب التحقيقات الفدرالي (FBI) في وحدة متعددة الأطراف للمراقبة و تحليل التهديد حيث يمكن أن ترصد أي إشارة للتهديد.

لقد واجهت " الهيئة الرئاسية PCCIP " بعض المشكلات القانونية في التطبيق حيث أن القطاع الخاص بحاجة إلى تأكيد و ضمان بان المعلومات الحساسة المشتركة مع الحكومة محمية و غير متاحة للأطراف الأخرى المنافسة, كما ترى الهيئة أن تعمم الأحكام الجنائية المطبقة في مجال التعديات في امن الشبكات و سوء الاستخدام, إلى الأشكال الأخرى للجرائم الالكترونية و الجرائم المتصلة بالتكنولوجيا و تكنولوجيا المعلومات, كما أوصت الهيئة الرئاسية بتوسيع البرامج البحثية و التطوير الهادف إلى تطوير الإمكانيات الضعيفة حاليا مثل : كشف التطفل و الاختراق.

و ينسق مكتب ضمان البنية التحتية الحساسة (CIAO) تطوير الخطة الوطنية المبنية على خطط القطاعات و تشمل الخطة الوطنية بحد أدنى على[1] :

1. تقدير الانكشاف الأولي متبوعا بتقدير دوري لكل قطاع من الاقتصاد و كل قطاع حكومي ربما يكون هدفا لهجوم.
2. خطة إصلاحية تعويضية للتخفيف من الاستغلال المقصود للانكشافات المحددة.
3. مركز وطني للتحذير من الهجمات المهمة على البنية التحتية.
4. خطة للاستجابة للهجمات الراهنة من اجل فصل الضرر و تقليله و كذا التأثير للإعادة الفورية للخدمات الأساسية.
5. برامج تربوية و توعية لتحسيس الأفراد بأهمية الأمن.
6. البحث الفدرالي و التطوير اللذان يساعدان في تطوير نشر التكنولوجيا لتقليل الانكشاف.

[1] البداينة ذياب, **مرجع سابق**, ص 342.

خاتمة الفصل:

مع التطور التكنولوجي الحاصل في العالم, أصبح الفضاء الالكتروني مصدرا للتهديدات و المخاطر, و التي امتدت لتشمل جميع النواحي سواء السياسية أو الأمنية أو الاقتصادية, الأمر الذي فتح المجال للعمليات الاستخباراتية التي تستهدف الأجهزة و البرامج و المؤسسات المالية و الملكية الفكرية, و بالتالي أصبح الطرف الأقوى هو من يتمكن من التحكم في هذه المعلومات و استغلالها لصالحه.

و في الأخير يمكن القول, أن هناك نمطا متصاعدا من الاستخبارات التي تدعى "الاستخبارات السيبرية ", تتبناها الدول بهدف المساعدة في تحقيق أهدافها الإستراتيجية داخل الفضاء الالكتروني, و أيضا دعم العمليات التخريبية ضد الدول الأخرى, و هو نمط من المتوقع أن يزداد في الفترة القادمة مما يجعلنا أمام حرب سيبرية مفتوحة.

الخاتمة

في نهاية هذه الدراسة , والتي هي تحت موضوع " التخطيط الاستراتيجي الأمريكي لبرنامج الأمن القومي للولايات المتحدة الأمريكية (آلية التعامل مع الثغرات الاستخباراتية) ", والتي تشكل محور أساسي في السياسة الأمنية الأمريكية , كما أنها تزيل الغموض الذي كان يعتري هذه الثغرات الأمنية , وعن كيفية مساهمتها في التأثير على البنية التحتية المعلوماتية للولايات المتحدة الأمريكية , حيث يعتبر موضع اهتمام من طرف العديد من المهتمين و المتخصصين في شؤون السياسة الأمنية الأمريكية , سواء كانوا من الجانب المحلي , أو الدولي , كما يحظى أيضا بالاهتمام الكبير من طرف صانع القرار السياسي الأمريكي.

وفي معالجة الإطار التاريخي و الزمني في مواكبة الحيثيات و الوقائع لأهم العوامل المؤدية لنشأة و بروز هذه الثغرات الأمنية في الشأن السياسي الداخلي الأمريكي , حيث شهدت عدة تجاوزات و تدخلات عوامل خارجية مختلفة , و التي قد أثرت على الولايات المتحدة خاصة في الانتخابات الرئاسية , وعن مدى درجة تأثيرها على مثل هذه الأحداث والتطورات , طبعا لما لا يتناسب مع مصلحة الولايات المتحدة الأمريكية , ونظرتها الشاملة لمختلف دول العالم.

فالخلاصة العامة في دراستي للدور الروسي ومكانة " أجهزة الاستخبارات الروسية FSB " في التأثير على صناعة القرار الأمريكي, إذ يجب أن نأخذ بعين الاعتبار الأهمية الإستراتيجية , التي مثلها هذا الجهاز الاستخباراتي و التي تعد حادثة استثنائية في التاريخ السياسي المعاصر للولايات المتحدة الأمريكية , وهذه الأهمية يمكن أن نرصدها من خلال دراستي للتدخل الروسي في الشؤون الأمريكية , من خلال الفرضيات الآتية , والتي تم تأكيدها :

- إن عملية الاختراق تخضع في جزء كبير منها إلى الأنشطة السرية , والتي تقوم بها أجهزة الاستخبارات الروسية , والتي قد تخفى عنا في تحليلنا حتى بالنسبة للموقف الأمريكي تجاه هذه الحادثة , وعليه نكون واعين تماما بالنقص , الذي قد يعترض دراستي أمام العمليات السرية بتلك المذكورة في تحليلنا لدور هذه الأجهزة .
- أن هذه النشاطات السرية , تهدف إلى تحقيق المصالح الإستراتيجية السياسية و الأمنية و الاقتصادية لروسيا الاتحادية .

وما يمكن أن يلفت الانتباه أيضا , هو أننا أمام دراسة سياسية أمنية خارجية لقوى عظمى تطمح للإمبراطورية , فمن الطبيعي أن تكون عرضة للانكشافات و الاختراق لما لديها من امتيازات عالمية

ومصالح كونية اقتصادية, عسكرية وسياسية يصعب على جهاز , أو وكالة استخباراتية أن تدير و تحمي تلك الشبكة المعقدة التي تتكون منها البنية التحتية المعلوماتية الحساسة أو الكشف الدقيق عن مختلف التهديدات و تتبع مصدرها الحقيقي في العالم , من دون تكاثف الجهود, مع التسليم بالتفاوت الذي يمكن أن يحصل , وإضافة إلى ذلك فان الكثير من هذه النشاطات تتسم بالسرية , وقد لا يسمع بتلك النشاطات , إلا بعد كشفها في وسائل الإعلام.

و في الختام, نرى انه في الوقت الذي توسع فيه نطاق الأنشطة التي تشتمل على التهديدات شديدة الحساسية عبر الانترنت بشكل كبير على مدار السنوات القليلة الماضية, لم تتغير صناعة النظم الأمنية إلا بالقدر الضئيل جدا, نقاط الضعف القابلة للإصابة التي تم تحديدها و استثمارها في أوائل التسعينات القرن العشرين ظلت كما هي و ما يزال يتم استغلالها بشكل اكبر في مطلع القرن الواحد و العشرين, و في الوقت الذي يسرت فيه التحسينات التي أدخلت على التقنية و الاتصالات تنفيذ الهجمات, لا يزال هناك بطء في أسلوب إدراك الهيكليات الأمنية التي يمكن أن تعالج نقاط الضعف.

لا يوجد حل أو علاج شامل لقضايا الأمن الالكتروني, إذ يجب على كل دولة أن تقيم ما تحتاجه و ما يتناسب مع أنشطتها و تحديد المخاطر التي يجب التعامل معها, و بعد ذلك يتوافر عدد هائل من الحلول ذات القدرة العالية التي يمكن تنفيذها بل و الأهم صيانتها و استدامتها, إن المستهلكين في الفضاء الالكتروني سواء أكانوا من الحكومات أو القطاعات الخاصة أو المجتمع, لا يزالون يسعون للحصول على الأمن المعلوماتي و اقل قدرة على تحمل الفشل, على الرغم من زيادة الوعي بالتهديدات, لكن عادة ما تتخذ الإجراءات الأمنية بعد اختراق البيانات و الأنظمة.

تحتاج التقنية إلى إعادة هيكلة لكي يمكنها تقليل النزعة إلى شن الهجمات في الفضاء الالكتروني, كما سوف يتطلب هذا إعادة النظر و بشكل جذري في الطريقة التي يتم بها تقديم الخدمات إلى الشبكة, " إن المنهج القديم للأمن الذي يصور امن المعلومات بالحديقة المسورة التي تتم حمايتها عبر جدران الحماية و الشبكات الداخلية, يبدو انه لا يتفق مع الواقع الفعلي", فالأفكار المبدئية المتعلقة بهيكلية الخاصة بالشبكات القادرة على البقاء, التي يمكن أن تساهم و إن كان بشكل ضئيل في توفير خدمات ضرورية عند التعرض لهجوم , لكن الأنظمة القوية و الموثوقة و المعتمدة على هذه المفاهيم لم تظهر بعد في مجال المنتجات و لم يتم نشرها على نطاق واسع على الرغم من أن ظهور معيار الشبكة المرنة, ينبغي أن يتجه و بشكل ما نحو التعامل مع هذه القضايا.

أما بالنسبة للفضاء الالكتروني, يجب أن يقوم التركيز عل حماية المعلومات فالمعلومات موجودة سواء كانت مخزنة أو قيد النقل عبر الفضاء الالكتروني, و هي معرضة في كلتا الحالتين لخطر الاختراق و التجسس دون الإحساس بأي تغيير يذكر, و بمجرد قرصنة المعلومات يمكن تغييرها أو يعاد التزويد بها و استخدامها لتكرار عمليات الاحتيال, قد تقلل ضوابط الدخول من هذه المخاطر في نطاق خاص, و لكن ليس عند وضع المعلومات في نطاق عام.

قائمة المراجع

أولا : الكتب باللغة العربية

1) الشهراني سعد بن علي, **إدارة عمليات الأزمات الأمنية**, مركز الدراسات و البحوث, جامعة نايف العربية للعلوم الأمنية, الرياض, 2005.

2) البداينة ذياب, **الأمن و حرب المعلومات**, دار الشروق للنشر و التوزيع, ط 1, عمان, الأردن, 2006.

3) البصيلي جاسم محمد, **الحرب الالكترونية – أسسها و أثرها في الحروب**, المؤسسة العربية للدراسات و النشر, ط 2, بيروت, 1989.

4) أيلين ليبسون, **الاستخبارات الأمريكية بعد الحادي عشر من سبتمبر : سد الثغرات**, مركز الإمارات للدراسات و البحوث الإستراتيجية, ط 1, أبو ظبي, 2005.

5) جيمس كلابر, **تقدير موقف التهديدات العالمية من قبل " مجتمع الاستخبارات الأمريكية " للجنة الاستخبارات بمجلس الشيوخ**, السفير للنشر و التوزيع, ترجمة شهاب الإدريسي, 2013.

6) عبوي زيد منير, **إدارة الأزمات**, دار كنوز المعرفة للنشر و التوزيع, عمان, 2007.

7) كريم خشبة, **تسريبات سنودن : إدارة العلاقات الدولية في عصر التسريبات**, المركز الإقليمي للدراسات الإستراتيجية, يونيه 2014.

ثانيا : المجلات و المقالات

8) الشعلان فهد احمد, **اتخاذ القرارات أثناء الكوارث و الأزمات**, مجلة الفكر الشرطي, المجلد السابع, العدد الرابع, الإمارات العربية المتحدة, يناير 1999.

9) السيد طه سعيد, **عملية صنع و اتخاذ القرار الإداري**, مجلة الفكر الشرطي, المجلد السابع, العدد الرابع, الإمارات العربية المتحدة, يناير 1999.

10) عادل عبد الصادق, **الاستخبارات الجديدة : إشكالات التجسس الالكتروني في العلاقات الدولية**, مجلة السياسة الدولية, عدد 195, يناير 2014.

ثالثا : الرسائل و المذكرات

11) الردادي محمد بن عودة, **دور القيادات الوسطى في اتخاذ القرارات و اثر ذلك على كفاءة الأجهزة الأمنية**, رسالة ماجستير (غير منشورة), أكاديمية نايف للعلوم الأمنية, الرياض, 1417 هـ.

12) الجابري عباد بن عبيد, **اتخاذ القرارات في المنظمات الأمنية**, رسالة ماجستير (غير منشورة), المركز العربي للدراسات الأمنية و التدريب, الرياض, 1989.

13) الهذلي سعد بن عليوي, **مهارة القائد الأمني في اتخاذ القرار في الظروف الطارئة**, رسالة ماجستير (غير منشورة), أكاديمية نايف العربية للعلوم الأمنية, الرياض.

14) العبد القادر محمد علي, **عملية اتخاذ القرارات**, رسالة ماجستير (غير منشورة), المركز العربي للدراسات الأمنية و التدريب, الرياض, 1989.

رابعا : المصادر باللغة الأجنبية

15) Arquilla. J and Ronfeldt, **Cyberwar Is Coming**, comparative strategy, Vol 12, No 2, 1993.

16) Boni. W. C. and Kovacich. G, **I – Way Robbery: Crime on the Internet**, Boston: Butterworth-Heinemann, 1999.

17) **Bears in Midts: Intrusion into the Democratic National Committee**, party reports, 2016.

18) Cohen. L. E. & Felson. M, **Social Change and Crime Rate Trends: Routine activity approach**, Americain Sociological review, Vol 44, 1979.

19) **Clinton compaigns also hacked in Attacks**, Washington Post Press, November 2016.

20) Davis. I, **Crime and the Net: an Overvew of Criminal Activity on the Internet and the Legal Community's Response**, 1998.

21) **Defense Silence Board Report of the Defense Silence Board Task Force on Information Warefare-Defense (I W-D)**: office of the Under Secretary of Defense for Acquisition and Technology, Washington DC, 1996.

22) Developing Your Cyber Intelligence Analyst Skills, **The State of Security**, Jan 27, 2014.

23) Denning. D. E, and Baugh. Jr. W.E, **Hiding Crimes in Cyberspace**, 1999.

24) Ehler. V, **Information Warefare and International Security**, 1999.

25) **FBI took months to warns Democrats of Suspect Russian**, on the site: www. FBI.com

26) **"Fixing Intelligence"**, foreign affairs, Vol 81, No 1, (January-February 2002).

27) **Foreign Spies Stealing U.S Economic Secrets in Cyberspace**, office of The National Counterintelligence Executive, October 2011.

28) Gerard. J. J. M, **Infrastructure Valnerabilities: New Role for DND Department of National Defense- War- Peace and Security**, Canada, 1999.

29) GAO/AIMD, Report to Congressional Requesters, **Computer Attacks at Department of Defense Pose Increasing Risks**, 22 may 1996.

30) Icove. D: Seger. K, & Vonstorch. W, **Computer Crime: A Crimefighter information services The Information Society**, Vol 1, No 4, 1995.

31) Joseph. S Nye. **The Reality of Virtual Power**, Moscow Times, February 4, 2012.

32) **Natoinal Intelligence Director: Hackers have targeted 2016 Presidential Compaigns**, Washington DC, 2016.

33) Nick Feilding, and Ian Cobair, **Revealed: U.S Spy Operation That Manipulates Social Media**, The Guardian on 21 march 2014.

34) Operational Levels of Cyber Intelligence, **Intelligence Levels of Cyber Intelligence, Intelligence and National Security Alliance**, September 2013.

35) PCCIP (President's Commission on Critical infrastructure Protection), **Critical Foundations: Protecting America's Infrastructures**, the report of the President's Commission on Critical Infrastructure Protection, October 1997.

36) **Private Security Says Russia was behind John Podesta's Hack**, Intelligence Community reports, 2016.

37) **Released Emails Suggest the D.N.C Derided the Sanders Compaigns**, Dec 2016.

38) Sakkas. P. E, **Espionage and Sabotage in the Computer World**, international journal of intelligence and counterintelligence, Vol 5, No 2, 1995.

39) **Spy Agency Consensus Grows that Russia Hacked D.N.C Protecting of Personal Data in the United States**, New York, 2016.

40) Strategic Cyber Intelligence, **Intelligence and National Security Alliance: Cyber Intelligence Task Force**, march 2014.

41) Shirley Hung, **The Chinese Internet: Control thought the Layers**, Massachusetts Institute of Technology, Harvard University, October 30, 2012.

42) **Trump, Putin, Russia, DNC/Clinton Hack**, Confidential Documents, 2016.

43) **The Most revealing Clinton compaign emails in Wikileaks** on: www.wikileaks.org.com

44) **"The Economic Impact of Cybercrime and Cyber Espionage"**, Macafee Report, July 2013.

45) **U.S officials warned DNC of Hack months before party**, center of studies, Chicago, sept 2016.

46) **U.S Wrestles with how to Fight Back Against Cyberattacks, The Future of Cyberterrorism Crime & Justice International**, march 2016.

47) **Why Security Experts Think Russia was Behind the D.N.C breach**, national Security reports, Washington DC, 2016.

48) **White House Confirms Pre-Election Warning to Russia over Hacking**, white house reports, 2016.

خامسا : المواقع الالكترونية

49) **أبعاد و خلفيات دور الاستخبارات في الانتخابات و السياسة**, على الموقع الالكتروني :
http://www.almassira.com/suscribe/signup/index

50) داود عمر داود, **العامل الروسي في فوز ترامب**, على الموقع التالي : www.raialyoum.com

51) فتحي التريكي, **حقيقة الاختراق الروسي للانتخابات الأمريكية**, الخليج الجديد, على الموقع الالكتروني :
www.newKhaleej.com

52) جوزيف ناي, **الكرملين و الانتخابات الأمريكية**, مركز الجزيرة للدراسات, على الموقع الالكتروني :
http://www.aljazeera.net/documents/index

53) **وزارة الأمن الداخلي الأمريكية**, على الموقع التالي : www.dhs.gov

54) **وثائق "سنودن" تطارد قمة الثمانية,, و تكشف تجسس بريطانيا على قمة ال20**, جريدة الوطن, 18 يونيه 2013, على الرابط التالي : http://www.elwatannews.com/news/details/203056

55) **كلمة ونستون ويلي, أمام لجنة الشؤون الحكومية التابعة لمجلس الشيوخ في 26 فبراير 2003**, على الموقع التالي : http://www.cia.gov/cia/public_affairs/speeches/2003/wily_speech_02262003.html .

56) **حرب الفضاء الالكتروني : التهديد التالي للأمن القومي و كيفية التعامل معه**, مركز الإمارات للدراسات و البحوث الإستراتيجية, على الرابط التالي : http://google/rQVHjr .

57) هشام ملحم, **الدور الروسي في الانتخابات الأمريكية**, على الموقع الالكتروني :
http://www.alarabiya/documents.com أو على الرابط : http://ara.tv/y87r .

- ملخص المذكرة-

أولا : باللغة العربية

- نستخلص من هذا الموضوع , أن كون تعرض الولايات المتحدة الأمريكية للاختراق و التجسس الالكتروني من طرف الاستخبارات الروسية من خلال التدخل المباشر و المساهمة في التأثير على نتائج الانتخابات الرئاسية الأمريكية لحساب مرشح على مرشح أخر, و التي تعد سابقة لا مثيل لها في تاريخ الانتخابات الأمريكية, و أيضا عن فشل الاستخبارات الأمريكية و التي تعد احد الأنظمة أو الأجهزة الأساسية بصفتها الأداة الأولى عن الدفاع ضد شتى التهديدات المحتملة و عن عجزها في احتواء الأزمة الأمنية أو اتخاذها لإجراءات و تدابير استباقية و وقائية ردعية تمكنها من التعرض لهذا النوع من الهجمات (ذات الطابع المعلوماتي) , و خاصة تلك المتعلقة بأمنها القومي , كما تعد الجهة الرسمية و المسؤولة عن تقييم المخاطر و التهديدات الداخلية و الخارجية التي تحيط بالولايات المتحدة الأمريكية , كما يسلط الضوء, عن طبيعة أداء الاستخبارات الأمريكية و إستراتيجيتها المنتهجة لتعزيز و حماية البنى التحتية المعلوماتية الحساسة من الانكشاف من خلال سد الثغرات, و عن مدى دقة و سرعة استجابة الاستخبارات الأمريكية لمتطلبات و تداعيات هذه الفجوات الأمنية و انعكاسها على البنية التحتية للأمن القومي الأمريكي .

ثانيا : باللغة الانجليزية

- We conclude from this subject that the fact that the United States of America is exposed to penetration and electronic espionage by the Russian intelligence through direct intervention and contribute to influence the results of the US presidential election for the candidate of another candidate, which is an unprecedented precedent in the history of the American elections , And the failure of the US intelligence, which is one of the basic systems or devices as the first tool to defend against various potential threats and its inability to contain the security crisis or to take proactive measures and preventative measures deterrent to exposure to this type of Especially those related to its national security. It is also the official body responsible for assessing internal and external risks and threats surrounding the United States of

America. It also sheds light on the nature of the performance of the US intelligence and its strategy to strengthen and protect the structures. Sensitive information infrastructure through the filling of the gaps, and the accuracy and speed of the response of US intelligence to the requirements and implications of these security gaps and their reflection on the infrastructure of US national security.

ثالثا : باللغة الفرنسية

- Nous concluons de ce fait que le fait que les États-Unis d'Amérique sont exposés à la pénétration et à l'espionnage électronique par le renseignement russe par une intervention directe et contribuent à influencer les résultats des élections présidentielles américaines pour le candidat d'un autre candidat, Un précédent sans précédent dans l'histoire des élections américaines, et l'échec de l'intelligence américaine, qui est l'un des systèmes ou dispositifs de base comme premier outil de défense contre diverses menaces potentielles et son incapacité à contenir la crise de sécurité ou à prendre des mesures proactives Et mesures préventives dissuasives à l'exposition à ce type de spécialement ceux liés à sa sécurité nationale. C'est aussi l'organe officiel chargé d'évaluer les risques et les menaces internes et externes entourant les États-Unis d'Amérique. Il met également en lumière la nature de la performance du renseignement américain et sa stratégie pour renforcer et protéger les structures. L'infrastructure d'information sensible grâce au remplissage des lacunes et l'exactitude et la rapidité de la réponse du renseignement américain aux exigences et aux implications de ces lacunes en matière de sécurité et à leur réflexion sur l'infrastructure de la sécurité nationale des États-Unis.