جامعة العربي التبسي –تبسة–
كلية الحقوق والعلوم السياسة.
قسم العلوم السياسية.

Université Laarbi Tbessi –Tebessa–
Faculté de droit et science politique
Département de science politique

استراتيجيات الدول الكبرى في حماية أمنها الالكتروني (دراسة حالة: الولايات المتحدة الأمريكية)

مذكرة مكملة لنيل شهادة ماستر أكاديمي في العلوم السياسة

تخصص: دراسات استراتيجية

من إعداد الطلبـــــة:

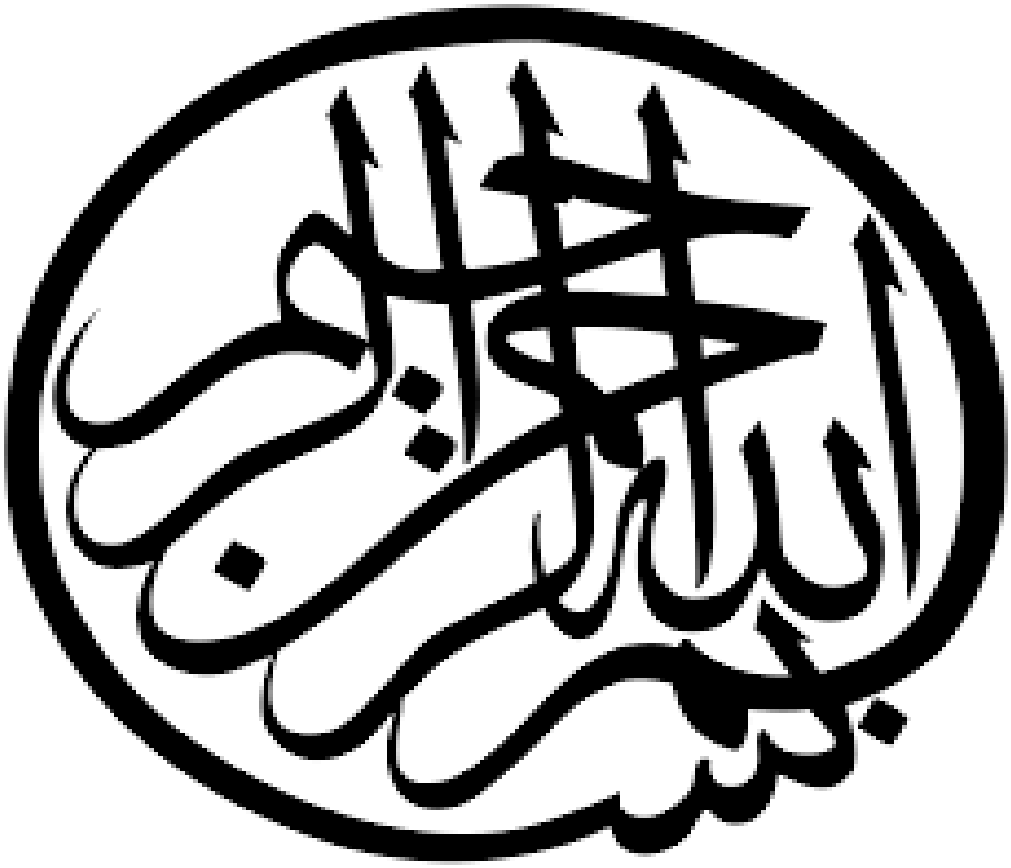
- خالـد سليمان
- أسماء باهـــي

تحـــــت إشـــــراف:

الأستاذة: نسرين نموشي

الإسم واللقـــب	الصفـــــــة	الدرجـــة العلمية
أمير عبـــــــاد	رئيســـــــا	أستاذ مساعد قسم "أ"
نسرين نموشـــــي	مشرفـا ومقـــررا	أستاذ مساعد قسم "أ"
سميـــة بلعيـــد	عضـــوا مناقشـا	أستاذ مساعد قسم "أ"

الموسم الجامعي: 2018/2017



شكر وعرفـــان

نتوجه بجزيل الشكر و الامتنان لكل من ساعدنا من قريب او من بعيد على انجاز هذا العمل المتواضع و في تذليل ما واجهناه من صعاب و متاعب نخص بالذكر الأستاذة المشرفة على عملنا "**نسرين نموشي** " التي لم تبخل علينا بتوجيهاتها و نصائحها القيمة لاتمام هذا البحث

كما نشكر أعضاء الملجنة العلمية المناقشة لموضوعنا،

الأستاذ: "**أمير عباد**" والأستاذة "**سمية بلعيد**".

الإهـــداء

الى من ربياني صغيرا، الى من لا يمكن للكلمات ان توفيهما حقهما أو تعبر عن مكنونات قلبي تجاههما، الى القلب الناصع بالبياض، الى الشمعة المتقدة المنيرة ظلمة حياتي، الى من ساهمت في جعل عالمي مشرقا كابتسامتها الحنونة الى كل الخير الذي عرفت الى **والدتي** الكريمة، الى من كلله الله بالهيبة و الوقار و من علمني العطاء دون انتظار الى من جعلني احمل اسمه و قوته و صبره الى **الوالد الأب** الأروع في العالم شكرا الى الروح التي ساندتني و أزهرت بوجودها حياتي الى القلوب الطاهرة التي تساندني أينما كنت اخوتي: **وليد، محمد ، أيمن.**

الى من تحلو بالاخاء و تميزو بالوفاء و العطاء أصدقائي رفاق دربي: **نذير، عبدو، أنور، باديس، سيف، تقي، رستم، إلياس، جهاد، عصام، علام، شوشو، أمير، عبد الرزاق، نجم، صلاح(اللاح)، هشام.**

الى الجوهرتين: **" شيراز وجبريل"**

أهذي ثمرة هذا العمل إليكم جميعا وإلى كل طالب علم مع جزيل الشكر و الامتنان والتحيات الخالصة لكم

خالد

سليمـــان

الإهداء

كيف يمكن للبذرة أن تصدق ان هناك شجرة ضخمه مخبأةً بداخلها...ماتبحث عنه موجود بداخلك

شمس التبريزي

الى روحك السلام .. مولانا شمس

الى كل من آمن أن ما بداخله عظيم ..الى من آمن بالانسانية..

الى كل المكافحات في الدنيا

الى النساء .. كلكن تستحققن أسمى ما في الاحترام و الحب..

الى الأستاذة الأولى و الأخيرة التي علمتي و ستبقى تعلمني ..انتِ الحياة.. أمي

الى أعظم رجل أتغنى افتخارا بحبه باحترامه بتقديسه .. أبي

الى أخي الذي لطالما فهمني كأنه مرآتي .. بفضلك أنا أقوى .. أسامة

الى من أغني له كل يوم " جاري يا حمودة " الى القلب الأحن و الأكرم .. أحبك بشدة أخي أحمد

الى زميلي في اعداد المذكرة .. أعتقد أننا حققنا معجزة أن لا نتشاجر بسبب المذكرة .. شكرا لتفهمك و تفانيك في العمل

الى خولة .. شكرا لقدسية الحب الذي جمعنا

الى أحلى ما في الورود .. زهرة

الى المعنيين المتلازمين الايمان و اليقين .. الى الفتاتين ايمان و نور اليقين

الى كل عائلتي .. الى كل من يحبني أو يكرهني..

الى قِطي

أسماء باهي

مقدمة

رافق التأسيس لنظام دولي جديد مجموعة من التحولات على مستوى الواقع الدولي والأطر النظرية والمفهومية، وذلك بظهور فواعل وتفاعلات مستحدثة داخل بنية النظام الدولي، وظهور مقاربات ونظريات جديدة مفسرة لهذا الواقع الدولي، فمن المتغيرات الجديدة التي جاء بها النظام الدولي الجديد، الثورة في الشؤون المعلوماتية كبعد خامس في الجيوستراتيجيا الذي برز فيه مفهوم الأمن الإلكتروني، فقد تكرس هذا المفهوم متحولا في الشقين العلمي والعملي من خلال التوسع في مفهوم الأمن من جهة والتعمق في وحداته من جهة أخرى، خصوصا مع بروز إسهامات مدرسة كوبنهاغن للأمن التي كان لها الفضل الكبير في هذا المجال، إضافة للتطور التكنولوجي والثورة الصناعية الثالثة، فقد أفضى الظهور المجسد للامن الإلكتروني إلى تحيين صفة الحرب تجاهه فاصبحنا نتحدث عن الحرب الالكترونية والحماية الالكترونية من الهجمات المعادية له، خاصة في الدول الكبرى التي تعتمد على المعلوماتية كفضاء رسمي يقلص الكثير من الاعباء على كاهلها، من خلال تقريب الإدارة من المواطن وتطوير المعاملات وتسريعها في القطاعات المالية والاقتصادية والإدارية الحكومية وحتى القطاعات الامنية (كمؤسسات الجيش والشرطة وغيرها من الوحدات) لهاته الدول، وعليه توجب على هاته الدول بناء منظومات واستراتيجيات لمواجهة أي تهديد لكيانها الالكتروني وتقنين جرائمه وهذا لحماية المنظومة الالكترونية التابعة لها، وسنحاول من خلال هذه الدراسة التطرق لتجربة الولايات المتحدة الأمريكية في مجال حماية الأمن الإلكتروني كدراسة حالة، باعتبارها القوة الأولى عالمياً وفق التصنيف الجوستراتيجي للقوة غير أن ظهور البعد الخامس للقوة (الفضاء السيبراني) كبعد جديد يضاف للأبعاد الأخرى وما صاحبه من قابلية شديدة للعطب جعل دولة عظمى كالولايات المتحدة الأمريكية لا تستطيع تحقيق أمنها الإلكتروني بشكل كامل أو بمستوى أضعف مقارنة مع دول أخرى هامشية في مجالات القوة الجوستراتيجية التقليدية كإستونيا مثلاً.

على هذا النحو تسعى هذه الدراسة للبحث في أحد جوانب الأمن وهو الأمن الالكتروني للدول الكبرى واستراتيجية حماية هذا الأمن من التهديدات المستحدثة في الفضاء السيبراني خاصة، بالخوض في الجانب المعرفي للأمن الالكتروني ومفاهيمه وعلاقته بالمفاهيم الأخرى المشابهة، وكذا الاستراتيجية المتبعة لحماية أمن المعلومات للدول الكبرى، وعلى الصعيد العملي أخذنا دراسة حالة (الولايات المتحدة الأمريكية) أنموذجا في حماية امنها الإلكتروني من التهديدات والهجمات على كيانها المعلوماتي، من خلال رصد مختلف استراتيجياتها المتبعة في هذا المجال، مع محاولة الاستشراف بمستقبل التعاون الدولي في هذا المجال.

1/ دوافع اختيار الموضوع:

نقسم الدوافع إلى:

أ- **دوافع ذاتية:** من أجل ضمان النتائج المرجوة من أي بحث لا بد من توفر الرغبة الداخلية لدى الباحث في دراسة الموضوع اضافة إلى تناسب قدرته لدراسة موضوع من أجل بحث علمي هادف، وهو ما تحقق كرغبة منا لدراسة هذا الموضوع.

وأيضا نعتقدا أن الخوض في دراسة مثل هذه الموضوعات في حقل الدراسات الاستراتيجية يدعمنا بقدر من الخبرة والاحاطة، وكذا مسايرة الوضع الدولي العام، خاصة في الجانب المعلوماتي. والأهم من ذلك حالة التطور التكنولوجي في المجال الرقمي واعتماده من الدول بالتالي يصبح حالة من المتغيرات الأمنية الواجب الدراسة مننا.

أ) **دوافع موضوعية:**

ترتبط الدوافع الموضوعية لاختيارنا هذا الموضوع في:

- الاستفادة من تجسيد النتائج العلمية والنظريات التي وصل اليها المفكرين في الحقل الاستراتيجي.
- قياس مدى امكانية تأثير العامل المعلوماتي على تهديد الأمن القومي للدول.
- تداخل وترابط الحقول المعرفية لدراسة هذا الموضوع انطلاقا من الدراسات الاستراتيجية ومرورا بمقاربات الأمن الجديدة وصولا لدراسات السلام الالكتروني، فالدراسات الاستشرافية.
- استخراج أهم التهديدات الكترونية التي شكلت خطراً على أمن المعلومات.
- المساهمة في صياغة جملة الاقتراحات والبدائل الاستراتيجية كحلول لمعضلة التهديدات الأمنية.

2/ إشكالية الدراسة:

مثل ما يعرف عن البحوث العلمية ودراساتها فإنها تأتي استجابة لحل تعقيدات ومشكلات بحثية عادة ما يعبر عنها في شكل سؤال مركزي، وأسئلة فرعية تخوض في البحث محل الدراسة، حيث تتمحور الدراسة على استراتيجيات الدول الكبرى في حماية أمنها الالكتروني من التهديدات الإلكترونية، وكذا كيفية مواجهة الأخطار المستمرة من التهديدات لهذا الأمن ومدى استخدام الآليات المواجهة لها، والتعرف على جهود

الولايات المتحدة الامريكية في تحرير مسار كيانها المعلوماتي ومواجهة أخطاره وكذا التعاون الدولي مع باقي الامم والفواعل، وعليه نطرح الإشكالية التالية:

- ✓ **هل من استراتيجية ناجزة لحمـــاية الدول أمنها الإلكترونـــــي والحد من تهديداته ؟**

الأسئلة الفرعية:

- ماذا نقصد بمفهوم الاستراتيجية؟
- كيف يمكن تعريف الأمن الإلكتروني وما هي أبرز التهديدات الإلكترونية؟
- ما هي المحددات الأساسية التي تحكم علاقات الدول الكبرى في الجانب الالكتروني؟
- ما آليات الدول الكبرى في الحد من الهجمات الالكترونية؟
- كيف تحمي الولايات المتحدة الأمريكية أمنها الإلكتروني؟
- كيف يمكن أن تسهم الجهود الدولية في تثبيت الاستقرار الالكتروني؟.

الفرضيات:

أ/ الفرضية المركزية:

- ✓ **ببنـاء إستراتيجية مشتركة للأمن الالكتروني، من شأنه أن يساهم في مواجهة التهديدات المعلوماتية تدريجيا.**

ب/ الفرضيات الفرعية:

- ✓ **اعتماد آلية الشراكة الدولية في مواجهة الأخطار المعلوماتية، سيحكم السيطرة على تفشي ظاهرة القرصنة الالكترونية.**
- ✓ **كلما تم تبني استراتيجية الكترونية متعددة الأبعاد في الأمن القومي الأمريكي قائمة على الفعل الاستباقي، أدى ذلك للتخفيف من حدة العطب الذي يمكن ان تحدثه التهديدات الالكترونية.**

3/ أهداف الدراسة:

- التعرف والتحكم الجيد في الإطار النظري للدراسة انطلاقا من الاستراتيجيات المعالجة لظاهرة تهديدات الأمن الالكتروني.
- التعرف على أسباب ظهور الأمن الالكتروني كأمن وطني.
- معرفة الأسباب الظاهرية والباطنية التي أدت إلى اشتعال الحروب الالكترونية وكذا استراتيجية تأمين الكيان المعلوماتي.
- تأثير الواقع الدولي في التركيز على جانب الأمن المعلوماتي.
- تحديد أبرز الآليات المعتمدة من طرف الدول الكبرى في حماية الكيان الإلكتروني.
- التعرف على النموذج الأمريكي –محل الدراسة– في كيفياته المعتمدة للحد من التهديدات الالكترونية.

4/ حدود الدراسة:

أ) **الحدود الزمانية:** يعتبر الحصر التاريخي لمجال الدراسة أمر ضروري لتسديد الجهد وتوضيح المقصود منها، وبما أن الدراسة تدور حول استراتيجيات حماية الأمن الإلكتروني، فإن الحدود الزمانية للدراسة ستحدد انطلاقا من ظهور الأمن الإلكتروني على المستوى العلمي والعملي، ثم مرورا بنهاية الحرب الباردة والتأسيس لنظام دولي جديد إلى غاية الآن.

ب) **الحدود المكانية:** تتمحور دراستنا في حدودها المكانية، على الدول الكبرى إضافة دراسة الحالة وهي الولايات المتحدة الأمريكية، وبالتالي الحدود المكانية تتمحور حول هذا الحيز المكاني.

5/ أهمية الدراسة:

أ) الاهمية العلمية:

- رصد أهم التغيرات النظرية والمخرجات الفكرية التي يمكن أن تساعدنا في التحول في التوسع في مفهوم الأمن.
- التعرف على أنجع النماذج الاستراتيجية لحماية أمن المعلومات.
- التعرف على الاستراتيجيات والوسائل التي تضمن القضاء على التهديدات المعلوماتية.

ب) الأهمية العملية:

- اسقاط الطروحات والاقترابات النظرية التي قدمت في فهم معنى الاستراتيجية الامنية ة تفسير أسباب ودوافع الهجمات الالكترونية، وتقييم مدى نجاعة حماية الامن الالكتروني.

- تحديد أبرز التهديدات المعلوماتية التي واجهت المنظومة الالكترونية للدول الكبرى.
- التعرف على أبرز الآليات المعتمدة في مواجهة التهديدات الالكترونية.
- التعرف على التقنينات الدولية في اطار مكافحة الجريمة الإلكترونية.
- الكشف على نموذج الجهود الدولية في صد وعرقلة الهجمات الالكترونية.

6/ المناهج والتقنيات المتبعة:

-**المنهج الوصفي التحليلي**: لأننا بصدد رصد وجمع وترتيب نظريات وافكار ومعلومات ومعطيات تساعدنا في فهم المسألة ومحاولة تحليل علمي لاتباع الدول الكبرى لحماية أمنها الإلكتروني.

-**المنهج دراسة حالة**: تم استخدام المنهج دراسة حالة من خلال اسقاط الضوء على الكيان الإلكتروني الامريكي كأمن قومي والاستراتيجيات المتبعة من الولايات المتحدة الأمريكية في حماية أمنها الالكتروني.

-**المنهج التاريخي**: حيث سنحاول في هذا البحث الاستعانة بأسلوب العرض الكرونولوجي المشتق من المنهج التاريخي، ومن خلاله رصد مجموعة من الاحداث التاريخية خاصة فيما يتعلق بكرونولوجيا تهديدات الولايات المتحدة الامريكية لامنها الإلكتروني.

-**المنهج المقارن**: اعتمدنا في دراستنا على دراسة المقارنة بين الدول الكبرى في حماية كياناتها المعلوماتية وكذا النموذج دراسة الحالة (الولايات المتحد الامريكية).

-**تقنية السيناريو**: اعتمدنا على تقنية السيناريو في دراستنا لمستقبل التهديدات الالكترونية و الشراكات الدولية للحد من العطب في المستقبل.

7/ ضبط المفاهيم:

- **الاستراتيجية**: نستخدم مصطلح الاستراتيجية في دراستنا في الفصل الأول كمقاربة مفاهيمية و في الفصل الثاني والثالث في الاطار التطبيقي للدراسة.
- **الامن الإلكتروني**: ونعتمد على المفهوم في الدراسة كأحد المفاهيم الأساسية في الدراسة في الفصل الأول و الثاني والفصل الثالث.
- **أمن المعلومات والأمن السيبراني**: ونقصد به في دراستنا مصطلح الأمن الإلكتروني لما جاء في عديد الدراسات.

7/ الخطـــــــــــة:

- **مقدمة.**
- **الفصل الأول: مقاربة مفهومية للاستراتيجية، والأمن في الفكر الانساني.**

- المبحث الأول: تطور مفهوم الاستراتيجية في الفكر الانساني.

المطلب الأول: المفهوم الضيق للاستراتيجية، الاستراتيجية التقليدية.

المطلب الثاني: الاستراتيجية كمفهوم موسع، الاستراتيجية الحديثة.

المطلب الثالث: المفاهيم ذات الصلة بالاستراتيجية.

- المبحث الثاني: مفهوم الأمن الالكتروني.

المطلب الأول: تعريف الأمن الالكتروني.

المطلب الثاني: ظهور الأمن الالكتروني.

المطلب الثالث: علاقة الأمن الإلكتروني بالمفاهيم ذات الصلة.

- المبحث الثالث: التهديدات المعلوماتية، ومواجهتها.

المطلب الأول: تأثير العولمة في الأمن الإلكتروني.

المطلب الثاني: تأثير التهديدات الإلكترونية على الكيان المعلوماتي.

المطلب الثالث: اجراءات الحد من التهديدات المعلوماتية.

المطلب الرابع: الجهود الاممية في بناء السلام السيبراني.

- **الفصل الثاني: مواجهة الدول الكبرى للتهديدات الالكترونية.**

- المبحث الأول: إدخال المعلوماتية في الكيان الأمني للدول الكبرى.

المطلب الاول: تحيين المنظومة السياسية و الإدارية للدول.

المطلب الثاني: عصرنة القطاعات و المؤسسات الوطنية.

المطلب الثاني: عالمية البيانات الوطنية و الإدارية للدول (ربطها بالشبكة العالمية)

- المبحث الثاني: التهديدات الإلكترونية لقطاعات الدول.

المطلب الأول: اتلاف البيانات المؤسساتية و الإدارية.

المطلب الثاني: القرصنة بسحب المعلومات الشخصية.

المطلب الثالث: الجوسسة على العمل الممارس للدول الكترونيا.

- المبحث الثالث: الشراكات الدولية في إطار سلامة الأمن الإلكتروني.

المطلب الأول: الشراكة الأمريكية والدول الأوروبية لمكافحة الجريمة الإلكترونية.

المطلب الثاني: الشراكة الأوروبية تحت غطاء الناتو في تأمين السيرورة السيبرانية.

المطلب الثالث: الجهود الاممية و الدول الغربية في إطار الحماية الإلكترونية.

- **الفصل الثالث: الاستراتيجية الامريكية في تأمين كيانها الالكتروني.**

- المبحث الاول: قراءة عامة للامن الالكتروني الامريكي.

المطلب الأول: عصرنة القطاعات و المؤسسات الأمريكية.

المطلب الثاني: اعتماد المعلوماتية في الأمن القومي الأمريكي.

المطلب الثالث: تقنين الامن المعلوماتي.

- المبحث الثاني: التهديدات المعلوماتية، وطرق مواجهتها في الولايات المتحدة الأمريكية.

المطلب الأول: أبرز الهجمات التي عانت منها أمريكا.

المطلب الثاني: إنشاء الجيش الإلكتروني الأمريكي.

المطلب الثالث: الآلية الدفاعية الأمريكية في مواجهة العطب الإلكتروني.

- المبحث الثالث: مستقبل التعاون الدولي في إطار الحماية الدولية للمعلوماتية.

المطلب الاول: مستقبل التهديدات الإلكترونية.

المطلب الثاني: الإتفاقيات الدولية في إطار الحماية الدولية للمعلوماتية.

- **الخاتمة.**

الفصل الأول

بفعل التغير في الواقع الدولي لجانبه النظري والعملي فإن الاستراتيجية لعنصر في الواقع الدولي أيضا قد تحولت من مفهومها الضيق، إلى المفهوم الموسع لتصبح شاملة لأبعاد الأمن، وبالتالي أصبحت تعنى الاستراتيجية أيضا بالأمن الإلكتروني كأحد أبعاد الأمن، وعليه سنتطرق لتحديد مفهوم الاستراتيجية بشقيها الضيق والواسع، وكذا ربطه بالأمن الإلكتروني ونبرز أيضا التهديدات التي تواجهها الدول و الشراكة في بناء السلام الإلكتروني الذي بدوره سنحدد مفهومه ودلالاته أيضا في هذا الفصل.

المبحث الأول: تطور مفهوم الاستراتيجية.

نتطرق في هذا المبحث لمفهوم الاستراتيجية في جانبها الضيق، مرورا بالجانب الواسع لها، مع تحديد اهم المفاهيم ذات الصلة بالاستراتيجية.

المطلب الأول: المفهوم الضيق للاستراتيجية.

إن مصطلح الاستراتيجية هو مصطلح ذو اصل عسكري، ومن الناحية التاريخية ارتبط لفظ الاستراتيجية بالحرب وإدارتها، وعند ظهور علم الحرب أصبحت استراتيجية الحرب فرعا من فروعه.[1]

ويعود تاريخ الاستراتيجية إلى كتابات المفكر الصيني (سان تزو)، الذي ارشد القادة العسكريين من خلال كتابه (فن الحرب، إلى التخطيط في الحرب)، من أجل النصر وقد صاغ رأيه في الاستراتيجية بعبارة ذات دلالات هي: تظاهر في الشرق واضرب في الغرب.

حيث عرف كارل فون كلاوزفيتش الاستراتيجية بأنها: (استخدام الاشتباك وسيلة للوصول إلى هدف الحرب).[2]

و يقول الجنرال الفرنسي اندريه بوفر (ليست مجرد رياضة عقلية تنطوي على الغرور أو التحذلق , وإنما هي نمط من التفكير يجب برغم تعقيده أن يكون بمثابة مرشد عملي لتحقيق غايات السياسة على خير وجه وخاصة لتفادي الأخطار الجسيمة التي يظهر لنا التاريخ الحديث أمثلة عديدة منها).[3]

وفي تعريف ليدل هارت، فإن الاستراتيجية: (فن توزيع استخدام مختلف الوسائل العسكرية لتحقيق هدف السياسة)، أما كولين آرون يعرفها بأنها (عملية أو مسار تحويل القوة العسكرية إلى مخرجات سياسية).[4]

وسوكولوفسكي يرى بان الاستراتيجية تمثل، مجموعة من المعارف النظرية التي تعالج قوانين الحرب كصراع مسلح دفاعاً عن مصالح طبقية محددة، وتدرس الاستراتيجية في ضوء التجارب العسكرية والأوضاع السياسية

---

[1]–مصطفى طلاس وآخرين , الاستراتيجية السياسية العسكرية , الجزء الأول الطبعة الأولى ,دار طلاس للدراسات والترجمة والنشر ,(دمشق) 1991. ص 33.

[2]–دينا محمد جبر، مقالة من موقعIASJ ، التاريخ: 2018/02/11 بتوقيت 22: 17 رابط المقال:
https: //www.iasj.net/iasj?func=fulltext&aId=27060

[3]–مصطفى طلاس، مرجع سابق. ص ص 36–37.

[4]–منير شفيق، الاستراتيجية والتكتيك في علم الحرب، الدار العربية للعلوم، بيروت: 2008. ص 27.

والعسكرية والطاقات الاقتصادية والمعنوية، وأساليب تصريف الحروب، ووجهات نظر العدو المحتمل وأوضاع الحرب المقبلة وطبيعتها وطرائق الإعداد لها وتسيير دفتها وفروع القوات المسلحة، وأسس استخدامها الاستراتيجي بالإضافة الى أسس الحرب المادية والتقنية وتظل في الوقت نفسه مجال النشاط العملي للقيادة السياسية والعسكرية العليا في القيادة العامة ومقرها، والمتعلق بـ: فن إعداد البلاد للحرب وتصريف الصراعات المسلحة في ظل أوضاع تاريخية محددة.[1]

أما المفهوم العام الأمريكي للاستراتيجية فقد عرف دليل ضباط أركان القوات المسلحة الأمريكية لعام 1959 الاستراتيجية بأنها فن وعلم استخدام القوات المسلحة للدولة لغرض تحقيق أهداف السياسة العامة عن طريق استخدام القوة أو التهديد باستخدامها.[2]

وفي تعريف للمدرسة العربية نجد أن المدرسة المصرية عرفت الاستراتيجية بأنها: (أعلى مجال في فن الحرب وتدرس طبيعة وتخطيط وإعداد وإدارة الصراع المسلح وهي أسلوب علمي نظري وعملي يبحث في مسائل إعداد القوات المسلحة للدولة واستخدامها في الحرب معتمداً على أسس السياسة العسكرية كما انها تشمل نشاط القيادة العسكرية العليا بهدف تحقيق المهام الاستراتيجية للصراع المسلح لهزيمة العدو).[3]

المطلب الثاني: المفهوم الموسع للاستراتيجية، الاستراتيجية الحديثة

إذا كان تعبير الاستراتيجية قد اشتق أصلا من الكلمة اليونانية، وتعني فن القيادة، فإن استخداماتها المعاصرة قد تعددت وشملت العديد من الميادين، فقد يوصف موقع دولة بأنه استراتيجي، كان يقال (الموقع الاستراتيجي لقناة السويس أو الخليج العربي، وقد يوصف قرار سياسي أو اقتصادي بأنه استراتيجي، كما يطلق إلى معاهدة الحد من الأسلحة المتطورة، فيشار إلى معاهدة الحد من الأسلحة الاستراتيجية، كما توصف بعض المواد والسلع الاقتصادية بأنها استراتيجية كالنفط مثلا، واخيرا فقد يوصف نمط من التفكير أو الدراسات المتخصصة بأنه تفكير استراتيجي أو دراسات استراتيجية.4

---

[1]–المارشال سوكوفسكي، الاستراتيجية العسكرية السوفياتية، ترجمة خيري حماد، بيروت. ص 46.

[2]–محمد بنحمو، الاستراتيجية، المفهوم والنظرية، مركز راشيل كوري لحقوق الانسان، شوهد بتاريخ 2018/03/02 بتوقيت 19:55 رابط المقالة:

http: //rachelcenter.ps/news.php?action=view&id=10294

[3]–محمد بنحمو، مرجع سابق. ص 48.

[4]–عبد القادر محمد فهمي، المدخل إلى دراسة الاستراتيجية، دار مجدلاوي للنشر والتوزيع، عمان: 20.ص.18.

تعرف اليوم كلمة استراتيجية انتشارا واسعا غير مسبوق فبعد خروجها من حقل المعارك احتلت تقريبا كل مجالات النشاط الانساني، واصبح الجميع يدعي تبني استراتيجية خاصة، الأمر الذي دفع بالباحث جون بول شارنيه للقول: إننا نشهد انحرافا في معنى الكلمة يهدد بإخراج المصطح من خصوصيته أو الانقاص من أهميته أو تمييعه.1

فالاستراتيجية قد ظهرت قبل العلاقات الدولية بأشواط طويلة، ودخلت المجالات التطبيقية في الحياة السياسية والعسكرية قبل العلاقات الدولية، على الرغم من أن مفهوم الاستراتيجية قد ظهر ملازماً للمعارك والحروب وإدارة وقيادة الجيوش في المعارك، وعلى هذا الأساس إذا ما أردنا أن نضع مقاربة في مجالات العمل والتطبيق والشمول فنجد أن الاستراتيجية تعمل في المجالات كافة منها الداخلية والخارجية والتي تشتمل على الأمور السياسية والعسكرية والاقتصادية والاجتماعية والثقافية ... الخ، بحيث أصبح هناك استراتيجية عسكرية واستراتيجية سياسية واستراتيجية اقتصادية واستراتيجية اجتماعية وثقافية اضافة إلى الاستراتيجية العليا الشاملة للدول، بينما تعمل العلاقات الدولية في الخارج فقط، على الرغم من إن العلاقات الدولية هي نتاج للشؤون الداخلية ونابعة من الداخل ولكن هي تختص في العلاقات الخارجية ما بين الدول فقط، على عكس الاستراتيجية التي تعمل في الداخل والخارج وتشمل كل شيء.

وهناك نقطة جدا مهمة يجب ذكرها أن العلاقات الدولية لم تنشأ إلا بعد نشوء الدول القومية، بمعنى أن ظهور الدول القومية في منتصف القرن السابع عشر، صاحب معه ظهور العلاقات بين الدول وهذه العلاقات تطورت مع تطور الحياة السياسية والاقتصادية والاجتماعية للدول مما أدى إلى ظهور مصطلح العلاقات الدولية على أسس قانونية نظمتها الشرائع التي ولدت بعد معاهدة وتفاليا، وهذا الكلام يثبت أن العلاقات الدولية تعد حقلاً حديثاً بالمقارنة مع مصطلح الاستراتيجية الذي يعد تاريخ نشأته تتجاوز العشرين قرن من الآن.

و في النهاية يمكن القول أن الاستراتيجية في أبسط معانيها تعني الوسيلة أو الطريقة التي تؤدي بنا إلى تحقيق أهدافنا المتعلقة بالدرجة الأولى بالدولة ولذلك نجد أنها تحتل مكانة كبيرة في حقل العلاقات الدولية في

[1]–مصطفى بخوش، تطور الفكر الاستراتيجي في حقل العلاقات الدولية ،مجلة دراسات شرق اوسطية، عدد 59، شوهد بتاريخ 2018/03/02 بتوقيت 22: 55. ص. 3 رابط المقال:

https: //platform.almanhal.com/Files/2/442

أحد فروعه، كما تجدر الإشارة إلى أن مصطلح الاستراتيجية غير مرتبط بالحرب فقط، فنجد استراتيجية اقتصادية، سياسية، اجتماعية.[1]

وبدخول مصطلح الاستراتيجية الى ميادين متعددة: سياسية اجتماعية، اقتصادية، بدأت تظهر وجهات نظر مختلفة، حول مفهوم الاستراتيجية، إذ يرى البعض ان مفهوم الاستراتيجية ارتبط بقرارات التي يتم اتخاذها بغرض تحقيق أهداف معينة ومن هذه الزوايا تعرف الاستراتيجية، بانها قرارات صادرة ومؤثرة تتخذها المؤسسة لتعظيم قدرتها على الاستفادة بما تتيحه البيئة من فرص لوضع أفضل الوسائل لحمايتها. [2]

أن مفهوم الاستراتيجية هو أكبر وأكثر فائدة من أن نقصره على الاستخدام العسكري فقط. وبهذا فإننا ننطلق في هذه الدراسة إلى آفاق أوسع وأرحب في المفهوم الواسع للاستراتيجية ، ولكننا قبل أن نبلغ هذا المدى سوف نستصحب المفهوم العسكري قليلاً ونحن نكتب عن مفهوم "استراتيجية العلاقات الخارجية" لنلاحظ كيف تم استخدام هذا المصطلح في الإطار العسكري في مقابل المفهوم الواسع للاستراتيجية وخاصة في مسائل الأمن القومي.[3]

المطلب الثالث: المفاهيم ذات الصلة بالاستراتيجية.

للاستراتيجية مجموعة من المفاهيم المتداخلة فيما بينها والمركبة لها في حقل العلاقات الدولية:

الفرع الأول: التكتيك.

يعتبر Clausewitz أن التكتيك هو النظرية النسبية لاستخدام القوة المسلحة في المعركة، انه العملية التي تستخدم الذكاء، المعرفة والتنظيم كما يشير نابليون في أحد تعليقاته، يعتبر Antoine Grouard في كتابه للاستراتيجية: موضوع- ارشاد- عناصر والصادر عام 1895 أن التكتيك له ثلاثة أجزاء: التكتيك الأولي، أو التكتيك المفصل، يضم أساليب القتال للوحدات الصغيرة في كل جيش؛ تكتيك المجموع أو

---

[1]-صباح بالا، الاستراتيجية الدولية، الموسوعة السياسية، شوهد بتاريخ 2018/02/10 رابط المقالة:
http: //political-encyclopedia.org/2017/08/05

[2]-محمد احمد عوض، الإدارة الاستراتيجية، (الأصول، الأسس النظرية)، الدار الجامعية. الاسكندرية. 1999.ص10.

[3]-عمر فضل الله، تعريف الاستراتيجية ،مدونة عمر فضل الله، ،شوهد بتاريخ 2017/12/15 بتوقيت 16:35 رابط المقال:

http: //www.omarfadlalla.com/?p=2342

للجيوش الثلاثة (المشاة، الفرسان، المدفعية) يعمل لمعرفة دور كل جيش في المعركة؛ التكتيك الكبير أو تكتيك الوحدات الكبيرة، وهو مهارة قادة الجيش، الفن الذي يتبعه قائد الجيش لتحديد دور كل من جيوشه في المعركة، للنصح باستخدام قوات الاحتياط، وجعلها تتدخل في الوقت المناسب وفي الشروط الملائمة.[1]

والصلة بين التكتيك والاستراتيجية تكمن في:

- الاستراتيجية هو الالتزام بالخطة في أن فحوى التكتيك هو تكييف الخطة حسب الموقف
- الاستراتيجية هي الخطة الشاملة للوصول الى الهدف النهائي في حين أن التكتيك هو خطة جزئية لتحقيق هدف جزئي.
- الاستراتيجية طويلة وبطيئة وبعيدة المدى في حال أن التكتيك هو ردة فعل وقصير المدى.
- توضع الاستراتيجية لنتائج مستقبلية في حين أن التكتيك لنتائج حالية.
- الاستراتيجية تقوم على التخطيط والتفكير المنطقي في حال التكتيك يقوم أكثر على الإبداع.[2]

الفرع الثاني: التخطيط الاستراتيجي:

نحكم على التخطيط الاستراتيجي بأنه ،تقديم الدعم والسند المطلوب لتحقيق المصالح الاستراتيجية الوطنية على الساحة الدولية، ويتضمن كذلك تعزيز القدرات التفاوضية للدولة في حوار المصالح الدولية وتعزيز بناء شراكة دولية عادلة بين الدولة والأسرة الدولية وتعزيز السلام والأمن الدولي والحفاظ على البيئة الدولية، وذلك من خلال تحقيق التوازن بين مقتضيات المصلحة الوطنية ومقتضيات المصلحة العالمية.

التخطيط الاستراتيجي ترجمة لاستراتيجية محددة، إذ هو الذي يصوغ تفصيلات عملية تحويلها إلى تطبيق عملي، ويوضح أن هدف هذا التخطيط هو «التخطيط للمهمة الموكلة إلى الاستراتيجية العسكرية، أي وضع القوات المسلحة في أقصى وضع ملائم متفوق على العدو قبل بدء العمليات لأنه يتناول كيف يتم ذلك».

---

[1]- صلاح نيوف، مدخل إلى الفكر الاستراتيجي، الاكاديمية العربية المفتوحة بالدنمارك.

[2]- ملاذ المدني، الفرق بين الاستراتيجية والتكتيك، اراجيك، شوهد بتاريخ 2018/02/12 رابط المقالة:
https: //www.arageek.com/2012/09/16/difference-between-tactics-and-strategies.html

ولكن التخطيط الاستراتيجي لا يكون ناجعا إلا إذا اكتملت عناصره، من المرونة في الخطة إلى بعد النظر والاستمرار في التخطيط والتنفيذ إلى إعداد خطة الإمكانات المتوافرة، وحساب الاحتمالات وحرية الحركة.. وغيرها من العناصر الضرورية لإعداد خطة محكمة.

وبناء على كل هذه المعلومات ينتهي المؤلف إلى أن الاستراتيجية «هي العملية التي تمتد من لحظة تحديد الهدف من الحرب إلى تحقيقه مرورا بالتطبيق»، ولذلك فإن أي استراتيجية لا بد من أن تنطلق من تحديد الهدف الذي تعمل من أجل تحقيقه.[1]

[1]–محمود الهلال سيد، فن علم الحرب ،موقع الجزيرة.نت، شوهد بتاريخ 2017/12/29 رابط المقال:
http: //www.aljazeera.net/knowledgegate/books/2009/6/4/

المبحث الثاني: مفهوم الامن الإلكتروني.

يتمحور هذا المبحث في تحديد مفهوم دقيق للأمن الإلكتروني ومفاهيمه المحملة، مع نظرة لجذور نشأته، إضافة لإبراز أهم المفاهيم المشابهة له وذات الصلة به أيضا.

المطلب الأول: تعريف الأمن الإلكتروني.

يُعد مفهوم «الأمن الإلكتروني «Cyber Security أحد أهم مفاهيم الحقبة القادمة، التي ربما تشهد «حروبًا الكترونية» تحل محل الحروب التقليدية، لتصل إلى نفس مداها في الخسائر المادية، وربما تتعداه.[1]

وفي نظرة اخرى لتعريف الأمن الالكتروني، الوسائل والأدوات والإجراءات المطلوب توفيرها لضمان حماية المعلومات من الاخطار الداخلية والخارجية،[2] وفي تحديد أخر للأمن الإلكتروني هو المساعدة على حماية أصول وموارد منظمة ما من النواحي التنظيمية والبشرية والمالية والتقنية والمعلوماتية بحيث تتمكن من أداء المهمة الموكلة إليها إلكترونيا.[3]

وأيضا يتضمن الامن الالكتروني تأمين البينات والمعلومات التي تتداول عبر الشبكة الداخلية والخارجية من الاختراقات الالكترونية وحماية الفضاء الالكتروني منها بشتى أنواعها، فهو السلاح الاستراتيجي الوحيد من تكتيكات الحروب الحديثة ولهذا كان انشاء هذه الهيئة خطوة بالغة الاهمية، والأمن السيبراني كأمن المعلومات يرتكز على ثلاث ركائز أساسية لا يمكن لواحدة أن تتخلف عن الأخرى وهي: التوفر والموثوقية والخصوصية. فالمعلومة يجب أن تكون متوفرة عند الحاجة إليها وموثوقة المصدر آمنة من العبث أو التغيير، إلى جانب أنه لا يطلع عليها إلا المخول له الاطلاع عليها، وكل ذلك لا يتم إلا عن طريق تحقيق معايير الأمن السيبراني الصحيحة.[4]

---

[1] محمد محمود السيد، كيف سيواجه العالم تحديات الأمن السيبراني؟، مجلة السياسة الخارجية، شوهد بتاريخ2018/01/17 رابط المقال:

http: //www.siyassa.org.eg/News/4925.aspx

[2] محمد غيطاس، مركز الجزيرة للدراسات.

[3] حمدون أتوريه، دليل الأمن السيبراني للدول النامية، الإتحاد الدولي للاتصالات، 2006. ص8.

[4] فيصل اليوسف ،الأمن السيبراني والفضاء الالكتروني، جريدة اليوم، السعودية، شوهد بتاريخ 3 نوفمبر 2017 رابط المقال:

http: //www.alyaum.com/article/4213196

وفي سياق أخر تم تعريف الامن الالكتروني بأنه " حماية البيانات الالكترونية والسرية المهنية والملكية الفكرية والبنى التحتي الأساسية للاتصالات باعتبار ان الشبكات المحلية تتصل بالشبكات العالمية للأنترنت".[1]

يرتكز على ثلاث ركائز أساسية لا يمكن لواحدة أن تتخلف عن الأخرى وهي: التوفر والموثوقية والخصوصية. فالمعلومة يجب أن تكون متوفرة عند الحاجة إليها وموثوقة المصدر آمنة من العبث أو التغيير، إلى جانب أنه لا يطلع عليها إلا المخول له الاطلاع عليها، وكل ذلك لا يتم إلا عن طريق تحقيق معايير الأمن السيبراني الصحيحة.[2]

و أبرز تعريف شامل للأمن الالكتروني، هو عبارة عن مجموع الوسائل التقنية والتنظيمية والادارية التي يتم استخدامها لمنع الاستخدام الغير مصرح به وسوء الاستغلال واستعادة المعلومات الالكترونية ونظم الاتصالات والمعلومات التي تحتويها وذلك بهدف ضمان توافر واستمرارية عمل نظم المعلومات وتعزيز حماية وسرية وخصوصية البيانات الشخصية واتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين من المخاطر في الفضاء السيبراني. اذاً فالأمن الإلكتروني هو سلاح استراتيجي بيد الحكومات والإفراد لا سيما أن الحرب السيبرانية أصبحت جزءاً لا يتجزأ من التكتيكات الحديثة للحروب والهجمات بين الدول.[3]

يتضمن تامين البيانات والمعلومات التي تتداول عبر الشبكات الداخلية أو الخارجية والتي يتم تخزينها في خوادم داخل أو خارج الشكرة من الاختراقات.[4]

وابرز تعريف للأمن الإلكتروني الذي جاي في برنامج آسيا ،بانها تأمين سيرورة البيانات المخزنة في الخوادم، وتعتبر منظومة جديدة في المؤسسة العسكرية للدول، وهي الحامية لأشكال البيانات المرقمنة إلكترونيا.

فمنذ سنة 2010، بعد الهجمات المركز الإيرانية لنظام الأمن الإلكتروني العسكري للدول الغربية منها الولايات المتحدة الامريكية، اعتمدت الدول نظام تسليح إلكتروني متطور لحماية ك القطاعات التي تحوي بيانات رقمية سواء اقتصادية او ادارية.. الخ.[1]

---

[1]–مؤتمر الأمن السيبراني والدفاع السيبراني –تحديات وآفاق –، الجامعة اللبنانية والوكالة الجامعية الفرانكفونية auf،لبنان ص27.

[2]–فيصل اليوسف، مرجع سابق.

[3]–الامن السيبراني، الهيئة اللبنانية المنظمة للاتصالات، لبنان، شوهد بتاريخ: 2017/07/2 رابط المقال:
http: //www.tra.gov.lb/Cybersecurity–AR

[4]–عبد الله المبارك ،الفرق بين الامن الإلكتروني وامن المعلومات، مقالة بموقع linkdin شوهد ،بتاريخ،2018/03/12 رابط المقال:
https: //www.linkedin.com/pulseبين–ما–الفرق–و–information–abdullah–cyber–security–

بعد تحديد مفهوم الامن الإلكتروني والذي يصطلح أيضا بالأمن السيبراني، حيث نجد أن الأمن الإلكتروني يعنى بحماية البيانات المخزنة في الخوادم سواء المتصلة بالشبكة العالمية أو الشبكة المحلية من أي تهديدات تجاه هاته البيانات، كما ان هاته الأخيرة تتمثل في معلومات بطابع بيانات الدولة والفرد أو الدولة، الدولة أو الفرد والفرد.

المبحث الثاني: ظهور الأمن الالكتروني.

ان الثورة التكنولوجية التي شهدها القرن العشرين والتي أدت الى تغيرات خطيرة في شتى المجالات والتي تتجاوز أثارها السلبية آثارها الايجابية لا تعتبر ثورة عادية على الاطلاق باعتبارها في تطور هائل ومستمر فكل سنة تفوق ما قبلها بأضعاف من الانجازات في مختلف الميادين وعلى كافة المستويات ومن ثم يتضاعف الانتاج العلمي والمعرفي والتقني بشكل هائل حتى أصبحنا عاجزين عن متابعة ما يجرى حولنا.

يتم استخدام تكنولوجيا الاتصال والمعلومات للتعبير عن حالات الصراع بل هي أصبحت ساحة للصراع، كما أنها تستخدم في حل تلك الصراعات وتسويتها، وتغيرت أساليب الصراع مع ثورة التكنولوجيا والمعلومات وأصبح الصراع التقني هو الأكثر ظهوراً، وساهم الطابع التكنولوجي في ايجاد طرق جديدة للصراع بديلة للحرب المباشرة بين الدول، حيث ساهمت الآليات التكنولوجية في مساعدة المنظمات والدول في التنسيق بين جهودها والتفاعلات فيما بينها الكترونيا بعيداً عن الاتصال المباشر، وأدت الثورة التكنولوجية الى تغير شكل الحرب وأدواتها والفاعلين فيها مما ساعد على اختلاف درجة التهديد وآثاره وطبيعته ومصادره وظهور حرب الشبكات وحروب الفضاء الإلكتروني.

هذه المرحلة تتسم بالاستخدام الكثيف للتكنولوجيا ومن ثم فهي تتسم بتزايد درجات الخطر والتهديد واتساع ساحة المعركة وتنوع وسائلها، وأصبحت شبكة الانترنت أحد معالم ذلك المجتمع الجديد واكثرها تأثيراً وانتشاراً، ومن ثم أصبحت الجريمة العالمية سمة أساسية من سمات عصر المعلومات وأصبحت الجرائم أكثر تعقيداً وانتشرت الجماعات الاجرامية العالمية مستفيدة من آليات وأدوات الثورة التكنولوجية في الاتصالات وانتقال الأفراد والأفكار، وأصبح الارتباط الوثيق بين التكنولوجيا والأمن لأن الدول أصبحت تعتمد على التكنولوجيا بشكل كبير في عمليات الاتصالات والخدمات والانتاج ونظراً لاعتماد الدول على أنظمة معلومات أصبح من

[1] Emmanuel menet. la cyber guerre et la strauction des relations international. le cas nord coreen. programmen asie. decembre 2017. P.p2-3

السهل استهدافها وتدميرها من قبل الارهابيين، فلم يعد الارهاب فقط يهدف الى التأثير على الرأي العام، بل أصبحت البنية التحتية للدول هدف من أهداف الارهاب لتحقيق أهدافه المختلفة. [1]

أصبحنا نعيش في مجتمع المعلومات وهناك بعض المحددات التي ترتبط بخصوصية مجتمع المعلومات وهى أن المجتمع الشبكي دفع الجماعات المسلحة والتنظيمات الارهابية أن تجعل شبكات التواصل الاجتماعي عنوان لهويتها الالكترونية وتستخدمها لنشر أفكارها ونسقها الفكري والقيمي، وبالتالي أصبحت بنية المعلومات محل استهداف من قبل التنظيمات الارهابية سواء من خلال الاستهداف المادي المباشر والذى يتمثل في تدمير البنية التحتية التى تعتمد على النظم المعلوماتية، واستهداف مراكز الارسال، ولكن الأخطر من كل ذلك هو نشر الفيروسات وسرقة المعلومات من قبل القراصنة.

تتمثل المخرجات الأساسية لثورة التكنولوجيا والمعلومات في الطابع الإلكتروني والمعلومات والفضاء الإلكتروني، كلمة الفضاء الإلكتروني cyber مقتبسة من علم cybernétiques ، وهو عبارة عن نظرية الاتصالات والتحكم المنظم في التغذية العكسية التي تعتمد عليها دراسات الاتصالات والتحكم في الحياة وفي الآليات التي صنعها الانسان. ويتم وصف الفضاء الإلكتروني أي فضاء الانترنت بـ cyber space .

كلمة سايبر صاغها الروائي ويليام جيبسون لتعبر عن رؤيته لشبكة حاسوب كونية تربط الناس والآلات ومصادر المعلومات ومن ثم يمكن للإنسان أن يتحرك وكأنه يبحر في فضاء افتراضي، ومن ثم أصبحت السيبرانية اسم لعلم الاتصالات والمعلومات والتحكم، واستخدم جيبسون مصطلح الفضاء الإلكتروني cyber space في كتابه الكلاسيكي عام 1984. [2]

المطلب الثالث: المفاهيم ذات الصلة بالأمن الإلكتروني.

الفرع الأول: الحرب الإلكترونية: لم يحدد مفهوم مجمع عليه حول مفهوم الحرب الإلكترونية، إلا أنه تم وضع مسار لمفهوم الحرب الالكترونية من مجمعه الخبراء ذو الاختصاصات حيث، عرف كل من ريتشارك

[1]–التقرير العالمي لتكنولوجيا المعلومات، مجلة الشرق الأوسط ،شوهد بتاريخ 21 /2018/02: الرابط:
https: //aawsat.com/home/article/336976

[2]التقرير العالمي لتكنولوجيا المعلومات، المرجع نفسه.

كلارك وروبرت كناكي الحرب إلكترونية بأنها «جهد وعمل تقوم به دولة أو جهة ما تحاول من خلالها قرصنة واختراق حواسيب وشبكات تابعة لدولة أو طرف أخر بهدف تحقيق تعطيل في سيرورتها او نشاطاتها".[1]

يتعلق مضمون الحرب الإلكترونية بالتطبيقات العسكرية للفضاء السيبراني، حيث تعني –في أحد تعريفاتها– قيام دولة أو فواعل من غير الدول بشن هجوم إلكتروني في إطار متبادل، أو من قبل طرف واحد. وبرغم ذيوع مسمي الحرب الإلكترونية إعلاميا، فإنه يعد مصطلحا قديما كان بالأساس مقصورا على رصد حالات التشويش على أنظمة الاتصال، والرادار، وأجهزة الإنذار، بينما يكشف الواقع الراهن في الفضاء الإلكتروني عن دخول شبكات الاتصال والمعلومات إلى بنية ومجال الاستخدامات الحربية.[2]

الفرع الثاني: الحرب الرقمية: تلك الإجراءات التي يتم اتخاذها للتأثير بشكل سلبي على المعلومات ونظم المعلومات وفي نفس الوقت الدفاع عن هذه المعلومات والنظم التي تحويها. [3]

تعرف الحرب الرقمية بأنها الإجراءات التي يتم فيها التأثير بشكل سلبي على نظم المعلومات وكذلك الإجراءات المضادة التي تهدف للدفاع عن هذه المعلومات والنظم التي تحتويها والقيام باستخدام التقنيات الرقمية لإخافة وإخضاع الآخرين على خلفية دوافع سياسية أو عرقية أو دينية.

وتشمل القيام بالعمليات التي من شأنها تنفيذ الهجمات الرقمية التي تتضمن العمليات النفسية، والخداع العسكري، والهجمات الفيزيائية والهجمات على شبكات الكمبيوتر وتخريبها وقرصنة المعلومات والسعي للسيطرة على منظومات الخصم الرقمية وكذلك استخدام هجوم بالفيروسات والحرمان من الخدمات لتركيع مواقع الخصم، مما يؤدي إلى التقليل من مقدرة الخصم على الاتصال وإبطاء قدرته وجعله يخطئ في اتخاذ القرارات.

أصبحت الحرب الرقمية اليوم واقعاً ملموساً في ساحات الصراع الواقعية والافتراضية في مجابهات معلنة أحياناً وخفية في أحيان كثيرة فهي قد فاقت الحرب الإعلامية ووسائلها والحرب الاقتصادية وأدواتها والحرب التقليدية بعدتها وعتادها وأثرت بشكل كبير على مجريات الأحداث عالمياً فهي تتعدى الحدود الإقليمية للدول لتصل إلى

---

[1] Richard A. Clarke & Robert knake, Cyber War, HarperCollins (2010), p: 6

2–عادل عبدالصادق، حروب المستقبل.. الهجوم الإلكتروني على برنامج إيران النووي، مجلة السياسة الدولية، مؤسسة الأهرام، أبريل 2011.

3–سعد عطوة الزنط، الارهاب الالكتروني، إعادة صياغة استراتيجية الأمن القومي، المركز القومي للبحوث الاجتماعية والجنائية من 10 إلى 16 ديسمبر 2010. الو.م.أ.ص.2.

مراكز التحكم في قرارات الدول وأماكن صنع سياساتها الدفاعية والإقتصادية وانتشرت ترسانتها بشكل رهيب إذ لا يكاد يخلو منها بيت أو مؤسسة في جميع أنحاء العالم.[1]

الفرع الثالث: الإرهاب الإلكتروني: ينطلق تعريف الإرهاب الإلكتروني من تعريف الإرهاب, وفي ضوء التعريفات السابقة يمكن القول بأن تعريف مجمع الفقه الإسلامي الدولي التابع لمنظمة المؤتمر الإسلامي يعتبر من أفضل التعاريف الاصطلاحية للإرهاب وأقربها إلى الصواب؛ لقصر ألفاظه وإيجاز عباراته, ولشموله مختلف أنواع الإرهاب وأشكاله.

وتأسيساً على ما سبق يمكننا تعريف الإرهاب الإلكتروني بأنه: العدوان أو التخويف أو التهديد المادي أو المعنوي الصادر من الدول أو الجماعات أو الأفراد على الإنسان، في دينه أو نفسه أو عرضه أو عقله أو ماله بغير حق ,باستخدام الموارد المعلوماتية والوسائل الإلكترونية ,بشتى صنوف العدوان وصور الإفساد.[2]

فالإرهاب الإلكتروني يعتمد على استخدام الإمكانيات العلمية والتقنية, واستغلال وسائل الاتصال والشبكات المعلوماتية, من أجل تخويف وترويع الآخرين, وإلحاق الضرر بهم, أو تهديدهم. استخدام التقنيات الرقمية لإخافة واخضاع الآخرين أو هو القيام بمهاجمة نظم المعلومات على خلفية دوافع سياسية أو اقتصادية أو أمنية او عرقية أو دينية. [3]

الفرع الرابع: الفضاء الالكتروني: المجال العالمي فيه بيئة من المعلومات تتألف من ترابط شبكة البنى التحتية للمعلومات التي تتضمن الأنترنت وشبكات الاتصالات السلكية واللاسلكية وأنظمة الحواسيب وما ضم من معالجات وأجهزة تحكم. [4]

تُستخدم كلمة Cyberمقترنة بكلمة Space لتُعبر عن أشهر تعبير في عصر المعلومات، واستُخدمت Cyberspaceللتعبير عن الإنترنت في عام 1991، وأصبح هذا المفهوم أشمل وأوسع من الإنترنت ليضُم كل الاتصالات والشبكات وقواعد البيانات ومصادر المعلومات، وأصبحت بنية النظام

1-صلاح الدين أبو بكر الزيداني، طبول الحرب الرقمية، مجلة المسلح، بتاريخ 2016/01/14، شوهد بتاريخ 2018/01/29 بتوقيت 14: 31: رابط المقال

http: //www.almusallh.ly/ar/thoughts/633-vol-44-38

[2]-حمد فتحي سرور, المواجهة القانونية للإرهاب, الطبعة الأولى، القاهرة: دار النهضة العربية, 2008 ص 22.

[3]-سعد عطوة الزنط، مرجع سابق. ص.3.

[4]-مجاهد فخ الدين قاسم أحمد، ترجمة الصفحات من (1-61) من كتاب الأمن الالكتروني والحرب الالكرتونية لمؤلفيه بيتر وارن سينغر وألن أ،فريدمان، بحث تكميلي لنيل شهادة الماجستير في الترجمة، جامعة السودان للعولم والتكنولوجيا، السودان.ص ص17-18.

الإلكتروني تعني المكان الذي لا يُعد جزءاً من العالم المادي أو الطبيعي حيث أنها ذو طبيعة افتراضية رقمية الكترونية تتحرك في بيئة الكترونية حيوية تعمل من خلال خطوط الهاتف وكابلات الاتصالات والألياف البصرية والموجات الكهرومغناطيسية. ووصف «وليام جيبسون» العالم الإلكتروني بأنه «عبارة عن شبكات الكمبيوتر والاتصالات الإلكترونية وهو عبارة عن شبكة كمبيوتر خيالية تحتوي على كم هائل من المعلومات التي يُمكن الحصول عليها لتحقيق الثروة والسلطة.[1]

الفرع الخامس: أمن المعلومات: حماية المعلومات أو انظمة المعلومات من النفاذ غير المصرح أو السرقة أو التعديل أو التشهير لحفظ سرية وخصوصية العملاء وبقاء المعلومات وفقا لنهج CIA، وترمز للسرية والكمال والتوفر وهي جزء أساسي في جميع مراجع أمن المعلومات. [2]

الفرع السادس: القرصنة: التوصل الى المعلومات السرية والشخصية واختراق الخصوصية وسرية المعلومات بسهولة، أي تسريب البيانات الرئيسية والرموز الخاصة ببرامج شبكة الأنترنت. [3]

يشير مفهوم القرصنة الإلكترونية إلى ممارسات غير مشروعة على شبكات الحاسب الآلي، تستهدف التحايل على نظام المعالجة الآلية للبيانات بغية إتلاف المستندات المعالجة إلكترونيّا.

ويقوم بهذه الممارسات قراصنة معلومات محترفون، أو شركات متنافسة ضد بعضها البعض، أو فيما بين موظفي المنشأة الواحدة؛ حيث قدرت بعض الدراسات الحديثة أن 85% من عمليات اختراق برامج الحاسب الآلي تتم من خلال موظفي الشركات.

ويعود تاريخ أول عملية قرصنة إلى عام 1878 بإحدى شركات الهاتف المحلية الأميركية، ويعتبر الخبراء الفترة من 1980 إلى 1989 العصر الذهبي للقرصنة.

يتعلق تأمين الشبكات بحماية البيانات والأفراد والهيئات من المتطفلين وقراصنة المعلومات الذين يتداخلون في الاتصالات عبر الشبكات المفتوحة. ومن هذا المنطلق يمكن تصنيف شبكات المعلومات إلى شبكات خاصة وهي التي تكون مغلقة على عدد محدود من المستخدمين مثل الشبكات الداخلية للمؤسسات

---

[1]–عادل عبد الصادق ،الفضاء الالكتروني والرأي العام.. تغير المجتمع والادوات والتأثير،المركز العربي لأبحاث الفضاء الالكتروني ،شوهد بتاريخ 2018/01/12: رابط المقال:
http: //accronline.com/article_detail.aspx?id=2725

[2]–عبد الله المبارك ،الفرق بين الامن الإلكتروني وامن المعلومات، مرجع سابق.

[3]–سعد عطوة الزنط، مرجع سابق، ص4–5.

الكبرى وشبكات عامة وهي التي تكون مفتوحة لعدد كبير جداً من المستخدمين مثل شبكة المعلومات الدولية (الإنترنت).[1]

[1] القرصنة الالكترونية، الاكاديمية العربية البريطانية للتعليم العالي، م ذ و :شوهد بتاريخ 2018/2/10، رابط المقال: http: //www.abahe.co.uk/information-technology-enc/71102-piracy.html

المبحث الثالث: التهديدات المعلوماتية، ومواجهتها.

المطلب الأول: تأثير العولمة في الأمن الالكتروني.

لقد تغيرت الحروب التقليدية، وأصبحت الجيوش العسكرية في كافة أنحاء العالم تهتم بحرب المعلومات ودورها في حروب المستقبل[1]، والتي يتوقع الكثير حدوثها في الفضاء الإلكتروني، وأصبح هناك مناورات يتم إجراؤها للتدريب على هذا النوع الجديد من الصراع وكيف يمكن مواجهته والاستعداد له، والحرب الإلكترونية بشكل عام من أجل خرق السيادة الوطنية لأى دولة والحصول على معلومات استخباراتية وتجنيد العملاء وغيرها، وطبيعة الحرب لا تتغير ولكن سمات الحرب تتغير مع تطور أدوات الحرب، وظهور الطائرات من دون طيار، وهى حرب من دون نار أو دخان أو قصف ولكن لها جانب عنيف من حيث الاختراقات والقرصنة ونشر الفيروسات وغيرها من الأساليب، وبالرغم من فداحة الخسائر، فإن الأسلحة بسيطة لا تتعدى في أغلب الأحوال «الكيلو بايتس» التي تتمثل في فيروسات إلكترونية تخترق شبكة الحاسب الآلي، وتنتشر بسرعة بين الأجهزة، وتبدأ عملها في سرية تامة وبكفاءة عالية، وهي في ذلك لا تفرق بين المقاتل والمدني، وبين العام والخاص، وبين السري والمعلوم، ومن الضروري للعديد من الدول في العالم من خلال الاتفاقيات الدولية لضبط وتسليم المجرمين وإصدار العديد من القوانين التشريعية لتجريم أي استخدام غير أمن لتكنولوجيا المعلومات والاتصالات بالإضافة إلى التعاون والتنسيق الدائم مع الانتربول الدولي في مجال تبادل المعلومات والاتصالات والخبرات الأمنية والفنية، وبات من الصعب تخيل صراعاً عسكرياً اليوم دون أن يكون لهذا الصراع العسكري أبعاداً إلكترونية.[2]

تبدو العولمة المعلوماتية في المحرك الأساسي: الابتكار التكنولوجي في مجال تكنولوجيات المعلومات. وعلى الرغم أن العولمة أخذت شكلا اقتصاديا في بداية ظهورها إلى أن التطورات التكنولوجية العالمية قد نحت بها إلى طرح قضية العولمة في أنساق أخرى كالمعلوماتية والتجارة الإلكترونية، بحيث صار بوسع المستفيدين الحصول على المعلومات من أي مكان في العالم عبر استثمار تكنولوجيا الاتصال الحديثة من خلال شبكة الأنترنت والتي أصبحت تمثل نموذجا عالميا مثاليا للعولمة المعلوماتية يتاح للأفراد التواصل دون أي عوائق بينهم مما يسمح بالتداول الحر للمعلومات ومن هنا تبدأ الأهمية الحقيقية للعولمة المعلوماتية. ولذا يمكن القول أن

---

[1]–عزرائيل لوربار، التكنولوجيا العسكرية وسائل القتال والمخابرات، عرض: عدنان أبو عامر، الرعوت للنشر، تل الربيع 2012. ص.31.

[2]–عباس بدران، الحرب الإلكترونية: الاشتباك في عالم المعلومات: مركز دراسات الحكومة الإلكترونية بيروت.لبنان 2010.ص.15.

العولمة المعلوماتية هي ذلك الشكل من أشكال التواصل الإنساني عن طريق توظيف تكنولوجيا المعلومات والاتصالات في إلغاء حدود الزمن والمكان. إن العولمة المعلوماتية تعتبر إحدى أهم النقاط السلبية التي تنجر عن الانخراط في ركب مجتمعات المعلومات، وذلك لسبب بسيط هو أن حرية الولوج التي ينادي بها هذا المجتمع قد تتحول إلى جانب غاية في السلبية في حالة ما إذا جلب المد المعلوماتي فيما جلب معه عولمة معلوماتية تقود جوانب الحياة وتعو لم أنماط التفكير مع المعلومات، بل وتفرض تحديات جديدة على الأخصائيين في ميدان المعلومات. [1]

العولمة قد غيرت بشكل تدريجي الحقائق على الأرض وبينما كانت قوة العولمة في حالة مد وجزر منذ العقود التي سبقت الحرب العالميه الأولى، إلا أنها اليوم تعاني من التراجع بسبب التطورات الجيوسياسية والإندفاع من أجل إبطاء رتم التغير التقني ولكن بالرغم من كل ذلك فإن التحول الرقمي سوف يدفع بالعوله للإمام وإن كان بشكل مختلف فالخاصية الرئيسية للإنترنت هو البناء غير المناطقي فعندما نفكك الحدود التقليدية فإن هذا يشكل تحديا مباشرا لإساس نظام السيادة.

إن هذا تطور إيجابي عميق لآنه يسهل من حرية التعبير وتبادل البضائع والأفكار عبر الحدود ولكن مثل كل الإختراعات البشرية فإن من الممكن إساءة استخدام الإنترنت كما رأينا من خلال الزيادة في الجرائم السيبرانيه والتحرش على الإنترنت وخطاب الكراهية والتحريض على العنف والتطرف على الإنترنت.

إن التقليل من تلك الإساءات خلال السنوات المقبلة سيتطلب تعاونا دوليا وثيقا من أجل التأسيس لقواعد مشتركه وتطبيقها فلا يوجد حل منعزل حيث لا يمكن لأي حكومة لوحدها التعامل مع المشكلة. [2]

المطلب الثاني: تأثير التهديدات المعلوماتية على الكيان المعلوماتي.

يقصد بالتهديدات الإلكترونية، تلك الهجمات التي تتم باستخدام آليات وشبكات إلكترونية كالإنترنت وأجهزة الحاسب الآلي وتهدف إلى إلحاق الضرر بأجهزة أو شبكات إلكترونية أخرى أو سرقة المعلومات الموجود

1-بوطورة، أكرم. مجتمع المعلومات وتحديات العولمة: بين ثقافة التقييم وتقييم الثقافة: دراسة ميدانية على أخصائي المكتبات والمعلومات بالشرق الجزائري. رسالة ماجستير: قسنطينة: علم المكتبات ،2006.ص.190.

[2] Carl blidt. cyber-governance-lagging-crime-and-abuse.project syndicate. Le22/01/2018. liens: https: //www.project-syndicate.org/commentary/cyber-governance-lagging-crime-and-abuse-by-carl-bildt-2018-01/arabic

عليها. وهو ما يعنى أن إلكترونية التهديدات وفقًا للدراسة تشير إلى كل من أداة الهجوم، أي الآليات المستخدمة في شنه، وإلكترونية الهدف المتعرض له. فقد تتعرض أهداف إلكترونية إلى هجمات غير إلكترونية، كالهجمات الحركية أو المادية Kinetic attacks ، أو الهجمات الكهرومغناطيسية، والتي تؤدي إلى إحداث الضرر بها وربما توقفها عن العمل.

فالهجمات الحركية هي تلك الهجمات غير المبرمجة non software-based attacks التي يتم توجيهها للشبكات الإلكترونية الخاصة بالدول أو المنظمات عن طريق استخدام العبوات الناسفة أو الصواريخ أو القنابل لإلحاق الضرر بهذه الأهداف أو تدميرها. كما يمكن للنبضات الكهرومغناطيسية أن تولد تيارات قوية بإمكانها أن تعطل خطوط وشبكات الكهرباء أو أن تدمر مكونات رئيسية في أجهزة الحاسب الآلي، هذه الهجمات المادية والكهرومغناطيسية تختلف عن الهجمات الإلكترونية، والتي لا تكون فقط موجهة إلى أهداف إلكترونية، وإنما تمثل آليات الهجوم الإلكترونية العنصر الرئيسي فيها. ومن ثَمَّ هذه التهديدات غير الإلكترونية تقع خارج موضوع الكتاب، والتي تركز بالأساس على التهديدات الإلكترونية من حيث الأداة والهدف.

ويلاحظ أيضا أن التهديدات الإلكترونية لا تستهدف الإضرار بالبشر بصورة مباشرة، وإنما التأثير على الفضاء الإلكتروني الذي بات يشكل مكونا رئيسيا في مسار حياتهم. فهي تؤثر على الأنظمة والشبكات والأجهزة التي يستخدمها الأفراد وتعتمد عليها الدول، ومن ثم تؤثر على أسلوب الحياة ذاتها بشكل يهدد أمن الدولة ككل، ولكنها لا توجه ضد بشر كما هو الحال في الأسلحة التقليدية التي قد تستخدم للقتل المباشر.

وفي هذا المبحث سيتم عرض أهم الآليات الإلكترونية الهجومية وأكثرها استخداما، ثم بيان الأشكال والأنواع المختلفة للتهديدات الإلكترونية التي تؤثر في أمن الفواعل، وأخيرًا تحديد مصادر هذه التهديدات، أي ماهية الفواعل التي تقوم باستخدام تلك الآليات في شن هجمات إلكترونية.[1]

حيث، وقعت عدد من الهجمات الضخمة على مواقع وخوادم حكومية في جورجيا إبان النزاع بين روسيا وجورجيا، مما أعطى مفهوم الحرب الإلكترونية نمط أكثر واقعية. ولم يكن الهدف من هذه الأعمال تحقيق

[1] نوران شفيق ،أشكال التهديدات الإلكترونية ومصادرها. بقلم الدكتورة نوران شفيق، المركز الأوروبي لدراسة مكافحة الارهاب والاستخبارات ،شوهد بتاريخ 2018/02/10 الرابط:

https: //www.europarabct.com

تدمير مادي حقيقي. لكن هذه الهجمات أضعفت الحكومة الجورجية في فترة حاسمة من النزاع. كما أنها أثرت على قدرتها على التواصل مع الرأي العام الداخلي والخارجي.

وإن لم تكن هذه التقارير تحمل التهديد الكافي، فإن فيروس ستوكسنت الذي ظهر في عام 2010 شهد قفزة نوعية وكمية في القدرات المدمرة للحرب الإلكترونية. ففي صيف عام 2010، انتشرت أخبار بأن نحو 45000 منظومة سيمنس صناعية حول العالم أصيبت بفيروس حصان طروادة الذي يمكنه التلاعب بعمليات تقنية مهمة خاصة بمحطات الطاقة النووية في إيران. وعلى الرغم من أن تقييم حجم الأضرار لا يزال غير واضح، لكنه أظهر المخاطر المحتملة للبرامج الضارة حيث تؤثر على أنظمة الكمبيوتر الهامة التي تدير إمدادات الطاقة أو شبكات النقل. وللمرة الأولى، كان هذا بمثابة دليل على أن الهجمات الإلكترونية يمكنها أن تسبب أضرار مادية حقيقية وتهدد حياة البشر.

هذه الحوادث أوضحت أمران:

- حتى الآن، لا يزال يعتبر أخطر جهات في المجال الإلكتروني هي الدول. على الرغم من الوفرة المتزايدة للإمكانيات الهجومية في الشبكات الإجرامية والتي قد تستخدم في المستقبل من قبل جهات غير حكومية مثل الإرهابيين ومنظمات التجسس المتطورة والتخريب في النطاق الإلكتروني لا يزال بحاجة إلى إمكانيات وإصرار وترشيد التكاليف للدول.
- وحتى الآن لا يوجد ضرر مادي وإرهاب إلكتروني نشط فعلياً. لكن تكنولوجيا الهجمات الإلكترونية تتطور بشكل واضح من مجرد مصدر إزعاج لتشكل تهديدا خطيراً ضد أمن المعلومات والبنية التحتية الوطنية.

ليس هناك شك أن هناك بعض الدول تستثمر بالفعل أموال طائلة في القدرات الإلكترونية التي يمكن استخدامها لأغراض عسكرية. ويبدو للوهلة الأولى أن سباق التسلح الرقمي يقوم على منطق واضح وحتمي، لأن مجال الحرب الإلكترونية يقدم ميزات عديدة: فهي غير تقليدية وغير مكلفة وجميع المزايا تصب منذ البداية في الجانب الهجومي.

علاوة على ذلك، ليس هناك رادع فاعل في الحرب الإلكترونية لأن تحديد المهاجم عملية صعبة جداً وفيها يكون الالتزام بالقانون الدولي مستحيل تقريباً. وفي ظل هذه الظروف، قد يكون أي شكل من أشكال الرد العسكري مشكلة كبيرة جداً، من الناحية القانونية والسياسية.

من ناحية أخرى، تتطور قدرات الدفاع الإلكتروني بالقدر نفسه كما قامت معظم الدول الأوروبية بتعزيز دفاعاتها بشكل كبير في السنوات الأخيرة. والدفاع الإلكتروني الجيد يُسهل التعامل مع هذه التهديدات، لدرجة أن المخاطر الثانوية الباقية تعتبر مقبولة مثل التهديدات التقليدية.[1]

لكن بدلاً من الحديث عن الحرب الإلكترونية كحرب في حد ذاتها – يتم وصف الهجمات الإلكترونية الأولى باعتبارها «عملية تسلل رقمي» أو «هجمات 9/11 في العالم الإلكتروني» – وهو وصف مناسب إلى حد كبير للحديث عن الهجمات الإلكترونية كوسيلة من وسائل الحرب. إن مخاطر الهجمات الإلكترونية حقيقية وتتطور أكثر فأكثر. في نفس الوقت، ليس هناك داعي للخوف لأن هذه التهديدات في المستقبل القريب لن يكون من السهل التنبؤ بها أو السيطرة عليها تماماً.[2]

وإضافة لذلك تصاعد المخاطر الإلكترونية، خاصة مع قابلية المنشآت الحيوية (مدنية وعسكرية) في الدول للهجوم الإلكتروني عليها عبر وسيط وحامل للخدمات، أو شل عمل أنظمتها المعلوماتية، الأمر الذي يؤثر في وظائف تلك المنشآت. وبالتالي، فإن التحكم في تنفيذ هذا الهجوم يعد أداة سيطرة استراتيجية بالغة الأهمية، سواء في زمن السلم أو الحرب.[3]

وعلاوة على ذلك فالتأثير المعلوماتية في شكلها الفردي تكمن في، أنه لأي شخص أن يكون هو الجاني في الهجمات السيبرانية، وبخاصة أن المعدات اللازمة لشن هجوم سيبراني يمكن الوصول لها، وليست مكلفة، ويمكن شنها من أي مكان تتوافر فيه خدمة الإنترنت. فلكي يعمل الردع لابد من أن يقلق المهاجم من كشف هويته، ومن ثم تعرضه للعقاب أو الانتقام، بيد أن صعوبة تحديد مرتكب الهجمات بدقة، قد يسفر عن

---

[1] التهديدات الجديدة: الأبعاد الالكترونية، مجلة الناتو ،شوهد بتاريخ 2018/01/11، الرابط:
https: //www.nato.int/docu/review/2011/11-september/Cyber-Threads/AR/index.htm

[2] -التهديدات الجديدة: الأبعاد الالكترونية، المرجع نفسه.

[3] -عادل عبدالصادق، الفضاء الإلكتروني والعلاقات الدولية: دراسة في النظرية والتطبيق القاهرة: المكتبة الأكاديمية، 2016: 22-26.

استهداف طرف ثالث لا علاقة له بالهجوم إبتداءًا، وهو الأمر الذي لا يُضعف فقط من منطق الردع وفلسفته، لكنه يخلق عدوًا جديدًا أيضًا.[1]

ونبرز أهم الهجمات الالكترونية ذات الطابع الدولي فيمايلي:

• إستونيا – أبريل 2007: بدأت سلسلة من الهجمات التي يطلق عليها DDoS attacks ضد المواقع التي تديرها الحكومة الإستونية، وتسبب الهجوم في عرقلة ولوج المواطنين إلى بعض المواقع مثل موقع الحزب السياسي الذي ينتمي إليه رئيس الوزراء. من جهة أخرى، استُخدمت الروابط التي ترعاها الحكومة في تضليل المستخدمين، وإعادة توجيههم إلى صور للجنود السوفييت، واقتباساتٍ من مارتن لوثر كينج عن محاربة الشر.

• جورجيا – أغسطس 2008: شهدت جورجيا بالتزامن مع حربها ضد روسيا في أغسطس 2008 مجموعة من الهجمات السيبرانية، وإن كان ضررها الفعلي في حده الأدنى، من حجب بعض المواقع المستهدفة. ويتفق معظم المحللين على أن القوميين الروس هم المسئولون عن الهجوم، ولكن دون دليل يذكر

• كوريا الجنوبية والولايات المتحدة يوليو 2009: تم استهداف مواقع البيت الأبيض، ووكالة الأمن القومي، والإدارة الاتحادية للطيرانFederal Aviation administration ، ووزارة الخارجية، والخدمة السرية Secret Service، والخزانة، ولجنة التجارة الاتحاديةFederal Trade Commission ، فضلًا عن جهاز المخابرات الوطني في كوريا الجنوبية.

• وكذلك الهجوم على شركة سوني بيكتشرز الأمريكية في عام 2014، بسبب فيلم من إنتاج هوليوود، عن زعيم كوريا الشمالية كيم يونغ أو .(واستخدم فيروس ستكسنت – سابقًا- لمهاجمة برنامج إيران النووي في نوفمبر 2007، ويُعتقد أنه من تطوير الولايات المتحدة وإسرائيل، وقد تم اكتشافه في عام 2010

• وفي يوليو 2011، أعلن نائب وزير الدفاع ويليام لين أن أكثر من 24 ألف ملف من ملفات وزارة الدفاع قد سرق. قبل ذلك ببضعة أشهر، تم اختراق إحدى المختبرات العلمية الرئيسية التابعة لحكومة الولايات المتحدة، ولم تعلن الحكومة الأمريكية عن هوية مرتكبي الهجوم

[1]–رغدة البهي، الردع السيبراني: المفهوم والاشكاليات والمتطلبات، المركز الديموقراطي العربي شوهد بتاريخ: 2018/02/09 الرباط:

http: //democraticac.de/?p=43837#_ftn30

• وفي عام 2012، تم تدمير 35 ألف جهاز كمبيوتر في شركة النفط السعودية أرامكو ، لتخريب صادرات النفط. وألقت المخابرات الأمريكية اللوم على إيران. وفي عام 2016، هاجم القراصنة إحدى الوكالات الحكومية السعودية، بالإضافة إلى منظمات في قطاعات الطاقة والصناعة والنقل، والهيئة العامة للطيران المدني التي تنظم الطيران السعودي.

• وشهد عام 2016، التسلل الروسي إلى خوادم البريد الإلكتروني للجنة الوطنية الديموقراطية، كما تم اختراق البريد الإلكتروني الخاص بجون بوديستا رئيس الحملة الانتخابية الرئاسية لهيلاري كلينتون. وقام وسطاء بتسريب رسائل إلكترونية إلي موقع ويكليكس، وعلى إثرها قامت الولايات المتحدة بطرد، دبلوماسيًا روسيا.

إنه يصعب تحديد حجمها الحقيقي وبخاصة أن عديد منها لا يتم التبليغ عنه، وتتمثل القواسم المشتركة بين تلك الحالات في صعوبة تحديد مرتكبي تلك الهجمات على وجه الدقة، وغياب الرد المضاد، كنتيجة لها. والأهم أنها ليست حكرًا على الدول المتقدمة ذات أنظمة المعلومات الهائلة والمتطورة فحسب.[1]

المطلب الثالث: اجراءات الحد من التهديدات المعلوماتية.

المتأمل لواقع الأمن المعلوماتي يجد أن تحقيق تقدم في هذه القضية لن يتم إلا من خلال تغيير النظرة الحالية التي تنظر إليها على أنها قضية تقنيه بحته تقع ضمن نطاق تخصص التقنيين والمختصين في المجال الالكتروني, والانتقال بتلك النظرة إلى اعتبار الأمن المعلوماتي من ركائز الأمن القومي الشامل بحيث يرتفع مستوى التعامل معها إلى مستوى التعامل السياسي والاستراتيجي. ويجب أن تشمل منظومة التعامل مع مخاطر الأمن المعلوماتي وانعكاساتها على الأمن القومي البدء في تنفيذ برنامج شامل على مستوى مؤسسات وهيئات الدولة (الحكومية – الخاصة) يستهدف التدريب على صد الهجمات الالكترونية الشاملة وتنويعاتها المختلفة سواء بالفيروسات، لأن قضية الأمن المعلوماتي من شأنها في حال عدم القدرة على التغلب عليها أن تفتت الدول وتتيح المجال لما يطلق عليهم « الطابور الخامس» لتدمير الدول من الداخل تحت مسمى الوطنية الزائفة والخادعة, إن تغير طرق تهديد الدول خاصة من خلال تهديد الأمن المعلوماتي يتطلب تغيير الطرق

[1]–رغدة البهي، المرجع نفسه.

والآليات التي يتم من خلالها مواجهه هذا الخطر لضمان الحفاظ على تماسك الدولة ووجودها من الأساس. [1] فتمثلت اجراءات الحد من التهديدات الالكترونية في:

- عسكرة الفضاء الإلكتروني، وذلك سعيا لدرء تهديداته على أمن الفضاء الإلكتروني، وبرز في هذا الإطار اتجاهات، مثل التطور في مجال سياسات الدفاع والأمن الإلكتروني، وتصاعد القدرات في سباق التسلح السيبراني، وتبني سياسات دفاعية سيبرانية لدي الأجهزة المعنية بالدفاع والأمن في الدول، وتزايد الاستثمار في مجال تطوير أدوات الحرب السيبرانية داخل الجيوش الحديثة.
- إدماج الفضاء الإلكتروني ضمن الأمن القومي للدول، وذلك عبر تحديث الجيوش، وتدشين وحدات متخصصة في الحروب الإلكترونية، وإقامة هيئات وطنية للأمن والدفاع الإلكتروني، والقيام بالتدريب، وإجراء المناورات لتعزيز الدفاعات الإلكترونية، والعمل على تعزيز التعاون الدولي في مجالات تأمين الفضاء الإلكتروني، والقيام بمشروعات وطنية للأمن الإلكتروني.
- الاستعداد لحروب المستقبل، حيث تبني العديد من الدول استراتيجية حرب المعلومات بحسبانها حربا للمستقبل، والتي يتم خوضها بهدف التشتيت، وإثارة الاضطرابات في عملية صناعة القرار لدي الخصوم، عبر اختراق أنظمتهم، واستخدام ونقل معلوماتهم. وهنا، تري الدول الكبرى أن من يحدد مصير تلك المعركة المستقبلية ليس من يملك القوة فقط، وإنما القادر على شل القوة، والتشويش على المعلومة. [2]
- تحديث القدرات الدفاعية والهجومية، حيث سعت الدول إلى تحديث النشاط الدفاعي لمواجهة مخاطر الحرب السيبرانية، والاستثمار في البنية التحتية المعلوماتية، وتأمينها، وتحديث القدرات العسكرية ، والمشاركة الدولية في حماية البنية المعلوماتية، والاستثمار في رفع القدرات البشرية داخل الأجهزة الوطنية المعنية. وهنا، يتعلق التوجه الأخطر بنقل تلك القدرات من الدفاع إلى الهجوم عن طريق استخدام تلك الهجمات في إطار إدارة الصراع والتوتر مع دول أخرى. [3]

---

[1]-فتحي شمس الدين ،الأمن المعلوماتي وتهديد الأمن القومي ،روزا اليوسف ،شوهد بتاريخ 2018/02/11: الرابط: /http: //www.rosaelyoussef.com/article/2109

2- E. Nakashima. U.S. Accelerating Cyberweapon Research", The Washington Post, online e-article,

https: www.washingtonpost.com/world/national-security/us-accelerating-cyberweapon-research/13/03/2012/gIQAMRGVLS_story.html

[3]-عادل عبدالصادق، القوة الإلكترونية: أسلحة الانتشار الشامل في عصر الفضاء الإلكتروني، مجلة السياسة الدولية، العدد 188، أبريل 2012.ص 64.

- عمل الفضاء الإلكتروني على إعادة تشكيل قدرة الأطراف المؤثرة، مثل الولايات المتحدة. فبعدما كانت الأخيرة تملك ما يشبه الاحتكار لمصادر القوة، بعد انتهاء الحرب الباردة، برزت عملية انتشار القوة بين أطراف متعددة، سواء أكانت دولا، أم من غير الدول.[1]

إن مواجهة مخاطر الجرائم المعلوماتية تعتمد بشكل كبير على تبني استراتيجية أمنية- مجتمعية متكاملة، والتي تعمل فيها أجهزة مكافحة الجريمة الرسمية في الدولة جنباً إلى جنب مع أفراد المجتمع ومؤسسات القطاع الخاص، هو ما يمكن من خلاله مكافحة الأنشطة الإجرامية في الفضاء الإليكتروني والتقليل من مخارطها والحد من انتشارها، وهذه الرؤية تتسق مع نتائج الدراسات التي أجريت في بلدان مختلفة من العالم حول التعامل مع جرائم الإنترنت، والتي أوضحت أهمية مشاركة العديد من المصادر والمؤسسات الخاصة في تحمل جزءًا من المسؤولية فيما يتعلق بمكافحة هذه الجرائم والسيطرة عليها. [2]

يقول مركز الدراسات الاستراتيجية والدولية إن المعلومات التي يتم جمعها حول قرصنة الإنترنت غير كاملة بسبب عدم متابعة الكثير من الدول بصورة مستمرة عمليات القرصنة وعدم كشف الشركات عن ما تتعرض له من هجمات،ويوصي المركز بمواجهة القرصنة عن طريق تعاون دولي من خلال اتفاقية دولية لتطبيق القانون وتشديد العقوبات على جرائم القرصنة والتعاون مع منظمة التجارة العالمية، إضافة إلى تحديد الحكومات خسائر القرصنة وحصر الشركات المخاطر التي تواجهها.

كما أن هناك مسؤولية تقع على المجتمعات للتصدي لهذه الجرائم، وتتمثل هذه المسؤولية في توعية الناس بمفهوم الجريمة الإلكترونية، وأنها الخطر القادم والحرص على ألا يقعوا ضحية لها.[3]

المطلب الرابع: بناء السلام السيبراني.

الصراع باللجوء إلى الحرب السيبرانية، يؤثر في كل دولة، ولذا فإن من مصلحة الجميع أن تتوفر لهم القدرة على استعادة السلام والأمن في أعقاب مثل تلك الحرب.

الحرب السيبرانية، موجودة بيننا الآن، ابتداءً من التدخل في الانتخابات، وانتهاءً بتسريب أسلحة سيبرانية من مخزون وطني. وكما هي الحال مع معظم التطورات في الحرب، فإن العالم غير مستعدّ إلى حدٍّ كبير. ويطرح حفظ السلام السيبراني تحديات كبيرة، سوف نستكشفها في بحثنا.

---

[1]-عادل عبد الصادق، المرجع نفسه ص 71.

[2]-عبدالله بن فازع القرني، مواجهة جرائم الإنترنت: نحو إستراتيجية أمنية – مجتمعية متكاملة، مقال منشور على موقع جريدة الرياض شوهد بتاريخ 2018/02/21 الرابط:

http: //www.alriyadh.com/912032

[3]-القرصنة الالكترونية.... سلاح العصر الرقمي ،الجزيرة. نت،شوهد بتاريخ: 2018/02/13 ،الرابط:

/http: //www.aljazeera.net/knowledgegate/newscoverage/2015/1/5

إن كل مسرح للحرب الآن، يتضمن حرباً سيبرانية. وقد استعمِلت في الهجمات الموجهة لشلّ قدرات الخصم... ويمكن استغلالها أيضاً في الحرب التقليدية من خلال إحداث تداخل إلكتروني مع المعلومات الاستخبارية وأنظمة الاتصالات.

ومع قلة ما تسترشد به الدول، وضآلة الخبرة التي تستند إليها، يضطر العديد منها إلى التعلّم بعد أن يدفع الثمن. في سياق الحرب، يستغرق الأمر وقتاً طويلاً لفهم أثر التكنولوجيات الجديدة. وما على المرء إلّا أن يتأمل مثال الألغام الأرضية لمعرفة السبب.

فبينما كانت تعتبر في السابق سلاحاً مشروعاً لإخماد حركة العدوّ، تتفق معظم الدول الآن على أن الألغام الأرضية أسلحة عشوائية وغير متناسبة، وتسبب المعاناة للمدنيين بعد وقت طويل من انتهاء الصراع. ويمكن أن تكون الحرب السيبرانية تنطوي على عواقب غير معروفة تجعل زعماء العالم في المستقبل يتفقون على الحظر لأسباب مقززة مماثلة في أعقاب اكتشافها. وهنالك، مع ذلك، جهود تُبذل لسدّ الثغرات في المعرفة. وقد حاول باحثون، من أمثال زميلي، مايكل روبنسون، تشخيص صفات الحرب السيبرانية لفهم كيف يمكن إجراؤها بفاعلية وعلى نحو أخلاقي. ومن بين هذه الجهود، وضع قوانين حرب سيبرانية للسيطرة على الأسلحة السيبرانية وتقييدها.

وقد بدأت هذه الجهود تؤتي أكلها، مع تقديم دليل تالين الإرشادي – الذي نُشر أول مرة عام 2013 – تحليلاً شاملاً لكيفية تطبيق القانون الدولي القائم، على الفضاء الإلكتروني.

ولكن، بينما تركز نسبة كبيرة من البحوث على كيفية إجراء الحرب السيبرانية، فإن النزر اليسير من الأبحاث، يدور حول استعادة السلام في أعقاب الصراع عبر الإنترنت بين الدول القومية. واعتماد الدولة على البنية التحتية الحساسة، يجعل الحاجة إلى فهم الضرر الذي يمكن أن تحدثه الحرب السيبرانية، محلّ تركيز شديد. حيث يمكن أن تصاب أنظمة الكمبيوتر التي تشغل الخدمات الأساسية في المستشفيات، ومحطات الطاقة النووية، ومحطات معالجة المياه، ببرامج حاسوبية ضارة متطورة، تقاوم الإزالة وتطيل المعاناة المدنية – مثلما تستمر الألغام الأرضية في البقاء فترة طويلة بعد انتهاء الصراع. والأضرار المادية للأسلحة السيبرانية تجعل حفظ السلام السيبراني، عامل تمكين أساسي للمساعدة على تحقيق السلام الدائم.

فبعد الصراع التقليدي، تجري التدخلات التي ترمي إلى استعادة السلام والأمن على الساحة الدولية. والأمم المتحدة بعرباتها البيضاء وخوذاتها الزرقاء، هي منظمة حفظ السلام المعترف به على أوسع نطاق. وهي ذات تاريخ طويل من حفظ السلام في أنحاء العالم، حيث تطورت لتتناسب مع الطبيعة المتغيرة للحرب من صراع بين الدول، إلى صراع داخل الدولة الواحدة على مرّ السنين. ومع نشوء الحرب السيبرانية، سوف تحتاج قوات

حفظ السلام بصورة متزايدة، إلى العمل في هذا النطاق. ولكن، هل الأمم المتحدة والمنظمات المماثلة مستعدة لهذا الهجوم المتوقع، أم أنها ستعاني تكرار الإخفاقات الماضية، بعد أن وقعت في شراك التغيرات في طبيعة الصراع؟. وقد انهارت محادثات الأمم المتحدة المطولة حول الحرب السيبرانية في العام الماضي؛ بسبب عدم إمكانية التوصل إلى توافق وسط الشكوك التي ذكِر أنها تعكس صورة حقبة الحرب الباردة. وبغض النظر عن ذلك، لا بُدّ من طرح أسئلة حول استراتيجية الأمم المتحدة بشأن استعدادها لمعالجة التهديدات السيبرانية.[1]

[1] هيلجي جانيك،حفظ السلام في الفضاء الالكتروني ،الخليج، بتاريخ ،2018/02/05 الرابط:

http: //www.alkhaleej.ae/alkhaleej/page/2c4692bd-05cc-43a4-9fa9-1b682df40056

تطور مفهوم الاستراتيجية من المفهوم الضيق الذي يعنى بالشؤون العسكرية وميادين الحرب ليصبح موسع المفهوم لمجالات متعددة ، السياسة، الاقتصادية والاجتماعية وحتى مجالات الأمن الإلكتروني محل دراستنا حيث استخلصنا مفهوم الأمن الالكتروني الذي تعددت اصطلاحاته إلى الأمن السيبراني وأمن المعلومات والأمن الرقمي...، فقد واجهت الدول عديد التهديدات الالكترونية على كياناتها مما حتم عليها وضع آليات مشتركة للحد من هذا التهديد عبر أليات قانونية وآليات أخرى ردعية.

الفصل الثاني

نتطرق في هذا الفصل إلى تحديد الكيفيات المنتهجة من طرف الدول الكبرى في عصرنة قطاعاتها ومؤسساتها وإدخال المعلوماتية في جهازها وأيضا نتكلم عن الكيفيات التي تواجه بها الدول إشكاليات العطب الإلكتروني، وأيضا أبرز الشراكات الدولية و الاتفاقيات التي اتبعتها الدول في إطار الحد من التهديدات المعلوماتية.

المبحث الأول: ادخال المعلوماتية في الكيان الأمني للدول الكبرى.

المطلب الأول: تحيين المنظومة السياسة والادارية للدول.

لعل أهم حدث عرفه قطاع الاتصالات وجعله يتحول من مجرد قطاع مساند لبعض الانشطة المتفرقة الى قطاع محوري له تأثير هام على مختلف المجالات، الاقتصادية والاجتماعية والثقافية والسياسية، هو ادخال الرقمنة التي شملت تدريجيا مختلف انظمة معالجة ونقل المعلومة:

الفرع الأول: الترميز الرقمي

المتأمل في التقنيات الرقمية يلاحظ أن اهم العناصر التي تكمن فيها التأثيرات المباشرة على الانسان من خلال حياته اليومية، تتمثل في الترميز الرقمي لجميع المعلومات بصفة الكترونية باعتماد القاعدة الثنائية في مجال الرياضيات، ويمكن هذا الترميز من مسك المعلومات في جميع اشكالها ووضعها على الخط ليتقبلها الحاسوب اثناء معالجته. ويتميز هذا الترميز بتوفير قدرة فائقة لترجمة المعلومات، في اشكالها المتعددة سواء منها المجسمة كالنصوص والصور والصوت او كذلك المجردة كالعلاقات والافتراضات، في شكل نماذج تقريبية خاضعة لإرادة الانسان من خلال معالجتها من طرف الحاسوب والتحكم فيها وتغييرها واخراجها في اشكال ومعاني جديدة ومختلفة من اصولها وكذلك من توسيع رقعة ترويجها خاصة لدى الشرائح الاجتماعية المقصية سابقا من هذه المعالم.

ولم تقتصر التقنيات الرقمية علي ترميز المعلومة بصفة الكترونية فقط بل اجتاحت ايضا تقنيات الارسال والاتصالات واصبحنا ايضا نتحدث عن الارسال الرقمي الذي مكن من تطوير قدرات شبكات الارسال الى درجات خالية ومن اخضاع الارسال للمعالجة الالية. وبالتالي من تعديد الوظائف والخدمات ومن ادماج مختلف المجالات التي يشملها قطاع الاتصالات وخاصة شبكات الهاتف وشبكات تراسل المعطيات والارسال الاذاعي والتلفزي وشبكة الأنترنت وغيرها.

الفرع الثاني: رقمنة انظمة التراسل

في هذا الاطار شهدت انظمة التراسل أخيرا، تطورا ملحوظا فبرزت تكنولوجيات جديدة من اهمها التكنولوجيا البصرية، ذلك أن تطوير نظرية الليزر وصناعة الالياف البصرية من جهة واكتشاف المضخمات البصرية من جهة اخرى امكن استعمال انظمة تراسل بصرية جديدة كنظام الهرم الرقمي

المتزامن (SDH) الذي تصل سعته إلى 2,5 جيغابيت في الثانية أي ما يعادل ارسال 39 الف مكالمة متزامنة لكل ليف بصري واحد.

ولعل من اهم المستجدات التي شهدها قطاع الاتصالات في الفترة الأخيرة ظهور تقنية الارسال المتعدد الاطوال الموجية (WDM) وقد بلغت سرعة التدفق بهذا النظام مؤخرا 40 جيغابيت في الثانية أي ما يقارب 625 الف مكالمة متزامنة لكل ليف بصري واحد. وتجدر الاشارة الى أن انظمة التراسل السابقة الذكر تحتوي على درجة كبيرة من الذكاء تمكن المشغل من التحكم فيها وصيانتها واستغلالها الاستغلال الامثل اذ توفرت طاقة ربط ديناميكية، كما تمنح شبكات هذه الأنظمة في شكلها الحلقي مستوي تامين مرتفع.

الفرع الثالث: رقمنة شبكات النفاذ

ومن جهتها وحتي تتمكن من مواكبة التطور الحاصل في شبكات التراسل ومن الاستجابة لحاجيات المستعمل النهائي من حيث السعة، شهدت شبكات النفاذ تطورات هامة بفضل اعتماد تكنولوجيات نفاذ جديدة من اهمها تكنولوجياDSL التي تعتمد على تقنيات ترميز جديدة. فبواسطة تجهيز خط المشترك الذي يشترط أن يكون ذو جودة عالية، بجهاز محول (MODEM) تسمح تقنيات من تبادل المعطيات بسعة تصل الى حوالي 50 ميغابيت في الثانية وذلك باعتبار المسافة الفاصلة بين المشترك ومركز التحويل.

وبالرغم من حداثة استعمال تقنيات فان ظهور الشبكات متعددة الخدمات والتطورات الكبيرة التي شهدتها انظمة التراسل والتحويل، دفعت مشغلي الاتصالات الى استعمال الانظمة البصرية في شبكات النفاذ، ويمكن لهذه الانظمة التي وقع اعتمادها حاليا توفير 622 ميغابيت في الثانية. كما أنه من المتوقع أن تدخل انظمة الاكبر سعة حيز الاستعمال في شبكات النفاذ في المستقبل في حالة تزايد الحاجة لسعة اضافية.

وبالتوازي مع التطور الذي شهدته تكنولوجيات النفاذ المعتمدة على الكوابل، فان تقنيات النفاذ الراديوي حققت هي الأخرى نجاحات كبيرة فيما يتعلق بتطوير السعة، فإلى جانب تكنولوجيا كواحدة من اهم التكنولوجيات المستقبلية اذ تشتغل في شريط الذبذبات 2.4 – 40 جيغا هرتز وتوفر سعة تصل الى 50 ميغابيت في الثانية في اتجاه المستعمل.

الفرع الرابع: رقمنة انظمة التحويل

وفي نفس الاطار وحتى لا تمثل عائقا يعرقل التطور الذي عرفته شبكات التواصل والنفاذ شهدت انظمة التحويل تطورات هامة وعديدة. فبهدف مسايرة النسق المتزايد لسرعة تدفق المعطيات وامام محدودية التحويل الدوري لتحقيق ذلك ظهرت طريقة تحويل الحزم التي تمكن من سرعة تدفق اكبر وتعتمد على آليات مراقبة ذات جذوي مرتفعة تضمن بدرجة كبيرة التقارب بين المعلومات المرسلة والمقبولة. واصبح من الممكن تركيب تجهيزات لمئات الالاف من المنخرطين.

الفرع الخامس: شبكات الهاتف الجوال

إلى جانب التطورات الهامة التي عرفتها شبكات الاتصال القارة فان شبكات الهاتف الجوال مرت هي الاخرى بثلاث مراحل هامة منذ ظهورها أي في اواخر الستينات، ففي الفترة الاولى التي امتدت اواخر الثمانينات ظهر الجيل الاول للهاتف الجوال الذي يعتمد على انظمة تناظرية مثل 450. اما الفترة الثانية فتميزت بظهور نظام اتصالات سابق.

ورغم هذا النجاح فان سرعة التدفق التي توفرها انظمة تراسل المعطيات والجديدة في نظام، لم تكن كافية مما ادي الى ظهور شبكات الجيل الثالث للهاتف الجوال الذي يمثل اهم المستجدات في قطاع الاتصالات في بداية هذا القرن. ويسمح هذا النظام الذي يستعمل تقنية نفاذ تعتمد على اسناد رمز وحيد لكل مستعمل خلال كل مكالمة، من توفير سرعة تدفق تصل حاليا الى 2 ميغابيت / ث.[1]

ففي اطار تحيين المنظمة بدأت العملية بالإدارة الإلكترونية، التي هي منظومة إلكترونية متكاملة تهدف إلى تحويل العمل الإداري العادي من إدارة يدوية إلى إدارة باستخدام الحاسب وذلك بالاعتماد على نظم معلوماتية قوية تساعد في اتخاذ القرار الإداري بأسرع وقت وبأقل التكاليف.
ويمكن للإدارة الإلكترونية أن تشمل كلاً من الاتصالات الداخلية والخارجية لأي منظمة. والهدف من ذلك هو إدخال الشفافية الكاملة والمساءلة مما يؤدي إلى تحسين الإدارة الإلكترونية داخل أي منظمة. ففي ألمانيا، على

[1]Phil Williams, Cert Coordination Center، "Implications for Business." Organized Crime and Cyber-crime 2002:p p 1-7.

نحند علي العمري،مظاهر الثورة الرقمية ونتائجها ،مفهوم، العدد السابع عشر،شوهد بتاريخ 2018/01/23، الرابط: http: //www.mafhoum.com/press9/265T44.htm

سبيل المثال، تستهدف هذه المبادرة بصورة خاصة المنظمات الحكومية، حيث إن المساءلة العامة تشكل أهم الأساسيات في تعزيز الشفافية داخل هذه المؤسسات أو المنظمات، كما أن هناك عمليات مماثلة يجري تطويرها في العديد من الشركات الأمريكية للمساعدة على الامتثال للقوانين. [1]

حيث تمر تحيين المنظومة الادراية والسياسة للدول عبر مراحل:

- المرحلة الأولى: تمثل هذه المرحلة الجهود الأولية للمؤسسات الحكومية للظهور على الأنترنت لتعريف المواطنين بنشاطاتها وطرق عملها، وفي بعض الأحيان تعرف بنشاطات دوائرها وأنواع الخدمات التي تقدمها للمواطنين مع الاستمارات الواجب ملئها للحصو على هذه الخدمات.
- * المرحلة الثانية: تسعى الوحدة الادارية والسياسة إلى احالة قسم من أعمالها إلى المواطن، عبر السماح له بالتعامل مع قواعد البيانات وادخال المعلومات المطلوبة عبر الموقع أ السحابة التابعة للمؤسسة الادارية، وبذلك يكون المواطن هو احد المشاركين في انجاز الخدمة، وهذا ما يساعد المؤسسة الحكومية على تقليص كلف الانجاز، ففي تسديد الضرائب السنوية للشركات المساهمة في بريطانيا على سبيل المثال اذا ما تم ملء الاستمارة عبر الشبكة فتكون مجانا اما ارسالها ورقيا فيجب ان تسدد معها قيما مالية تغطي جهد الموظف الذي تتحمله دائرة الضرائب لإدخال هذه المعلومات الكترونيا.
- المرحلة الثالثة: في هذه المرحلة يجري التركيز على ازالة التضارب والتناقض في مصادر المعلومات التي تحصل عليها المؤسسات الحكومية من المواطنين، لذا يجري توثيق المعلومات التي تحتاجها المؤسسات الحكومية في مصدر واحد، فمثلا هوية الاحوال المدنية تحتاجها دوائر الدولة وليس المواطن الذي يعرف كل بياناته الشخصية. [2]

المطلب الثاني: عصرنة القطاعات والمؤسسات الوطنية

عصرنة الادارة العامة والمؤسسات تقتضي قبل كل شيء وجود اخلاقيات ليس فقط في جعل الوظيفة العامة أكثر استقامة أو استجابة للتطوير، بل وفي كونها جوهرا المواجهة الحقيقية للفساد التي لا تقتصر فقط على اللوائح والنظم والإجراءات، وإنما بصفة خاصة في النفوس والاتجاهات والضمائر. [3]

---

[1] الادارة اللكترونية واهميتها في تشكيل حكومة المستقبل ،الخليج الاقتصادي،شوهد بتاريخ: 2018/02/17، الرابط: http: //www.alkhaleej.ae/economics/page/ea7bae04-7ab8-4af9-beda-65893e8e04c6

[2] السديري محمد بن أحمد، مفاتيح النجاح في تطبيق الحكومة الالكترونية، المؤتمر الوطني السابع عشر للحاسب الآلي، جامعة الملك عبد العزيز، السعودية 2004، ص 98.

[3] –جردير ليلى، التنمية الادارية كمدخل لتجسيد الحكم الرشيد، مذكرة ماجستير، تخصص الديموقراطية والرشادة، كلية الحقوق جامعة منتوري ،قسنطينة.2011.ص149.

وقد ظهرت في دول كثيرة جهود لتحسين وعصرنة الادارة بما يضمن مكافحة الفساد وتقديم الخدمات للمواطن ذات الجودة عالية، فقد انشات البرتغال ما يسمى وثائق النوعية للخدمات العامة التي تشمل بوضوح التزامات الإدارة بتقديم الخدمات للمواطن، وفي ايرلندا أصبحت خدمة المواطن في صلب أحدث حركة إصلاح حكومي كما يظهر من عنوانها «وضع حكومة افضل»، ويذكر أن هدف هذه الحركة أن تنظر إلى الشعب على أنهم زبائن وعملاء ومواطنون في الدولة، كما ذهبت جهود الاصلاح في الأرجنتين إلى أبعد من الإصلاح المالي في الدولة حيث تم انشاء مكاتب التوقف الواحد، الذي بموجبه يستطيع المواطن انجاز كل ما يحتاجه من مكان واحد، لبدء عمل جديد أو لتوسيع عمل قديم وبالتالي تزيل أكثر من 50% من مدة الانتظار ففي الادارات العامة.[1]

اذا كان تطبيق العصرنة الالكترونية دفعة واحدة يؤدي إلى خلل في استراتيجية التطبيق كون الانتقال نحو واقع معين يرتبط دائما بتهيئة الظروف والمناخ الملائم، فإن أفضل سيناريو للوصول إلى تطبيق سليم لاستراتيجية العصرنة، هو العمل على تقسيم خطة الوصول إلى المرحلة النهائية لادخال المعلوماتية في الكيان الامني للدول الكبرى، حيث تعتمد الإدارة الإلكترونية للدول الكبرى على آليات العصرنة الأساسية وهي:

-الحاسب الآلي.

-تقنيات المعلومات.

-تقنيات الاتصالات.

-البريد الإلكتروني.

-شبكة الإنترنت.

-كذلك تعتمد الإدارة الإلكترونية مجموعة آليات إدارية من أهمها:

-إعادة الهندسة.

-القياس المرجعي.

-التخطيط الاستراتيجي.

-التقييم المتوازن.

-تخطيط موارد المشروع.

-تخطيط الجودة لمنع الخطأ.

ويبدو التجديد في استخدام هذه الآليات ضمن منظومة الإدارة الإلكترونية في أمرين أساسيين:

[1]-جوزيف اس ناي، جوندي دوناهيو، الحكم في عالم يتجه نحو العولمة، ترجمة: محمد الشريف الطرح، دار العبيكان للنشر، الطبعة الأولى.الرياض.2002.ص338.

الأول: أن هذه الآليات تستخدم كمجموعة متكاملة ومترابطة وبصفة مستمرة، وذلك على خلاف ما درجت عليه الإدارة التقليدية من استخدام مجزأ ومتباعد لتلك الآليات أو بعضها.

الثاني: ابتكار برامج على الحاسب الآلي لتطبيق تلك الآليات إلكترونياً بدرجة متزايدة باستمرار من جانب وإدماجها في صلب عمليات المنظمة من جانب آخر.

ومن ثم تتميز العصرنة بمجموعة من السمات الأساسية التي تعكس الخصائص النابعة من ارتباطها بتقنيات المعلومات والاتصالات بالدرجة الأولى، كما توضح المحتوى التقني الفائق الجودة لهذا النموذج الإداري المستحدث. وتعتبر المرونة الفائقة والتحرر البالغ من قيود الزمان والمكان هي السمة الأولى والرئيسية للإدارة الإلكترونية والتي تسهم في تكوين باقي السمات المميزة لها. والمعنى أن الإدارة الإلكترونية تتعامل في كل وقت ومن أي مكان، وتتخذ القرارات في مختلف مجالات النشاط متحررة من قيود الوقت والمسافة. وتتمثل أهم السمات الأخرى للإدارة الإلكترونية في السرعة، التشابكية، التنويع، تجاوز الوسطاء، التصميم حسب الطلب مع الإنتاج الكبير، التكيف السريع، التكامل، التطور المستمر، التحرر من القوالب والهياكل الجامدة، التحرر من المعاملات الورقية، العمل من بعد.

ويؤدي تطبيق الإدارة الإلكترونية في اطار العصرنة إلى إحداث تغييرات تنظيمية تتوافق تماماً مع متطلبات نماذج التميز التنظيمي من أهمها ما يلي:

-التوسع في الأتمتة بما يؤدي إلى تخفيض أعداد العاملين حتى في المستويات الإدارية خاصة الإدارة الوسطى والوظائف الإشراقية.

-إعادة تصميم الأعمال باستبعاد الأنشطة والمهام التي يتم أتمتتها، وإدخال عناصر التكامل والتمكين في الاعتبار.

-إعادة تصميم نظم التخطيط بإضفاء عناصر المرونة واستشعار التغييرات من خلال الربط الآني بنظم رقابة وقياس الأداء.

-استثمار فرق العمل الطارئة بدلاً من التكوينات والتقسيمات التنظيمية الدائمة، ومن ثم يتم التحول إلى التنظيم الشبكي حيث يكون الربط آنياً بين الوحدات الإستراتيجية وفرق العمل المختلفة بوسائط إلكترونية تسمح بالتواصل والتفاعل والتنسيق المستمر والعمل المشترك وتبادل المعلومات بينها جميعاً .[1]

[1]-عبد الرحمان تيشوري، الادارة الاكترونية،الحوار المتمدن،العدد 1418،شوهد بتاريخ 2018/02/19 الرابط: http: //www.ahewar.org/debat/show.art.asp?aid=270234

المطلب الثالث: عالمية البيانات الوطنية للدول.

مع ثورة الاتصالات الرقمية وما وفرته من تسهيل وسرعة في عمليات التواصل والوصول إلى مصادر المعلومات، ومع ما تحمله هذه الثورة من نتائج ذات آثار إيجابية على الفرد والمجتمع إذا تم استغلال وسائل الاتصال والتقنية الحديثة على الوجه الأمثل، فإن آثارها السلبية تبرز مع التمرد على القواعد الأخلاقية والضوابط القانونية والمبادئ الأساسية التي تنظم شؤون الحياة الإنسانية،[1] لقد شهدت السنوات العشر الماضية ثورة في عالم الحكومات التي نقلت معظم خدماتها إلى الإنترنت وأصبح بإمكان أي مواطن أن يقوم بالخدمات العامة، مثلا كتجديد دفتر السواقة وجواز السفر عبر مواقع الإنترنت الحكومية وبطريقة آمنة وسرية. وذلك حسب الدكتور عباس بدران، مدير مركز دراسات الحكومة الإلكترونية في بيروت، الذي شرح في حديث لبرنامج «**ديجيتال**» في مونت كارلو الدولية العوامل التي أدت إلى تحول الحكومات من مفهوم الحكومة الإلكترونية إلى الحكومة الذكية خاصة في البلدان المتقدمة تكنولوجيا كفرنسا واستونيا والمملكة المتحدة وكوريا..[2]

إن تطوير أساليب وإجراءات العمل في الدول الكبرى التي تنتهج نظام رقمنة المعطيات, أحد الجوانب الهامة والأساسية والإجراءات بالطابع الإلكتروني الذي ينطلق من الخصائص الأساسية الثلاث لتقنية المعلومات وهي (التخزين) للمعلومات بكميات كبيرة وعلى وسائط صغيرة تغني عن الملفات الورقية (النقل) للمعلومات عبر وسائل الاتصال الإلكترونية المختلفة إلى أماكن مختلفة , وفي أوقات مختلفة, ثم (المعالجة) للمعلومات طبقاً لإجراءات ذكية يضعها الإنسان وفقاً لمتطلباته من خلال البرمجة. ولا شك أن ادخال البيانات في اطار رقمنة النظام على مستوى الشبكة العالمية، ترتكز على مبدأ القدرة على تبادل المعلومات مع الحكومات المماثلة أو المواطن أو قطاع الأعمال , وهذا يتطلب تحقيق الانفتاح والتكامل والترابط , مع الأخذ في الاعتبار أهمية ودور البرمجيات في نجاح تحول الأعمال إلى الشكل الإلكتروني , بحيث تكون تلك البرمجيات قادرة على تحقيق أهداف الحكومات من خلال القدرة على التعامل مع كبير جداً من المواطنين والحكومات وقطاع الإعمال , ومرنة وقابلة والصيانة والاستمرار على العمل دون توقف. ولقد ظهر مفهوم الحكومة الإلكترونية أول مرة في الولايات المتحدة في إطار برنامج إعادة اختراع الدولة حيث

[1]–مصطفى القايد،مفهوم المواطنة الرقمية ،منصة ت–ج التعليمية، شوهد بتاريخ 2018/02/20 الرابط:
https: //www.new–educ.com/definition–of–digital–citizenship

[2]–نسيب بيطار ،من الحكومة الالكترونية الى الحكومة الذكية، مقالة من فرانس 24 بالعربية،شوهد بتاريخ: 2018/02/21، الرابط:

http: //www.france24.com/ar/20140114

دعي هذا البرنامج إلى التوسع في استخدام تقنيات حديثة في مجال تقديم الخدمات العامة وخاصة تلك الخدمات التي تمس عدداً كبيراً من المواطنين[1]

وتتألف عملية تطوير وبناء مشروع التحول إلى عالمية البيانات من ثلاث مراحل أساسية لاتعتمد بعضها علي بعض، ولا توجد ضرورة أو حاجة لإنجاز مرحلة قبل أخرى. وتتمثل هذه المراحل فيما يلي:[2]

الفرع الأول: التوسع في نشر المعلومات الحكومية والوصول إليها عبر الويب.

ترتبط هذه المرحلة بالنشر باستخدام تكنولوجيا المعلومات والاتصالات لتوسيع قاعدة الوصول للمعلومات والخدمات الحكومية، حيث يتدفق من أداء المصالح والدوائر الحكومية المختلفة والمتنوعة قدرا ضخما من المعلومات التي لها فائدة كبيرة لجمهور المستخدمين من المواطنين، ومنشآت الأعمال، والمنظمات المدنية الأخرى. وتساهم تكنولوجيا المعلومات والاتصالات المرتبطة بشبكة الإنترنت العالمية في مساعدة المستخدمين وتمكينهم من الاستفادة من هذا الكم الهائل المتدفق من المعلومات من خلال توفيرها وإتاحتها بسرعة وسهولة وفي الوقت الحقيقي لحدوثها. مما يؤدى إلى زيادة شفافية الإدارة، وتقديم خدمة أكثر جودة وبتكلفة أقل، وبإجراءات يسيرة وسريعة ومبسطة، مع اعتماد معلومات أصح وأدق، وتوفير آليات اتصال أفضل وأسرع، وضمان ثقة المتعاملين لقاء الاستجابة لحاجاتهم ومتطلباتهم.

الفرع الثاني: توسيع المشاركة المدنية في تطوير الحكومة الإلكترونية.

إن توسيع مبدأ المشاركة المدنية والتوسع فيها يؤدي إلي بناء الثقة بالحكومة ومشروعاتها. وتتضمن الحكومة الإلكترونية وجود اتصالات ذات اتجاهين بدءً بالوظائف الأساسية كالاتصال عبر البريد الإلكتروني

[1]-يحيى محمد علي أبو مغايض، الحكومة الإلكترونية في المؤسسات العامة بالمملكة العربية السعودية, الرياض: 2004،ص44.

[2] Bruno Lanvin,(2002). The E_Government Hand Book for developing countries". Center for democracy and Technology,p.p25-30

للاستفسار عن معلومات، أو الحصول علي نماذج واستمارات من الموظفين العموميين للتغذية العكسية المرتدة لتقديم الخدمات المستفسر عنها. [1]

وفي ترتيب التطور الرقمي العالمي، تتصدر سنغافورة التصنيف العالمي للدول من حيث جاهزية الشبكات لعام 2015، وينضم إليها كل من الولايات المتحدة واليابان من خارج القارة الأوروبية ضمن أفضل 10 مراكز في هذا التصنيف. وصنف مؤشر جاهزية الشبكات لعام 2015 سنغافورة كأفضل دولة في العالم من حيث الاستفادة من تقنيات المعلومات والاتصالات، وأثرها الواسع على الحياة الاجتماعية والاقتصادية، لتزيح سنغافورة بالتالي فنلندا عن الصدارة التي حافظت عليها منذ عام 2013. كما انضمت دولة آسيوية أخرى إلى قائمة أفضل 10 دول في هذا التصنيف، وهي اليابان، التي نجحت في تسلق سلم الترتيب بإنجاز مثير للإعجاب بلغ 6 مراتب لترتقي إلى المرتبة العاشرة في الترتيب وذلك بالاستناد إلى المعايير المحكومة لها.

وحلت السويد في المرتبة الثالثة خلف فنلندا، في حين احتلت الولايات المتحدة الأميركية المركز السابع، لتكون الأعلى تصنيفًا بين مجموعة السبعة الكبار، تليها المملكة المتحدة بالمركز الثامن، في حين احتلت ألمانيا، رابع أكبر اقتصاد في العالم، المرتبة الـ13، متراجعة مرتبةً واحدة عن ترتيبها العام الماضي.[2]

[1] Karen L., Jungwoo L.,(2001). Developing fully functional E_Government: A four stage model". Government information quarterly 18,122-136.

[2]-التقرير العالمي لتكنولوجيا المعلومات، مجلة الشرق الأوسط ،شوهد بتاريخ 21 /2018/02: الرابط: /https: //aawsat.com/home/article/336976

المبحث الثاني: التهديدات الالكترونية لقطاعات الدول الكبرى.

المطلب الأول: اتلاف البيانات المؤسساتية والادارية للدول.

إن المعلومات المعالجة آليا هي أساس عمل النظام المعلوماتي، لأنها ذات قيمة مادية واقتصادية، لذلك تعد هدفا للجرائم الإلكترونية من خلال التلاعب فيها او إتلافها، لعرقلة سيرورة الكيان المعلوماتي للدول.

يكون التلاعب في المعلومات الموجودة على النظام المعلوماتي بطريقة مباشرة أو غير مباشرة، فيتم التلاعب المباشر عن طريق إدخال معلومات بمعرفة المسؤول عن القسم المعلوماتي، كضم مستخدمين غير موجودين بالعمل بهدف الحصول على مرتباتهم، الإبقاء على مستخدمين تركوا العمل للحصول على مبالغ شهرية، أو عن طريق تحويل لمبالغ وهمية لدى العاملين بالبنوك باستخدام النظام المعلوماتي بالبنك، وتسجيلها وإعادة ترحيلها وإرسالها لحساب آخر في بنك آخر، بهدف اختلاس الأموال أو اتلاف المحتويات، [1] أما التلاعب الغير مباشر، فيتم عن طريق التدخل لدى المعلومات المسجلة بالنظام المعلوماتي باستخدام أحد وسائط التخزين، أو التلاعب عن بعد بمعرفة أرقام وشفرات الحسابات. [2] بذلك تخريب أو إتلاف أجهزة المعلومات أو احدى مكوناتها، [3]

فالإتلاف في المجال المعلوماتي قد يقع على المكونات المادية المتصلة بالحاسب الآلي وملحقاته كالشاشة أو لوحة المفاتيح أو الفارة أو الأشرطة أو الأقراص الممغنطة والسحابة الالكترونية وغيرها مما له علاقة بهذا المجال[4].

ومن أشهر الطرق التي يتبعها القراصنة في عمليات اتلاف المحتويات، نجد:

الفرع الأول: طريقة استغلال الثغرات

1-محمد الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، الطبعة الثانية، دار النهضة العربية، القاهرة، 1994.ص82.

2-Le rapport du conseil du l'Europe, 15,18 novembre 1976.

3-محمد السعيد رشدى، الانترنت والجوانب القانونية لنظم المعلومات، بحث مقدم إلى المؤتمر العلمي الثاني لكلية الحقوق ،جامعة حلوان

4 - Tom forester, Essential proplems to Hig-Tech Society First MIT Pres edition, Cambridge, Massachusetts, 1989,

وذلك أن كثيراً من المواقع تحتوي على ثغرات، فيقوم المهاجم بالبحث عن الثغرات، ثم يقوم بمهاجمة الموقع عن طريق تلك الثغرة، وقد يستطيع التحكم ببعض محتويات الصفحة، وقد يستطيع الحصول على اسم المستخدم وكلمة المرور الخاصة بإدارة الموقع، ومن ثم يقوم بالاستيلاء على الموقع.

واكتشاف الثغرة قد يكون ميسوراً؛ وذلك باستخدام بعض البرامج التي تقوم بالبحث عن ثغرات المواقع، وقد يأخذ المخترق بعض الثغرات التي تم الإعلان عنها، فيبحث عن موقع لم يقم بسد تلك الثغرة فيقوم باستغلالها.

وقد يبحث المهاجم عن الثغرات بشكل عشوائي، فيخترق أي موقع يجد فيه هذه الثغرة، وقد يبحث عن ثغرات في مواقع بلد معين، أو موقع معين، وهذا أصعب مما قبله.

وأصعب من ذلك اختراق الخوادم الخاصة بشركات الاستضافة، فهي عبارة عن أجهزة ضخمة تضم العديد من المواقع التي تعد بالمئات أو الآلاف، والحماية الأمنية الخاصة بها، والدعم الفني المقدّم لها يعدّ متقدماً جداً، وهو بالطبع يختلف من شركة إلى أخرى، ومع ذلك فهي ليست بمنأى عن الهجمات الإلكترونية، واختراقها أشد ضرراً، فمن يستطيع الاختراق فإنه يستطيع التحكم بمئات المواقع.

الفرع الثاني: طريقة هجمات حجب الخدمة (Denial of Service)

وهو: «نوع من الهجوم على الشبكات من خلال إغراقها بالبيانات والرسائل غير المهمة؛ من أجل منعها من العمل.

الكثير من هذه الهجمات مثل ضربة الموت (Ping of Death) والدموع (Teardrop) تستغل الهفوات والأخطاء البرمجية الموجودة في بروتوكولات TCP/IP من أجل القيام بالأعمال التخريبية.»[1]

فعلى سبيل المثال تم الهجوم على شبكة سي إن إن (CNN) وذلك عن طريق نشر فيروس يحمل اسم «Anticnn.exe» يعرض العلم الصيني مصغراً في إحدى زوايا الموقع، وحين يقوم أي مستخدم بالنقر على هذا العلم تظهر نافذة منبثقة تحتوي على شريط تحميل وصورة للزعيم الصيني الراحل ماوتسي تونغ مؤسس الحركة الشيوعية في الصين، وتظهر تحت الصورة عبارة مكتوب عليها: « إنه عمل العلم الأحمر: قم بعمل معقول للتعبير عن وطنيتك»، ثم يقوم الفيروس بعد ذلك بمحاولة الاتصال بموقع شبكة سي إن إن وعمل ضغط هائل عليه باستخدام أوامر HTTP وأوامر. [2]

[1] –Hacking the human: social engineering techniques and security countermeasures, by Ian Mann,p11.

[2] –Scene of the cybercrime: computer forensics handbook, by Debra Littlejohn Shinder,p313.

كثيراً ما يطلب المهاجمون من بعضهم – خاصة إذا كان يجمعهم هدف معين – التكاتف من أجل تدمير موقع معين، وذلك باستخدام بعض البرامج الشهيرة لتوجيه الضربات الإلكترونية، فيقوم المهاجمون بتنزيل البرنامج وتنصيبه على أجهزتهم، ثم بعد ذلك يتم الاتفاق على وقت معين، ومن ثم تبدأ المجموعة بالهجوم، وذلك بإدخال بيانات الموقع المستهدف، ثم يقوم بالضغط على إحدى إيقونات البرنامج، ومن ثم يقوم البرنامج بتوجيه ضربات متتابعة للموقع المستهدف، وكثير من المواقع لا تصمد أمام الهجمة، وبعضها يتم تعطيلها مدة قصيرة فقط، وبعضها لا تفيد معها مثل هذه الهجمات لتقدم وقوة النظام الأمني للموقع.

الفرع الثالث: الدخول والبحث الجماعي في موقع معين

هناك بعض الطرق السهلة والتقليدية التي لا تحتاج إلى خبرة أو برامج متقدمة، وهي قريبة من الطريقة التي قبلها، والنتيجة فيها واحدة، وهي حجب الخدمة مؤقتاً، والطريقة باختصار: تتفق مجموعة كبيرة من المهاجمين على الدخول إلى الموقع في وقت واحد، ثم يقومون بالبحث سوياً عن كلمة معينة، وتكون تلك الكلمة من الكلمات التي تتكرر بكثرة، مثل (which)(to)(the)، فإذا كان العدد كبيراً، وقدرة الموقع لا تتحمل هذا العدد الضخم، فإن الموقع يتعطل عن الخدمة مؤقتاً، قد تكون المدة قصيرة جداً، ولكن الموقع إذا كان مشهوراً قد تتأثر سمعته بين رواده، ومثل ذلك – أيضاً – الدخول الجماعي على موقع معين، والضغط على زر التحديث، مما يؤدي إلى تعطل الموقع مؤقتاً، كما فعلت مجموعة فرنسيّة في عام 1995 عندما طلبت من أعضائها الدخول إلى مواقع فرنسية حكومية والضغط المستمر على زر التحديث (Refresh) في المتصفح لمدّة ساعة كاملة، الأمر الذي أدى إلى توقف عمل بعض المواقع، بسبب كثرة عدد المستخدمين الذين انهالوا على الجهاز الخادم للصفحة بطلباتهم الإلكترونيّة المتكررة لعرض الصفحة.[1]

[1] –Encyclopaedia of Teaching of Internet, By A Kumar, p p290–300.

المطلب الثاني: القرصنة بسحب المعلومات الخصوصية

القرصنة اختراق لأجهزة الحاسوب عبر شبكة الإنترنت ويقوم بهذه العملية شخص أو مجموعة من الأشخاص لديهم خبرة واسعة في برامج الحاسوب، إذ يمكنهم بواسطة برامج مساعدة اختراق حاسوب أخر والتعرف على محتوياته.

يتعرض البعض لقرصنة البريد الالكتروني أو الصفحة الشخصية على مواقع التواصل الاجتماعي، وهو ما يعد خرقا للخصوصية وأحيانا يرتبط الأمر بخسائر مادية أيضا عند اختراق البيانات البنكية عن طريق الإنترنت. يعتبر التعرض لمثل هذه القرصنة بمثابة جرس إنذار للتأكد من سلامة برنامج الحماية من الفيروسات المستخدم فالاعتماد على برامج مجانية يتم تحميلها من الإنترنت، يسهل من عمل القراصنة ولا يوفر الحماية المطلوبة للبيانات.[1]

بدأت ظاهرة القرصنة والاختراق مع بداية ظهور الحاسبة الالكترونية، وازدادت بشكل كبير مع تقنية الشبكات، حيث يشمل الاختراق الهجوم على شبكات الحاسب من قبل مخترقي الأنظمة الالكترونية ومنتهكي القوانين، كما في التطور الحاصل في مجال سرية المعلومات التي تغطي الانترنت بالإضافة إلى تقنيات أخرى كالإتصالات،[2] فيشير مفهوم القرصنة الإلكترونية إلى ممارسات غير مشروعة على شبكات الحاسب الآلي، تستهدف التحايل على نظام المعالجة الآلية للبيانات بغية إتلاف المستندات المعالجة إلكترونيّا، ويقوم بهذه الممارسات قراصنة معلومات محترفون، أو شركات متنافسة ضد بعضها البعض، أو فيما بين موظفي المنشأة الواحدة؛ حيث قدرت بعض الدراسات الحديثة أن 85% من عمليات اختراق برامج الحاسب الآلي تتم من خلال موظفي الشركات.[3] يستخدم قراصنة الإنترنت أساليب عديدة لاختراق أو تعطيل شبكات الحاسوب المستهدفة، وقد يكون ضرر بعض هذه الأساليب محدودا يقتصر على سرقة معلومات محددة من حاسوب مستهدف، وقد يكون مدمرا يؤدي إلى تعطيل شبكة بأكملها وتسريب بيانات مستخدميها وبريدهم الإلكتروني. ومن أبرز أساليب القراصنة لتعطيل شبكات الحاسوب ما يعرف بهجوم الحرمان من الخدمة

[1] القرصنة الالكترونية، dwعربي، شوهد بتاريخ 2018/02/22،الرابط:
/ http: //www.dw.com/ar

[2] الحوار نت، القرصنة الالكترونية،شوهد بتاريخ2018/03/01،الرابط:
http: //www.alhiwar.net/ShowAdv.php?Tnd=70

[3] القرصنة الاكترونية،الاكاديمية العربية اللبريطانية المفتوحة للتعليم العالي،شوهد بتاريخ2018/03/01، الرابط:
http: //www.abahe.co.uk/information-technology-enc/71102-piracy.html

(Denial-of-service)أو الحرمان من الخدمة الموزع (DDoS) وهي هجمات تستهدف عادة مؤسسات حكومية أو شركات كبرى كالبنوك مثلا، وهدفها جعل جهاز أو شبكة حاسوب غير متاحة للمستخدمين المستهدفين، أي حرمانهم من الخدمة التي تستضيفها خوادم الشبكة.[1]

ونميز أيرز محطات القرصنة للدول الكبرى:

لا يمكن فعليا تحديد الفترة الزمنية لأول عملية اختراق، وذلك لأن مفهوم الاختراق قديما لم يكن يعني مجرد اختراق شبكة حاسوب أو موقع إلكتروني، وإنما كان اختراق أي جهاز لتحقيق هدف خاص يسمى اختراقا، وعلى هذا الأساس يمكن القول إن عام 1903 شهد أول عملية اختراق في التاريخ، تطورت الاختراقات بعدها لتصل إلى حد الحروب الإلكترونية.

في عام 1903 كان الفيزيائي جون أمبروز فلمنج يستعد لعرض إحدى العجائب التكنولوجية المستجدة وهي نظام تلغراف لاسلكي بعيد المدى ابتكره الإيطالي جوليلمو ماركوني، في محاولة لإثبات أن رسائل شفرة مورس يمكن إرسالها لاسلكيا عبر مسافات طويلة، وكان ذلك أمام جمهور غفير في قاعة محاضرات المعهد الملكي الشهيرة بلندن.

في عام 1932 تمكن خبراء التشفير البولنديون ماريان ريجيوسكي وهنري زيجلاسكي وجيرزي روزيكي من فك شفرة جهاز إنيغما الذي استخدمه بشكل خاص الألمان خلال الحرب العالمية الثانية لإرسال واستقبال رسائل سرية.

في عام 1971 ابتكر جون درابر –الملقب بكابتن كرنتش– وصديقه جو إنغريسيا الصندوق الأزرق الذي استخدماه للتحايل على نظام الهاتف وإجراء مكالمات هاتفية بعيدة المدى مجانا.

- سيتي بنك كان ضحية إحدى أكبر عمليات القرصنة الإلكترونية (غيتي) الثمانينيات والتسعينيات

- ونقفز إلى عام 1981 حيث تشكلت مجموعة قراصنة «نادي فوضى الحاسوب» في ألمانيا، ومجموعة «أسياد البرامج» (وير لوردز) في أميركا التي تتألف من العديد من المتسللين المراهقين ومخترقي الهاتف والمبرمجين والعديد من قراصنة الحاسوب الذين يعملون في الخفاء.

[1] تعرف على مفهوم وتاريخ القرصنة الالكترونية واشهر القراصنة في العالم،igider للمعلوماتية ،شوهد بتاريخ،2018/03/01الرابط:

http://www.igiderinform.com/2017/09/electronic-piracy.html

- في عام 1988 ظهرت «دودة موريس» -إحدى أوائل ديدان الحواسيب المعروفة التي أثرت في البنية التحتية للإنترنت وانتشرت في الحواسيب وعلى نطاق واسع داخل الولايات المتحدة، واستغلت الدودة نقطة ضعف في نظام يونيكس «ناون 1» واستنسخت ذاتها بانتظام وتسببت بإبطاء أداء الحواسيب لدرجة عدم القدرة على استخدامها.

وعند اعتقال مطور هذه الدودة روبرت تابان موريس أصبح أول قرصان يدان تحت قانون «احتيال الحاسوب وإساءة الاستخدام»، وهو الآن أحد القراصنة الأخلاقيين (أصحاب القبعات البيضاء) حيث يعمل بروفيسورا في معهد ماساتشوستس التكنولوجي.[1]

وفي صيف عام 1994 تمكن قرصان روسي يدعى فلاديمير ليفين من اختراق بنك «سيتي بنك» الأميركي وتحويل عشرة ملايين دولار من حسابات عملاء إلى حساباته الشخصية في فنلندا وإسرائيل مستخدما حاسوبه المحمول. حكم عليه بعد اعتقاله بالسجن ثلاث سنوات، واستعادت السلطات كافة المبلغ المسروق باستثناء أربعمائة ألف دولار.

- أنونيموس تبنت مسؤولية العديد من الهجمات التي استهدفت مواقع إنترنت إسرائيلية (غيتي(

اختراقات القرن الـ21

في ديسمبر/كانون الأول 2006 أجبرت ناسا على حجب رسائل البريد الإلكتروني التي تأتي مع مرفقات قبل إطلاق المركبات الفضائية خشية اختراقها، وذكرت مجلة «بيزنس ويك» الأميركية أن خطط إطلاق مركبات الفضاء الأميركية الأخيرة حصل عليها مخترقون أجانب غير معروفين.

في عام 2007 تعرضت شبكات حاسوب الحكومة الإستونية لهجوم من نوع الحرمان من الخدمة من طرف مجهولين، وذلك بعد جدال مع روسيا بشأن إزالة نصب تذكاري، وتعطلت في الهجوم بعض الخدمات الحكومية الإلكترونية والخدمة المصرفية عبر الإنترنت، وفي ذلك العام اخترق حساب بريد إلكتروني غير سري لوزير الدفاع الأميركي من طرف مجهولين ضمن سلسلة كبيرة من الهجمات للوصول إلى شبكات حاسوب البنتاغون.

وفي صيف عام 2008 اخترقت قاعدة بيانات حملات المرشحين الجمهوري والديمقراطي في الولايات المتحدة من قبل مجهولين قاموا بتحميل تلك البيانات، وفي أغسطس/آب اخترقت شبكة حواسيب في جورجيا من طرف مخترقين مجهولين خلال فترة صراعها مع روسيا.

[1] [1] تعرف على مفهوم وتاريخ القرصنة الالكترونية واشهر القراصنة في العالم، المرجع نفسه.

وفي يناير/كانون الثاني 2009 وخلال العدوان الإسرائيلي على قطاع غزة تعرضت بنية الإنترنت التحتية في إسرائيل لهجمات إلكترونية عديدة تركزت على مواقع إلكترونية حكومية، ونفذت الهجمات باستخدام نحو خمسة ملايين حاسوب على الأقل وفقا لمجة «ناتو ريفيو» الإلكترونية، وتبنت مجموعة القراصنة المجهولين (أنونيموس) الكثير من تلك الهجمات.

شبكة حواسيب سوني بيكتشرز تعرضت لهجمة إلكترونية مدمرة (أسوشيتد برس) حرب إلكترونية[1].

في يناير/كانون الثاني 2010 عطلت جماعة تطلق على نفسها اسم «الجيش الإيراني السيبراني» خدمة البحث على الإنترنت لمحرك البحث الصيني الشائع «بايدو»، وكان يتم تحويل مستخدمي محرك البحث إلى رسالة سياسية إيرانية، وكانت الجماعة ذاتها اخترقت «تويتر» في ديسمبر/كانون الثاني 2009 مع توجيه رسالة مشابهة.

وفي أكتوبر/تشرين الأول 2009 اكتشف فيروس «ستكسنت» وهو برمجية خبيثة معقدة مصممة لتعطيل أنظمة التحكم الصناعية من إنتاج سيمنز كالتي تستخدمها إيران وإندونيسيا إلى جانب دول أخرى، الأمر الذي أثار تكهنات بأنها سلاح إلكتروني حكومي استهدف برنامج إيران النووي.

في يناير/كانون الثاني 2011 أعلنت الحكومة الكندية تعرض وكالاتها لهجوم إلكتروني ضخم من بينها وكالة البحث والتطوير الدفاعي الكندية، وأجبرت الهجمات وزارة المالية ومجلس الخزانة الكنديين على فصل اتصالهما بالإنترنت.

وفي يوليو/تموز 2011 أعلن نائب وزير الدفاع الأميركي أن قراصنة إنترنت سرقوا 24 ألف ملف من وزارة الدفاع في عملية واحدة خلال مارس/آذار، مضيفا أن الوزارة تعتقد أن وراء الهجوم دولة وليس أفرادا أو مجموعة قراصنة.

في أكتوبر/تشرين الأول 2012 اكتشفت شركة أمن المعلومات الروسية «كاسبرسكي» هجوما إلكترونيا عالميا حمل اسم «أكتوبر الأحمر»، وقالت إنه يجري منذ عام 2007 على الأقل ويعمل على جمع معلومات من سفارات وشركات أبحاث ومؤسسات عسكرية وشركات طاقة وغيرها، مشيرة إلى أن أهداف الهجوم الرئيسية هي دول في أوروبا الشرقية ودول الاتحاد السوفياتي السابق وآسيا الوسطى، وبعض دول أوروبا الغربية وشمال أميركا.

وفي أواخر نوفمبر/تشرين الثاني 2014 تعرضت شبكة حواسيب شركة سوني بيكتشرز اليابانية في الولايات المتحدة لهجوم إلكتروني عنيف نتجت عنه سرقة عدد من الأفلام السينمائية الحديثة التي لم يكن

[1] [1] تعرف على مفهوم وتاريخ القرصنة الالكترونية واشهر القراصنة في العالم، المرجع نفسه.

بعضها قد عرض بعد، وتسريب مئات آلاف رسائل البريد الإلكتروني والبيانات الشخصية لحسابات معروفة، ووصفت بعض تلك الرسائل بالمحرجة، وبشكل عام تكبدت الشركة نتيجة هذا الهجوم –الذي نسب إلى كوريا الشمالية أو متعاطفين معها– خسائر قدرت بنحو مائة مليون دولار[1]

المطلب الثالث: الجوسسة على العمل الممارس للدول.

أصبح التجسس الإلكتروني أحد أخطر وأجدى أنواع التجسس، فقد طغى بإمكانياته الهائلة ودقة نتائجه على أساليب التجسس المعهودة في السابق،[2]إن تقنيات وآليات الجوسسة ستظلُّ حكرا على بعض الدول، لأنَّ تجنيد العملاء، وطريقة اختيارهم، من المرضى النفسيين، والأذكياء المغامرين، ومن المدمنين المهربين، والممثلين البارعين لا ينصرُ الدول، ويهزم دولا أخرى، وفق المفهوم التقليدي للجوسسة فقط، ولكنه اليوم أصبح علما محتكرا عند بعض الدول، لأن تجنيد الجواسيس، في كل قطاعات الحياة يُسهم في بناء الأمم التي جندتهم، ويساعدها على الازدهار.[3]

تنوّعت مصادرة المعلومات الإلكترونية وآليات الحصول عليها، من ذلك:

– استخبارات المصادر المفتوحة: وهي العمليات الاستخباراتية المستخلصة من المصادر المفتوحة مثل الإنترنت.

– استخبارات الاتصالات: التنصت على الاتصالات واعتراضها مثل التنصت على المكالمات الهاتفية) ويضم استخبارات الإشارات والاستخبارات الإلكترونية.

– الاستخبارات بالأقمار الصناعية: توفر مجموعة من المعلومات المستخلصة من عدد من أصول التجميع مثل الأقمار الصناعية الاستطلاعية أو طائرات المراقبة.

---

[1]تعرف على مفهوم وتاريخ القرصنة الالكترونية واشهر القراصنة في العالم، المرجع نفسه.

[2]الهام محمد علي، التجسس الإلكتروني: سلاح إسرائيل الذهبي لمراقبة العرب،نون بوست،شوهد بتاريخ،2018/03/04، الرابط:

https: //www.noonpost.org/content/13821

[3]توفيق أو شومر ،تقنيات الجوسسة الحديثة،جريدة الجسر الالكترونية،شوهد بتاريخ 2018/03/04 الرابط:

http //www.aljisr-news.com/news/?p=56712

– الاستخبارات الفنية: تعتمد على خصائص علمية وفنية في أنظمة الأسلحة والأجهزة التقنية وغيرها.[1]

نفذ هاكرز مجهولون هجمات واسعة على عدد كبير من المؤسسات والإدارات الرئيسية في مختلف دول العام.

وأكدت وسائل إعلام أن من بين المؤسسات والهيئات التي تعرضت لهذه الهجمات النظام الصحي الوطني في بريطانيا وشركة الاتصالات الإسبانية تيليفونيكا، ومشغل الشبكات الخلوية الروسية «MegaFon» ومنظمات كبيرة أخرى.

وذكرت RT أن شركة «MegaFon» الروسية أغلقت عددا من خوادم شبكتها الحاسوبية بسبب الهجمات الإلكترونية، مشيرة إلى أن الحواسيب هوجمت ببرمجيات خبيثة من نوعransomware» »، والتي كنتيجة لها يطالب القراصنة بدفع مبالغ مالية للوصول إلى البيانات المشفرة عن طريق فيروس.

من جانبها، قالت رئيسة الوزراء البريطانية تيريزا ماي، إن الهجمات الإلكترونية على مستشفيات المملكة المتحدة هي جزء من هجمة دولية كبرى.

وذكر موقع «ويكيليكس» أنه كان قد حذر سابقا من انتشار غير منضبط للبرمجيات الخبيثة من قبل الاستخبارات الأمريكية، وذلك في سلسلة نشراته

وكان الموقع نشر في 7 مارس الماضي، أكبر عملية تسريب لوثائق سرية من وكالة الاستخبارات المركزية الأمريكية تحت مسمى Vault7 وكما يشير موقعPolitico ، البرنامج الذي أنتجته وكالة الأمن القومي الأمريكية، يسمح للبرمجيات الخبيثة بالانتشار عبر بروتوكولات تبادل الملفات المثبتة على أجهزة حواسيب كثير من المؤسسات حول العالم.

وأكد Politicoأن الهاكر في هذه الهجمات يستخدمون البرامج التي استخدمتها وكالة الأمن القومي الأمريكية على شكل واسع، وفقا لتغريدة العميل السابق للوكالة، إدوارد سنودون.

وكتب سنودون مغردا في موقع تويتر: «أوه! قرار وكالة الأمن القومي الأمريكية صناعة وسائل هجوم ضد البرمجيات الأمريكية يهدد حاليا حياة المرضى في المستشفيات».

من جانبها، أكدت شركة «كاسبرسكي لاب» الروسية المتخصصة في مجال الأمن والحماية الإلكترونية أن الهاكر يستخدمون في هجماتهم فايروسا برمجيا لتشفير محتويات الأجهزة يسمىWannaCry، مشيرة إلى

[1] التجسس في العصر الرقمي،الروابط للبحوث، شوهد بتاريخ،2018/01/7 الرابط:
http: //rawabetcenter.com/archives/59323

أن 74 بلدا تضررت به.

وأوضحت الشركة أنها رصدت نحو 45 ألف هجمة ببرنامج التشفيرWannaCry.

وأكدت «كاسبرسكي لاب» أن الاتحاد الروسي كان من أكثر البلدان تضررا من هذه الهجمات الإلكترونية، موضحة أن الهجوم الذي وقع بعد ظهر اليوم ضد حواسيب مشغل الشبكات الخلوية الروسية «MegaFon» لم يؤثر على جودة الاتصالات.

وفي تفاعل من شركة مايكروسوفت «Microsoft» في هذا الشأن، أكدت أنها قامت بتحديث أنظمة تشغيل «Windows» ومضاد للفايروسات المجاني الخاص بها، لتوفر بذلك للمستخدمين حماية من الفايروس المشفرWannaCry » ».

وفي وقت لاحق، أكدت وزارة الداخلية الروسية حقيقة حدوث هجمات فيروسية إلكترونية على أجهزتها، مشيرة إلى أن انتشار الفيروس أوقف.

ووفقا لوكالة «إنترفاكس»، فقد أكد مصدر مطلع في الوزارة، أن الهجمات على خوادم وزارة الداخلية الروسية لم تؤد إلى تسريب المعلومات.

كما حث سنودن الكونغرس الأمريكي للتحقق من درجة ضعف أنظمة التشغيل المستخدمة في المستشفيات في الولايات المتحدة، على خلفية الهجمات على المرافق الطبية في بريطانيا .[1]

[1] الهاكرز يشنون هجوما واسع النطاق على مؤسسات حكومية في عشرات الدول حول العالم، منتدى التكنولوجيا العسكرية والفضاء،بتاريخ،2018/01/07،الرابط:

http: //army-tech.net/forum/index.php?threads

المبحث الثالث: الشراكات لدولية في اطار سلامة الأمن الالكتروني.

المطلب الأول: الشراكة الأمريكية والدول الأوروبية لمكافحة الجريمة الالكترونية.

تم قبول مصطلح «جرائم الإنترنت» على نطاق واسع واعتمد من قبل مجلس أوروبا في اتفاقية الجرائم الحاسوبية (2001م) ،[1] ومن الصعب قياس تكاليف الجريمة الالكترونية، ولكنها تنمو وتكثر بشكل متزايد[2]. وقد حذر الخبير الروسي يوجين كاسبرسكي Eugene Kaspersky المدير العام لشركة كاسبرسكي لاب Kaspersky Lab المتخصصة في مجال أمن الحواسيب، خلال كلمته أمام مؤتمر الفضاء السيبراني السنوي عام 2012 ،الذي نظمته ورشة عمل يوفال نيئمان بمركز بحوث الامن القومي الاسرائيلي، من أن استمرار تطوير الاسلحة السيبرانية وانتشارها Cyber Weapons من شأنه أن يغير وجه العالم الذي نعرفه، وأن البنية التحتية للعالم ليست مستعدة بعد لحماية نفسها من مثل هذه الاسلحة. [3]

وضمن الجهود الدولية لمكافحة الجرائم الالكترونية، تم إطلاق برنامج اليوم العالمي للأنترنيت الأمن،[4] Safer internet Dayالذي يحتفل العالم به خلال شهر شباط/فبراير من كل عام -لأول مرة عام 2004 كمبادرة من الاتحاد الأوروبي والمنظمة الأوروبية للتوعية بشبكة الإنترنت إنسيف المهتمة بالقضايا ذات الصلة بالإنترنت. ويهدف اليوم العالمي إلى رفع الوعي بالمخاطر الكامنة في الإنترنت وأهمية الحفاظ على الخصوصية لدى الآخرين من خلال رفع الوعي بحالات الخطر والاستخدام السيء وعواقبه القانونية إضافة إلى تطوير معايير وأنظمة أخلاقية وسلوكية لائقة عند استخدام الإنترنت، إلى جانب توفير أدوات وبرامج تقنية وعملية

---

[1] Oerlemans, Jan-Jaap, Investigating cybercrime, Leiden University,HIOA bibliotik, norway. 2017 ,p 20.

[2] Sofaer and Goodman. Cyber Crime and Security The Transnational Dimension, p 4, liens http: //media.hoover.org/sites/default/files/documents/0817999825_1.pdf..1.2017

[3] UK Safer internet Day.4.2.2014
https: //www.saferinternet.org.uk/safer-internet-day/safer-internet-day-2016

[4] د. نضال أدلبي، تطوير وتنسيق التشريعات السيبرانية في المنطقة العربية ومواجه الجرائم السيبرانية، الأمم المتحدة، الإسكوا،نقل بتصرف، ص ص 14- 18.

مفيدة وسهلة الاستخدام وصولًا إلى تعزيز العمل المشترك نحو إيجاد آليات مناسبة للعمل نحو استخدام آمن للإنترنت.[1]

و أبرز شراكة بين الدول الاوروبية فيما بينها والولايات المتحدة الامريكية وبعض الدول الاخرى نجد اتفاقية بودابست، فتعتبر الاتفاقية الدولية الأكثر أهمية في هذا المجال هي اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية، التي اعتمدت في عام 2001.[2] وفي بحثنا هذا حرصنا على إستعراض هذه الاتفاقية كونها نموذج للجهود الدولية لمعالجة هذه الجرائم والتصدي لها، ومن ثم نستعرض أهم الإتفاقيات الدولية في هذا الجانب ،وتم تناول البحث وفق السياق الآتي:

الفرع الأول: الإتفاقية الاوربية لمكافحة الإجرام المعلوماتي والمسماة (بودابست) لعام2001م:

- هو صك دولي ملزم بشأن هذه المسألة. وهو بمثابة المبدأ التوجيهي لأي بلد لوضع تشريع وطني شامل لمكافحة جرائم الإنترنت وكإطار للتعاون الدولي بين الدول الأطراف في هذه المعاهدة.[3]

ونظرا لازدياد الجرائم المتعلقة بالكمبيوتر شرعت الدول المتمدينة بوضع تشريعات خاصة لمكافحة جرائم الكمبيوتر التي تعتبر ظاهرة مستحدثة على علم الإجرام ومن هذه الدول الولايات المتحدة وفرنسا وباقي دول الإتحاد الاوربي الذي وضع إتفاقية حول جرائم الكمبيوتر سنة 2001م، والتي أوصت فيها الدول الأعضاء بإتخاذ كافة الإجراءات التشريعية وغيرها حسب الضرورة لجعل الدخول إلى جميع نظم الكمبيوتر أو أي من أجزائه بدون وجه حق جريمة جنائية بحسب القانون المحلي، كما أوصت هذه الإتفاقية على مجموعة من المبادئ العامة المتعلقة بالتعاون الدولي في مجال الشئون الجنائية، وحددت كذلك الإجراءات المتعلقة بطلبات المساعدة المتبادلة بين الدول في غياب الإتفاقيات الدولية.[4]

---

[1] د. ناصر بن محمد البقمي، مكافحة الجرائم المعلوماتية وتطبيقاتها في دول مجلس التعاون لدول الخليج العربي، مركز الإمارات للدراسات والبحوث الإستراتيجية، الطبعة الاولى، 2008م.. الصفحة 42-43.

[2] How can we combat cyber crime?. A group of researchers are aiming to shed new light on how legislation can be used to stop these criminals. Article from university of oslo. 2015/05/12. available at http: //sciencenordic.com/how-can-we-combat-cyber-crime.

[3] Cypercrime-Budapest Convention and related standards-council of europe. 2015/05/19. availble at http: //www.coe.int/en/web/cybercrime/the-budapest-conventio

[4] د. عبد العال الديربي، الاستاذ محمد صادق إسماعيل، كتاب الجرائم الالكترونية ،المركز القومي للإصدارات القانونية. الطبعة الاولى 2012. ص64، شوهد بتاريخ 2018/01/08الرابط:
https: //books.google.no/books?id=4d4sDAAAQBAJ&pg=PT

وقد اعتمد الاتحاد الأوروبي التشريع على غرار اتفاقية بودابست:[1]

- ويهدف واضعوا هذه الإتفاقية حث الدول الأعضاء على المواءمة بين القوانين الوطنية ونصوص الإتفاقية علاوةً على ضرورة استكمال الادوات القانونية لهذه الدول في المسائل الإجرائية وذلك بُغية تحسين الإتفاقية قدرات النيابات العامة على إجراء التحقيقات وجمع الادلة، [2]وقّعت على هذه الاتفاقية 30 دولة، ولأهمية هذه الاتفاقية انضمَّ إليها العديد من الدول من خارج المجلس الأوروبي، وأبرز هذه الدول الولايات المتحدة الأمريكية، التي صادقت عليها في 22 سبتمبر (2006) م. ودخلت حيز النفاذ في الأول من يناير (2007م .[3](اما جمهورية المانيا الفدرالية فقد صادقت على الاتفاقية عام 2009، وصادقت فرنسا على الاتفاقية في 10 كانون الثاني 2006. أما مملكة النرويج فقد صادقت على هذه الإتفاقية سنة 2006.

واشتملت الاتفاقية على عدة جوانب من جرائم الإنترنت، بينها الإرهاب وعمليات تزوير بطاقات الائتمان ودعارة الأطفال. [4] وتهدف الاتفاقية إلى:

- توحيد عناصر القانون الجزائي المحلي مع الأحكام المتعلقة بالجرائم الإلكترونية.
- توفير الاجراءات القانونية اللازمة للتحري وملاحقة الجرائم المرتكبة الكترونيًا بواسطة الكمبيوتر.
- تعيين نظام سريع وفعال للتعاون الدولي.

---

[1] Cybercrime. EU Regulatory Framework on Cybercrime.norway.university of oslo. 2015/12/22. available athttp: //www.jus.uio.no/ifp/english/research/projects/nrccl/signal/research-prongs/cybercrime/.

[2] Council of Europe. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. 2008/06/16. https: //rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId

[3] يونس حرب – جرائم الكمبيوتر والانترنت– ايجاز في المفهوم والنطاق والخصائص والصوروالقواعد الاجرائية للملاحقة والاثبات، ورقة عمل مقدمة الى مؤتمر الامن العربي 2002 – تنظيم المركز العربي للدراسات والبحوث الجنائية – ابو ظبي 10-12 /2/2002.

[4] جان فرنسوا هنروت – أهمية التعاون الدولي والتجربة البلجيكية في تبادل المعلومات بين عناصر الشرطة والتعاون القضائي– أعمال الندوة الاقليمية حول: »الجرائم المتصلة بالكمبيوتر– برنامج تعزيز حكم القانون في بعض الدول العربية– مشروع تحديث النيابات العامة

- الحفاظ بشكل سريع على البيانات المخزّنة على أجهزة الكمبيوتر وحفظها والإفصاح الجزئي عن حركة هذه البيانات المخزنة على الكمبيوتر.
- جمع معلومات عن حركة البيانات وعن إمكان وجود تدخّل في محتواها. [1]

واستنادا إلى المواد المشار إليها (2- 13) فإن الاتفاقية تلزم الدول الاعضاء فيها (دول الاتحاد الاوربي وأية دولة توقع عليها أو تريد أن تنضم إليها) بإتخاذ الاجراءات والتدابير التشريعية الملائمة لتجريم تسع جرائم في ميدان الجرائم المعلوماتية وهي:

- الدخول غير القانوني المتعمد illegal access .
- الاعتراض غير القانوني illegal interception .
- التدخل المتعمد أو الارادي في المعطيات interference data بالتدمير damaginأو الحذف deletion أوالتشويه والافساد deterioration أو تبديلها أو تغيرها أو تعديلها alteration أوتعطيلها أو كبتها أو إخمادهاsupperession .
- التدخل المتعمد في الانظمةsystem interference .
- التزوير المتعمد باستخدام جهاز الكمبيوتر computer-related forgery
- إساءة استخدام الاجهزة Misuse of devices.
- الاحتيال المتعمد باستخدام الكمبيوتر computer-related fraud.
- الجرائم المرتبطة بدعارة الأطفال.
- الجرائم المرتبطة بحق المؤلف copyright and related offences.

وتناولت المادة (11) من الاتفاقية القواعد العامة المتعلقة بالمساهمة الجنائية والعقوبة بشأن الجرائم المشار في المواد من (2- 10)، وقد أوجبت الاتفاقية على الدول الاعضاء إتخاذ تدابير تشريعية للنص على المسؤولية عن الشروع والتدخل والتحريض في إرتكاب هذه الجرائم أو ما تختاره الدولة منها وذلك بغرض وجود رادع عام لما لهذه الجرائم من تأثير شديد على إقتصاديات الدول، وكذلك النص على مسؤولية الاشخاص المعنوية عن الافعال التي ترتكب لمصلحة الشخص المعنوي من قبل أي شخص يتصرف لمصلحته سواء كان إستنادا الى تمثيل قانوني أو بإعتباره مناطاً به إتخاذ قرار عن الشخص القانوني أو لانه خاضع لسلطته بما في ذلك افعال التحريض والتدخل والمساعدة الجنائية، وكذلك مسؤولية الرؤساء عن غياب أو تخلف الرقابة والإشراف والتحكم بتصرفات الاشخاص المعنيين بالعمل. يلاحظ هنا وفقاً للإتفاقية إمتداد نطاق المساءلة الجنائية

[1] سكاي برس، لعبة تؤدي بحياة عشرات المراهقين الروس،بتاريخ: 2018/03/01 الرابط:
http: //www.skypressiq.net/2017/3/1/%D9%84

للشخصين الطبيعي والمعنوي. أما بالنسبة للعقوبات والتدابير فقد أوجبت الاتفاقية على الدول الاعضاء في الإتفاقية إقرار العقوبات الملائمة والفعالة لهذه الجرائم بما فيها العقوبات المانعة للحرية بالنسبة للأشخاص الطبيعيين مثلما هو الحال في القانون الامريكي والغرامات المالية بالنسبة للأشخاص المعنوية[1] .

ومن أهداف الإتفاقية حماية الأطفال من الإستغلال الجنسي، فقد صاغت الإتفاقية في إطار دولي قواعد قانونية لمكافحة هذا الإستغلال الغير قانوني وهذا ما نظمته المادة (9) من الإتفاقية. [2]

وفي إحترام حقوق الانسان، تؤكد ديباجتها وكذلك المادة رقم (15) أنه يجب الاخذ بعين الاعتبار الحاجة إلى ضمان وجود توازن مناسب بين المصالح المتحصلة من إجراء عملية قمعية واحترام حقوق الانسان الاساسية، ونص على ذلك أيضا العهد الدولي الخاص بالحقوق المدنية والسياسية التابع للامم المتحدة. [3]

ونظمت الاتفاقية تسليم المتهمين، حيث تنص المادة 24 على وجوب تسليم المتهمين بين الاطراف فيما يتعلق بالجرائم الملحوظة في المواد من (2 – 11) من الإتفاقية، شرط أن تكون تلك الجرائم معاقبا عليها بموجب القوانين المرعية الإجراء في بلد كل من الطرفين المعنيين بحرمان من الحر ية لفترة أقصاها سنة على الاقل، أو بعقوبة أشد في غياب اتفاق آخر جاري على أساس التشريعات المتبادلة الموحدة أو معاهدة نافذة حول موضوع تسليم المتهمين. [4]وحول التنسيق التقني، تفرض المادة (25/ 3) من الاتفاقية، في حالة الاتصلات المتعلقة بطلبات التعاون المشترك « أن تتم هذه الاتصالات عبر قنوات توفر القدر الكافي من الامان والتوثيق بما في ذلك التشفير إذا تطلب الامر ذلك.

وعن التعاون الدولي، تنص المادة (35) من الاتفاقية « كل دولة نقطة اتصال يمكن الاتصال بها على مدار 24 ساعة وكذا على مدار الاسبوع لضمان تقديم المساعدة الفورية أثناء التحقيق في الإنتهاكات القانونية

---

[1] الاتحاد الودلي للاتصالات، مرجع سابق.

[2] اتفاقية بودابست لمكافحة الجرائم المعلوماتية،شبكة قوانين الشرق،شوهد بتاريخ: 2018/02/08،الرابط:
http: //eastlaws.blogspot.com/2010/03/23-11-2001.html

[3] قرار المجلس بتاريخ 29 مايو 2000 ،متعلق بمكافحة استغلال الاطفال في إنتاج المواد الاباحية على الانترنت (JAI/375/2000) الجريدة الرسمية للاتحاد الاوروبي، 9 يونيو

[4] كريستينا سكولمان–برنامج تعزيز حكم القانون في بعض الدول العربية، اعمال الندوة الاقليمية حول الجرائم المتصلة بالكمبيوتر، المملكة المغربية، 2007، ص 47.

المتعلقة بنظم وبيانات إلكترونية، أو بهدف جمع أدلة ذات طابع إلكتروني عن إنتهاكات قانونية. [1] وقد طبقت كثير من البلدان الإتفاقية في إطار قوانينها الوطنية. ويتضح ذلك على سبيل المثال في تشريع رومانيا الذي يلتزم بنص الإتفاقية بشكل كبير. ويعتبر التشريع الروماني كاملاً وسهل الفهم وفعالاً في الوقت نفسه. [2]

وبالتالي يمكن القول ان الإتفاقية تغطي مجموعة كبيرة من الجرائم الجنائية، وأنها تميزت بأهمية قانونية من حيث ركزت على إتخاذ التدابير التشريعية الموضوعية لمكافحة هذه الجريمة، وألزمت الدول إضافةً للقواعد الموضوعية الإهتمام بالقواعد الإجرائية، وعن أهمية المسؤولية الجنائية جاهد المشرع لتقنين قواعدها، وألزم الدول الاعضاء إتخاذ تدابير تشريعية ووضع القواعد القانونية لتنظيمها، وأوجبت تعزيز أطر التعاون الدولي والإقليمي لاسيما توقيع معاهدات لتسليم المجرمين بين الدول حتى يفوت الفرصة على المجرمين الهروب من هذه الجرائم. [3]

المطلب الثاني: الشراكة الاوروبية تحت غطاء الناتو في تأمين السيرورة السيبرانية.

بعد عام واحد من هجمات 9/11، يتأهب الناتو لهذا النوع الجديد من التحدي الأمني.حيث أطلق حلف الناتو دعوة هامة لتحسين قدراته الدفاعية ضد الهجمات الإلكترونية كجزء من التزام براغ المتعلق بالقدرات والذي تم الموافقة عليه في نوفمبر 2002، لكن في السنوات التالية، ركز التحالف بشكل أساسي على تنفيذ تدابير الحماية السلمية المطلوبة للجانب العسكري.

شجعت الهجمات الإلكترونية التي وقعت في استونيا في ربيع عام 2007 التحالف لإعادة التفكير في احتياجه إلى سياسة دفاع إلكتروني ودفع التدابير المضادة للهجمات إلى مستوى جديد. ومن ثم وضع التحالف للمرة الأولى في تاريخه سياسة رسمية «للدفاع الإلكتروني» تم اعتمادها في كانون الثاني/يناير من عام 2008، لتضع ثلاث دعائم أساسية لسياسة الحلف تجاه الفضاء الإلكتروني.

---

[1] دعاوى الجرائم الإلكترونية وأدلة إثباتها في التشريعات العربية بين الواقع والمأمول، ضمن فعاليات المؤتمر الثالث لرؤساء المحاكم العليا (النقض، التمييز، التعقيب) في الدول العربية المنعقد في جمهورية السودان خلال الفترة 9/25.23/م الموافق 7-1433/11/9هـ.ص 10.

[2] ربيع محمد يحيى، كتاب اسرائيل وخطوات الهيمنة على ساحة الفضاء السيبراني في الشرق الاوسط، دراسة حول استعدادات ومحاور عمل الدولة العبرية في عصر الانترنيت(2002. 2013)، ص 77.

[3] خالد محي الدين احمد ،الجرائم المتعلقة بالرغبة الأشباعية باستخدام الكمبيوتر ،اعمال الندوة الاقليمية حول الجرائم المتصلة بالكمبيوتر ،الدار البيضاء، 2007،ص 37.

- **التبعية**، بمعنى تقديم المساعدة عند الطلب، وخلاف ذلك تم تطبيق مبادئ مسؤولية الدولة ذات السيادة؛
- **عدم التكرار**، بمعنى تفادي التكرار الغير ضروري للهياكل والقدرات – على المستوى الدولي والإقليمي والوطني؛ و
- **الأمن**، بمعنى التعاون القائم على الثقة مع الأخذ في الاعتبار حساسية المعلومات ذات الصلة التي يمكن الوصول إليها والمخاطر الممكنة.

وقد شكل هذا خطوة نوعية للأمام. كما مهدت الطريق لاتخاذ القرار الرئيسي في لشبونة لمتابعة قضية الدفاع الإلكتروني باستمرار كبند مستقل بذاته على أجندة الناتو.

لقد أرسى الناتو أسس بناء منظومة الدفاع الإلكتروني، مع بداية الهجمات مثل هجمات كوسوفو في عام 1999 واستونيا في عام 2007 وتأثرت بشكل كبير بالتغيرات الجذرية في مفهوم التهديد الدولي منذ أيلول/سبتمبر 2011. حيث تم تطوير أول آلية وقدرات للدفاع الكتروني تابعة للحلف، بما يعتبر إعداد مبدئي لسياسة الدفاع الإلكتروني.

ثم نجح الناتو في وضع أسس للتوجيه الذاتي والاختبار الفعلي، من خلال قرارات لشبونة في تشرين الثاني/نوفمبر من عام 2010. وبذلك، لا يكفي الناتو التحديث اللازم للهياكل القائمة مثل تحديث قدرة استجابة الناتو للحوادث الإلكترونية، لكنه أيضاً بداية للتعاون والمشاركة في مواجهة تحديات الدفاع الإلكتروني الفعلية والمتزايدة.

تماشياً مع المفهوم الاستراتيجي الجديد للناتو تم تعريف سياسة الناتو المنقحة بشأن الدفاع الإلكتروني ضد التهديدات الإلكترونية بأنها مصدر محتمل للدفاع المشترك وفقاً للمادة الخامسة من ميثاق الناتو. علاوة على ذلك، فإن السياسة الجديدة – وخطة العمل اللازمة لتطبيقها – تضع لدول الناتو توجيهات وعدة أولويات واضحة بشأن كيفية إحراز تقدم في الدفاع الإلكتروني بما في ذلك تعزيز التنسيق داخل الناتو وشركائه.

وفور تفعيل قرارات لشبونة بشكل كامل، سيقوم الحلف ببناء خطة «الدفاع الإلكتروني « المحدثة. وبذلك، يثبت الناتو مجدداً بأنه أهلاً لهذه المهمة. [1]

المطلب الثالث: الجهود الأممية في بناء السلام الالكتروني.

حتى يسهل لكل دولة الاستمرار والعيش مع غيرها من الدول فإنها تحتاج إلى قدرٍ من الأمن والنظام. وتشكل الجريمة إحدى القضايا الرئيسية في الكثير من دول العالم، وتشغل بال الحكومات والمختصين والأفراد على حد سواء. ولقد أثبت الواقع العملي أن الدولة – أي دولة – لا تستطيع بجهودها المنفردة القضاء على الجريمة مع هذا التطور الملموس والمذهل في كافة ميادين الحياة. فنتيجة للتطور الملموس والمذهل في الاتصالات وتكنولوجيا المعلومات وظهور الإنترنت والانتشار الواسع والسريع لها أدى إلى ظهور أشكال وأنماط جديدة من الجرائم منها الجرائم المتعلقة بشبكة الإنترنت وهي نوعٌ من الجرائم المعلوماتية، التي باتت تشكل خطرا لا على سرية النظم الحاسوبية أو سلامتها أو توافرها فحسب، بل تعدت إلى أمن البنى الأساسية الحرجة[2]

ومع تميزها بالعالمية وبكونها عابرة للحدود فإن مكافحتها لا تتحقق إلا بوجود تعاون دولي على المستوى الإجرائي الجنائي، بحيث يسمح بالاتصال المباشر بين أجهزة الشرطة في الدول المختلفة، وذلك بإنشاء مكاتب متخصصة لجمع المعلومات عن مرتكبي الجرائم المتعلقة بالإنترنت وتعميمها. [3]

فمثلا في جرائم البث والنشر الفيروسي قد يكون مرتكب الهجوم يحمل جنسية دولة ما، ويشن الهجوم الفيروسي من حواسيب موجودة في دولة أخرى، وتقع الآثار المدمرة لهذا الهجوم في دولة ثالثة. فمن البديهي أن تقف مشاكل الحدود والولايات القضائية عقبة أمام اكتشاف هذه الجرائم ومعاقبة مرتكبيها، لذا فإن التحقيقات في الجرائم المتصلة بالحاسب الآلي وملاحقتها قضائيا تؤكد على أهمية المساعدة القانونية المتبادلة بين

---

[1] التهديدات الجديدة: الأبعاد الإلكترونية،مجلة الناتو ،الذكرى العاشرة، شوهد بتاريخ **2018/04/08 الرابط:** **https: //www.nato.int/docu/review/2011/11-september/Cyber-Threads/AR/index.htm**

[2] تدابير مكافحة الجرائم المتصلة بالحواسيب، مؤتمر الأمم المتحدة الحادي عشر لمنع الجريمة والعدالة الجنائية- المنعقد في بانكوك في الفترة 18-2005/4/25م – وثيقة رقمA/CONF.203/14 ..

[3] جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة 1998م ص 75.

الدول، حيث يستحيل على الدولة بمفردها القضاء على هذه الجرائم الدولية العابرة للحدود، لأن جهاز الشرطة في هذه الدولة أو تلك لا يمكنه تعقب المجرمين وملاحقتهم إلا في حدود الدولة التابع لها بمعنى آخر أنه متى ما فرّ المجرم خارج حدود الدولة يقف الجهاز الشرطي عاجزا.

لذلك أصبحت الحاجة ماسة إلى وجود كيان دولي يأخذ على عاتقه القيام بهذه المهمة وتتعاون من خلاله أجهزة الشرطة في الدول المختلفة، خاصة فيما يتعلق بتبادل المعلومات المتعلقة بالجريمة والمجرمين بأقصى سرعة ممكنة بالإضافة إلى تعقب المجرمين الفارين من وجه العادلة.

الفرع الأول: منظمة الإنتربول:

أسس الأنتربول، الذي هو أكبر منظمة شرطية في العالم، عام1923 ، ومهمته تتمثل في تقديم المساعدة إلى أجهزة إنفاذ القانون في بلدانه الأعضاء ال 186لمكافحة جميع أشكال الإجرام عبر الوطني , للإنتربول بنى تحتية متطورة للإسناد الفني والميداني, تمكين قوى الشرطة في سائر أنحاء العالم من مواجهة التحديات الإجرامية المتنامية في القرن الحادي والعشرين. وتركز المنظمة اهتمامها على ستة مجالات إجرامية أعطتها الأولوية هي الفساد؛ المخدرات والإجرام المنظم؛ الإجرام المالي تقع الأمانة العامة للإنتربول في ليون بفرنسا، وهي تعمل على مدار الساعة وطوال أيام السنة ,للإنتربول ستة مكاتب إقليمية في مختلف أرجاء العالم.

تهدف المنظمة إلى تأكيد وتشجيع التعاون بين أجهزة الشرطة في الدول الأطراف وعلى نحو فعّال في مكافحة الجريمة الإلكترونية من تجميع البيانات والمعلومات المتعلقة بالمجرم والجريمة، وذلك عن طريق المكاتب المركزية الوطنية للشرطة الدولية الموجودة في أقاليم الدول المنضمة إليها،[1] وتتبادلها فيما بينها، بالإضافة إلى التعاون في ضبط المجرمين بمساعدة أجهزة الشرطة في الدول الأطراف،[2] ومدها بالمعلومات المتوفرة لديها على إقليمها وخاصة بالنسبة للجرائم المتشعبة في عدة دول ومنها جرائم الإنترنت، ومن الأمثلة على دور الإنتربول

---

[1] Malcom Anderson: " Policing the world: Interpol the Politics of International Police Co-Operation " , Clarendon press.Oxford,1989,p 168-185

[2] بيروت تستضيف مؤتمرا للملكية الفكرية، منشور في مجلة حماية الملكية الفكرية، العدد الثاني والخمسون، الربع الثاني 1997م، ص.11

في ما يتعلق بالجرائم المتعلقة بالإنترنت: ما حصل في الجمهورية اللبنانية عندما تم توقيف أحد الطلبة الجامعين من قبل القضاء اللبناني بتهمة إرسال صور إباحية لقاصرة دون العشرة أعوام من موقعه على شبكة الإنترنت. وذلك أثر تلقي النيابة اللبنانية برقية من الإنتربول في ألمانيا بهذا الخصوص.[1]

ولقد مرت جهود المنظمة في هذا المجال بمراحل عديدة، إلى أن تم إنشاء عدة مراكز اتصالات إقليمية في كل من طوكيو، نيوزيلندا، نيروبي، أذربيجان، بيونس أيرس لتسهيل مرور الرسائل، ويضاف إلى ذلك مكتب إقليمي فرعي في بانكوك. ونظرا لتنوع أنظمة الدول المختلفة، فقد كان هناك خيارين لأنظمة الاتصال، داخل هذه الشبكة، أولهما هو نموذج يخصص للدول المركزية وتجرى الاتصالات العالمية للشرطة فيها من خلال الجمعية العامة واللجنة التنفيذية بواسطة السكرتارية العامة، والثاني للدول اللامركزية وتجري الاتصالات فيه مباشرة بين أجهزة الشرطة في الدول المختلفة.

وعلى غرار هذه المنظمة أنشأ المجلس الأوربي في لكسمبورج عام 1991م شرطة أوربية لتكون همزة وصل بين أجهزة الشرطة الوطنية في الدول المنظمة ولملاحقة الجناة في الجرائم العابرة للحدود ومنها بطبيعة الحال الجرائم المتعلقة بالإنترنت. [2]

أما على المستوى العربي نجد أن مجلس وزراء الداخلية العرب أنشأ المكتب العربي للشرطة الجنائية،[3]بهدف تأمين وتنمية التعاون بين أجهزة الشرطة في الدول الأعضاء في مجال مكافحة الجريمة وملاحقة المجرمين, في حدود القوانين والأنظمة المعمول بها في كل دولة. بالإضافة إلى تقديم المعونة في مجال دعم وتطوير أجهزة الشرطة في الدول الأعضاء.

ويقوم الانتربول بعملية ملاحقة مجرمي المعلوماتية عامة وشبكة الإنترنت خاصة، عن طريق تعقب الأدلة الرقمية وضبطها, والقيام بعملية التفتيش العابر للحدود لمكونات الحاسب الآلي المنطقية والأنظمة المعلوماتية وشبكات الاتصال بحثا عن ما قد تحويه من أدلة وبراهين على ارتكاب الجريمة المعلوماتية.، كلها أمور

---

[1] فتيحة محمد قوارري" المواجهة الجنائية لقرصنة المصنفات الإلكترونية " Peer to peer مجلة الحقوق الكويت العدد الأول، السنة الرابعة والثلاثة مارس2010 ص45

[2] جميل عبد الباقي الصغير ،مرجع سابق.ص144.

[3] محمد الأزهر، حقوق المؤلف في القانون المغربي دراسة مقارنة في الملكية الأدبية والفنية، تقديم عبد الله درميش، دار النشر المغربية 1944، ص62 -61

تستدعي القيام ببعض العمليات الشرطية والفنية والأمنية المشتركة، وهي من شأنها صقل مهارات وخبرات القائمين على مكافحة تلك الجرائم، وبالتالي وضع حد لها. [1]

الفرع الثاني: جهود منظمة الأمم المتحدة

لقد عملت الأمم المتحدة منذ نشأتها على رسم سياسة ناجعة في مجال منع الجريمة وتحقيق العدالة الجنائية، عبر إقرار العديد من التوصيات وإنشاء اللجن المتخصصة ومن بينها اللجنة الاستشارية لخبراء منع الجريمة ومعاملة المجرمين الذي عهد إليها مهمة مكافحة الجريمة وتقديم المشورة للأمين العام، وإيجاد البرامج ووضع الخطط ورسم سياسات لتدابير دولية في مجال منع الجريمة، ومعاملة المجرمين وتعقد مؤتمرات دورية كل خمس سنوات وذلك تعزيز وتبادل المعارف والخبرات بين الأخصائيين من مختلف الدول من أجل تدعيم التعاون الدولي والإقليمي في مجال مكافحة الجريمة، ويعتبر مؤتمر الأمم المتحدة السابع لمنع الجريمة ومعاملة المجرمين الذي تم انعقاده مدين ميلانو بإيطاليا في سنة 1985 م والذي انبثق عن هذا المؤتمر مجموعة من القواعد التوجيهية والتي توجت بالمصادقة على هذه المبادئ في هافانا بكوبا عام 1990 م. [2] فقد أكد هذا المؤتمر على وجوب تطبيق التطورات الجديدة في مجال العلم والتكنولوجيا في كل مكان لصالح الجمهور. وبالتالي لمنع الجريمة على نحو فعال كما أكد على أن التكنولوجيا بما أنها قد تولد أشكالا جديدة من الجريمة فإنه ينبغي اتخاذ تدابير ملائمة ضد حالات إساءة استعمال المخلة لهذه التكنولوجيا، وأشاروا إلى مسألة الخصوصية التي يمكن أن تخترق عن طريق الإطلاع على البيانات الشخصية المخزنة داخل نظم الحسابات الآلية والتي تشكل انتهاكا لحقوق الإنسان واعتداء على حرمة الحياة الخاصة وأكد المؤتمر على وجوب اعتماد ضمانات ملاءمة لصون السرية كذلك أكد المؤتمر عبر قواعده التوجيهية على ضرورة تشجيع التشريعات الحديثة التي تجرم وتتناول جرائم الحاسب الآلي باعتبارها نمطا من أنماط الجريمة المنظمة كغسيل الأموال والاحتيال المنظم وفتح حسابات وتشغيلها بأسماء وهمية.

وأهم مبادئ مؤتمر هافانا (1990م):

1

[2] محمد الأمين ومحسن عبد الحميد أحمد، معايير الأمم المتحدة في مجال العدالة الجنائية ومنع الجريمة أكاديمية نايف العربية للعلوم الأمنية، الرياض، الطبعة الأولى 1998، ص 19.

-تحديث القوانين الجنائية الوطنية بما في ذلك التدابير المؤسساتية.

-تحسين أمن الحاسب الآلي والتدابير الفنية.

-اعتماد إجراءات تدريب كافية للموظفين والوكالات المسؤولة عن منع الجريمة الاقتصادية والجرائم المتعلقة بالحاسب الآلي والتحري والإدعاء فيها.

-تلقين آداب الحاسب الآلي كجزء من مفردات مقررات الاتصالات والمعلومات.

-اعتماد سياسات تعالج الاشكالات المتعلقة بالمجني عليهم في تلك الجرائم.

-زيادة التعاون الدولي من أجل مكافحة هذه الجرائم.

ولم تقف جهود الأمم المتحدة عند هذا الحد بل ,واصلت جهودها عبر عقد عدة مؤتمرات أهمها المؤتمر التاسع لمنع الجريمة ومعاملة المجرمين والذي عقد في القاهرة عام 1995 , وكان من أهم توصياته عمل من أجل حماية حياة الإنسان الخاصة وملكيته الفكرية في مواجهة مخاطر التكنولوجيا ,وعمل كذلك على التنسيق وتعزيز التعاون بين أعضاء المجتمع الدولي لاتخاذ الإجراءات المناسبة للحد منها. [1]

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

[1] مؤتمر الأمم المتحدة لمنع الجريمة والعدالة الجنائية، الجزيرة نت،شوهد بتاريخ: 2018/04/21، الرابط:
http: //www.aljazeera.net/encyclopedia/events/2015/4/21

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

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

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

- المحققين الخاصين الذين يعملون بالتنسيق مع أجهزة العدالة الجنائية يمكن أن يلعبوا دوراً مهماً في مكافحة جرائم الإنترنت.[1]

وقد قدمت شركة « فاير آي FireEye » المتخصصة في مجال التصدي للهجمات الالكترونية المتقدمة 8 إجراءات مهمة لتفادي مخاطر تزايد الهجمات الالكترونية التي تستهدف دول الخليج العربي، بعدما كشفت عن جملة من التصورات والرؤى التحليلية بشأن مشهد الهجمات الالكترونية في مناطق أوروبا والشرق الأوسط وأفريقيا، وعلى وجه الخصوص في دول مجلس التعاون الخليجي، وتمثلت هذه الإجراءات في ما يلي:

1) التوقع الدائم بأن تكون تلك الشركات مستهدفة.
2) أنه من الممكن تخطي حدود الضوابط الأمنية المتوفرة لديها.
3) التأكد دائما من أن ليس هناك أي كيان تجاري بمنأى عن الهجمات.
4) وضع إطار عمل خاص بالمخاطر ذات الصلة بالأنترنت.
5) الحصول على منصة استخبارات التهديدات الأنسب لتحسين قدرات الكشف عن الهجمات المحتملة.

[1] عبدالله بن فازع القرني، مواجهة جرائم الإنترنت: نحو إستراتيجية أمنية – مجتمعية متكاملة، مقال منشور على موقع جريدة الرياض ،شوهد بتاريخ 2018/04/21 على الرابط:
http: //www.alriyadh.com/912032

6) إنشاء خدمة الاستجابة للحوادث الطارئة وإدارتها، والتي من شأنها تمكين الشركات من اكتشافها والتفاعل مع هجمات APT بالسرعة الممكنة.

7) تسخير التكنولوجيا المناسبة القادرة على تحديد واكتشاف هذه التهديدات الجديدة.

8) وضع خطة استجابة واضحة والعمل على تحضيرها استعدادا للتعامل مع أي حالة اختراق. [1]

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

إن الدول الكبرى في البعد الخامس من أبعاد الجيواستراتيجية هي تلك التي تمتلك الترسانة المعلوماتية القادرة على المواجهة، والدفاع من أي تهديد قد يعصف بالكيان الإلكتروني للدول الكبرى.

لقد تأثرت الدول الكبرى بعديد من الهجومات الالكترونية و السيبرانية مما حتم عليها بناء ترسانة معلوماتية لها و الدخول في شراكات أممية لحماية الكيان الإلكتروني في عملية التجريم و المواجهة و الدفاع.

الفصل الثالث

نتطرق في هذا الفصل إلى دراسة الحالة، الولايات المتحدة الأمريكية حيث سيتضمن هذا الفصل كيفيات عصرنة القطاعات في المؤسسات الأميركية، وكذا أهم الجرائم الموقعة في امريكا الكترونيا و التهديدات التي واجهتها و الآليات للحد والخروج من العطب الإلكتروني، وإلى استشراف الأمن الإلكتروني.

المبحث الأول: قراءة عامة للأمن الالكتروني الأمريكي.

المطلب الأول: عصرنة القطاعات الأمريكية.

ظهرت الفكرة الأولى لعصرنة القطاعات في الولايات المتحدة الأمريكية عام 1935م عندما أثيرت مسألة جدول الرواتب حال نفوذ قانون الضمان الاجتماعي، و كان موضوع هذه المشكلة يتمحور حول كيفية إصدار أرقام الضمان الاجتماعي لـ 26. مليون عامل أمريكي، هذا الأمر تطلب مساحة لحفظ الوثائق تقدر بـ 26 ألف قدم مربع، حيث لا يوجد أي مبنى في مدينة واشنطن يمكنه استيعاب هذا الكم الهائل من الأوراق سواءا من حيث الوزن أو المساحة، هذا ما جعل الدولة تلجأ إلى مصانع شركة كوكا كولا في مدينة BALTIMORE لحفظ الأوراق، و في نفس العام قامت وزيرة العمل الأمريكية Frances Perkins باستشارة مساعدها الأول في الحاسوب الذي أنتجته شركة IBM الأمريكية خصيصا لهذه الغاية، و في بداية الخمسينات من القرن الماضي عملت مؤسسة الضمان الاجتماعي في الولايات المتحدة على إنشاء أول حاسوب معد لخدمة أغراضها العملية، وفي شهر أوت من عام 1955م استلمت المؤسسة أول مبرمج للقيام بخدمات متعددة، أهمها استلام الاشتراكات أطلق عليه اسم The IBM705 وهو أول حاسوب قام بتغطية نشاط الحفظ و تقديم خدمات الضمان الاجتماعي.[1]

- إن بدايات أمريكا في استخدام التقنية في الدوائر الحكومية كانت في عهد كلينتون عندما كان يترأس الولايات المتحدة الأمريكية في سنة 1993م حيث أدرك بأنه يجب أن تقوم الحكومة باستثمار التقنية واستغلالها لتسهيل تقديم الخدمات للمواطنين بسلاسة أكثر،،كان الفكرة قيد التنفيذ وطبقت حتى عام 1998م بدأت نشاطات الحكومة الالكترونية بشكل ملحوظ، وأصبح للولايات المتحدة الامريكية موقع الكتروني شامل لجميع الخدمات التي يحتاجها المواطن(usa.gov) ، حيث أصبحت الخدمات متمركز حول المواطن ، ولكن في عام 2000م تم خلع الرئيس الامريكي السابق بيل كلينتون وابتدأ عهد بوش،،حيث قام بعملية تنظيف لجميع الطاقم الذي كان مواليا "لكلينتون وكون له طاقم عمل جديد،،وبذلك انتهت جميع الخطط التي كانت لم تستكمل بعد والتي كانت تهدف لتطوير الحكومة الالكترونية ،في سنة 2001م جاء بوش بخطط جديدة ووضع أهداف جديدة لتطوير الحكومة الالكترونية فكون فريق أسماه (Quicksilver)

[1] سوسن زهير المهتدي ،تكنولوجيا الحكومة الإلكترونية، دار أسامة للنشر و التوزيع، الأردن، 2011، ص ص 19-20.

هذا الفريق كان مسؤولا" عن تحقيق الأهداف التي وضعها بوش، ولكن كان هناك صعوبات واجهت عملية التطوير وادخال التقنية للدوائر الحكومية، ومن أهم هذه الصعوبات:

-culture agency والمقصود بها أن الناس يختلفون جميعا في الثقافة والمعتقدات وكذلك الحال في الدوائر الحكومية، حيث أنها تضم موظفين من مختلف الجنسيات وكل له ثقافة مختلفة.

- trust وهي تمثل انعدام ثقة الناس بالحكومة.

-stakeholders resistance وهي تمثل الناس الذين لهم مصالح مع الحكومة سواء"كانوا مواطنين أو موظفين أو شركات،، فطبعا" إذا حصل وطبقت التقنية في الدوائر الحكومية فإنه من الممكن أن تحل التقنية محل الموظفين، يعني ممكن أن يفقد بعض الناس مقاعدهم الوظيفية.[1]

ومع بدايات القرن ال 21 تراجع ترتيب أمريكا حسب تصنيف الأمم المتحدة من المرتبة الأولى عالميا في عام 2005م إلى المرتبة الرابعة في 2008م. لعل من أهم ما يميز التجربة الأمريكية في هذا المجال هو تأثير فهم ودعم القيادة لمشروع الحكومة الإلكترونية. فعند التأمل في التاريخ، نجد أن أول من بدأ بإدخال هذا المصطلح إلى البلاد هو الرئيس السابق بل كلنتون في عام 1997م حيث حدد ضرورة إدخال خدمات إلكترونية من خلال مواقع الجهات الحكومية. وقام خلال فترة رئاسته الثانية بتشكيل فريق عمل للتخطيط والتنسيق لإدخال تقنيات الحكومة الإلكترونية في الجهات الحكومية. يأتي بعد ذلك الرئيس السابق جورج بوش في 2000م (وهو من حزب مختلف) ويلغي تقريباً كل ما خططت له إدارة كلنتون ويبدأ بفهم وخطط جديدة للمشروع مما سبب تأخيرا للمشروع و الكثير من المصادر الضائعة. شهد مشروع الحكومة الإلكترونية تطوراً ملحوظاً في عصر بوش ربما بسبب استمرار إدارته لفترتين رئاسيتين (8 سنوات) ولولا ذلك لربما جاء الرئيس الجديد بأفكار مخالفة. كذلك مما يمكن للتجربة الأمريكية أن تفيدنا هو ضرورة التخطيط السليم لكيفية ربط المؤسسات والدوائر الحكومية المختلفة إلكترونياً من خلال شبكات عمل وسياسات عمل بيني (Interopérabilité Standards).فالأمر في أمريكا مختلف عن معظم دول العالم، فالحكومة مكونة من ثلاثة طبقات (مستويات): المستوى الفيدرالي (الرئاسي) والمستوى الخاص بكل ولاية)كل ولاية لها أنظمة مختلفة) والمستوى المحلي (كل مدينة داخل كل ولاية لها إهتمامات مختلفة). فكيف يمكن ربط جميع المدن أو الضواحي بمختلف مؤسساتها بجميع الولايات بمختلف قوانينها بالحكومة المركزية الفيدرالية في بوابة واحدة؟ من المنجزات في هذا

[1] J. FLOUR, J.-L. AUBERT, Les obligations, Armand Colin, 1994, p.105

الباب هو مشروع البنية الفيدرالية (Federal Architecture) والذي يهدف إلى ربط ودمج مستويات الحكومة المختلفة.[1]

المطلب الثاني: اعتماد الامن الالكتروني في الامن القومي الأمريكي.

يعد المجلس الهيئة الأساسية للرئيس للنظر في مسائل الأمن القومي والسياسة الخارجية مع كبار مستشاريه للأمن القومي ومسؤولي رئاسة الوزراء .ومنذ إنشائه إبان حكم الرئيس الأسبق ترومان تحددت وظيفته في تقديم المشورة .

يتولى مستشار الأمن القومي الدفاع عن سياسة الرئيس أمام الكونغرس في قضايا السياسة الخارجية، ويعود تاريخ إحداث هذا المنصب للرئيس دوايت آيزنهاور عام 1953، متجاوزا بذلك سلطة ووظيفة السكرتير التنفيذي، ويختار الرئيس بكل حرية مستشاره للأمن القومي لعدم سلطة ورقابة للكونغرس عليه في هذه المسألة.

وتوسع دور المستشار للأمن القومي، ليصبح بمثابة المبعوث الشخصي للرئيس للوفود الأجنبية، الحريص على تطبيق قرارات الرئيس، مع تقديم النصيحة والمشورة له، ولذلك يختار الرئيس لهذا المنصب من يشاطره رؤيته ويتقارب مع أفكاره ويثق فيه.

يلاحظ على عمل المجلس أن هيكلته غير منصوص عليها في قانون الكونغرس، وأن عمله واتخاذ القرار فيه تهيمن عليهما السرية، مما يجعل من الصعب تحديد دور المجلس وهيكلته بشكل دقيق، مع أن المجلس مؤسسية رئيسية في السلطة التنفيذية، ومكلف طبقا للقانون باتخاذ القرارات في القضايا المستجدة والراهنة[2].

ومع استناد الهجمات الأخيرة الأكبر في التاريخ على برمجيات الخبيثة طورتها وكالة الأمن القومي لاستخدامها ضد خصومها، فإن الأمر بات قضية حساسة بالنسبة للولايات المتحدة، ومنذ الصيف الماضي،

[1] A.–M. Leroyer, L'épreuve d'Internet, précité, p. 180

[2] الحرب الرقمية،مركز الجزيرة للابحاث، شوهد بتاريخ:2018/02/12، الرابط:
http://www.aljazeera.net/encyclopedia/organizationsandstructures/2015/6/30

بدأت مجموعة تطلق على نفسها اسم "وسطاء الظل" في نشر أدوات البرمجيات المسروقة من مخزون حكومة الولايات المتحدة من أسلحة القرصنة الخاصة بها.

وبحسب صحيفة نيويورك تايمز قال باحثون في شركة سيمانتيك لأمن المعلومات الإلكترونية إن الهجوم الجديد استخدم نفس أداة القرصنة "إترنال بلو" التي استخدمت في هجوم "وانا كراي"، فضلا عن طريقتين أخريين لتعزيز انتشاره.

ولم تعترف وكالة الأمن القومي NSA بأدواتها المستخدمة في هجمات أو غيرها من الهجمات، ولكن المتخصصين في أمن الكمبيوتر يطالبون الوكالة بمساعدة بقية العالم على الدفاع عن الأسلحة التي أنشأتها، ومن بينهم شركة إدت IDT، وهn مجموعة مقرها نيوارك تعرضت لهجوم منفصل ف أبريل 2017 استخدمت أدوات قرصنة مسروقة من الوكالة.

وقال جولان بن أوني، كبير موظفي المعلومات العالمية في IDT، إن وكالة الأمن القومي الأمريكية تحتاج للقيام بدور قيادي في العمل عن كثب مع بائعي منصاب أنظمة الأمن والتشغيل مثل آبل ومايكروسوفت لمعالجة الطاعون الذى أطلقته للعنان"، وحذر المسئولين الفيدراليين من احتمال وقوع هجمات أكثر خطورة في المستقبل القريب.

ومع تزايد خطورة هذه الهجمات، حذرت بريطانيا من أنها على استعداد للرد على مثل هذه الهجمات بالغارات الجوية وربما إرسال قوات، خاصة أنها كانت الأكثر تضررا فD هجوم "وانا كراي" الذى تسبب في شلل نظام الرعاية الصحية البريطاني، وقدرت التصريحات الرسمية الخسائر الأولية، وقتها بعشرات ملايين الجنيهات الإسترلينية. وتم توجيه أصابع الاتهام في أعقاب الهجوم السابق، مايو الماضي، إلى كوريا الشمالية.

وبحسب صحيفة الديلي تليجراف، البريطانية، فإن وزير الدفاع البريطاني، مايكل فلين، اقترح أن تطلق بريطانيا ضربات جوية كرد على أي هجوم سيبراني مستقبلي، إذ حذر من أن استهداف الأنظمة البريطانية يستدعى الرد من الجو أو الأرض أو البحر أو الفضاء الإلكتروني.[1]

[1] الهجمات الالكترونية وتاثيرهاعلى الدول، اليوم السابع، شوهد بتاريخ2018/03/12، الرابط:
https://www.youm7.com/story/2017/6/28/

اكد رئيس القيادة السيبرانية، أن الجهود التي تبذلها الحكومة الأمريكية لصد الهجمات السيبرانية "الإلكترونية" ضد الدولة هي جهود غير مجدية، وشدد على ضرورة تعزيز القدرات السيبرانية الهجومية للجيش الأمريكي.

"نحن في مرحلة حرجة" هكذا قال الأميرال مايكل روجرز، مدير وكالة الأمن القومي، في جلسة استماع للجنة القوات المسلحة في مجلس الشيوخ، وأضاف "يجب علينا التفكير في الكيفية التي سنعزز بها قدراتنا على الجانب الهجومي للوصول إلى مرحلة الردع."

حيث انتقد روجرز تركيز جهود القيادة السيبرانية –التي تم إطلاقها كقسم من وكالة الأمن القومي الأمريكي في عام 2010– على الناحية الدفاعية فقط، معتبراً من خلال خطابه أمام الكونغرس أن الإستراتيجية الدفاعية البحتة وانتهاج مبدأ رد الفعل فقط، سيعملان –في نهاية المطاف– على تراجع القدرات السيبرانية عن تلبية الحاجات.

ما جاء في خطاب روجرز يعتبر استكمالاً للنهج الذي كان يتبعه سلفه كيث ألكسندر، والذي تقاعد العام الماضي وافتتح شركة لخدمات الأمن السيبراني، حيث أيّد الأخير طوال فترة خدمته توجيه الموارد نحو تعزيز القدرات هجومية بشكل أكبر، ولكن المخاوف التي بزغت لدى البيت الأبيض ووزارة الخارجية ووزارة الدفاع الأمريكية حول النتائج الضارة والغير مقصودة التي قد تنجم عن استخدام الأسلحة السيبرانية والتي قد تضر بالعلاقات الدبلوماسية مع الدول، أدت إلى ترك القدرات الهجومية السيبرانية الأمريكية في حدها الأدنى.

أفاد روجرز أن الرئيس أوباما لم يقرر بعد تفويضه بتطوير ونشر أدوات الهجوم السيبرانية، حيث أوضح أن صنّاع القرار لا يزالون غير مقتنعين بأن الوقت قد حان لانتهاج المبدأ الهجومي، وأضاف "علينا أن نعمل على وضع صنّاع القرار بصورة القدرات الموجودة لدينا وما يمكننا القيام به"، وعندما سُئل من قبل جون ماكين عمّا إذا كان يوافق على أن مستوى الردع ضد الهجمات السيبرانية غير مجدي، أجاب روجرز "هذا صحيح."

أكد روجرز أن التهديد الإلكتروني آخذ بالازدياد، فالهجمات السيبرانية لا تسعى لتعطيل أو عرقلة القدرات السيبرانية الأمريكية فحسب، إنما تسعى لـ"تأسيس وجود دائم على شبكاتنا"، واتهم روجز حكومات إيران وروسيا والصين بتوجيه هجمات قراصنة الانترنت "الهاكرز" الفردية على الشبكات الأمريكية، حيث أوضح أنه يوجد رابط قوي ومباشر ما بين هذه الهجمات وتوجيهات هذه الدول بالهجوم أو بالتدخل، وأضاف أن القيادة السيبرانية الأمريكية تعمل على ملاحقة الأدلة التي توضح محاولة الحكومات الأجنبية إرباك

محللي القيادة السيبرانية، من خلال استخدام "شركاء" غير حكوميين لتنفيذ هجمات سيبرانية لا يمكن نسبها إلى الدولة بشكل مباشر.

تم تأييد وجهات نظر روجرز حول الهجوم السيبراني من قبل العديد من أعضاء مجلس الشيوخ، وعلى الأخص ماكين، الذي استخدم هذه المنصة لانتقاد تعامل إدارة أوباما مع الحوادث السيبرانية الأخيرة، حيث قال ماكين في بداية جلسة الاستماع "إن الهجوم الإلكتروني الذي حصل في نوفمبر من كوريا الشمالية على شركة سوني، كشف عن عيوب خطيرة في استراتيجية قيادة الأمن السيبراني" وتابع بقوله "إن الفشل في وضع استراتيجية سيبرانية رادعة، زاد من إصرار خصومنا على مواصلة قيامهم بالهجمات بشكل يهدد أمننا القومي على نحو متزايد."

سبق لروجرز الإشارة إلى إنه من الضروري تعيين حكومة كوريا الشمالية بوصفها مسؤولة عن هجوم سوني، بهدف ردع الدول الأخرى عن اتخاذ إجراءات مماثلة، علماً أن تسمية كوريا الشمالية كدولة مسؤولة عن الهجمات الإلكترونية كان بادرة غير مسبوقة بالنسبة للولايات المتحدة.

ومن جهتهم يشير المسؤولون في الإدارة الأميركية، أن العقوبات المالية التي تم فرضها ضد المسؤولين في كوريا الشمالية في أعقاب الهجوم الالكتروني، والاتهامات التي تم توجيهها في العام الماضي إلى خمسة مسؤولين عسكريين صينيين بسرقة أسرار من الشركات الأمريكية، تظهر عزم الإدارة الأمريكية على مساءلة الخصوم عن الانتهاكات السيبرانية.

أما ماكين ونواب آخرون، فيسعون لتطبيق إجراءات أكثر صرامة، حيث يقول السناتور أنجوس كينج "أعتقد أنه من المهم جداً تطوير القدرات الهجومية السيبرانية، وعلاوة على ذلك، يجب الإفصاح عن هذه القدرات ونشرها"، ويقتبس كينج من الفيلم السينمائي الكلاسيكي دكتور سترينجلوف الذي يسخر من مخاوف نشوب النزاع النووي أثناء الحرب الباردة ليوضح وجهة نظره حول ضرورة الإفصاح والنشر، حيث يقول "إذا قمت ببناء جهاز يوم القيامة "الجهاز النووي الروسي"، يجب أن تقول للعالم بأجمعه أنك قمت بتصنيعه، وإلا لن يتحقق الغرض منه".[1]

[1] مراسلة لتغطية شؤون الأمن القومي بالولايات المتحدة إلين ناكاشيما الرابط:

https://www.noonpost.org/content/5921

المطلب الثالث: تقنين الأمن المعلوماتي في التشريع الأمريكي.

تبعت الولايات المتحدة الأمريكية السويد حيث شرعت قانونا خاصة بحماية أنظمة الحاسب الآلي (1976م – 1985م)، وفي عام 1985)م) حدّد معهد العدالة القومي خمسة أنواع رئيسة للجرائم المعلوماتية وهي: جرائم الحاسب الآلي الداخلية، جرائم الاستخدام غير المشروع عن بعد، جرائم التلاعب بالحاسب الآلي، دعم التعاملات الإجرامية، وسرقة البرامج الجاهزة والمكونات المادية للحاسب. وفي عام (1986م) صدر قانونا تشريعاً يحمل الرقم (1213) عرّف فيه جميع المصطلحات الضرورية لتطبيق القانون على الجرائم المعلوماتية كما وضعت المتطلبات الدستورية اللازمة لتطبيقه، وعلى اثر ذلك قامت الولايات الداخلية بإصدار تشريعاتها الخاصة بها للتعامل مع هذه الجرائم ومن ذلك قانون ولاية تكساس لجرائم الحاسب الآلي[1].

في الولايات المتحدة ينظم جرائم الكمبيوتر والانترنت مجموعة من التشريعات على المستوى الفدرالي وكذلك على المستوى المحلي في مختلف الولايات، فعلى المستوى الفدرالي يمثل القسم (18) من قانون الولايات المتحدة التشريع الرئيس لجرائم الكمبيوتر (المادة 1030) حيث تتضمن اعتبار الافعال التالية من قبيل الجريمة:

1 – التوصل غير المصرح به (الدخول) الى احد انظمة الكمبيوتر الحكومية وكشف المعلومات السرية، وكشف المعلومات من جهة غير مصرح بها تلقيها.

2 – الدخول غير المصرح به الى اي كمبيوتر والتوصل الى معلومات غير مسموح الاطلاع عليها.

3 – الدخول غير المصرح به الى اي كمبيوتر ومن ثم ارتكاب احتيال.

4 – الحاق اضرار جراء الدخول غير المصرح به اسواء للنظام او البرامج او للمعلومات المخزنة فيه.

5 – بث او تهديد بارتكاب ضرر لأي كمبيوتر عبر الولايات او للتجارة الاجنبية بغرض ابتزاز اموال او منافع من اي شخص طبيعي او معنوي.

[1] The hacker Crackdown law and Disorder on the Electronic fron– tier by Bruce sterling pp.159.1994.

أما القسم (1462) من الفصل (18) من قانون الولايات المتحدة فانه يحظر استخدام الكمبيوتر لاستيراد مواد مخلة بالآداب الى داخل الولايات المتحدة الامريكية.

في حين ان القسم (1463) من الفصل (18) يحظر نقل اية مواد فاحشة عبر الولايات او الجهات خارجية.

ويجرم القسم (2251) من ذات الفصل توظيف اي قاصر او اغرائه في المشاركة في انشطة جنسية بما فيها خلق وتصوير مواد وبثها لجهات خارجية.

ويحظر القسم (22051) من ذات الفصل استخدام الكمبيوتر الاخلال برعاية قاصر بقبول استغلاله – مع العلم – في انتاج مواد تنطوي على استغلال جنسي.

ويعتبر القسمين (2252، 2252 /أ) من ذات الفصل نقل وتبادل المواد الفاحشة ذات الصلة بالأطفال جريمة.

أما القسم (1028) من الفصل (18) من قانون الولايات المتحدة فانه يعتبر انتاج او نقل او ادارة جهاز يتضمن نظام كمبيوتر بقصد استخدامه بتزوير الوثائق او انتاج وثائق تعريف مزورة جريمة ويعتر القسم (2319) من ذات الفصل الاخلال بحق المؤلف جريمة فدرالية.

وعلى مستوى الولايات، فان الاطار العام لتشريعات الولايات المتحدة في حقل جرائم الكمبيوتر والانترنت يتمثل بما يلي:

1. كل ولاية من الولايات الخمسين تملك حرية التشريع الخاص بها وليس هناك آلية على مستوى الولايات او المستوى الفدرالي تتطلب تبني الولاية شكلا او محتوى محددا لقوانينها، وذلك بالرغم من وجود مشاريع توحيدية ومحاولات وتصريحات تهدف الى توحيد التدابير التشريعية.

2. ان الاطار العام لتوحيد قوانين جرائم الكمبيوتر يعتمد على مشروع قانون نموذجي تم وضعه من قبل هيئة اكاديمية عام (1998)، حيث يقسم احكام جرائم الكمبيوتر والانترنت الى ثماني طوائف (ويجب ان

يلاحظ ان هذا هو تقسيم القانون النموذجي لكنه يعتمد هنا كاطار للوقوف على مواقف التشريعات القائمة والنافذة في الولايات).[1]

جرمت غالبية الولايات المتحدة الامريكية استخدام الكمبيوتر لارتكاب الاحتيال، كاستخدام الكمبيوتر او الشبكة او اي جزء منهما بقصد الحصول على المال و أو المنافع او الخدمات باستخدام وسائل وهمية او زائفة او عن طريق وعود او مظاهر كاذبة، ويلحظ توجه البعض لإدماج احتيال الكمبيوتر ضمن نصوص الاحتيال التقليدية المقررة في قوانين هذه الولايات بدل وضع نصوص تشريعية مستقلة بشأن احتيال الكمبيوتر. واقامت عدد من الولايات المسؤولية عن سرقة الكمبيوتر والتي يمكن ان تتضمن العديد من الافعال مثل سرقة المعلومات، وسرقة البرامج وسرقة اجهزة الكمبيوتر، وسرقة خدمات الكمبيوتر. وجرمت غالبية الولايات استخدام الكمبيوتر لارتكاب سرقة بالمعنى التقليدي، كسرقة الممتلكات والاستيلاء على الأموال من غير المعطيات او الاجهزة او البرامج، وقليل من الولايات جرمت حيازة معطيات او برامج الكمبيوتر المتحصلة من الجريمة. وقد نصت عدد من تشريعات الولايات على سرقة الهوية او وسائط التعريف، فاعتبرت من قبيل الجريمة – متى ما توفر العلم وقصد تحقيق منافع مادية – الحصول على او حيازة او نقل او استخدام، او محاولة الحصول او الحيازة او النقل او الاستخدام، لواحدة او اكثر من وثائق التعريف الشخصية او الارقام الشخصية او اية وسائل تعريفية للشخص او لشخص اخر غير مصرح له قانونا بحيازتها، وهذه التشريعات لا توصف عموما كجزء من تشريعات جرائم الكمبيوتر، ومع ذلك يتم ادخالها ضمن نطاق تشريعات جرائم الكمبيوتر بسبب اتصال سرقة الهوية بأنشطة الاختراق والدور الرئيسي الذي تلعبه هذه الانشطة في هذا الحقل.

جرائم تزوير الكمبيوتر (الوثائق والمعطيات الالكترونية): – جرمت بعض الولايات انشطة تزوير الكمبيوتر، ويعرف تزوير الكمبيوتر بانه " قيام الشخص بإنشاء او تعديل او الغاء اي معطيات خاصة باي كمبيوتر او شبكة كمبيوتر بحيث ينجم عن فعله تغيرا في الحقيقة المتعلقة بوثيقة معنوية او تعليمات ". وعلى الاقل فان ولاية واحد اعتبرت من قبيل جرائم الكمبيوتر حيازة اجهزة ووسائل التزوير التي تشمل الكمبيوترات أو معداتها أو برامجها المصممة خصيصا او المستخدمة في ارتكاب التزوير.

[1] **See**: – Susan W. Brenner, State Cybercrime Legislation in the United States of America: A Survey, 7 RICH. J.L. & TECH. See 28/03/2018: http://www.richmond.edu/jolt/v7i3/article2.html

المقامرة والافعال الاخرى التي تستهدف الاخلاق والآداب العامة: – ان ولاية امريكية واحدة فقط جرمت المقامرة على الخط وهي ولاية Louisiane ، فقط اعتبرت هذه الولاية المقامرة بواسطة الكمبيوتر جريمة، ويتضمن ذلك القيام بأي سلوك او المشاركة بسلوك يتضمن اللعب كاللوتري والمضاربات بأنواعها تحت خطر خسارة ذلك الشخص اي قيمة، وذلك باستخدام الانترنت او الويب عن طريق اي كمبيوتر، كما اعتبر قانون هذه الولاية من قبيل الجريمة تطوير او تزويد خدمات كمبيوتر البرامج او اي منتج اخر لدخول الانترنت وعرض اي نشاط يتصل بالمقامرة او بالأعمال المكونة لهذا الفعل مع توفر احتمال تحقق الخسارة وذلك بقصد تحقيق مكاسب من وراء هذا السلوك، ويجري العمل على اتخاذ تدابير تشريعية لتجريم المقامرة على الخط في عدد من الولايات الاخرى، وعلى الاقل فان ولاية واحدة تبنت تشريعات لتنظيم التعامل مع الكحول وبيعها عبر الانترنت وتتجه ولايات اخرى لوضع مثل هذا التشريع، وبعض الولايات اعد تشريعات تهدف الى اعتبار بيع السجائر عبر الانترنت لمواطني هذه الولايات عملا غير قانوني.

الجرائم ضد الحكومة: – عدد قليل من الولايات الامريكية اعتبر من قبيل جرائم الكمبيوتر استخدام الكمبيوتر لتعطيل تطبيق القانون او تعطيل خدمات حكومية، فقط حظرت ولاية الينوي استخدام الكمبيوتر للتسبب بتعطيل او قطع اي خدمة او اية عملية او اجراءات حكومية محلية او انشطة المؤسسات العامة. والعديد من الولايات جرمت استخدام الكمبيوتر لتعطيل او قطع اي خدمة اساسية، ويشمل ذلك خدمات المؤسسات العامة والخاصة ذات النفع العام والخدمات الطبية وخدمات الاتصال وكافة الخدمات الحكومية، ويشمل ايضا تعريض الامن العام الخطر. واعتبرت بعض الولايات استخدام الكمبيوتر للحصول على معلومات تعتبرها الدولة او اي دائرة سياسية من قبيل المعلومات السرية. ويحظر قانون ولاية فرجينيا الغربية الدخول غير المصرح به الى اية معلومات مخزنة داخل كمبيوتر مملوك او متصل بجهات التشريع بالولاية، وجرم قانون جزيرة Rhode استخدام الكمبيوتر لتدمير اي دليل تقصد تعطيل اي تحقيق رسمي، واعتبرت ولاية Utah عدم الابلاغ عن جريمة الكمبيوتر بمثابة جريمة.

ثمة جهود تشريعية واسعة في حقل حماية المعلومات والخصوصية معروضة على المؤسسات التشريعية في معظم الولايات المتحدة الامريكية، ففي ولاية اريزونا هناك مشروع قانون لحظر توفير البيانات الشخصية الخاصة باي موظف حكومي على شبكة الانترنت او اي موقع معلوماتي او حيازة اي معلومات شخصية تهدد بالخطر سلامة اي موظف حكومي او سلامة عائلته او حصول تهديد يظهر انه كان نتيجة توفير المعلومات

الشخصية. وهنالك مشروع قانون في ولاية كاليفورنيا بشأن حظر افشاء معلومات حول عناوين منازل الضباط والموظفين الحكوميين عبر الانترنت كما ان العديد من الولايات يجرى فيها نظر مشاريع قوانين تتعلق بتجريم ارسال البريد الالكتروني غير المرغوب به او غير المطلوب spamming [1] وهناك مشروع قانون في ولاية نيوجرسي يهدف الى تغليظ العقوبات على جرائم الدخول الى او تدمير انظمة الكمبيوتر المنزلية

ان مراجعة تشريعات جرائم الكمبيوتر النافذة في مختلف الولايات المتحدة الامريكية يشير الى اهمية التوجه نحو وضع تشريع شامل وموحد لمعالجة هذه الجرائم، بسبب وجود اختلاف حقيقي في مستويات الحماية وتحديد انماط هذه الجرائم، بل وبسبب الاختلاف في الاصطلاحات المستخدمة واثر ذلك على توفير الحماية، اضافة الى التباين بشان العقوبات المقررة لهذه الجرائم.

ويرجع التباين والاختلاف بين تشريعات الولايات المتحدة الامريكية في هذا الحقل الي عوامل عديدة، اولها التطور السريع الذي شهدته ظاهرة جرائم الكمبيوتر والانترنت والأجهزة الإلكترونية، برغم حداثة الظاهرة، وهو ما ادى الى تباين درجة الاستجابة من ولاية الى اخرى، خاصة في ظل عدم الاتفاق على انماط الجرائم ومحدداتها، بل وعلى مفاهيم الاصطلاحات المتصلة بها والعناصر المتضمنة فيها، واكثر من ذلك الخلط والتشتت الحاصل بشان الكثير من المفاهيم المتصلة بهذه الظاهرة. واما العامل الثاني فهو عامل قديم جديد، يتمثل باستمرار حالة الخلاف بشأن ما اذا كانت جرائم الكمبيوتر والانترنت ظاهرة جديدة تتطلب تشريعات خاصة ام انها مجرد وسائل جديدة لارتكاب جرائم تقليدية لا تحتاج الى نصوص جديدة، وان اكثر ما تحتاجه مجرد اعادة مراجعة النصوص القائمة، هذا على الرغم من ان الاتجاه الفقهي العام في مختلف دول العالم قد حسم لصالح وجوب التعامل مع جرائم الكمبيوتر كظاهرة جديدة تتطلب تدابير تشريعية خاصة. اما العامل الثالث فهو الطبيعة المعقدة لجرائم الكمبيوتر والسمة المميزة لها باعتبارها جرائم عابرة للحدود تتطلب تعاونا وتنسيقا فيما بين الدول وتجعل التدابير المحلية غير ذات اثر ما لم يتحقق انسجاما دوليا في انشطة المكافحة، ومن هنا فان كل ولاية تنظر لمفهوم تحقيق نصوصها لمتطلبات التعاون الدولي وفق مفهومها الخاص.

ان الحقيقة التي تظهر جراء مراجعة مختلف تشريعات جرائم الكمبيوتر والانترنت في الولايات المتحدة هي ان هناك فجوة بين بناء وفعالية هذه التشريعات مقارنة بتشريعات الجرائم التقليدية او ما يسمى جرائم

[1] *See, e.g.,* H. B. 6443, Gen. Assem, 1999 Reg. Sess. Conn. 1999; H. B. 242, 140th Gen. Assem., Reg. Sess. (Del. 1999); H. B. 1287, Gen. Assem., 1999 Reg. Sess. (N.C. 1999).

العالم الحقيقي، ولعل مرد ذلك الطبيعة الخاصة لجرائم الكمبيوتر والاثار المختلفة لها عن غيرها من الجرائم، واتصال الافعال فيها بإحداث مساس بالكافة بل وبالعناصر الاساسية في بناء المجتمع ونظامه السياسي والاقتصادي والاجتماعي، وستظل تشريعات جرائم الكمبيوتر في اية دولة غير ذات اثر في ظل اغفال الحاجة الملحة للتحرك الدولي الشامل لمكافحة خطر هذه الجرائم وحل مشكلات الاختصاص وتنازع القوانين ومشكلات صلاحيات جهات التحقيق الوطنية خارج الحدود وتنظيم انشطة الملاحقة ضمن تعاون دولي متوازن وفاعل.

المبحث الثاني: التهديدات المعلوماتية، وطرق مواجهتها في الولايات المتحدة الأمريكية.

المطلب الأول: أبرز الهجمات التي عانت منها أمريكا.

أفاد تقرير للبيت الأبيض بأن القرصنة الإلكترونية كلفت الولايات المتحدة بين 57 و109 مليارات دولار عام 2016.

وأشار التقرير إلى عمليات القرصنة التي استهدفت مؤسسات خاصة وعامة، ومنها قطع الخدمة وانتهاك البيانات وسرقة الحقوق الفكرية.

وحذر التقرير من نشاطات قرصنة إلكترونية تقوم بها دول، كما نبه إلى خطورة خاصة تتميز بها بعض الهجمات، وهي تلك التي تستهدف بنية تحتية حساسة كالطرق السريعة وشبكات الكهرباء وأنظمة الاتصالات والسدود وشبكة إنتاج الأغذية، حيث قد يمتد تأثير هذه الهجمات خارج نطاق الجهة المستهدفة بشكل مباشر.

وعبر التقرير عن قلق خاص من الهجمات التي تستهدف القطاع المالي وقطاع الطاقة، بسبب اتصالها بقطاعات أخرى مما يجعل تأثيرها متشعبا.[1]

وأيضا من بين التهديدات التي عانت منها الولايات المتحدة الأمريكية، حيث تمت قرصنة رسائل البريد الإلكتروني لـ350 عميلا من بينهم أربع إدارات حكومية أمريكية.

إضافة إلى أن مجموعة من العملاء لدى الشركة كانوا عرضة للخطر بسبب الاختراق السالف الذكر بما في ذلك:

-إدارات الولايات المتحدة في مجال الطاقة والأمن الداخلي والدفاع

-خدمة البريد في الولايات المتحدة

[1] القرصنة الإلكترونية كلفت امريكا بين 7 و 102 مليار، بي بي سي عربي، شوهد بتاريخ 2018/04/16 الرابط: http://www.bbc.com/arabic/business-43093413

-المعاهد الوطنية للصحة

-عمالقة الإسكان "Fannie Mae" و "Freddie Mac"التي تمول وتضمن الرهون العقارية في الولايات المتحدة.

كما كان لهيئة الفيفا رسائل بريد إلكتروني في خادم ديلويت الذي تم اختراقه إلى جانب أربعة بنوك عالمية وثلاث شركات طيران ومصنعين للسيارات متعددة الجنسيات وعمالقة الطاقة وشركات أدوية كبيرة.[1]

الفرع الأول: أهم الاختراقات التي عانى منها الكيان الإلكتروني الأمريكي من قرصنة.

- في عام 1994، وفي فجر عصر الإنترنت، استطاع فلاديمير ليفين، وهو موظف في شركة تجارية متواضعة، اختراق أنظمة سيتي بنك الأمريكية ، واحدة من عمالقة الصناعة المصرفية في الولايات المتحدة. هذا القرصان، الذي استخدم جهاز كمبيوتر محمول قياسي، استطاع كسر نظام أمن إحدى أهم أنظمة الدفع الأكثر تطورا في العالم.

تصرف ليفين بحذر، وحول مبالغ صغيرة نسبيا من حسابات الشركات المستثمرة لدى سيتي بنك إلى شركاء في جميع أنحاء العالم. وبلغ إجمالي المبلغ المسروق 10,7مليار دولار. لكن نظام الأمن الإلكتروني للبنك اكتشف أخيرا آثار القرصان وأصدر مكتب التحقيقات الفدرالي أمرا باعتقال ليفين.

اعتقل ليفين أثناء عبوره الترانزيت في مطار لندن إلى الطائرة المتجهة نحو موسكو وتم تسليمه للمحاكمة في الولايات المتحدة، وعقد صفقة مع الادعاء، حيث حكم بالسجن لمدة ثلاث سنوات. وقد أعاد جميع المسروقات والتي تم تقديرها بـ 400000$ لسيتي بنك. لا يزال ليفين رمزا للقراصنة الروس. وكان القرصان الأول الذي تصدر عناوين الصحف العالمية .

- لم يكن مبلغا كبيرا من المال، المبلغ الذي سرقه هذا القرصان، ايغور كلوبوف، الذي تخرج بعمر 24 عاما من قسم الاقتصاد في جامعة موسكو الحكومية ، حيث كان يقتحم البيانات المالية لقائمة الملياردريات الامريكيين البالغة 400شخصا. اقتحم قواعد ائتمان الأثرياء، وقام بصفقات مع المتواطئين معه على شبكة الإنترنت، مما ساعدهم بالحصول على 1.5 مليون دولار.

وقع ايغور في عام 2007 عندما حاول التظاهر بأنه الملياردير تشارلز ويلي .حيث كتب كلوبوف شيكا وهميا

[1] اختراق "ديتلويت" يطال المؤسسات الأمريكية،ار تي عربي، شوهد بتاريخ 2018/04/21، الرابط: https://arabic.rt.com/it/903750

لشراء سبائك الذهب بقيمة سبعة ملايين دولار، ولكن تم كشف الخدعة عندما اتصل تاجر الذهب بالبنك للتحقق من أن الشيك كان أصليا. وبدوره البنك اتصل بويلي الذي أكد أنه لم يوقع على الشيك. قام المحققون بعملية جذب لكلوبوف إلى نيويورك لكي يستلم الذهب، حيث ألقي القبض عليه. قضى القرصان فترة في السجن، وهو يعمل الآن كخبير أمني رفيع في شركة أمن الإنترنت سايبر سيك ومقرها نيويورك ، وتحول الصياد إلى حارس للطريدة.

- في عام 2016 كشفت وثيقة سرية أمريكية أن قراصنة معلوماتية في الاستخبارات العسكرية الروسية حاولوا مرارا اختراق الأنظمة الانتخابية الأمريكية قبل الانتخابات الرئاسية في العام 2016، ما أثار قلقا جديدا حول مدى تدخل روسيا.

إلا أن عملية التسريب المفترضة للوثيقة التابعة لوكالة الأمن القومي الأمريكية "إن إس إيه"، شكلت إحراجا جديدا للاستخبارات .وسارعت الإدارة الأمريكية الساعية لوقف التسريبات فور نشر التقرير إلى توقيف المتعاقدة ريالييتي ليه وينر (25 عاما) بتهمة انتهاك قانون التجسس.

وأعلن نائب وزير العدل رود روزنستين في بيان أن "نشر مواد سرية دون تصريح يهدد أمن أمتنا ويقوض ثقة الرأي العام في الحكومة. لا بد من محاسبة الأشخاص الذين تعهد إليهم وثائق سرية يتعهدون حمايتها عندما يخالفون هذا الالتزام."

الوثيقة تشير إلى أن عملية القرصنة مرتبطة بالاستخبارات العسكرية الروسية

من جانبه، نشر موقع "ذي إنترسبت" الإخباري الذي يركز على شؤون الأمن القومي تقرير "إن إس إيه" الاثنين. وتشير الوثيقة إلى عملية قرصنة مرتبطة بالاستخبارات العسكرية الروسية استهدفت شركات أمريكية خاصة تؤمن خدمات لتسجيل الناخبين وتجهيزات لحكومات الولايات.

وتابعت الوثيقة أن عملية القرصنة استمرت طيلة أشهر حتى قبل أيام فقط على الاقتراع الرئاسي الذي تم في 8 تشرين الثاني/نوفمبر.

ولم تتوصل وكالة الأمن القومي إلى تحديد ما إذا كان للقراصنة دور مؤثر على نتيجة الانتخابات، بحسب "ذي إنترسبت"، إلا أن مسؤولين في الاستخبارات الأمريكية أكدوا مرارا أن إحصاء الأصوات لم يتأثر بأي قرصنة.

وتابع الموقع أن الوثيقة حملت تاريخ 5 أيار/مايو 2017 ولم يكشف كيفية حصوله عليها. لكن وبعد ساعة فقط على نشره الوثيقة، أعلنت وزارة العدل توقيف وينر الموظفة لدى شركة متعهدة متعاقدة أمنية في أوغوستا بولاية جورجيا بتهمة تسريب معلومات سرية إلى "وسيلة إعلامية إلكترونية"[1].

وتناولت وثيقة "إن إس إيه" أيضا الادعاءات الأمريكية بأن الرئيس الروسي فلاديمير بوتين قاد جهودا منسقة تشمل القرصنة والتضليل الإعلامي للتدخل في الانتخابات الأمريكية من أجل مساعدة دونالد ترامب على الفوز أمام هيلاري كلينتون.

وتابعت الوثيقة بحسب "ذي إنترسبت" أن "عناصر من المديرية الرئيسية للاستخبارات العامة الروسية... نفذوا عمليات تجسس معلوماتي ضد شركة أمريكية جرى التعاقد معها في آب/أغسطس 2016 من أجل الحصول على معلومات عن برامج معلوماتية مرتبطة بالانتخابات."

الفرع الثاني: ابرز القراصنة المهددين للأمن السيبراني الأمريكي.

وكشفت الوثيقة أن القراصنة من خلال محاولتهم سرقة بيانات الدخول واستخدامهم وسائل تصيد البريد الإلكتروني لزرع البرامج المخربة، "تمكنوا من الدخول إلى حسابات عدة لجان انتخابية محلية أو على صعيد الولايات."

لكنها شددت على أنه لا يزال من غير الواضح مدى نجاح هذه الجهود وماهية البيانات التي سرقت.

واستهدفت القرصنة الروسية شركة "في آر سيستمز" ومقرها فلوريدا وتوفر نظام التعريف عن الهوية في الانتخابات الذي استخدم في ثماني ولاية. وقالت الشركة في بيان إنها نبهت مستخدميها عندما لاحظت عملية التصيد وأن أيا منهم لم تنطل عليه الحيلة.

[1] وثيقة أمريكية مسربة: قراصنة تسرب بيانات أمريكية، فرانس 24 بالعربية، بتاريخ:2018/03/16 الرابط: http://www.france24.com/ar/2017060

وتابع بيان الشركة أن "محاولات التصيد الإلكتروني ليست غريبة عنا ولدينا سياسات وإجراءات لحماية مستخدمينا وشركتنا."

وشددت الشركة على أن أيا من منتجاتها لا يستخدم في عمليات تسجيل الأصوات أو إحصائها.

ويأتي نشر هذه الوثيقة قبل ثلاثة أيام من إدلاء المدير السابق لمكتب التحقيقات الفدرالي (إف بي آي) جيمس كومي الذي أقاله ترامب، بشهادته أمام الكونغرس الخميس في شأن التدخل الروسي في الحملة الانتخابية في 2016[1].

- في ديسمبر 2016، تم إضافة يفغيني بوغاشيف ، وهو روسي من مواطني أنابا، على البحر الاسود، منتجع على الساحل يقع على بعد حوالي 900 ميلا الى الجنوب من موسكو، الى قائمة العقوبات الاميركية الجديدة، حيث اتهم بالتدخل في الانتخابات الرئاسية الأميركية. بوغاشيف بالفعل يعتبر موضع اهتمام من قبل الحكومة الامريكية وأجهزة الأمن الخاصة. في فبراير عام 2015، قبل فترة طويلة من الانتخابات، عرضت FBIمكافأة 3 مليون دولار للحصول على معلومات عن مكان وجوده.

الحادث الذي دفع مكتب التحقيقات الفيدرالي لوضع الكثير من المال للحصول على رأس بوغاشيف، كان اختراعه لفيروس جديد تماما سماه "اللعبة انتهت زيوس "أو .GOZ وضع بوغاشيف وجماعته اقوى فيروس في التاريخ – يستطيع الفيروس نسخ الأرقام المصرفية وبطاقات الائتمان وكلمات السر والمعلومات المالية الحساسة الأخرى دون أن يترك أي أثر. ويقدر مكتب التحقيقات الفدرالي أن مخترع GOZ احرز أكثر من 100 مليون دولار.

مكتب التحقيقات الفدرالي ما زال يبحث عن بوغاشيف ، ولكن ليس لديه حتى الآن أي فكرة عن مكان وجوده، على الرغم من إحدى الصحف البريطانية ذكرت أنه ربما كان يعيش في الآونة الأخيرة منذ 2014 في مسقط رأسه في أنابا.[2]

- وفي الفترة الأخيرة لعام 2017 كبد فيروس الفدية الخبيثة، الذى طال أكثر من 100 دولة حول العالم، الشركات والحكومات خسائر طائلة إذ أصاب أكثر من 200 ألف نظام، مطالبا كل نظام بدفع

[1] فرانس 24 بالعربية، المرجع نفسه.

[2] آفة البنوك و السياسيين:أربعة قراصنة مشهورون، كاتيون ، شوهد بتاريخ 2018/03/30 الرابط:
http://katehon.com/ar/article/af-lbnwk-wlsysyyn-rb-qrsn-rws-mshhwrwn

300 دولار في شكل عملة إلكترونية (بت كوين) لفك التشفير عن الملفات التي قرصنها فيروس "وانا كراي"، وقد استيقظ العالم اليوم الأربعاء، على هجوم استهدف شركات كبرى ومصارف وبنى تحتية في روسيا وأوكرانيا وانتقلت إلى غرب أوروبا ومنها إلى الولايات المتحدة.

وبينما لم يتضح بعد المسئول عن الهجوم الأخير، فإنه ربما يكون الأكثر تعقيدا في سلسلة من الهجمات التي تستخدم عشرات من أدوات القرصنة التي سرقت من وكالة الأمن القومي الأمريكية وتم تسريبها عبر الإنترنت في أبريل الماضي من قبل مجموعة تسمى وسطاء الظل.

ومع استناد الهجمات الأخيرة الأكبر في التاريخ على برمجيات الخبيثة طورتها وكالة الأمن القومي لاستخدامها ضد خصومها، فإن الأمر بات قضية حساسة بالنسبة للولايات المتحدة، ومنذ الصيف الماضي، بدأت مجموعة تطلق على نفسها اسم "وسطاء الظل" في نشر أدوات البرمجيات المسروقة من مخزون حكومة الولايات المتحدة من أسلحة القرصنة الخاصة بها. وبحسب صحيفة نيويورك تايمز قال باحثون في شركة سيمانتيك لأمن المعلومات الإلكترونية إن الهجوم الجديد استخدم نفس أداة القرصنة "إترنال بلو" التي استخدمت في هجوم "وانا كراي"، فضلا عن طريقتين أخريين لتعزيز انتشاره.

ولم تعترف وكالة الأمن القومي NSA بأدواتها المستخدمة في هجمات وانا كراي أو غيرها من الهجمات، ولكن المتخصصين في أمن الكمبيوتر يطالبون الوكالة بمساعدة بقية العالم على الدفاع عن الأسلحة التي أنشأتها، ومن بينهم شركة إدت IDT، وN مجموعة مقرها نيوارك تعرضت لهجوم منفصل في 23 أفريل 2017 استخدمت أدوات قرصنة مسروقة من الوكالة.[1]

المطلب الثاني: إنشاء الجيش الإلكتروني الأمريكي.

استحداث قيادة عسكرية مهمتها الرد على هجمات قراصنة المعلوماتية وتنفيذ عمليات في الفضاء الإلكتروني كان اعلان لوزارة الدفاع الامريكية في 22جوان 2010 ، واردف الاعلان ان تلك القيادة ستدخل حيز العمل في شهر اكتوبر القادم ، ويعكس ذلك تأكيدا على الاهمية القصوى التي تلعبها شبكة الانترنت في حياة الشعوب سلما أو حربا ويقدم انذار بإمكانية عسكرة الفضاء الالكتروني والذي اصبح يتعلق بالبنية التحتية

[1] الأمن القومي الأمريكي وراء الهجمات، اليوم السابع ، بتاريخ2018/04/10، الرابط:
https://www.youm7.com/story/2017/6/28

الكونية للمعلومات.

وكان البنتاجون قد أكد أن الأخطار المرتبطة بأمن الفضاء الالكتروني هي من أخطر التحديات التي يواجهها الاقتصاد والأمن القومي في القرن الحادي والعشرين. وكانت شبكات رقمية عسكرية أمريكية تعرضت لعدد كبير من الهجمات من قبل خبراء معلوماتية موهوبين، صينيين أو روس في الغالب، بحسب تقارير امريكية عديدة.

الفرع الاول: انشاء قيادة عسكرية امريكية.

وجاء قرار البنتاجون بانشاء تلك القيادة ليمثل طورا جديدا في مجال الحرب الالكترونية عن طريق الفضاء الالكتروني ، وتم استحداث تلك القيادة للمرة الأولى في تاريخ الولايات المتحدة لتعمل تحت لواء القيادة الاستراتيجية الأمريكية ومن المقرر أن تباشر عملها في الأول من أكتوبر القادم. ، وسيكون مقر القيادة الجديدة في فورت ميد بولاية ميريلاند وستكون جاهزة للانطلاق العملي في اوائل العام القادم. وتستهدف وزارة الدفاع الامريكية من تلك القيادة الجديدة ان تشرف على مختلف الجهود المتعلقة بالأنترنت في كل أجهزة القوات المسلحة، مع التأكيد انها لن تصل الى مستوى عسكرة فضاء الانترنت.

بل انها تعمل على حماية شبكات الجيش الأمريكي التي تتكون من على 15 ألف شبكة ونحو سبعة ملايين جهاز كومبيوتر حيث تحاول أكثر من 100 ألف وكالة استخبارات أجنبية دخول الشبكات الأمريكية بشكل غير مشروع حيث تتعرض لهجمات مستمرة و يتم محاولة دخولها عدة مرات يوميا ويتم مسحها ملايين المرات يوميا، مع تكرار وتعقيد هذه الهجمات.

ويتراوح هذا التهديد من قراصنة الانترنت من الهواة المراهقين إلى العصابات الاجرامية التي تعمل كمرتزقة انترنت لحكومات أجنبية ، وترصد تقارير امريكية ان الصين بنت برنامجا متطورا لحرب الانترنت.

وكان الرئيس باراك أوباما قد أعلن اعتزامه تعيين منسق لشبكات الانترنت للبيت الأبيض لكي يقوم بتنسيق الجهود الأمريكية من أجل حماية شبكات الكومبيوتر والتعاون الوثيق مع الشركات التي تملك أو تتحكم في الأنظمة المالية والكهربائية وغيرها[1].

أكد مسؤولون أمريكيون من "سايبر كوم، " CYBERCOM أن الجيش الأمريكي يستعد لإرسال فرق من القوات "الإلكترونية" إلى ساحات المعارك ومسارح العمليات الحربية، إذ تزمع العسكرية الأمريكية "أخذ المبادرة الهجومية ضد شبكات الكومبيوتر التابعة لأعدائها ."

[1] أمريكا والقيادة الالكترونية، السكينة، شوهد بتاريخ 2018/04/22، الرابط:
https://www.assakina.com/news/news1/9379.html

علما أن الجيش الأمريكي منذ 3 سنوات تدريبات على عمليات كهذه في مركز ضخم في جنوب كاليفورنيا.

الكولونيل روبرت ريان،Robert Ryan، أعلن أنه "في حين أن مهمة قوات الجيوش –بشكل عام– هي "الهجوم والتدمير"، فإن مهمة هؤلاء الجنود "الإلكترونيين" مختلفة تماما.

رايان أوضح أن "التدمير ليس هو الهدف العام بل "التأثير بوسائل غير حركية"؟ و"كيفية الوصول وخلق الارباك وكسب السيطرة؟"

أما الكولونيل ويليام هارتمان من القيادة الإلكترونية في الجيش الأمريكي، Colonel William Hartman، فأعلن أنه "تم فعلا ضم قوات العناصر الإلكترونية إلى فرق المشاة منذ 6 أشهر، كما ستوضع خطط عمليات لهم، حسب حاجة القادة العسكريين ."ولم يوضح الكولونيل طبيعة المهمات التي ستوكل لهؤلاء الجنود "الإلكترونيين"، فقط أشار إلى "جمع المعلومات أو اعتراض مخططات من يخططون لشن هجمات إرهابية أو عسكرية."

إلا أن صحيفة "النيويورك تايمز، "The New York Timesأوضحت أن القيادة الإلكترونية الأمريكية أو سايبركومقد سبق وعمدت إلى وضع "أجهزة مزروعة في شبكات تنظيم الدولة الإسلامية"، ما يسمح للخبراء بدراسة وتقييم تصرفات عناصر هذا التنظيم: كمحاكاة رسائل قادة التنظيم أو استبدالها من أجل جرهم لإرسال مقاتليهم إلى الأماكن التي ستتعرض لغارات جوية بواسطة الطائرات دون طيار أو الطائرات المقاتلة. كما سيعمل الجنود "الإلكترونيون" سيعملون على تأمين مهمة يطلق عليها اسم "الحرمان من الخدمة، "Denial of serviceوهي عبارة عن هجمات إلكترونية "تحول دون الوصول إلى المعلومات الموجودة على الحاسوب الشخصي."

وكانت القيادة "السيبيرية" أو "الإلكترونية" تشكل في الماضي جزءا ثانويا من القيادة الاستراتيجية للولايات المتحدة، إلاّ أن الرئيس الأمريكي دونالد ترامب أمر العسكريين الأمريكيين بضمها إلى قيادتهم الخاصة تأكيدا منه وإيمانا أنها باتت تكتسي أهمية بالغة.

من خوصصة الحروب، وحرب العمليات الخاصة إلى اعتماد قيادة سيبيربية إلكترونية، تشهد العسكرية الأمريكية تغيرات جذرية لن تؤثر عليها فقط بل على جيوش القوى الصاعدة والمنافسة".

ومع ذلك، فإن الطريق إلى كل هذا التكامل المستلهم عبر التقدم التقني وشبكة الإنترنت ليس واضحا بعد. ولا يزال يتعين على الجيوش أن تحدد هياكلها التنظيمية لدعم أنشطتها وقدراتها المتكاملة. وقال الجنرال موريسون، يوضح ذلك بقوله: "إنه تحليل مستمر، ولكن علينا أن ننظم أنفسنا لدعم مفهوم المعركة متعددة الأوجه".[1]

المطلب الثالث: الآلية الدفاعية الأمريكية في مواجهة العطب الإلكتروني.

اهتمت الولايات المتحدة الأمريكية بالأمن الإلكتروني افي كيانها من خلال تحصين نظامها ب:

- وضع وتنفيذ عقيدة دفاعية متماسكة بشأن استخدام القوة العسكرية للردع والاستباق والمنع والانتقام من النشاطات الخبيثة التي تقوم بها فواعل سيادية أو غير سيادية.
- نشر قدرات الدفاع السيبراني الأمريكية الحالية للدفاع بشكل استباقي عن الوكالات الحكومية المدنية والبنية التحتية الحيوية والتفكير في إنشاء خدمة الأمن السيبراني الاتحادية للانخراط في الوقت المناسب في العمليات الدفاعية.
- زيادة القدرة وإعطاء أولوية أكبر لجهود وكالات الاستخبارات الأمريكية لجمع العمليات الاستخبارية التكتيكية والاستراتيجية على الإنترنت لمواجهة أي تهديد للحكومة والبنية التحتية الحيوية للدولة.
- تعزيز المؤسسات والمعايير وعند الضرورة إنشاء مؤسسات جديدة تمكن الحكومات الملتزمة بالقانون من التحرك ضد التهديدات السيبرانية.
- إعطاء الأولوية للحفاظ على مكانة بارزة للشركات الأمريكية والغربية في الإنترنت.

فعلى غرار إنشاء المركز القومي لمكافحة الإرهاب (National Counterterrorism Center) بعد أحداث الحادي عشر من سبتمبر/ أيلول ،2011 لتبادل المعلومات الاستخباراتية بعد هذا الحادث الإرهابي، ولتفادي الإخفاق الأمريكي في منع هذه الهجمات الإرهابية لغياب التنسيق بين الوكالات الاستخباراتية الأمريكية، تعتزم إدارة الرئيس الأمريكي باراك أوباما إنشاء وكالة جديدة متخصصة في مكافحة الهجمات السيبرانية (الإلكترونية) ضد مؤسسات ووكالات أمريكية عقب تزايد تلك الهجمات التي تعرضت لها

[1] جنود الكترونيون ضمن الجيش الأمريكي، مونت كارلو، شوهد بتاريخ: 2018/02/16، الرابط:
https://www.mc-doualiya.com/articles/20171214

الولايات المتحدة الأمريكية[1]. .

مؤخراً، تعرضت الولايات المتحدة الأمريكية لعديد من الهجمات السيبرانية التي تهدد الأمن القومي والمصالح الأمريكية رغم الإنفاق العسكري الأمريكي المتزايد. ولم تقتصر تلك الهجمات على مؤسسات القطاع الخاص الأمريكي، ولكنها وُجهت -أيضاً- لمؤسسات ووكالات رسمية منها العسكري. ومن تلك الهجمات السيبرانية اخترق مؤيدون لتنظيم "داعش"، حساب القيادة المركزية الأمريكية، التي تشرف على العمليات العسكرية الأمريكية التي تشمل الشرق الأوسط ووسط آسيا بما فيها حربا العراق وأفغانستان وإدارة الضربات الجوية الأمريكية ضد تنظيم "داعش" في العراق وسوريا، على موقعي "تويتر" و"يوتيوب". وقد نشر منفذو تلك الهجمات رسائل تُهدد الجنود الأمريكيين المشاركين في هجمات على التنظيم مفادها "أيها الجنود الأمريكيون نحن قادمون فراقبوا ظهوركم[2]

- ومن قبلها تعرضت شركة "سوني" الأمريكية لهجمات إلكترونية في 24 نوفمبر/ تشرين الثاني الماضي من قبل مجموعة من القراصنة المدعومين من كوريا الشمالية- حسب اتهام مكتب التحقيقات الفيدرالي الأمريكي- لقيام الشركة بإنتاج فيلم "المقابلة" الكوميدي الذي يروي قصة خيالية عن اغتيال زعيم كوريا الشمالية كيم جونج أون. بالإضافة إلى قرصنة مجموعة تُطلق على نفسها "الخلافة الإلكترونية Cyber Caliphate"باختراق حساب مجلة "نيوزويك" على موقع "تويتر". وفي عام 2013 سيطر قراصنة على حساب وكالة "أسو شيتد برس "للأنباء على "تويتر" وبثوا تغريدة زائفة عن تفجيرات في البيت الأبيض تسببت في هبوط شديد في أسواق المال الأمريكية لفترة وجيزة .

يأتي تزايد الهجمات السيبرانية التي تتعرض لها الولايات المتحدة مواكباً للتغيرات في تكتيكات العمليات الإرهابية، وتحولها من تنفيذ هجمات إرهابية على أراضي الدولة لتنفيذ هجمات سيبرانية تكون خسائرها مساوية- وقد تفوق- خسائر الهجمات التقليدية خاصة عندما تتسبب في وقوع ضحايا مدنيين على نطاق واسع، وذلك في حال تعرض مثلاً البنية التحتية للدول المتقدمة التي تُدار من خلال الشبكة العنكبوتية كالمستشفيات ومحطات المياه والكهرباء وشبكات خدمات الطوارئ إلى هجمات إلكترونية، فضلاً عن الخسائر المادية التي ليست لها حدود. وبذلك انتقلت مكافحة الإرهاب من المواجهة المباشرة إلى الفضاء

[1] عمرو عبد العاطي، حرب أمريكية مضادة للإرهاب السيبراني، الخليج بتاريخ:2018/04/22، الرابط: http://www.alkhaleej.ae/supplements/page/e4b1fdf9-a839-4db1-8023-50ad4f43cd24

[2] عمرو عبد العاطي، حرب أمريكية مضادة للإرهاب السيبراني، المرجع نفسه.

الإلكتروني، فتحولت الحروب من شكلها التقليدي إلى حروب سيبرانية، وأصبحت الشبكة العنكبوتية ساحتها بعدما أصبح الإنترنت أحد أهم مرتكزات التنظيمات الإرهابية لمهاجمة الدول الكبرى، وقدراتها على تنفيذ عمليات إرهابية سيبرانية بأقل تكلفة مادية وبشرية مخلفة تكلفة مالية عالية لا تقل عن تنفيذ عمليات إرهابية على أراضيها .

ومع تزايد تلك الهجمات السيبرانية التي تتعرض لها الولايات المتحدة مؤخراً، وخوفاً من بيرل هاربر إلكتروني، وضع الرئيس الأمريكي قضية الأمن السيبراني على صدارة أجندته لعام ،2015 فقد ركز عليها في خطابه لحالة الاتحاد الذي ألقاه أمام جلسة مشتركة لمجلسي الكونغرس الأمريكي (النواب والشيوخ) في العشرين من يناير/ كانون الثاني الماضي، مؤكداً ضرورة مكافحة الولايات المتحدة التهديدات الجديدة مثل الهجمات السيبرانية. وقد كانت قضية تأمين المؤسسات والوكالات الأمريكية ضد هجمات سيبرانية على قمة لقاء الرئيس الأمريكي مع أعضاء الحزب الجمهوري بعد فوزه بالأغلبية في مجلسي الكونغرس في انتخابات التجديد النصفي التي أجريت في الرابع من نوفمبر/ تشرين الثاني الماضي .

وفي سياق الجهود الأمريكية لتعزيز الأمن السيبراني ضد هجمات إرهابية قد تنفذها منظمات إرهابية، أو دول تنافس الولايات المتحدة على قيادة النظام الدولي (روسيا والصين) أو دول تصنفها الولايات المتحدة على أنها أعداء لها (كوريا الشمالية وإيران(، أعلنت ليزا موناكو، مساعدة الرئيس الأمريكي للأمن الداخلي ومكافحة الإرهاب، عن اعتزام الإدارة الأمريكية تأسيس وكالة أمريكية جديدة مهمتها جمع وتحليل المعلومات لمنع هجمات تستهدف الأنظمة الإلكترونية للمؤسسات الحكومية والشركات داخل الولايات المتحدة، ودراسة العلاقات بين التهديدات السيبرانية التي تواجهها الولايات المتحدة حتى تصبح الوكالات والمؤسسات المعنية على دراية بهذه التهديدات بأسرع ما يمكن .

[1]

وحسب مصادر أمريكية فإن تأسيس تلك الوكالة التي ستحمل اسم "مركز التكامل الاستخباراتي للتهديدات السيبرانية (Cyber Threat Intelligence Integration Center)سيوحد جهود الأقسام الداخلية بالوكالات الأمريكية المناط بها حماية الولايات المتحدة الأمريكية من الهجمات السيبرانية مثل وكالة الاستخبارات المركزية، ووكالة الأمن القومي، ومكتب التحقيقات الفيدرالي.

وبخلاف المركز القومي لمكافحة الإرهاب الذي أُسس في أعقاب هجمات سبتمبر/أيلول الإرهابية لتنسيق

[1] عمر عبد العاطي، المرجع نفسه.

المعلومات المتعلقة بالإرهاب، والذي يتلقى المعلومات من الوكالات الاستخباراتية الأمريكية لمنع وقوع أحداث إرهابية مجدداً على الأراضي الأمريكية، فإن الوكالة الجديدة الخاصة بالأمن السيبراني ستعتمد بشكل كبير على المعلومات الواردة من شركات خاصة، حيث أكد الرئيس الأمريكي باراك أوباما، في خطاب له في جامعة ستانفورد بولاية كاليفورنيا في 13 فبراير/ شباط الجاري، أن الحكومة الأمريكية لا يمكنها وحدها مواجهة التهديدات السيبرانية الإرهابية التي تواجهها الولايات المتحدة مؤخراً، والتي ستتزايد مع تمتع المنظمات الإرهابية بقدرات لتنفيذ هجمات سيبرانية ضد مؤسسات ووكالات أمريكية رسمية وخاصة، وما يفرضه عصر المعلومات من تحديات، ولذا دعا أن تكون مهمة مواجهة تلك الهجمات السيبرانية مهمة مشتركة بين المؤسسات الأمريكية الرسمية والوكالات الاستخباراتية والقطاع الخاص الذي يمتلك الكثير من الشبكات الحاسوبية والبنى التحتية، ما يعني أن الحكومة الأمريكية لا يمكنها بمفردها مواجهة تلك التهديدات السيبرانية المتنامية في الوقت الراهن. وتعزيزاً لتلك الشراكة بين المؤسسات الأمريكية الرسمية والوكالات الاستخباراتية والقطاع الخاص التي دعا إليها أوباما في خطابه وقع الرئيس الأمريكي عقب الانتهاء من خطابه على أمر تنفيذي يُسهل عملية الشراكة بين الحكومة الأمريكية والقطاع الخاص.

ومع أهمية تأسيس تلك الوكالة لمواجهة الهجمات السيبرانية المتنامية ضد المؤسسات الأمريكية الرسمية وغير الرسمية، يرى عدد من المحللين الأمريكيين أنها ليست بالأهمية التي يتحدث عنها مسؤولو الإدارة الأمريكية، وذلك لأن مهمتها تقوم بها وكالات استخباراتية أمريكية حالية، حيث تضم إدارات مهمتها الأمن السيبراني للولايات المتحدة وحمايتها من هجمات سيبرانية مثل وكالة الأمن القومي، ووزارة الأمن الداخلي، ومكتب التحقيقات الفيدرالي، ووكالة الاستخبارات المركزية، ولذا يؤكد هؤلاء ضرورة العمل لتعزيز جهود تلك الإدارات وتعزيز أدائها بفاعلية وكفاءة وليس تأسيس وكالة جديدة.[1]

ورغم تأكيد مسؤولي الإدارة الأمريكية أن تلك الوكالة الجديدة التي تختص بحماية الأمن السيبراني الأمريكي لن تنتهك الخصوصية والحريات المدنية، يذهب منتقدو تأسيس تلك الوكالة إلى أنها ستنتهك خصوصية مستخدمي الشبكة العنكبوتية استناداً إلى ما كشفه إدوارد سنودين، المتعاقد السابق مع وكالة الأمن القومي، من أن الوكالة قامت بالتجسس على المواطنين الأمريكيين وانتهاك خصوصياتهم وحرياتهم المدنية التي يكفلها الدستور الأمريكي، ولذا يتخوف عدد من الأمريكيين أن الوكالة الجديدة ستعمل على زيادة المراقبة والتجسس

[1] عمر عبد العاطي، المرجع نفسه.

عليهم في انتهاك صريح للحقوق الدستورية للأمريكيين

. ومع تأكيد الإدارة أن الهدف من تلك الوكالة تعزيز الجهود الأمريكية لمحاربة التنظيمات الإرهابية التي بدأت تركز على تنفيذ هجمات سيبرانية ضد الولايات المتحدة، يرى عدد من الخبراء والمتخصصين في قضايا الأمن السيبراني أن تأسيس وكالة جديدة لمكافحة العمليات السيبرانية رغم وجود وكالات تقوم بتلك المهمة ما هو إلا إجراء بيروقراطي يقوض الجهود الأمريكية لمحاربة الإرهاب

.

يعكس عزم الإدارة الأمريكية لتأسيس وكالة أمريكية جديدة للتنسيق بين الوكالات الاستخباراتية الأمريكية لمكافحة العمليات السيبرانية الإرهابية التي تهدد الولايات المتحدة الأمريكية مؤخراً مدى الانشغال الأمريكي بتزايد نفوذ التنظيمات الإرهابية التي أحدثت تحولاً في تكتيكاتها استفادة من الثورة الاتصالاتية والتكنولوجية في عصر المعلومات لتنفيذ هجمات ضد الدول الكبرى، لا تقل خسائرها بل قد تفوق الهجمات التقليدية، ولكن هذا سيأتي على حساب الحريات المدنية والخصوصية التي يتمتع بها المواطن الأمريكي، التي أضحت محل انتهاك في أعقاب أحداث الحادي عشر من سبتمبر/أيلول الإرهابية إلى يومنا هذا تحت ادعاء حماية الولايات المتحدة من هجمات إرهابية مجدداً.[1]

[1] عمر عبد العاطي، المرجع نفسه.

المبحث الثالث: مستقبل التعاون الدولي في إطار الحماية الدولية للمعلوماتية.

المطلب الأول: مستقبل التهديدات الإلكترونية.

من المنتظر أن يشهد العالم العام المقبل تفخيخ عدد أكبر من البرامج الآمنة على أيدي مجموعات تستهدف فئات أكثر من الضحايا ضمن نطاق جغرافي أوسع، ما يصعّب ملاحظة هجماتهم ويعيق قدرة الشركات المستهدفة على التخفيف من وطأة تلك الهجمات، وذلك وفقاً لتنبؤات كاسبرسكي لاب بشأن التهديدات الموجهة في العام 2018، والتي تُظهر كذلك زيادة في هجمات أخرى يصعب إيقافها، مثل تلك التي تعتمد على برامج خبيثة متطورة تستهدف الأجهزة المحمولة، في ظلّ تزايد اعتماد المهاجمين على حيل جديدة لخرق أهداف تزداد تحصيناً باستمرار.

أظهرت الهجمات التي وقعت في 2017 مثل Shadowpad و ExPetya واستهدفت سلاسل توريد كبرى، مدى سهولة اختراق الشركات من خلال برامج خارجية. ومن المتوقع أن يزداد هذا الخطر في 2018 مع تبنّي بعض أخطر المهاجمين في العالم هذا التوجه بديلاً لوضع الأخطار على مواقع الإنترنت وانتظار قدوم الضحايا، أو لأن محاولاتهم الأخرى للاختراق باءت بالفشل.

وقال هوان أندريس جيريرو-سادي، رئيس الأبحاث الأمنية في فريق البحث والتحليل العالمي لدى كاسبرسكي لاب، إن الهجمات التي شُنّت على سلاسل التوريد استطاعت أن تتسبب بكوابيس مقلقة مثلما كان متوقعاً ، وأضاف: سوف يتزايد اهتمام المجرمين بوضع أبواب خلفية في البرامج المنتشرة مع تزايد نفاذهم إلى شركات التطوير البرمجي غير المحصَّنة. وستسمح لهم هجماتهم على سلاسل التوريد بالدخول إلى شركات عدة في القطاعات المستهدفة من دون أن تتم ملاحظتهم من جانب مسؤولي الأمن ولا من الحلول الأمنية. [1]

وتشمل أهمّ التنبؤات المتعلقة بالتهديدات الموجهة في العام 2018:

برامج خبيثة عالية المستوى تستهدف الأجهزة المحمولة .فخلال العامين الماضيين، كشف المجتمع الأمني عن برامج خبيثة متطورة تشكل عند استغلالها في أنشطة تخريبية، سلاحاً قوياً في وجه الأهداف غير المحصنة.

[1] أهم التهديدات التي تواجه عام 2018، صانعو الحدث ،شوهد بتاريخ 2018/04/04، الرابط:
/https://saneoualhadath.me

الهجمات المدمِّرة ستستمر في الازدياد .فقد كشفت هجمات Shamoon 2.0 و StoneDrillالتي جرى الإبلاغ عنها في أوائل العام 2017م، وهجمة ExPetr/NotPetya التي حدثت في يونيو، عن زيادة اهتمام المهاجمين بالهجمات الماحية للبيانات.

عمليات استطلاع وتصنيف ستسبق الهجمات لحماية قدرات الاستغلال الأمنية ذات الأهمية الكبرى لدى المهاجمين، وسيقضي المهاجمون وقتاً أطول في الاستطلاع واستعمال معدات تصنيف مثل BeEFلتحديد قابلية اللجوء إلى الهجمات القائمة على الانتظار وذات التكلفة المتدنية

هجمات معقدة سوف تستغل الجسور الواصلة بين نظام التشغيل والبرامج الثابتة في الحاسوب .الواجهة الموحدة للبرمجيات الثابتة الممتدة (UEFI) هي الواجهة البرمجية بين البرامج الثابتة ونظام التشغيل في الحواسيب الحديثة. وتتوقع كاسبرسكي لاب أن يستغل عدد أكبر من المجرمين القدرات المتطورة للواجهات الموحدة للبرمجيات الثابتة الممتدة لإنتاج برمجيات خبيثة يتمّ تفعيلها قبل أن تسنح الفرصة لتشغيل أي حلول أمنية مضادة، أو حتى نظام التشغيل نفسه.

اختراقات أكثر لأجهزة توجيه الأنترنت والموديم .لطالما تم تجاهل هذا المجال، المعروف بضعفه وقلّة تحصينه، والتغاضي عن اعتباره أداة للمهاجمين المتقدمين، فمثل هذه الأجهزة تتيح مدخلاً مهماً للمهاجمين يسمح لهم بالدخول إلى الشبكة مطولاً ومن دون أثر.

من جانب آخر، تهدف تنبؤات كاسبرسكي لاب المتعلقة بالتهديدات المحدقة بالشركات العاملة في المجالات الصناعية والتقنية، إلى مساعدة القطاعات المعتمدة على الترابط الإلكتروني الشديد في فهم التحديات الأمنية خلال الاثني عشر شهراً القادمة، والتجهيز لصدّها.

حيث من المرجح أن تواجه المركبات المتصلة تهديدات جديدة جرّاء زيادة التعقيد في سلاسل التوريد، ما يؤدي إلى سيناريو لا يوجد فيه طرف واحد مطلع اطلاعاً كاملاً على جميع الشفرات البرمجية في المركبة، ناهيك عن أن يكون في الأصل مسيطراً عليها. ومن شأن هذا الأمر أن يسهّل للمهاجمين اختراق تقنيات المركبة دون الكشف عنهم.

يمكن أن ترتفع الهجمات التي تستهدف اختراق الشبكات الخاصة لدى الجهات العاملة بمجال الرعاية الصحية، لاستهداف المعدّات والبيانات الطبية، بهدف الابتزاز أو إحداث تخريب ما أو القيام بما هو أسوأ، وذلك في ظلّ تزايد المعدات الطبية المتخصصة المتصلة بشبكات الحاسوب[1].

أما في قطاع الخدمات المالية، فتعني زيادة أمن المدفوعات عبر الإنترنت أن المجرمين سيحوّلون اهتمامهم إلى هجمات الاستحواذ على الحسابات المصرفية. وتشير تقديرات في القطاع إلى أن عمليات الاحتيال من هذا النوع سوف يصل حجمها إلى مليارات الدولارات.

من المرجح أن تكون أنظمة الأمن في المنشآت الصناعية عُرضة لخطر متزايد جرّاء الهجمات الموجهة التي تستهدف طلب الفدية؛ فالأنظمة التقنية التشغيلية أكثر هشاشة وضعفاً من شبكات تقنية المعلومات المؤسسية، وغالباً ما تكون مكشوفة لمخاطر الإنترنت.

كاسبرسكي لاب تتوقع كذلك أن تشهد هجمات موجهة تستهدف الشركات بغرض تثبيت برمجيات التعدين الخبيثة Miners ، لسرقة العملات المشفرة، وقد تصبح هذه الهجمات في الوقت المناسب مربحة ومجزية على المدى الطويل أكثر من هجمات طلب الفدية.[2]

المطلب الثاني: الإتفاقيات الدولية في إطار الحماية الدولية للمعلوماتية

أصبح لكل شخص يعيش في المجتمع الحق في الاتصال بغيره وتبادل المنافع المعنوية والمادية معه ليس فقط داخل دولته بل كذلك خارجها مع أبناء الدول الأخرى.

وإذا كانت الدول قد استطاعت الحد من ذلك الاتصال والتبادل في أوقات مضت تحت ستار حماية متطلبات أمنها القومي والاقتصادي إلا أنها لم تعد كذلك في ظل عصر السماوات المفتوحة بفعل تقدم وسائل الاتصال عبر الأقمار الصناعية، ووسائط نقل الأخبار المعلوماتية عبر الأثير والموجات الكهرومغناطيسية لدرجة يمكن القول معها أن سيادة الدولة الإقليمية قد انحسرت عن الإقليم الفضائي أو الهوائي واقتصرت على إقليمها الأرضي والمائي فقط، وقد كرست الأعمال القانونية الدولية حق الاتصال والحصول على المعلومات وتداولها ،وأكدت على أهمية ضمان ممارسته.

[1] أهم التهديدات التي تواجه عام 2018، المرجع نفسه.

[2] أهم التهديدات التي تواجه عام 2018، المرجع نفسه.

فقد نص القرار 59 الصادر عن الأمم المتحدة في 14 ديسمبر 1946 على أن "حرية الاستعلام هي حق أساسي للإنسان ،وهي حجر الزاوية لكل الحريات التي كرست الأمم المتحدة نفسها للدفاع عنها، وحرية الاستعلام تشمل جمع ونقل ونشر المعلومات في كل دون عقبات ".

كما نصت المادة 19 من الاعلان العالمي لحقوق الإنسان الصادر عن الجمعية العامة للأمم المتحدة في 10 ديسمبر 1948 على أن "لكل فرد الحق في حرية الرأي والتعبير ويشمل هذا الحق حرية اعتناق الآراء دون تدخل واستقاء وتلقي وإذاعة الأنباء والأفكار دون تقيد بالحدود الجغرافية وبأية وسيلة كانت "

وأخيرا نصت المادة 19 من العهد الدولي للحقوق المدنية والسياسية الصادر عن الأمم المتحدة في 16 ديسمبر 1966 على أن " لكل فرد الحق في حرية التعبير وهذا الحق يشمل حرية البحث عن المعلومات أو الأفكار من أي نوع واستلامها ونقلها بغض النظر عن الحدود ،وذلك إما شفاهة أو كتابة أو طباعة ،وسواء كان ذلك في قالب فني أو بأية وسيلة أخرى يختارها ".

وتنشأ ضرورة وجود توافق دولي محكم في مجال الحق في المعلومات على وجه الخصوص من سهولة حركة المعلومات في أنظمة تقنية المعلومات حيث يرجع لهذه السهولة في حركة المعلومات بأنه بالإمكان ارتكاب جريمة عن طريق حاسب آلي موجود في دولة معينة بينما يتحقق نجاح هذا النشاط الاجرامي في دولة أخرى.

وتستلزم مثل هذه الجرائم وجود تعاون دولي فعال والذي يعتبر ضروريا من أجل حماية حقيقية لأنظمة الاتصالات البعدية التي تمر بالعديد من الدول وينشأ حتما عن وجود أوجه خلاف بين القوانين الوطنية والخاصة بتقينة نظم المعلومات ما يعرف بالمعلومات المختبئة والذي ستكون لها نتيجة عكسية في صورة قيود وطنية على حرية حركة المعلومات.

وفي مجال الاجراءات فإن التوافق بين مختلف سلطات التدخل الوطنية سيكون هاما من أجل التيسير دون عقبة لطلب المساعدة القانونية الوطنية ،أنه قد تلتمس إحدى الدول المساعدة القضائية من دولة أخرى بحيث يمكن لهذه الأخيرة أن تباشر التدابير التي تكون طبقا لقوانينها الخاصة. [1]

الفرع الأول: التدابير الموضوعية.

[1] عبد العالي الديربى، التعاون الدولي ومتطلبات مكافحة الجرية الإلكترونية،المركز العربي لأبحاث الفضاء الإلكتروني، شوهد بتاريخ 2018/01/22، الرابط:

http://www.accronline.com/article_detail.aspx?id=7472

ينبغي على الدول أن تتبع سياسة جنائية مشتركة تهدف إلى حماية المجتمع من مخاطر الجريمة المعلوماتية وذلك من خلال تبنى التشريعات الملائمة لمواجهة الخطورة المتمثلة في إمكان استخدام شبكات الكمبيوتر والمعلومات الالكترونية في ارتكاب أفعال إجرامية مع إمكانية تخزين ونقل الدليل المتعلق بمثل هذه الأفعال عبر تلك الشبكات.

لذا من الأهمية بمكان مباشرة التدابير الآتية:

أولا: يجب على كافة الدول أن تتبنى التشريعية وغيرها من التدابير اللازمة لإدراك عملية الدخول غير المشروع إلى سائر أو جزء من أجزاء نظام الكمبيوتر كجريمة جنائية وفقا لأحكام قوانينها الوطنية إذا ما ارتكبت هذه الأفعال بصورة عمدية ويجوز لأي دولة أن تحدد من بين متطلبات ارتكاب الجريمة أن يكون ارتكابها من خلال اختراق تدابير الأمن أو بينة الحصول على بيانات الكمبيوتر.

ثانيا: ينبغي على أن تتبنى التدابير التشريعية وغيرها من التدابير اللازمة لإدراك أعمال الاعتراض دون حق والتي تتم بأساليب فنية كعمليات نقل الكمبيوتر إلى أو من خلال حاسب آلي آخر وكذا الاشارات الالكترومغناطيسية الصادرة من أحد نظم المعلومات والتي تحمل مثل تلك البيانات واعتبارها جريمة جنائية لأحكام قوانينها الوطنية إذا ما ارتكبت بصورة عمدية.

ثالثا: يجب على الدول أن تتبنى التدابير التشريعية اللازمة لإدراك أعمال الإضرار أو المحو أو الاتلاف أوالتعديل أو الإعاقة التي تستهدف بيانات الحاسب الآلي بدون وجه حق واعتبارها جريمة إذا ما ارتكبت بصورة عمدية.

رابعا: يجب على الدول أن تتبنى التدابير التشريعية اللازمة لإدراج أعمال الإعاقة الخطرة دون وجه حق بوظائف نظام الكمبيوتر من خلال ادخال أو نقل أو الإضرار أو محو أو اتلاف أو تعديل أو اعاقة بيانات الكمبيوتر وادراكها باعتبارها جريمة جنائية إذا ارتكبت بصفة عمدية.

خامسا: يجب على الدول أن تتبنى التدابير التشريعية اللازمة لامكانية مساءلة الأشخاص المعنوية جنائيا عن الجرائم الناشئة عن نظم المعلومات وذلك في الأحوال التي يؤدي فيها قصور الاشراف أو الرقابة من قبل الشخص الطبيعية إلى تسهيل ارتكابها.[1]

[1] عبد العالي الديربى، التعاون الدولي ومتطلبات مكافحة الجرية الإلكترونية، المرجع نفسه.

الفرع الثاني: التدابير الإجرائية.

وتتمثل هذه التدابير على النحو التالي:

أولا: يجب على الدول أن تتخذ التدابير التشريعية التي تخولها سلطة تفتيش:

- أحد أنظمة الكمبيوتر أو جزء منه وبيانات الكمبيوتر المختزنة به.
- أحد الوسائط التي قد تكون بيانات الكمبيوتر مختزنة به ،وذلك في أراضيها أو في أحد الأماكن الأخرى التي تمارس عليها سلطاتها لأغراض التحقيق.

ثانيا: يجب على الدول أو تتخذ التدابير التشريعية اللازمة لتخويل سلطاتها المعنية في اصدار الأمر لأي شخص سواء كان متواجدا في إقليمها في أي مكان آخر عليه سلطاتها السيادية لكي يقدم أي بيانات محددة واقعة تحت سيطرته ومخزنة في أحد أنظمة الكمبيوتر أو أحد الوسائط المستخدمة في تخزين البيانات وذلك بالصورة التي تطلبها تلك السلطات لأغراض التحقيق.

ثالثا: يجب على الدول أن تتبنى التدابير التشريعية اللازمة لتمكين سلطاتها المعنية من الحصول على نسخة حفظ سريعة للبيانات المخزنة في أحد نظم الكمبيوتر وذلك لأغراض التحقيقات وذلك إذا تبين أنها معرضة بصفة خاصة للفقد والتعديل.

رابعا: يجب على الدول أن تتبنى التدابير التشريعية اللازمة لإجبار الشخص الذي تتخذ حياله اجراءات الحفظ المشار إليها سلفا على الاحتفاظ بسرية الاجراءات لمدة محددة من الزمن وفقا للإطار الذي يسمح به القانون الوضعي.

خامسا: يجب على الدول أن تتخذ التدابير التشريعية اللازمة التي تكفل حفظ بيانات النقل والخاصة بأحد الاتصالات المحددة كما تكفل الحفظ السريع لتلك البيانات الخاصة بعملية النقل وبغض النظر إذا كان مقدم الخدمة واحدة أو أكثر ممن شاركوا في عملية نقل هذا الاتصال.

سادسا: يجب على الدول أن تتخذ التدابير التشريعية اللازمة لمد اختصاصها القضائي على أي من الجرائم المشار إليها إذا ما ارتكبت: [1]

[1] عبد العالي الديربى، التعاون الدولي ومتطلبات مكافحة الجرية الإلكترونية، المرجع نفسه

- بصورة كليه أو جزئية على أراضيها أو على متن باخرة أو طائرة أو قمر صناعي يحمل علمها أو مسجل لديها
- من قبل أحد مواطنيها إذا كانت الجريمة من الجرائم المعاقب عليها وفقا لأحكام القانون الجنائي الساري في محل ارتكابه أو إذا كانت الجريمة قد ارتكبت خارج الاختصاص الإقليمي لأي دولة.

الفرع الثالث: التدابير المباشرة على المستوى الدولي.

ويمكن تقسيم هذه التدابير إلى نوعين: الأولى: تتعلق بالتسليم والثاني: يتعلق بالمعونة المتبادلة.

أ- تسليم المجرم المعلوماتي

يجب على الدول أن تتعاون بعضها مع البعض ومن خلال تطبيق المواثيق الدولية ذات الصلة بشأن التعاون الدولي في المسائل الجنائية وعلى وجه الخصوص في مجال تسليم المجرم المعلوماتي حيث يجب تسليم مرتكبيها وذلك وفقا لمعيار معين لتكييف الجريمة كجريمة يجوز تسليم مرتكبيها:

-أن يكون الدخول إلى النظام أو البيانات قد تم بدون وجه حق وبنية الاخلال بسرية البيانات أو اعاقة نظام الكمبيوتر.

ثانيا: أن تبرم الدول فيما بينها اتفاقية تسليم مرتكبي الجرائم المعلوماتية.

ثالثا: إذا ما رفض طلب التسليم الصادر في شأن مرتكبي إحدى الجرائم المعلوماتية بناءا على جنسية الشخص المراد تسلميه نظرا لأن طرف المدعى يعتبر أنه يختص قضائيا بالجرمية محل الادعاء ،يقوم الطرف المدعي عليه بتقديم القضية إلى سلطاته بغرض السير في الدعوى الجنائية وعلى أن يبلغ الطرف المدعي بالنتائج المترتبة عليه

ب- المعونة المتبادلة

وتتمثل المعونة المتبادلة في الاجراءات التالية:[1]

أولا: يجب على الدول أن تقدم لبعضها البعض المعونة المتبادل وذلك بأكبر قدر ممكن لأغراض التحقيق والاجراءات الخاصة بالجرائم الجنائية المتعلقة بنظم وبيانات الحاسب الآلي.

ثانيا: يجب على الدول أنتقبل وتستجيب إلى طلبات المعونة المتبادلة من خلال وسائل الاتصال السريعة كالفاكس والبريد الالكتروني ،بالقدر الذي يوفر للطرف الطالب المستوى من الأمن والمصادقة.

[1] عبد العالي الديربى، التعاون الدولي ومتطلبات مكافحة الجرية الإلكترونية، المرجع نفسه

ثالثا: تخضع المعونة المتبادلة للاشتراطات المنصوص عليها في قوانين الدولة المدعية أو المنصوص عليها بموجب اتفاقيات المعونة المتبادلة.

رابعا: في الأحوال التي يسمح فيها للطرف المدعي عليه بتعليق طلب المعونة المتبادلة على اشتراط وجود جريمة مزدوجة ،يعتبر هذا الشرط محل اعتبار وبغض النظر عما إذا كانت قوانين هذه الدولة تضع الجريمة في نطاق ذات تصنيف آخر.

خامسا: تحدد كل دولة سلطة مركزية تنهض بالمسئولين ارسال طلبات المعونة المتبادلة والرد عليها وتنفيذها أو نقلها للسلطات المعنية للتنفيذ.

سادسا: تنفذ طلبات المعونة المتبادلة وفقا للإجراءات التي تحددها الطرف المدعي قما عدا الأحوال التي لا تتصل فيها تلك الاجراءات مع أحكام القانون السائد بالدولة المعدي عليه.

سابعا: يجوز للدولة المدعي عليها أن ترفض طلب المعونة إذا ما توافرت لديها القناعة بأن الالتزام بما ورد بالطلب قد يخل بسيادتها أو أمنها أو نظامها العام أو بأي من مصالحها الأساسية الأخرى.

ثامنا: يجوز للدولة المدعي عليها تأجيل التصرف في الطلب إذا كان هذا التصرف سيخل بالتحقيقات أو اجراءات الادعاء أو الاجراءات الجنائية التي تباشر بمعرفة السلطات المعنية.

تاسعا: يجب على الدول المدعي عليها أن تخطر الدولة المدعية بصورة فورية بنتائج تنفيذ طلب المعونة فإذا ما رفض الطلب أو تم تأجيله يجب تقديم الأسباب إلى الرفض أو التأجيل.

عاشرا: يجوز للدولة المدعية أن تطلب من الدولة المدعي عليها أن تحتفظ بسرية الوقائع والمحتويات التي يتضمنها الطلب ،فإذا لم يكن بمقدور الدولة المدعية عليها الوفاء بمتطلبات سرية الطلب فيجب عليها اخطار الدولة المدعية بذلك وعلى الاخيرة في هذه الحالة تحديد ما إذا كان سينفذ الطلب من عدمه.

الحادي عشر: يجوز في حالة الاستعجال ارسال طلبات المعونة المتبادلة مباشرة إلي السلطات القضائية بما فيها النيابة العامة لدى الدولة الدعية عليها وفي مثل الحالة يجب ارسال نسخة بنفس الطلب إلى السلطة المركزية القائمة لدى الدولة المدعي عليها.[1]

[1] عبد العالي الديربى، التعاون الدولي ومتطلبات مكافحة الجرية الإلكترونية، المرجع نفسه.

توصلنا في هذا الفصل إلى أن الولايات المتحدة الامريكية رائدة في مجال الأمن الإلكتروني وأهتمت بهذا القطاع كثيرا، من خلال اعتماده في الأمن القومي لها وبناء آليات واضحة للحد من خطورة أي تهديدات في هذا المجال لما عانته كثيرا فيه، وإضافة لذلك نجد أن مستقبل الأمن الإلكتروني يوحي بإنتاج حرب إلكترونية بين الدول.

الخاتمة

من خلال دراستنا لموضوع استراتيجيات الدول في حماية أمنها الإلكتروني في الكيفيات والآليات وتطرقنا لدراسة الحالة الولايات المتحدة الأمريكية، حيث أبرزنا في هذا المجال مجموع الاستراتيجيات بما فيها الآليات و الخطط والشراكات بين الدول في عملية تأمين المنظومة الإلكترونية لها، حيث استخلصنا من ذلك ما يلي:

- ✓ تطورت الاستراتيجية من المفهوم الضيق الذي يُعنى بالجانب العسكري والأمني إلى المفهوم الموسع الذي يشمل أغلب المجالات بما فيها الأمن الإلكتروني الذي أصبحت له استراتيجيات لحمايته.
- ✓ تعددت مفاهيم الأمن الإلكتروني، حيث توجد عديد التعريفات له منها من يعرفه على اساس أنه الأمن السيبراني الذي يعنى بالرقميات الخاصة ببيانات استخدام الشبكة، ومنه من يعرفه على أساس أمن المعدات المستخدمة في التكنولوجيا الحديثة.
- ✓ إن ظهور الأمن الإلكتروني مرتبط بظهور الحاسب الآلي وشبكة الأنترنت، حيث اعتمد الأمن الإلكتروني في كيانات الدول وأصبح أحد ركائز العمليات العامة فيها.
- ✓ اعتماد المعلوماتية فيا الدول خلق لها تهديدات إلكترونية عديدة، مما حتم على الدول مواجهة هاته التهديدات عن طريق بناء شراكات في إطار السلام الإلكتروني.
- ✓ أقامت الدول الكبرى عمليات إدخال وتحيين في منظومتها الإلكترونية عبر ثلاث مراحل:
  - التحيين: إدخال البيانات الخاصة بالأشخاص الطبيين والمعنويين في الخوادم غير المتصلة بالشبكات.
  - العصرنة: ربط البيانات المحيينة بالشبكة الداخلية.
  - عالمية البيانات: ربط البيانات المرقمنة بالشبكة العالمية عبر فضاءات لكل مجال فضائه.
- ✓ تأثرت الدول الكبرى بالتهديدات الإلكترونية بعدة أشكال، (الجوسسة، القرصنة، إتلاف و سحب البيانات....) مما حتم عليها بناء استراتيجيات لصد التهديدات، وهاته الاستراتيجيات تمثلت في تدابير داخلية، وإجراءات تعاونية دولية سواء في اتفاقيات وترسيمات قانونية للحماية و التجريم في أغلب الأحيان.

✓ أقيمت شراكات دولية في إطار الحماية من سوء السلوك الإلكتروني بين مجموع الدول الغربية أبرزها إتفاقية بودابست التي فصلت في التجريم الإلكتروني من السلوكيات التي يقوم بها الأفراد إلى السلوكيات التي تقوم بها المجموعات أو الدول.

✓ تعتبر الولايات المتحدة الأمريكية من بين الدول الرائدة في الأمن الإلكتروني ومن الدول الأولي المستخدمة للرقمنة.

✓ تأثرت الولايات المتحدة الأمريكية من جراء التهديدات الإلكترونية الممارسة ضدها من طرف الأفراد والدول على مصالحها، مما استلزم عليها بناء منظومة استراتيجية لصد هاته التهديدات بداية بتقنين الأمن الإلكتروني إلى اعتماده في الأمن القومي واستخدام آليات دفاعية متمثلة في الصد ومعرفة مصدر محاولة القرصنة...إلخ، وآليات هجومية متمثلة في بداية الهجوم قبل الهجوم عليها كالهجوم على المفاعل النووي الإيراني وسحب محتوياته.

✓ إن المتغيرات الجديدة في الوضع الدولي أفضت إلى التنبؤ بحرب عالمية الكترونية، فالدول جمعا تعتمد على المنظومة الإلكترونية في تسيير شؤونها كليا أو جزئيا، وتطور من قدراتها الإلكترونية فأصبحت أغلب أو جل سلوكياتها وحركاتها محفوظة في خوادم، وأغلب عملياتها سواء الفردية أو المؤسساتية عبر نظام شبكة المعلومات، فهذا كله يوحي بأن المهاجمة في الحروب المستقبلية سلاحها ضرب الكيان الإلكتروني.

=

قائمة المصادر والمراجع

أولا: المراجع بالعربية.

أ/الكتب:

1) نضال أدلبي، تطوير وتنسيق التشريعات السيبرانية في المنطقة العربية ومواجه الجرائم السيبرانية، الأمم المتحدة، الإسكوا،
2) ناصر بن محمد البقمي، مكافحة الجرائم المعلوماتية وتطبيقاتها في دول مجلس التعاون لدول الخليج العربي، مركز الإمارات للدراسات والبحوث الإستراتيجية، الطبعة الاولى، 2008م.
3) محمد الأزهر، حقوق المؤلف في القانون المغربي دراسة مقارنة في الملكية الأدبية والفنية، تقديم عبد الله درميش، دار النشر المغربية 1944،
4) محمد الأمين ومحسن عبد الحميد أحمد، معايير الأمم المتحدة في مجال العدالة الجنائية ومنع الجريمة أكاديمية نايف العربية للعلوم الأمنية، الرياض، الطبعة الأولى 1998،
5) مصطفى طلاس وآخرين , الاستراتيجية السياسية العسكرية , الجزء الأول الطبعة الأولى ,دار طلاس للدراسات والترجمة والنشر ,(دمشق) 1991.
6) جوزيف اس ناي، جوندي دوناهيو، الحكم في عالم يتجه نحو العولمة، ترجمة: محمد الشريف الطرح، دار العبيكان للنشر، الطبعة الأولى.الرياض.2002
7) يحيى محمد علي أبو مغايض، الحكومة الإلكترونية في المؤسسات العامة بالمملكة العربية السعودية, الرياض: 2004،
8) منير شفيق، الاستراتيجية والتكتيك في علم الحرب، الدار العربية للعلوم، بيروت: 2008.
9) لمارشال سوكوفسكي، الاستراتيجية العسكرية السوفياتية، ترجمة خيري حماد، بيروت.
10) عبد القادر محمد فهمي، المدخل إلى دراسة الاستراتيجية، دار مجدلاوي للنشر والتوزيع، عمان:2007 .
11) محمد احمد عوض، الإدارة الاستراتيجية، (الأصول، الأسس النظرية)، الدار الجامعية. الاسكندرية. 1999.
12) حمدون أتوريه، دليل الأمن السيبراني للدول النامية، الإتحاد الدولي للاتصالات، 2006.
13) عزرائيل لوربار، التكنولوجيا العسكرية وسائل القتال والمخابرات، عرض: عدنان أبو عامر، الرعوت للنشر، تل الربيع 2012.
14) عادل عبدالصادق، الفضاء الإلكتروني والعلاقات الدولية: دراسة في النظرية والتطبيق القاهرة: المكتبة الأكاديمية، 2016.
15) حمد فتحي سرور, المواجهة القانونية للإرهاب, الطبعة الأولى، القاهرة: دار النهضة العربية, 2008
16) [1]سوسن زهير المهتدي ،تكنولوجيا الحكومة الإلكترونية، دار أسامة للنشر و التوزيع، الأردن، 2011،
17) جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة 1998م

18)محمد السعيد رشدى، الانترنت والجوانب القانونية لنظم المعلومات، بحث مقدم إلى المؤتمر العلمي الثاني لكلية الحقوق ،جامعة حلوان

ب/المجلات العلمية والمدونات:

1. مصطفى بخوش، تطور الفكر الاستراتيجي في حقل العلاقات الدولية ،مجلة دراسات شرق اوسطية، عدد 59، شوهد بتاريخ 2018/03/02 بتوقيت 22: 55. رابط المقال:
https: //platform.almanhal.com/Files/2/442
2. دينا محمد جبر، مقالة من موقعIASJ ، التاريخ: 2018/02/11 بتوقيت 22: 17 رابط المقال:
https: //www.iasj.net/iasj?func=fulltext&aId=27060
3. محمد بنحمو، الاستراتيجية، المفهوم والنظرية، مركز راشيل كوري لحقوق الانسان، شوهد بتاريخ 2018/03/02 بتوقيت 19:55 رابط المقالة:
http: //rachelcenter.ps/news.php?action=view&id=10294
4. –صباح بالا، الاستراتيجية الدولية، الموسوعة السياسية، شوهد بتاريخ 2018/02/10 رابط المقالة:
http: //political-encyclopedia.org/2017/08/05
5. عمر فضل الله، تعريف الاستراتيجية ،مدونة عمر فضل الله، ،شوهد بتاريخ 2017/12/15 بتوقيت 16:35 رابط المقال:
http: //www.omarfadlalla.com/?p=2342
6. صلاح نيوف، مدخل إلى الفكر الاستراتيجي، الاكاديمية العربية المفتوحة بالدنمارك.[1]ملاذ المدني، الفرق بين الاستراتيجية والتكتيك، اراجيك، شوهد بتاريخ 2018/02/12 رابط المقالة:
https: //www.arageek.com/2012/09/16/difference-between-tactics-and-strategies.html
7. محمود الهلال سيد، فن علم الحرب ،موقع الجزيرة.نت، شوهد بتاريخ 2017/12/29 رابط المقال:
http: //www.aljazeera.net/knowledgegate/books/2009/6/4/
8. محمد محمود السيد، كيف سيواجه العالم تحديات الأمن السيبراني؟، مجلة السياسة الخارجية، شوهد بتاريخ2018/01/17 رابط المقال:
http: //www.siyassa.org.eg/News/4925.aspx
9. فيصل اليوسف ،الأمن السيبراني والفضاء الالكتروني، جريدة اليوم، السعودية، شوهد بتاريخ 3 نوفمبر 2017 رابط المقال:
http: //www.alyaum.com/article/4213196
10. الامن السيبراني، الهيئة اللبنانية المنظمة للاتصالات، لبنان، شوهد بتاريخ: 2017/07/2 رابط المقال:
http: //www.tra.gov.lb/Cybersecurity-AR
11. عبد الله المبارك ،الفرق بين الامن الإلكتروني وامن المعلومات، مقالة بموقع linkdin شوهد ،بتاريخ،2018/03/12 رابط المقال:

https: //www.linkedin.com/pulseبين-ما-الفرق-و-information-abdullah-cyber-security-

[1] Emmanuel menet. la cyber guerre et la strauction des relations international. le cas nord coreen. programmen asie. decembre 2017.

12. التقرير العالمي لتكنولوجيا المعلومات، مجلة الشرق الأوسط ،شوهد بتاريخ 21 /2018/02: الرابط: https: //aawsat.com/home/article/336976

13. صلاح الدين أبو بكر الزيداني، طبول الحرب الرقمية، مجلة المسلح، بتاريخ 2016/01/14، شوهد بتاريخ 2018/01/29 بتوقيت 14: 31: رابط المقال

http: //www.almusallh.ly/ar/thoughts/633-vol-44-38

14. مجاهد فخ الدين قاسم أحمد، ترجمة الصفحات من (1-61) من كتاب الأمن الالكتروني والحرب الالكرتونية لمؤلفيه بيتر وارن سينغر وألن أ،فريدمان، بحث تكميلي لنيل شهادة الماجستير في الترجمة، جامعة السودان للعولم والتكنولوجيا، السودان.

15. عادل عبد الصادق ،الفضاء الالكتروني والرأي العام.. تغير المجتمع والادوات والتأثير،المركز العربي لأبحاث الفضاء الالكتروني ،شوهد بتاريخ 2018/01/12: رابط المقال:

http: //accronline.com/article_detail.aspx?id=2725

16. القرصنة الالكترونية، الاكاديمية العربية البريطانية للتعليم العالي، م ذ و:شوهد بتاريخ 2018/2/10، رابط المقال:

http: //www.abahe.co.uk/information-technology-enc/71102-piracy.html

17. عباس بدران، الحرب الإلكترونية: الاشتباك في عالم المعلومات: مركز دراسات الحكومة الإلكترونية بيروت.لبنان 2010.

Carl blidt. cyber-governance-lagging-crime-and-abuse.project syndicate. Le22/01/2018. liens:

https: //www.project-syndicate.org/commentary/cyber-governance-lagging-crime-and-abuse-by-carl-bildt-2018-01/arabic

18. نوران شفيق ،أشكال التهديدات الإلكترونية ومصادرها. بقلم الدكتورة نوران شفيق، المركز الأوروبي لدراسة مكافحة الارهاب والاستخبارات ،شوهد بتاريخ 2018/02/10 الرابط:

https: //www.europarabct.com

19. التهديدات الجديدة: الأبعاد الالكترونية، مجلة الناتو ،شوهد بتاريخ 2018/01/11، الرابط:

https: //www.nato.int/docu/review/2011/11-september/Cyber-Threads/AR/index.htm

20. رغدة البهي، الردع السيبراني: المفهوم والاشكاليات والمتطلبات، المركز الديموقراطي العربي شوهد بتاريخ: 2018/02/09 الرباط:

http: //democraticac.de/?p=43837#_ftn30

21. فتحي شمس الدين ،الأمن المعلوماتي وتهديد الأمن القومي ،روزا اليوسف ،شوهد يتاريخ 2018/02/11: الرابط:

/http: //www.rosaelyoussef.com/article/2109

1- E. Nakashima. U.S. Accelerating Cyberweapon Research", The Washington Post, online e-article,

https: www.washingtonpost.com/world/national-security/us-accelerating-cyberweapon-research/13/03/2012/gIQAMRGVLS_story.html

22. عادل عبدالصادق، القوة الإلكترونية: أسلحة الانتشار الشامل في عصر الفضاء الإلكتروني، مجلة السياسة الدولية، العدد 188، أبريل 2012.

23. عبدالله بن فازع القرني، مواجهة جرائم الإنترنت: نحو إستراتيجية أمنية – مجتمعية متكاملة، مقال منشور على موقع جريدة الرياض شوهد بتاريخ 2018/02/21 الرابط:

http: //www.alriyadh.com/912032

24. هيلجي جانيك،حفظ السلام في الفضاء الالكتروني ،الخليج، بتاريخ ،2018/02/05 الرابط:

http: //www.alkhaleej.ae/alkhaleej/page/2c4692bd-05cc-43a4-9fa9-1b682df40056

25. نحند علي العمري،مظاهر الثورة الرقمية ونتائجها ،مفهوم، العدد السابع عشر،شوهد بتاريخ 2018/01/23، الرابط:

http: //www.mafhoum.com/press9/265T44.htm

26. الادارة اللكترونية واهميتها في تشكيل حكومة المستقبل ،الخليج الاقتصادي،شوهد بتاريخ: 2018/02/17، الرابط:

http: //www.alkhaleej.ae/economics/page/ea7bae04-7ab8-4af9-beda-65893e8e04c6

27. يونس حرب – جرائم الكمبيوتر والانترنت– ايجاز في المفهوم والنطاق والخصائص والصوروالقواعد الاجرائية للملاحقة والاثبات، ورقة عمل مقدمة الى مؤتمر الامن العربي 2002 – تنظيم المركز العربي للدراسات والبحوث الجنائية – ابو ظبي 10-12 /2002/2.

28. جان فرنسوا هنروت – أهمية التعاون الدولي والتجربة البلجيكية في تبادل المعلومات بين عناصر الشرطة والتعاون القضائي– أعمال الندوة الاقليمية حول: »الجرائم المتصلة بالكمبيوتر– برنامج تعزيز حكم القانون في بعض الدول العربية– مشروع تحديث النيابات العامة

29. عبد العالي الديربى، التعاون الدولي ومتطلبات مكافحة الجرية الإلكترونية،المركز العربي لأبحاث الفضاء الإلكتروني، شوهد بتاريخ 2018/01/22، الرابط:

http://www.accronline.com/article_detail.aspx?id=7472

30. بيروت تستضيف مؤتمرا للملكية الفكرية، منشور في مجلة حماية الملكية الفكرية، العدد الثاني والخمسون، الربع الثاني 1997م.

31. فتيحة محمد قوارري" المواجهة الجنائية لقرصنة المصنفات الإلكترونية " Peer to peer مجلة الحقوق الكويت العدد الأول، السنة الرابعة والثلاثة مارس2010

ج/ الدراسات غير المنشورة:

1) السديري محمد بن أحمد، مفاتيح النجاح في تطبيق الحكومة الالكترونية، المؤتمر الوطني السابع عشر للحاسب الآلي، جامعة الملك عبد العزيز، السعودية 2004،
2) جردير ليلى، التنمية الادارية كمدخل لتجسيد الحكم الرشيد، مذكرة ماجستير، تخصص الديموقراطية والرشادة، كلية الحقوق جامعة منتوري ،قسنطينة.2011.
3) بوطورة، أكرم. مجتمع المعلومات وتحديات العولمة: بين ثقافة التقييم وتقييم الثقافة: دراسة ميدانية على أخصائي المكتبات والمعلومات بالشرق الجزائري. رسالة ماجستير: قسنطينة: علم المكتبات ،2006.
4) [1]قرار المجلس بتاريخ 29 مايو 2000 ،متعلق بمكافحة استغلال الاطفال في إنتاج المواد الاباحية على الانترنت (JAI/375/2000) الجريدة الرسمية للاتحاد الاوروبي، 9 يونيو
5) كريستينا سكولمان–برنامج تعزيز حكم القانون في بعض الدول العربية، اعمال الندوة الاقليمية حول الجرائم المتصلة بالكمبيوتر، المملكة المغربية، 2007
6) دعاوى الجرائم الإلكترونية وأدلة إثباتها في التشريعات العربية بين الواقع والمأمول، ضمن فعاليات المؤتمر الثالث لرؤساء المحاكم العليا (النقض، التمييز، التعقيب) في الدول العربية المنعقد في جمهورية السودان خلال الفترة 23-25/9/م الموافق 7–1433/11/9هـ.
7) ربيع محمد يحيى، كتاب اسرائيل وخطوات الهيمنة على ساحة الفضاء السيبراني في الشرق الاوسط، دراسة حول استعدادات ومحاور عمل الدولة العبرية في عصر الانترنيت(2002. 2013).
8) خالد محي الدين احمد ،الجرائم المتعلقة بالرغبة الأشباعية باستخدام الكمبيوتر ،اعمال الندوة الاقليمية حول الجرائم المتصلة بالكمبيوتر ،الدار البيضاء، 2007،

د/ روابط الأنترنت:

1. عبد الرحمان تيشوري، الادارة الاكترونية،الحوار المتمدن،العدد 1418،شوهد بتاريخ 2018/02/19 الرابط: http: //www.ahewar.org/debat/show.art.asp?aid=270234
2. مصطفى القايد،مفهوم المواطنة الرقمية ،منصة ت–ج التعليمية، شوهد بتاريخ 2018/02/20 الرابط: https: //www.new–educ.com/definition–of–digital–citizenship
3. نسيب بيطار ،من الحكومة الالكترونية الى الحكومة الذكية، مقالة من فرانس 24 بالعربية،شوهد بتاريخ: 2018/02/21، الرابط:

http: //www.france24.com/ar/20140114
4. التقرير العالمي لتكنولوجيا المعلومات، مجلة الشرق الأوسط ،شوهد بتاريخ 21 /2018/02: الرابط: /https: //aawsat.com/home/article/336976
5. محمد الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، الطبعة الثانية، دار النهضة العربية، القاهرة، 1994.

1–Le rapport du conseil du l'Europe, 15,18 novembre 1976.

6. القرصنة الالكترونية، dwعربي، شوهد بتاريخ 2018/02/22،الرابط:

/ http: //www.dw.com/ar
7. [1]الحوار نت، القرصنة الالكترونية،شوهد بتاريخ2018/03/01،الرابط:

http: //www.alhiwar.net/ShowAdv.php?Tnd=70

8. [1]القرصنة الاكترونية،الاكاديمية العربية اللبريطانية المفتوحة للتعليم العالي،شوهد بتاريخ2018/03/01، الرابط:

http: //www.abahe.co.uk/information-technology-enc/71102-piracy.html

9. تعرف على مفهوم وتاريخ القرصنة الالكترونية واشهر القراصنة في العالم،igider للمعلوماتية ،شوهد بتاريخ،2018/03/01الرابط:

http://www.igiderinform.com/2017/09/electronic-piracy.html

10. [1]الهام محمد علي، التجسس الإلكتروني: سلاح إسرائيل الذهبي لمراقبة العرب،نون بوست،شوهد بتاريخ،2018/03/04، الرابط:

https: //www.noonpost.org/content/13821

11. [1]توفيق أو شومر،تقنيات الجوسسة الحديثة،جريدة الجسر الالكترونية،شوهد بتاريخ 2018/03/04 الرابط:

http //www.aljisr-news.com/news/?p=56712

12. التجسس في العصر الرقمي،الروابط للبحوث، شوهد بتاريخ،2018/01/7 الرابط:

http: //rawabetcenter.com/archives/59323

13. [1]الهاكرز يشنون هجوما واسع النطاق على مؤسسات حكومية في عشرات الدول حول العالم، منتدى التكنولوجيا العسكرية والفضاء،بتاريخ،2018/01/07،الرابط:

http: //army-tech.net/forum/index.php?threads

14. سكاي برس، لعبة تؤدي بحياة عشرات المراهقين الروس،بتاريخ: 2018/03/01 الرابط:

http: //www.skypressiq.net/2017/3/1/%D9%84

15. اتفاقية بودابست لمكافحة الجرائم المعلوماتية،شبكة قوانين الشرق،شوهد بتاريخ: 2018/02/08،الرابط:

http: //eastlaws.blogspot.com/2010/03/23-11-2001.html

16. د. عبد العال الديربي، الاستاذ محمد صادق إسماعيل، كتاب الجرائم الالكترونية ،المركز القومي للإصدارات القانونية. الطبعة الاولى 2012. ، شوهد بتاريخ 2018/01/08الرابط:

https: //books.google.no/books?id=4d4sDAAAQBAJ&pg=PT

17. القرصنة الإلكترونية كلفت امريكا بين 7 و 102 مليار، بي بي سي عربي، شوهد بتاريخ 2018/04/16 الرابط:

http://www.bbc.com/arabic/business-43093413

18. اختراق "ديتلويت" يطال المؤسسات الأمريكية،ار تي عربي، شوهد بتاريخ 2018/04/21، الرابط:

https://arabic.rt.com/it/903750

19. وثيقة أمريكية مسربة: قراصنة تسرب بيانات أمريكية، فرانس 24 بالعربية، بتاريخ:2018/03/16 الرابط:

http://www.france24.com/ar/2017060

20. آفة البنوك و السياسيين:أربعة قراصنة مشهورون، كاتيون ، شوهد بتاريخ 2018/03/30 الرابط:

http://katehon.com/ar/article/af-lbnwk-wlsysyyn-rb-qrsn-rws-mshhwrwn

21. الأمن القومي الأمريكي وراء الهجمات، اليوم السابع ، بتاريخ2018/04/10، الرابط:

https://www.youm7.com/story/2017/6/28

22. أمريكا والقيادة الالكترونية، السكينة، شوهد بتاريخ 2018/04/22، الرابط:
https://www.assakina.com/news/news1/9379.html

23. جنود الكترونيون ضمن الجيش الأمريكي، مونت كارلو، شوهد بتاريخ: 2018/02/16، الرابط:
https://www.mc-doualiya.com/articles/20171214

24. عمرو عبد العاطي، حرب أمريكية مضادة للإرهاب السيبراني، الخليج بتاريخ:2018/04/22، الرابط:
http://www.alkhaleej.ae/supplements/page/e4b1fdf9-a839-4db1-8023-50ad4f43cd24

25. أهم التهديدات التي تواجه عام 2018، صانعو الحدث ،شوهد بتاريخ 2018/04/04، الرابط:
/https://saneoualhadath.me

ثانيا: المصادر والمراجع باللغة الأجنبية.

أ/ المصادر:

1. H. B. 6443, Gen. Assem, 1999 Reg. Sess. Conn. 1999; H. B. 242, 140th Gen. Assem., Reg. Sess. (Del. 1999); H. B. 1287, Gen. Assem., 1999 Reg. Sess. (N.C. 1999).
2. **See**: - Susan W. Brenner, State Cybercrime Legislation in the United States of America: A Survey, 7 RICH. J.L. & TECH. See 28/03/2018:

ب/ الكتب:

1. Richard A. Clarke & Robert knake, Cyber War, HarperCollins (2010),
2. Bruno Lanvin,(2002). The E_Government Hand Book for developing countries". Center for democracy and Technology,
3. Karen L., Jungwoo L.,(2001). Developing fully functional E_Government: A four stage model". Government information quarterly 18,
4. Phil Williams, Cert Coordination Center، "Implications for Business." Organized Crime and Cyber-crime 2002:p
5. Tom forester, Essential proplems to Hig-Tech Society First MIT Pres edition, Cambridge, Massachusetts, 1989,
6. Hacking the human: social engineering techniques and security countermeasures, by Ian Mann,

7. –Scene of the cybercrime: computer forensics handbook, by Debra Littlejohn Shinder,

8. Encyclopaedia of Teaching of Internet, By A Kumar.

9. Oerlemans, Jan-Jaap, Investigating cybercrime, Leiden University,HIOA bibliotik, norway. 2017 ,

ج/ المقالات والدوريات:

1. Sofaer and Goodman. Cyber Crime and Security The Transnational Dimension, p 4, liens http: //media.hoover.org/sites/default/files/documents/0817999825_1.pdf..1.2017
2.UK Safer internet Day.4.2.20140
https: //www.saferinternet.org.uk/safer-internet-day/safer-internet-day-2016
3.How can we combat cyber crime?. A group of researchers are aiming to shed new light
4.on how legislation can be used to stop these criminals. Article from university of oslo. 2015/05/12. available at http: //sciencenordic.com/how-can-we-combat-cyber-crime.
5.Cypercrime-Budapest Convention and related standards-council of europe. 2015/05/19. availble at http: //www.coe.int/en/web/cybercrime/the-budapest-conventio
6.Cybercrime. EU Regulatory Framework on Cybercrime.norway.university of oslo. 2015/12/22. available athttp: //www.jus.uio.no/ifp/english/research/projects/nrccl/signal/research-prongs/cybercrime/.
7.Council of Europe. Convention for the Protection of Individuals with regard to Automatic
8.Processing of Personal Data. 2008/06/16.
https: //rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId

9. Malcom Anderson: " Policing the world: Interpol the Politics of International Police Co- Operation " , Clarendon press.Oxford,1989,

10.Estonia Cyber Security Strategy 2014-2017, Ministry of Economic Affairs and Communication, Estonia 2014,

11.J. FLOUR, J.-L. AUBERT, Les obligations, Armand Colin, 1994, p.105
A.-M. Leroyer, L'épreuve d'Internet, précité,

تطور مفهوم الاستراتيجية من المفهوم الضيق الذي يعنى بالشؤون العسكرية إلى المفهوم الموسع الذي اصبح يشمل أغلب المجالات، ومن بين بينها الأمن الإلكتروني الذي أصبح مصدر قوة للدول (البعد الخامس في الجيوستراتيجية) وعليه أصبحت الدول خاصة منها الكبرى تبني استراتيجيات من آليات و خطط ل وتبني شراكات مع باقي الأمم أمنها الإلكتروني من أجل حماية أمنها الإلكتروني من أي تهديد، فمن هاته الدول الولايات المتحدة الامريكية محل دراستنا تعتبر رائدة في مجال الأمن الإلكتروني وقوة عالمية، تعتمد على استراتيجيات الدفاع والهجوم وآليات قانونية في صد أي هجوم على كيانها الإلكتروني على ذلك أيضا تم بناء إتفاقيات بينها وبين الدول لتجريم أي سلوك عدواني للامن الإلكتروني الخاص بأي فاعل دولاتي سواء كان الولايات المتحدة أو أي دولة أخرى.

The development of the concept of strategy from the narrow concept of military affairs to the broad concept, which has become the most encompassing areas, including electronic security, which has become a source of strength for countries (the fifth dimension in geostrategic) and therefore the countries especially the major ones to adopt strategies of mechanisms and plans for the adoption of partnerships With the rest of the nations its cyber security. In order to protect its cyber security from any threat, it is the United States of America (case study) is a leader in the field of cyber security and a global force, based on strategies of defense and attack and legal mechanisms to repel any attack on the cyber entity to that was also built agreements between them States to criminalize any aggressive conduct of the electronic security of any State actor, whether the United States or any other State.