

البعد الجيو سياسي للأمن السيبراني

The geopolitical dimension of cybersecurity

أ.م.د. ضحى لعبيبي كاظم السدخان*

قسم الجغرافية، كلية التربية، جامعة ميسان، العراق

daha1969b@gmail.com

تاريخ الارسال: 2020-03-17 تاريخ القبول: 2021-03-18 تاريخ النشر: 2021-04-10

الملخص:

في أعقاب نشوة البدايات العامة للإنترنت، بدأ العلماء والمفكرون اعلانهم بأن التطور التقني سوف يؤدي الى نهاية ال¹جغرافيا منتصف التسعينيات، لقد أدى توسيع شبكات الاتصالات بين الدول إلى طوباوية لعالم أفضل، كما يؤدي الإنترنت إلى تسارع الزمن العالمي "الذي يحو حقيقة المسافات، تلك الفواصل الجغرافية التي، بالأمس، ما زالت تنظم سياسات الأمم وانتلافاتها". فأن الشبكات جزء لا يتجزأ من اقتصاداتنا وحياتنا السياسية والاجتماعية. و أصبحت الأداة المركزية للنشاط البشري. هذه الشبكات تشكل الفضاء الإلكتروني. الذي تحتفظ بمعلومات ذات قيمة هائلة، وهناك من يتحكمون في الآلات التي توفر الخدمات الحيوية. إنها تخلق فائدة اقتصادية هائلة، لكنها تشكل أيضاً مصدرًا رئيسيًا للمخاطر التي تهدد الدول بعد ان تطورت استخداماتها لتصبح اكثر تأثيراً في الهجمات الالكترونية العامة والخاصة. وهذا يشبه إلى حد كبير نزاع حول الانهار في الاراضي الرملية أو تضاريس متنازع عليها. بسبب حداثة التكنولوجيا، كما ان عدم وجود اتفاق واضح بين الدول بسبب الصراعات الجيو سياسية، فضلاً عن انتشار التجسس السيبراني والجريمة السيبرانية، في بيئة غير مستقرة يدعو إلى سوء تقدير وسوء تفسير وتصعيد غير مقصود للنزاع. ويتطلب تغيير هذا تحديد أدوات حكم الدولة الأكثر فعالية وأين قد نحتاج إلى مؤسسات وقواعد وقوانين جديدة. الكلمات المفتاحية : جيو سياسي، امن سيبراني، الفضاء الجغرافي، امن المعلومات، الكتروني، فضاء المعلومات.

Abstract :

In the wake of the euphoria of the general beginnings of the Internet, scholars and thinkers began to announce that technical development will lead to the end of geography in the mid-nineties. The expansion of communication networks between countries has led to a utopia for a better world, just as the Internet leads to the acceleration of global time, which erases the reality of distances, those geographical breaks. Which, yesterday, is still organizing the politics of nations and their coalitions " .Networks are an integral part of our economies and our political and social lives. And it became the central tool of human activity. These networks form cyberspace. Those who keep information of immense value, and there are those who control the machines that provide the vital services. They create tremendous economic benefit, but they are also a major source of risks to countries as their uses have evolved to become more influential in public and private cyber attacks. Much like a dispute over sandy rivers or disputed terrain. Because of the novelty of technology. Also, the lack of a clear agreement between countries due to geopolitical conflicts, as well as the spread of cyber espionage and cybercrime, in an unstable environment calls for miscalculations, misinterpretations and an unintended escalation of the conflict. Changing this requires identifying the most effective tools of state governance and where we may need new institutions, rules and laws.

Key words: (geopolitics, cybersecurity, geographical space, information security, electronic, information space)

مشكلة البحث: تكمن مشكلة البحث في التطور الرقمي في مجال الانترنت وما الت اليه حروب الفضاء الالكترونية والقرصنة السيبرانية للبيانات والمعلومات على صعيد الدولي والاستغناء عن الحروب الفتاكة للارواح والآليات الاخرى.

1. هل ادى التطور التقني في مجال الانترنت الى التصعيد الجيو سياسي؟.
2. مامدى حجم المشكلات التي تعاني منها الدول التي تتعرض الى الهجمات السيبرانية؟.
3. ماهو حجم التنافس على الصعيد السياسي والاقتصادي للامن السيبراني للدول التي استهدفت؟

الفرضية : لم يقتصر التطور التقني في العالم مقروناً باستخدام التقنيات الحديثة في المجالات الاقتصادية او الالكترونية بل تطور ذلك لياخذ مديات اوسع في الجغرافية السياسية والصراعات الجيو سياسية والحروب الالكترونية عبر الفضاء الجغرافي لتصبح العلاقات الدولية محفوفة

بالمخاطر بعيدة المدى فلا حدود طبيعية ولا حدود سياسية تعترضها واصبحت الهجمات السيبرانية متنوعة الاهداف فلا مصادر طاقة ولا مساحات شاسعة وامكانيات عسكرية ومقومات اخرى تقف امامها:

1. تم استخدام التطور التقني الرقمي في خلق المشاكل الجيو سياسية والجيو اقتصادية.
 2. ساهم الهجمات السيبرانية في تعطيل برامج نووية او التجسس على الاجهزة الامنية للدول العظمى.
 3. تقوم الدول او الشركات او الافراد بأعمال التجسس او القرصنة وسرقة البيانات من الاجهزة الخاصة والعامة بعد ادخال البرامج الخبيثة.
- هدف البحث: يهدف البحث الى دور واهمية التطور التقني عالمياً ودوره في شل الحركة السياسية او الاقتصادية والعسكرية عن طريقة القرصنة الكترونية ومدى حماية الانظمة السياسية من ايجاد برامج متطورة " الامن السيبراني " لحمايتها من التجسس والحفاظ على سريتها من القرصنة والمساومة وعمليات المنافسة.
- اهمية البحث: لابد من معرفة اهم التأثيرات الجيو سياسية للامن السيبراني ومدى امكانيات التعامل مع الاجهزة للحفاظ على سرية البيانات والمعلومات السياسية والاقتصادية والاجتماعية للأجهزة العامة والخاصة للدول او الافراد وبرامجها الامنية او بياناتها الشخصية والحفاظ على سريتها من الهجمات السيبرانية.
- حدود البحث: تتمثل حدود البحث في البعد الزمني للفترة ما بين 2007-2017 اما البعد المكاني والمتمثل بالتأثيرات السيبرانية على المستوى العالمي

المبحث الاول

البعد الجغرافي للأمن السيبراني

اولاً: مفهوم الأمن السيبراني

ثانياً: عناصر الامن السيبراني

ثالثاً: ركائز الأمن السيبراني الاستراتيجية

رابعاً: العوامل التي يقوم عليها الأمن السيبراني

اولاً: مفهوم الأمن السيبراني

تدرس الجغرافيا السياسية تنافس القوة والتأثير على الإقليم، على مستويات مختلفة من التحليل إنها مهمة ديناميات أي نزاع على هذه الأرض، و المتناقضات واستراتيجيات الجهات الفاعلة من أجل سيطرتها، وتخصيصها والدفاع عن مصالحها داخل الحيز الجغرافي. هناك الجغرافيا السياسية في الفضاء الإلكتروني، وهناك نهج دبلوماسي لإدارة الفضاء الإلكتروني. يتكون الفضاء الإلكتروني من أربع طبقات. هناك طبقة مادية، وهي شبكة عالمية من الكابلات ومحطة التبديل ومركز تخزين البيانات. هناك أيضًا طبقات منطقية وبيانات اجتماعية. جميع الطبقات الأربع هي "سياسية وجيوسياسية".⁽¹⁾

وتقسم الجغرافيا السياسية للفضاء الإلكتروني الى قسمين هما الجغرافيا الكلاسيكية والتقليدية في حين تنظر الجغرافيا الكلاسيكية سبل صياغة الجغرافيا السياسية وهذا يوضح ان للفضاء جغرافية مسؤولة عن تقرير البنية المادية لشبكة الإنترنت، على سبيل المثال، أن (80%) من حركة الإنترنت في العالم تمر عبر أمريكا الانجلو سكسونية. وساهم هذا في اعطاء الولايات المتحدة الأمريكية ميزة لمراقبة حركة الإنترنت العالمية. كما أنه يشكل سلوك حكومات الدول الأخرى، لأنها ستبدأ في التفكير في كيفية تغيير الوضع لذلك، فإن العنصر الرقمي لمبادرة الحزام والطريق المقترحة في أوروبا يمكن الأوروبيين من تجنب مثل هذه المراقبة الأمريكية. وهناك تأثير مباشر للمقومات الجغرافية الطبيعية والبشرية المؤدية الى اضرار في نظام الشبكات وعلى البنية التحتية الأساسية منها على سبيل المثال حدوث زلزال قوي في San Andreas Fault من الممكن ان يؤدي إلى تدمير منطقة وادي السيليكون، وهو المركز التي تتركز فيه شركات التكنولوجيا الفائقة في العالم. كما ان العواصف الشمسية يمكن أن تلحق الضرر بأنظمة الطاقة الوطنية، كذلك العوامل البشرية التي بدورها تقوم بالتأثير على تلك الشبكات، كالأقمار الصناعية، والإلكترونيات الطيران⁽²⁾، حيث تؤثر على إشارات الأقمار الصناعية لأنظمة الملاحة العالمية التي تعتمد عليها أجهزة الأمن والشرطة والأنظمة العسكرية وخدمات الطوارئ. وهذا الخلل يشجع المتسللين او القراصنة في نجاح الهجوم السيبراني الذي يقوم به "المتسللين، او المخابرات، او اصحاب الجريمة المنظمة" وهذا العمل لا يزال يعتمد على تقنية واحدة أو نقطة ضعف .

اما الجغرافيا السياسية التقليدية فأنها تركز على دراسة الفضاء، بعد ان سلطت الضوء على السلطة وعلى الأرض. وبالتالي، فإن التركيز على الإقليمية والناس والشبكات أمر أساسي

في تحليل الجغرافيا السياسية. (3) ومع ذلك، ففي الفضاء الإلكتروني، يصعب التقاط بعض هذه المفاهيم، مثل الإقليمية أو السيادة، لأنها لم تعد ملموسة، فإن القوى المتنافسة في الفضاء الإلكتروني تبحث عن نفس الميزة كما لو كانت على سطح الأرض، لذلك لا يزال مفهوم الجغرافيا السياسية الإلكترونية يرتبط ارتباطاً وثيقاً بالقوة بنوعيتها، فضلاً عن تطوره وتعيده (4).

وتمثل الجغرافيا السياسية الإلكترونية دراسة الفضاء الإلكتروني الذي يعتبر بمثابة المساحة التي تحددها أحداثيات الجغرافي. لذلك، هناك أبحاث عن القوة والنفوذ في هذا العالم الرقمي، في جميع العلوم والمجالات المتشابكة مثل الاقتصاد والدبلوماسية والطاقة. بالإضافة إلى ذلك، ترتبط الجغرافيا السياسية الإلكترونية ارتباطاً وثيقاً بالبيانات، حيث يتم البحث عنها وجمعها نظراً لأن المعلومات تمثل قوة، ويوفر الفضاء الإلكتروني حدوداً جديدة لالتقاطها، وهذا يدعو إلى تحديد مفهوم الفضاء الجغرافي أو الفضاء الإلكتروني فأن مصطلح الفضاء الإلكتروني يمثل حالياً مجالاً حيوياً للمعلومات، في العالم الحديث، وبمضمونه الجغرافي يستغني عن الحدود الطبيعية أو السياسية التي فصلت الدول عن بعضها البعض، بل هو مجالاً مهماً للمنافسة بأبعادها الجيو سياسية والجيو اقتصادية فضلاً عن المجالات الثقافية والاعلامية. أو بشكل أكثر دقة هو التوصيل البيني العالمي لمعدات الاتصالات. (5)

و "الفضاء الإلكتروني" الذي يولد بمساحة غير مرتبطة بحدود جغرافية فإن الموقع والموضع هنا لم يكن له دور استراتيجي في معركة الفضاء فلا يتأثر في قيام الحروب الإلكترونية أو الهجمات السيبرانية، كما تجري فيها عمليات تبادل غير مقيدة بين مواطني جميع الدول، بسرعة فورية تلغي أي فكرة عن البعد والمسافة بين الدول ونستطع القول انها بعيدة كل البعد عن نظرية "ماكندر وماهان وسبايكمان" (6). وبعد ان فسر التطور التقني على انه فضاء سياسي من نوع جديد ("افتراضي") تتعارض فيه مصالح مختلف الفاعلين السياسيين والدول المختلفة ومراكز القوى السياسية. بعد ظهورها تقريباً، وتحول الفضاء الإلكتروني إلى ساحة المعركة الخامسة (بعد البر والبحر والجو والفضاء) لمختلف القوى السياسية والعسكرية وما زالت كذلك (7). علاوة على ذلك، فإن العديد من المعارك بين المنظمات الاستخباراتية في

مختلف البلدان، وهياكلها العسكرية، وكذلك المعارك الجيو اقتصادية والإعلامية، بما في ذلك التخريب المالي⁽⁸⁾.

كما أصبح الانترنت احدى وسائل الاتصال السياسي والدبلوماسي في العلاقات الدولية المعاصرة ووسيلة اتصال فاقت جميع وسائط النقل المتطورة والسريعة، وبالرغم من استخداماته في الاغراض التجارية والاقتصادية بكل جوانبها، أصبح احد ابرز وسائط العصر الحديث في الحروب او ماتسمى " حروب الجيل الرابع" ومنها التدخل بشكل مباشر او الاعتداء على خصوصيات الدول وتعطيل برامجها النووية او كشف المخططات السياسية للدول ويمكن القول ان العالم اليوم يواجه العديد من المشاكل على الصعيد الجيو سياسي والجيو اقتصادي سيما وان الهجمات السيبرانية انتشرت بشكل كبير في الالونة الاخيرة مما يستدعي الحد منها وحماية شبكات المعلومات عن طريق الامن السيبراني⁽⁹⁾ اذ سنأتي الى بيان مفهومه وعناصره وركائزه.

اولاً: مفهوم الأمن السيبراني

كلمة الأمن السيبراني هي عبارة عن علم جديد لدور جميع القوانين والسياسات والأدوات والأجهزة والمفاهيم وآليات الأمن وطرق إدارة المخاطر والإجراءات والتدريب والممارسات الجيدة والتكنولوجيات التي يمكن استخدامها لحماية الناس والأصول المادية والحوسبة غير المادية (المتصلة بشكل مباشر أو غير مباشر بشبكة) من الدول والمنظمات (بهدف التوافر والنزاهة والأصالة والسرية وإثبات عدم التنصل)⁽¹⁰⁾. مع وجود تعاريف عديدة بينت مفهوم الامن السيبراني بأعتبره مجموعة من العمليات التقنية الحديثة والممارسات التي تحمي الشبكات وأجهزة الكمبيوتر والبيانات من الهجمات والأضرار والوصول غير المصرح به. وفي ضوء التقنيات الحديثة، عرف "الأمن" السيبراني والأمن المادي⁽¹¹⁾. بأنه مجموعة من الأدوات والاستراتيجيات الامنية والمبادئ التوجيهية ونهج إدارة المخاطر والإجراءات والتدريب والخبرة العملية والتأمين والتكنولوجيا، والتي يمكن استخدامها لحماية الفضاء الإلكتروني والتنظيم وموارد المستخدم⁽¹²⁾. وهو يمثل تنفيذ تدابير لحماية النظم والشبكات وتطبيقات البرمجيات من الهجمات الرقمية. تهدف هذه الهجمات عادة إلى اختراق البيانات الدقيقة والاساسية على اجهزة الكمبيوتر التي تتمتع بسرية⁽¹³⁾، وتغييرها وتدميرها، أو ابتزاز الأموال من المستخدمين، أو تعطيل التشغيل العادي للشركات. وله مفاهيم عديدة منها فلسفية ومنها تعاريف فنية⁽¹⁴⁾. ويوضح الجدول (1) نسبة الضرر التي تتعرض لها اجهزة الكمبيوتر من خلال البرامج الضارة، حيث اتت الصين بالمرتبة الاولى من بين الدول التي لديهم أعلى معدلات إصابة بالبرامج الضارة في أجهزة الكمبيوتر فقد بلغت نسبة الضرر الملحق بأجهزة الكمبيوتر العامة والخاصة (49%)، ولتت تايوان بالمرتبة الثانية بنسبة

(47.37%)، وتركيا(40.99%) ثم روسيا بنسبة (38.95%). واثت بولندا بالمرتبة الاخيرة من بين اعلى الدول لتبلغ (33.01%). وتوضح الخريطة(1) التوزيع الجغرافي للدول الاكثر تضرراً في العالم.

جدول (1) الدول التي لديهم أعلى معدلات إصابة بالبرامج الضارة في أجهزة الكمبيوتر

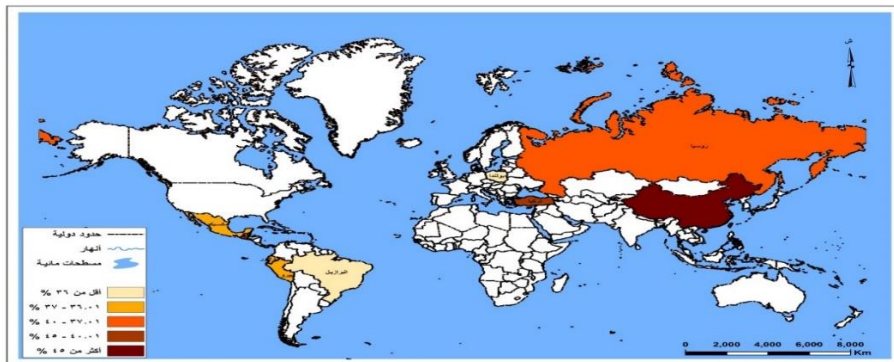
للمدة (2017-2007)

ت	الدول	النسبة % من الهجمات
1	الصين	49
2	تايوان	47.34
3	تركيا	40.99
4	روسيا	38.95
5	غواتيمالا	37.56
6	المكسيك	36.89
7	بيرو	36.23
8	اكوادور	36.22
9	البرازيل	34.68
10	بولندا	33.01

Source:Nazolt Senzen, 2019, Cybersecurity and its Impact on State Policy and Decision-making, Michkan, United States of America, Annual Cyber Monitor Reports, pp. 331-360

خريطة(1) الدول التي لديهم أعلى معدلات إصابة بالبرامج الضارة في أجهزة الكمبيوتر

للمدة (2017-2007)

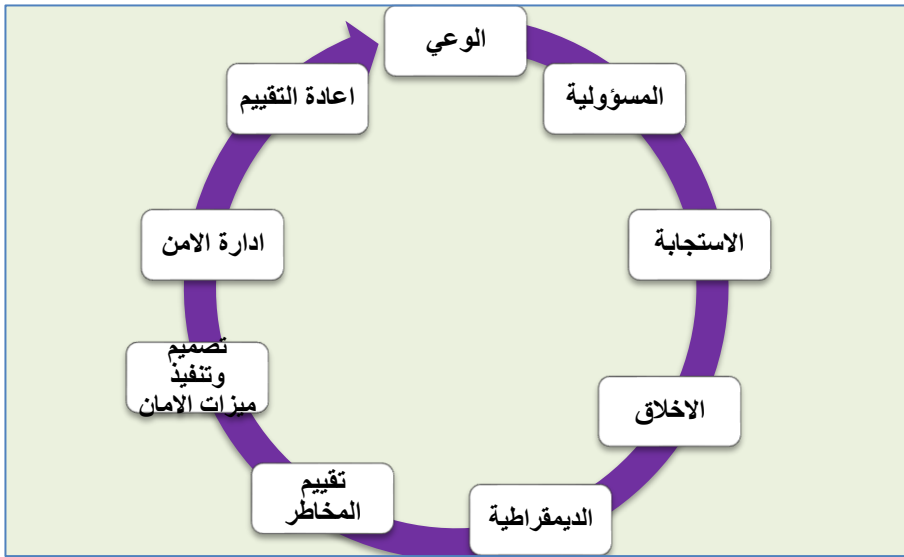


المصدر : عمل الباحثة اعتماداً على الجدول(1)

ثانياً: عناصر الامن السيبراني

مع التطور التقني لشبكات الانترنت بدأت الوكالات الحكومية والمؤسسات والمنظمات الأخرى والمستخدمون والأشخاص بالبحث حول طرق تطوير أنظمة وشبكات المعلومات وينبغي أن يتعاملوا مع الأمن السيبراني بدقة. وهذا يتطلب ثقافة تقنية تهتم بدراسة مخاطر الهجمات السيبرانية ومن أبرز عناصر الامن السيبراني التي تدعو المشاركون الاهتمام بها وتطوير السبل الكفيلة التي تجد الحلول المناسبة لحماية الشركات او الافراد من جهة ومن جهة اخرى ايجاد الأمن السيبراني للحفاظ على سرية المعلومات للبرامج الدولية ⁽¹⁵⁾ وبين الشكل (1) عناصر الامن السيبراني .

شكل(1) عناصر الامن السيبراني التكميلة



المصدر: عمل الباحثة

أ - الوعي: يجب أن يدرك المشاركون الحاجة إلى أمن أنظمة وشبكات المعلومات وما الذي يمكنهم فعله لزيادة الأمن؛

ب - المسؤولية: المشاركون مسؤولون عن أمن أنظمة وشبكات المعلومات وفقًا لدور كل منهم. يجب على المشاركين مراجعة سياساتهم وممارساتهم وإجراءاتهم بانتظام وتقييم ما إذا كانت ملائمة لبيئتهم الخاصة بالتطبيق؛

ج - الاستجابة: ويتطلب ذلك ضرورة الانتباه ومراعاة الوقت لمنع الحوادث الأمنية واكتشافها والاستجابة لها. ينبغي عليهم تبادل المعلومات، حسب الاقتضاء، بشأن التهديدات ونقاط الضعف ووضع إجراءات للتعاون الفوري والفعال في منع هذه الحوادث واكتشافها والاستجابة لها. قد يشمل ذلك تبادل المعلومات والتعاون عبر الحدود؛

د - الأخلاق: نظرًا لاختراق أنظمة وشبكات المعلومات في جميع أركان المجتمع الحديث، يحتاج المشاركون إلى مراعاة المصالح المشروعة للآخرين والاعتراف بأن أفعالهم أو تقاعسهم عن العمل يمكن أن تضر الآخرين؛

ه - الديمقراطية: من خلال ضمان الأمن بطريقة تتفق مع القيم المعترف بها في مجتمع ديمقراطي، بما في ذلك حرية تبادل الأفكار، والتدفق الحر للمعلومات، وسرية المعلومات والاتصالات، والحماية المناسبة للمعلومات الشخصية، والانفتاح والإعلان؛

و - تقييم المخاطر: على جميع المشاركين إجراء تقييم دوري للمخاطر، والذي: يسمح بتحديد التهديدات ونقاط الضعف؛ لديها قاعدة واسعة بما يكفي لتغطية العوامل الداخلية والخارجية الرئيسية مثل التكنولوجيا والعوامل المادية والبشرية والمنهجية المطبقة وخدمات الطرف الثالث التي تؤثر على الأمن؛ يجعل من الممكن تحديد درجة الخطر المقبولة؛ يساعد في اختيار أدوات التحكم المناسبة لتنظيم خطر حدوث ضرر محتمل لنظم وشبكات المعلومات، مع مراعاة طبيعة وأهمية المعلومات المحمية⁽¹⁶⁾؛

ز - تصميم وتنفيذ ميزات الأمان : ضرورة النظر من قبل المشاركين في الاعتبارات الأمنية كعنصر أساسي في تخطيط وتصميم وتشغيل واستخدام نظم وشبكات المعلومات؛

ح - إدارة الأمن : اتباعه المشاركون نهج متكامل لإدارة الأمن، استنادًا إلى تقييم ديناميكي للمخاطر، يغطي جميع مستويات أنشطة المشاركين وجميع جوانب عملياتهم؛

ط - إعادة التقييم : مراجعة المشاركين إعادة تقييم أمن أنظمة وشبكات المعلومات وإجراء التغييرات المناسبة على السياسات والممارسات والتدابير والإجراءات الأمنية، مع مراعاة ظهور تهديدات ومواطن ضعف جديدة⁽¹⁷⁾.

اذ نجد ان هناك عدد من الدول كانت لديها اصابات بالبرامج الضارة وبعض من عمليات التجسس السيبرانية الا ان التقييم الدوري لانظمة الشبكات لتلافي المخاطر السيبرانية فضلاً عن اكتشاف الهجمات بوقت مبكر ومعالجتها لتقليل المخاطر وتخفيف الاضرار وهذا دليل على ان هناك عدد من الدول لديها الحماية الكافية للحفاظ على شبكاتها العامة والخاصة من الهجمات السيبرانية بل نظراً للتطور التقني في هذا المجال اخذت العديد من الدول تتبع احداثها للحماية من المخاطر، ومنها عدد من الدول الاوربية فضلاً عن اليابان ضمن دول اسيا ويبين الجدول (2) الدول المتقدمة في كيفية الحفاظ على امن المعلومات في والحد من تعرضها الى الى البرامج الضارة حيث انت السويد بالمرتبة الاولى في انخفاض معدلات الاصابة بالبرامج الضارة في اجهزتها الالكترونية فقد بلغت نسبتها 19.88%، فيما انت فلندة بالمرتبة الثانية بنسبة (20.65%)، تلتها النرويج بنسبة (21.63%)، في حين جاءت اليابان بالمرتبة الرابعة ولن يكن الفارق كبير بين كل من المملكة المتحدة وسويسرا أذ تراوح ما بين (23.38-23.94%) والدنمارك وهولندا، والمانيا فقد تراوحت ما بين (24.12-24.86%) كما ظهرت هولندا الأكثر عرضة للجرائم الإلكترونية، اذ بلغت (20.3%)، قد يكون هذا بسبب العدد الكبير من هجمات مزود السحابة الواردة في حين حافظت السويد على مكانتها بأدنى معدلات للهجمات الالكترونية حيث بلغت نسبتها 8.6%، كما يلاحظ من خلال الجدول ان المدة ما بين عام 2007-2017 انخفضت نسبة اصابة تلك الدول بالبرامج الضارة يعود الى تطور تقنيات الحماية من التهديدات الالكترونية في تلك الدول على العكس من بقية الدول الاخرى في العالم فضلاً عن الاتفاقية التي وقعت في بودابست بين دول الاتحاد الاوربي وسنأتي الى عرضها لاحقاً

جدول(2) قائمة البلدان التي لديها أدنى معدلات إصابة بالبرامج الضارة الالكترونية(2007-2017)

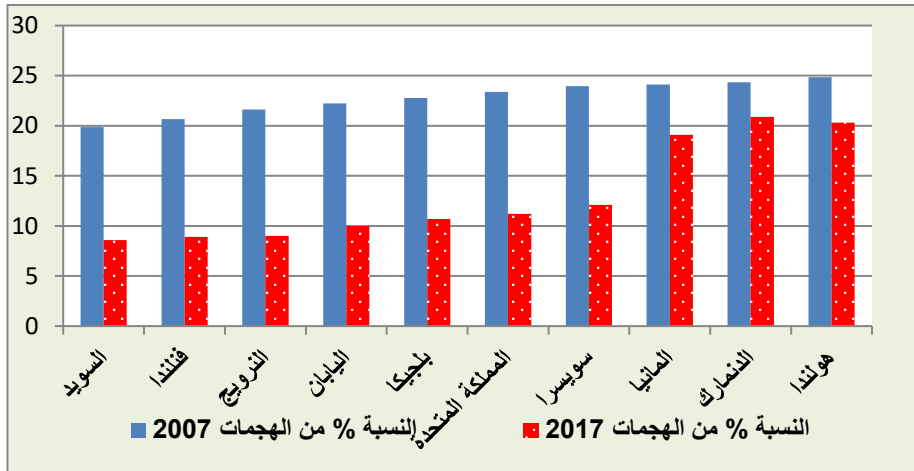
ت	الدول	النسبة % من الهجمات 2007	النسبة % من الهجمات 2017
1	السويد	19.88	8.6
2	فنلندا	20.65	8.9
3	النرويج	21.63	9
4	اليابان	22.24	10
5	بلجيكا	22.78	10.7
6	المملكة المتحدة	23.38	11.2
7	سويسرا	23.94	12.1
8	المانيا	24.12	19.1
9	الدنمارك	24.34	20.9

10	هولندا	24.86	20.3
----	--------	-------	------

Source: Nazalt Sensen, 2019, Cybersecurity and its Impact on State Policy and Decision-making, Michkan, United States of America, Annual Cyber Monitor Reports, pp. 331-360

ويبدو من الشكل (2) ان بعض الدول انخفض بها نسبة البرامج الضارة الى 50% ، عام 2017 كما في النرويج واليابان وبلجيكا وسويسرا الى ما كانت عليه عام 2007.

شكل(2) انخفاض البرامج الضارة للمدة 2007-2017



الباحثة اعتماداً على الجدول(2)

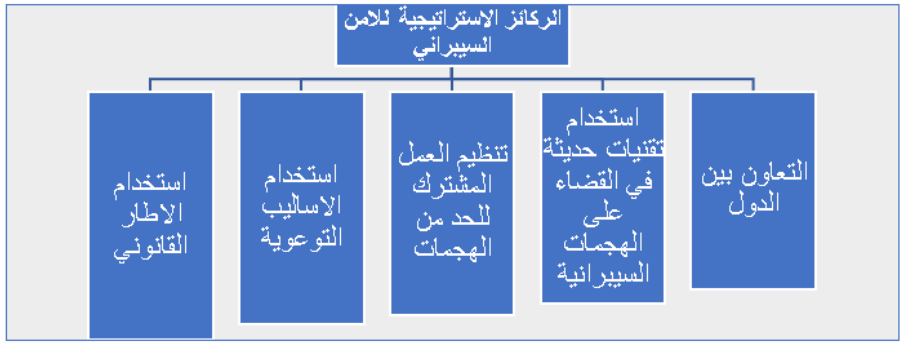
ثالثاً: ركائز الأمن السيبراني الاستراتيجية

يمثل الأمن السيبراني، الذي يتعلق بالأمن والسيادة العددية لكل دولة أو أمة، مخاطر اقتصادية واستراتيجية وسياسية تتجاوز الأمن الوحيد لنظم المعلومات⁽¹⁸⁾. وتكون كل من البيانات والأعمال المتعلقة بها، و الحوسبة الصناعية، جزءاً لا يتجزأ من أجهزة الكمبيوتر التي ترتبط بكافة الأجسام المكونة لتلك الاجهزة⁽¹⁹⁾.

كما تتطلب الاستراتيجية الوطنية للأمن السيبراني استمرارية سياسية ورؤية طويلة الأجل. يبدو أن المنشورات الحكومية المختلفة لديها إجماع على إدراك الحاجة إلى تنظيم وضمان الأمن والدفاع للأنظمة الفنية نفسها، وتلك الخاصة بالشركات التي تستخدم هذه الأنظمة.

ومع ذلك، من أجل تعزيز ثقافة عالمية وتحفيز البلدان على تكثيف جهودها للأمن السيبراني، طور الاتحاد الدولي للاتصالات مؤشر عالمي للأمن السيبراني (GCI) يقيس مستوى تنمية كل بلد في هذا المجال. وتم نشر التقرير الأول في نيسان من عام 2015،⁽²⁰⁾. ومهمة GCI تقييم مدى التزام البلدان بالأمن السيبراني مقابل خمس ركائز استراتيجية تتمثل في الشكل (3) الاتي.

الشكل (3) الركائز الاستراتيجية للأمن السيبراني



المصدر: الباحثة

حيث نجد ان الاطار القانوني والاساليب التوعوية وتنظيم العمل المشترك للحد من الهجمات لا تطبقها الدول التي تتصيد المعلومات والبيانات لاسيما البيانات المتعلقة بالبرامج النووية او العسكرية والامنية والامثلة كثيرة حول تلك الهجمات التي تقوم بها الدول على سبيل المثال هناك اشخاص منفردين او مجموعات لن يكن لها ارتباط بالمؤسسات الحكومية التابعة لدولهم بل يقومون بعمليات قرصنة وسرقة بيانات وتهكير من اجل الفدية، اذن لابد من ايجاد تقنيات حديثة في الوصول الى المتسللين واصحاب الخبرة في كيفية الوصول الى شبكات البيانات والمعلومات الخاصة بالدول او الافراد او الشركات، للقضاء على الهجمات السيبرانية، وهنا لابد من التعاون بين الدول على اساس احترام سيادة وامن الدولة وعدم التدخل في شؤونها او التجسس على سير الحركة السياسية او العسكرية والامنية. ومن أجل تحقيق أهداف هذه الركائز الخمس، يجب تحديد ثمانية أهداف استراتيجية تتمثل في الشكل (4)⁽²¹⁾:

الشكل (4) الاهداف الاستراتيجية لتحقيق ركائز الامن السيبراني



المصدر: الباحثة

ومن خلال الاهداف في اعلاه نجد ان خطوات تحقيق امن سيبراني يتطلب مناخ سياسي وتعاون دبلوماسي بين الدول حتى يكون التعاون للقضاء على تلك الهجمات مقرون بعلاقات الدول مع بعضها البعض في نظام سياسي توافقي مبني على العلاقات الدولية المترابطة من اجل انشاء حوكمة الكترونية قوية وتقييم المخاطر بشكل مستمر حتى على صعيد النظام السياسي للدولة الواحدة فهناك عمليات تجسس الكتروني او سرقة بيانات تحدث ضمن فيما بين مؤسساتها او انظمتها المالية والمصرفية وان التثقيف المستقبلي يتطلب تقنية عالية يستطع من خلالها الدول او المؤسسات حماية اجهزتها وشبكاتها ولايعني التثقيف نشر بوسترات تحد من سرقة البيانات فهي ليس بوقاية صحية بل تحتاج الى برامج تنبيه سريعة تعطي الابعاز المبكر عند قيام تلك العاملين بالهجمات السيبرانية بمختلف انواعها.

رابعاً: العوامل التي يقوم عليها الأمن السيبراني

يتم التعبير عن النهج الناجح للأمن السيبراني في شكل حماية متعددة المستويات تغطي أجهزة الكمبيوتر والشبكات والبرامج أو البيانات التي تحتاج إلى تأمين. يجب أن يكمل الموظفون وسير العمل والتقنيات بعضهم البعض في المؤسسات لتوفير حماية فعالة ضد الهجمات السيبرانية⁽²²⁾ التي تتعرض لها الدول اذ هناك فواعل رئيسة يستند عليها الامن السيبراني والتي تؤثر في جميع العمليات وهم:

1. العاملين: يجب على المستخدمين فهم المبادئ الأساسية لأمن المعلومات والالتزام بها، مثل اختيار كلمات مرور قوية والاهتمام بمرفقات البريد الإلكتروني والنسخ الاحتياطي للبيانات. معلومات إضافية عن المبادئ الأساسية للأمن السيبراني.
2. العمليات: يجب على المنظمة تطوير مجموعة من التدابير الأساسية لمواجهة الهجمات المستمرة ونجحت في تنفيذ الهجمات. يمكنك الاسترشاد بمجموعة واحدة من التدابير الموثوقة. يجب أن توضح هذه المجموعة من التدابير كيفية تحديد الهجمات وحماية الأنظمة وتحديد التهديدات والتصدي لها واستعادة الوظيفة بعد الهجوم.
3. التكنولوجيا: تمثل التكنولوجيا عنصر أساسي في تزويد المنظمات والأفراد بالأدوات التي يحتاجونها للدفاع ضد عمليات التهكير والتنصت لاسيما وان ابرز الاجهزة المعرضة للهجمات السيبرانية والتي تكون بحاجة ماسة الى الحماية هي الأجهزة الطرفية مثل أجهزة الكمبيوتر والأجهزة الذكية وأجهزة توجيه الشبكات وتتضمن التقنيات الأكثر شيوعاً المستخدمة لحماية هذه المكونات جدران الحماية من الجيل التالي وتصفية DNS وحماية البرامج الضارة وبرامج مكافحة الفيروسات وحلول حماية البريد الإلكتروني⁽²³⁾.

المبحث الثاني

الخصائص الأساسية للجريمة السيبرانية

أولاً: التهديد و الهجوم السيبراني

ثانياً: أنواع تهديدات الأمن السيبراني

ثالثاً: الحماية من التهديدات السيبرانية

رابعاً: عمليات التجسس السيبرانية

أولاً: التهديد و الهجوم السيبراني

في الخمسينيات من القرن الماضي، استخدمت كلمة "سيبراني" للإشارة إلى علم التحكم الآلي - علم فهم التحكم وحركة الآلات والحيوانات. تبع ذلك كلمة "cyber" التي تعني "محوسب". في حين جلبت التسعينيات مصطلحاً جديداً متعلقاً بالإنترنت. ظهرت كلمة "الفضاء السيبراني" لتعريف الفضاء المادي المخترع الذي أراد بعض الناس الاعتقاد بوجوده وراء الأنشطة الإلكترونية لأجهزة الحوسبة.

و يستخدم المصطلح بشكل حصري تقريباً لوصف مسائل أمن المعلومات. نظراً لأنه من الصعب تصور كيف يمكن للإشارات الرقمية التي تنتقل عبر سلك أن تمثل هجوماً، فقد اتخذت تصوراً للظاهرة الرقمية كظاهرة فيزيائية، فأن "الهجوم السيبراني" هو هجوم يتم شنه على فئة معينة او دولة او فرد معين (بمعنى التأثير على الأجهزة الرقمية) عن طريق الفضاء السيبراني. أصبح الفضاء الإلكتروني، وهو فضاء افتراضي غير موجود، التشبيه المجازي الذي ساعد على فهم الأسلحة الرقمية التي تهدف إلى إلحاق الضرر بالمجتمعات او الدول او الاجهزة الاستخباراتية والشركات وغيرها، ولكن ما هو حقيقي هو نية المهاجم وكذلك التأثير المحتمل. في حين أن العديد من الهجمات الإلكترونية هي مجرد إزعاج، إلا أن بعضها خطير للغاية، بل وربما يهدد حياة البشر. (24)

يعد التهديد إجراءً أو حدثاً سلبياً محتملاً تسهله إحدى الثغرات الأمنية التي تؤدي إلى تأثير غير مرغوب فيه على نظام الكمبيوتر أو على التطبيقات الإلكترونية، ويمكن أن يكون التهديد حدثاً " مقصوداً " (مثل القرصنة: مخترق فردي أو منظمة إجرامية) أو حدثاً " عرضياً " (مثل احتمال حدوث خلل في الكمبيوتر، أو احتمال وقوع كارثة طبيعية مثل زلزال أو حريق أو إعصار) أو غير ذلك من الظروف، وتنتهي التهديدات السيبرانية الى هجوم وقد يسرق أو يغير أو يدمر هدفًا محددًا من خلال اختراق نظام حساس. يمكن أن تتراوح الهجمات السيبرانية من تثبيت برامج التجسس على جهاز كمبيوتر شخصي إلى محاولة تدمير البنية التحتية لدول بأكملها يسعى الخبراء القانونيون إلى قصر استخدام المصطلح على الحوادث التي تسبب ضرراً مادياً، وتمييزه عن انتهاكات البيانات الروتينية وأنشطة القرصنة الأوسع نطاقاً. (25) و يمكن استخدام الهجوم الإلكتروني من قبل دول ذات سيادة أو أفراد أو مجموعات أو مجتمع أو منظمات، وقد ينشأ من مصدر مجهول. حيث يُطلق على المنتج الذي يسهل هجوماً إلكترونياً أحياناً اسم سلاح الإنترنت (26) .

ثانياً: أنواع تهديدات الأمن السيبراني

تأتي تهديدات الأمن السيبراني في ثلاث فئات واسعة من النوايا. يسعى المهاجمون إلى التجسس الإلكتروني لتحقيق مكاسب مالية أو تعطيل أنظمة وبرامج عسكرية او التجسس لرصد سير البرامج السياسية للدول (بما في ذلك تجسس الشركات - سرقة براءات الاختراع - تجسس الدولة)، يقع كل تهديد إلكتروني تقريباً في أحد هذه الأوضاع الثلاثة. فيما يتعلق بتقنيات

الهجوم، فإن الجهات الخبيثة لديها الكثير من الخيارات أو الطرق التي من خلال تستطيع الوصول الى مبتغاها فهناك عشرة أنواع شائعة من التهديدات السيبرانية كما في الشكل (5). اذ لابد من بيان ابرز الامثلة على تلك التهديدات التي تعرضت لها الدول.

الشكل (5) انواع التهديدات السيبرانية



المصدر: عمل الباحثة.

1. البرمجيات الخبيثة. البرامج التي تؤدي مهمة ضارة على جهاز أو شبكة مستهدفة، مثل إتلاف البيانات أو الاستيلاء على النظام، وهذا ما حصل في روسيا عام 2013، بعد ان أعلنت شركة أمن إنترنت روسية أنها اكتشفت برمجيات خبيثة على الملايين من الاشخاص المستخدمين لأجهزة Android المحمولة، خاصة في روسيا والدول الناطقة بالروسية.⁽²⁷⁾ فضلاً عن الهجوم السيبراني التي تعرض له البرنامج النووي الإيراني عام 2010، من اجل الحاق الضرر بأجهزة الطرد المركزي الخاصة بتخصيب اليورانيوم في بعض المنشآت النووية الإيرانية. واتهمت طهران الولايات المتحدة الأمريكية، بشن هذه الهجمات⁽²⁸⁾. ويبدو ان الحروب المستقبلية العابرة للقارات سوف تستغني عن استخدام الصواريخ واستبدال ذلك بأرسال جنود

وصواريخ الكترونية تخترق الشبكات الالكترونية وانظمة الحاسوب وتتلّف وتدمر كل الانظمة او البنى التحتية.

2. التصيد. وهو هجوم عبر البريد الإلكتروني يتضمن خداع مستلم البريد الإلكتروني للكشف عن معلومات سرية أو تنزيل برامج ضارة بالنقر فوق ارتباط تشعبي في الرسالة، التصيد بالرمح.²⁹ شكل أكثر تعقيداً من التصيد الاحتيالي حيث يتعرف المهاجم على الضحية وينتحل شخصية شخص يعرفه ويثق به ومثال ذلك. ماقامت به الهند أذ شنت مجموعة تجسس الكتروني هندية مشتبّه بها حملة تصيد احتيالي على الوكالات الحكومية الصينية والشركات المملوكة للدولة للحصول على المعلومات المتعلقة بالانشطة الاقتصادية التجارة والدفاع والعلاقات الخارجية³⁰. ففي حزيران من عام 2017. كشف باحثون أمنيون عن مجموعة تجسس الكتروني مرتبطة بإيران نشطة منذ عام 2013 التي استخدمت التصيد بالرمح وهجمات ثقب الري لاستهداف المؤسسات الحكومية والدفاع الشركات وشركات تكنولوجيا المعلومات وغيرها في إسرائيل والمملكة العربية السعودية والولايات المتحدة وألمانيا والأردن وتركيا تموز 2016، استهدفت مجموعة تجسس الكتروني صينية الصناعات الدفاعية في روسيا وبيلاروسيا ومنغوليا مع APTs التي تستخدم حملات التصيد لسرقة البيانات. وفي نيسان 2016. كان الاتحاد الديمقراطي المسيحي الألماني، الحزب السياسي لأنجيلا ميركل تم استهدافه في هجوم تصيد بيانات الاعتماد من قبل مجموعة تجسس الكتروني روسية.⁽³¹⁾

3. هجوم رفض الخدمة أو هجوم رفض الخدمة الموزع (DDoS) حيث يستولي المهاجم على العديد (ربما الآلاف) من الأجهزة ويستخدمها لاستدعاء وظائف النظام المستهدف، مثل موقع الويب، مما يتسبب في تعطله بسبب زيادة الطلب عليه. ومن ابرز تلك الدول التي نشأت منها اعلى نسبة من الهجمات لرفض الخدمة، الصين والتي تنصدر المرتبة الاولى بنسبة (29.56%)، ثم اتت الولايات المتحدة بنسبة 21.59%، ثم المملكة المتحدة بنسبة (16.17%) وهي الدول الاعلى في هجوم رفض الخدمة⁽³²⁾. جدول (3). خريطة (2).

جدول (3) الدول التي نشأت منها أعلى نسبة هجمات رفض الخدمة لعام 2017

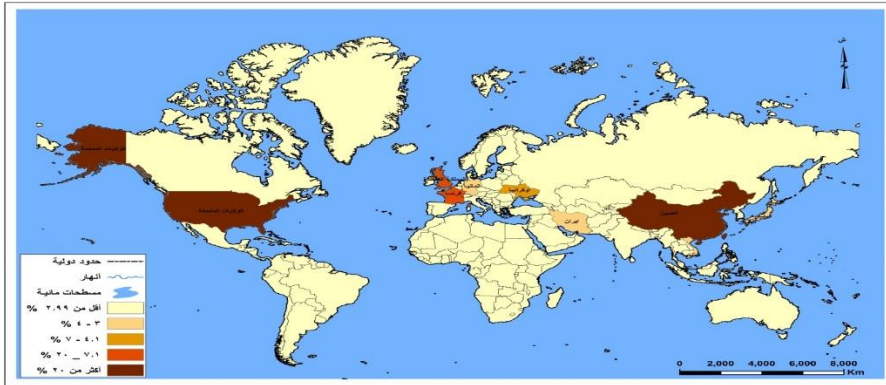
ت	الدول	النسبة % من الهجمات
1	الصين	29.56
2	الولايات المتحدة	21.59
3	المملكة المتحدة	16.17

4	فرنسا	8.72
5	اوكرانيا	4.06
6	سنغافورة	3.93
7	اليابان	3.81
8	فيتنام	3.76
9	المانيا	3.49
10	ايران	3
11	بقية الدول	10.91

Source: 1.Ernst, Delly, 2018, Electronic Information Warfare, China, Hong Kong, translated by Serzy Pardo, 2019, pp. 116-142.

2. A. mbtsquet, 2016 Network Warfare "The Internet" New York: Columbia University Press, pp. 88-117.

خريطة (2) الدول التي نشأت منها أعلى نسبة هجمات رفض الخدمة لعام 2017



المصدر: الباحثة اعتماداً على الجدول (3)

وفي عام 2015 تعرض نظام الطاقة في اوكرانيا الى انقطاع التيار الكهربائي و كانت نتيجة تنسيق مع العديد من شركات توزيع الطاقة الإقليمية، حيث تم استهداف أنظمة SCADA وشبكات مضيف النظام وتلفها. ثم استخدام البرامج الضارة لنقاط ضعف الشبكة، وإنشاء القيادة والتحكم، ومسح خوادم SCADA إلى تأخير الاستعادة. شن المهاجمون في وقت واحد هجوم رفض الخدمة على نظام المرسلين لمنع العملاء من الإبلاغ عن الاضطرابات. لما يقرب من 225000 أوكراني تأثرت بذلك واستمر الانقطاع من (3-6) ساعات. حتى تم ارجاع النظام. وفي كانون الثاني من عام 2013،⁽³³⁾ اعلن عز الدين القسام الإيراني مسؤوليته عن سلسلة أخرى من المسلسلات الموزعة لهجمات رفض الخدمة ضد مواقع بنك الولايات المتحدة، كجزء من عملية أبابيل المرحلة الثانية، وهناك امثلة كثيرة حول هجمات فض الخدمة التي تقوم

بها الصين والدول الاخرى، وفي اذار من عام 2010. أعلنت Google أنها عثرت على برامج ضارة تستهدف مستخدمي الكمبيوتر الفيتناميين. قالت Google إن البرنامج الضار لم يكن معقدًا بشكل خاص وكان يُستخدم للتجسس على "احتمال عشرات الآلاف من المستخدمين الذين قاموا بتنزيل برامج لغة لوحة المفاتيح الفيتنامية" البرامج الضارة أطلقت أيضًا هجمات رفض الخدمة الموزعة ضد المدونات التي تحتوي على معارضة سياسية، على وجه التحديد، معارضة جهود تعدين البوكسيت في فيتنام⁽³⁴⁾.

4. هجوم "رجل في الوسط" (MitM). حيث ينشئ المهاجم موقعًا بين مرسل الرسائل الإلكترونية ومتلقيها ويعترضها، وربما يغيرها أثناء النقل. يعتقد المرسل والمتلقي أنهما يتواصلان مباشرة مع بعضهما البعض. يمكن استخدام هجوم MitM في الجيش لإرباك العدو⁽³⁵⁾.

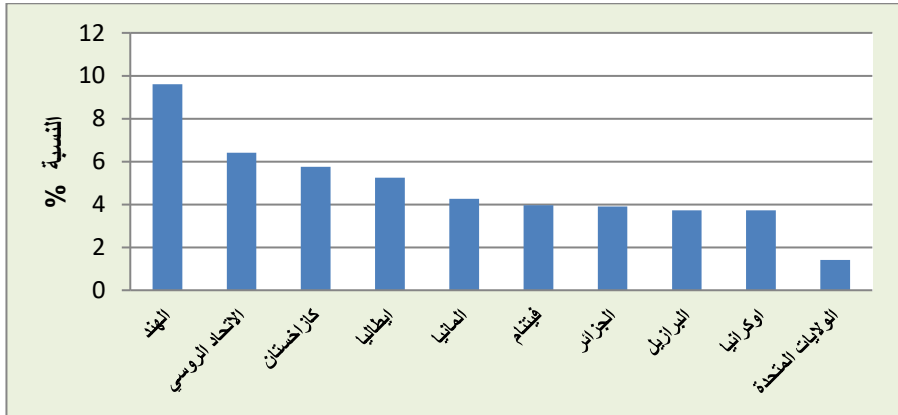
5. الاحتيال الإلكتروني : (الغش في الامتحانات، التصويت في الانتخابات، تزوير الوثائق الرسمية) حدثت في السنوات القليلة الماضية عدد كبير من الخروقات والاعتراضات في دول عديدة على نتائج الانتخابات واوعزت الدول ان هناك عمليات اختراق الكترونية وعملية احتيال الكتروني قد حصل في اجهزتها وتم تغيير نتائج الانتخابات فضلاً عن كشف بيانات الناخبين ففي نيسان من عام 2016. خرقت قاعدة بيانات لجنة الانتخابات الفلبينية (COMELEC)، وقامت بفضح المعلومات الشخصية لجميع الناخبين الفلبينيين المسجلين البالغ عددهم (55 مليوناً)، بما في ذلك بصمات الأصابع البيانات وأرقام جوازات السفر وتواريخ انتهاء الصلاحية ونوايا الترشح للمنصب، وفي آب من عام 2016⁽³⁶⁾ تم اختراق وكاليتين حكوميتين في هونغ كونغ في هجوم يُزعم أنه نفذهما الصين. وجاء الهجوم قبل أسابيع من الانتخابات التشريعية في هونغ كونغ⁽³⁷⁾.

6. حصان طروادة. سمي على اسم حصان طروادة للتاريخ اليوناني القديم، حصان طروادة هو نوع من البرمجيات الخبيثة التي تدخل إلى نظام مستهدف يبدو وكأنه شيء واحد، على سبيل المثال قطعة قياسية من البرامج، ولكن بعد ذلك يخرج الشفرة الضارة مرة واحدة داخل النظام المضيف ففي تموز من عام 2012. عثر حصان طروادة الملقب بـ "المهدي" على جمع البيانات من حوالي 800 مهمة من شركات هندسة البنية التحتية والوكالات الحكومية

والبيوت المالية والأوساط الأكاديمية في جميع أنحاء الشرق الأوسط وما وراءه، في الغالب في إسرائيل وإيران. يحتوي الفيروس على لغة سلاسل فارسية، وفي اب من عام 2011، تم اختراق بريد إلكتروني ووثائق من (480 عضواً) في البرلمان الياباني والمشرعين وموظفيهم لمدة شهر بعد هجوم تصيد احتيالي في زرع حضان طروادة على الأعضاء في أجهزة الكمبيوتر وخوادم النظام الغذائي. تواصلت الأجهزة المخطوفة مع خادم في الصين وقام المهاجمون بتضمين أحرف صينية في التعليمات البرمجية الخاصة بهم (38).

7. برامج دفع الفدية. هجوم يتضمن تشفير البيانات على النظام المستهدف والمطالبة بفدية مقابل السماح للمستخدم بالوصول إلى البيانات مرة أخرى. تتراوح هذه الهجمات من الإزعاج المنخفض المستوى إلى الحوادث الخطيرة بعد أن أصبحت تمثل تهديداً كبيراً للشركات والأفراد حيث تقوم معظم متغيرات برامج الفدية الحالية بتشفير الملفات على النظام/ الشبكة المصابة (برامج الفدية المشفرة)، على الرغم من أن بعض المتغيرات معروفة بمسح الملفات أو حظر الوصول إلى النظام باستخدام طرق أخرى (locker ransomware). بمجرد حظر الوصول إلى النظام، يطلب برنامج الفدية فدية لفتح الملفات، والتي غالباً ما تتراوح من (200 دولار - 3000 دولار) كما في دول أمريكا⁽³⁹⁾، بالرغم من الإبلاغ عن العملات الأخرى وبطاقات الهدايا في بعض الأحيان تستهدف متغيرات برامج الفدية دائماً الضحايا بشكل انتهازي، حيث تصيب مجموعة من الأجهزة الكمبيوتر إلى الهواتف الذكية، يتعرض الضحايا لخطر فقدان ملفاتهم، ولكنهم قد يتعرضون أيضاً لخسارة مالية بسبب دفع الفدية أو فقدان الإنتاجية وتكاليف تكنولوجيا المعلومات والرسوم القانونية وتعديلات الشبكة أو شراء خدمات مراقبة الائتمان للموظفين و العملاء. ويبين الشكل (6) الدول التي تتعرض فيها مستخدمي شبكات الانترنت إلى الهجوم السببراني لطلب الفدية.

شكل (6) الدول الأكثر تعرضاً لبرنامج دفع الفدية



Researcher acting on the source, Marina Magakia, 2019 , Cyber Security and Threat Policy: The United States' Efforts to Secure the Information Age. New York: Routledge, p490.

8. الهجمات على أجهزة إنترنت. أجهزة إنترنت و أجهزة الاستشعار الصناعية عرضة لأنواع متعددة من التهديدات السيبرانية. يتضمن ذلك المتسللين الذين يستولون على الجهاز لجعله جزءاً من هجوم DDoS والوصول غير المصرح به إلى البيانات التي يتم جمعها بواسطة الجهاز. نظراً لأعدادها وتوزيعها الجغرافي وأنظمة التشغيل التي غالباً ما تكون قديمة، فإن أجهزة إنترنت الأشياء هي هدف رئيسي للجهات الفاعلة الخبيثة⁽⁴⁰⁾.

9. التجسس الإلكتروني: تعد عمليات التجسس الإلكتروني خطيرة جداً لاسيما في عمليات الامن والاستخبارات او التجسس العسكري، والتي تمارسها بعض الدول للحصول على البيانات وهي اختراق نظام الشبكة للبيانات وسحبها او نشرها لاسيما في السنوات الاخيرة، فقد قامت حملة تجسس الكتروني إيرانية باستهداف الطاقة واجهزة الحكومة وقطاعات التكنولوجيا في المملكة العربية السعودية عام 2015. فضلاً عن تحديد باحثو الأمن السيبراني حملة تجسس الكتروني إيرانية استهدفت أكثر من 500 منظمة، معظمها في الشرق الأوسط، ركزت فيها على الدبلوماسية والدفاع والأمن والصحافة وحقوق الإنسان ومجالات أخرى. وفي نيسان عام 2017. كشف باحثو الأمن السيبراني عن حملة تجسس الكتروني متنامية نشأت في الصين أيضاً وتستهدف شركات البناء والهندسة والفضاء والاتصالات كذلك الوكالات الحكومية في

الولايات المتحدة وأوروبا واليابان. فضلاً عن جمع البيانات من منظمات الأرقام الصناعية والاتصالات والدفاع في الولايات المتحدة وجنوب شرق آسيا⁽⁴¹⁾. وفي عام 2014 برزت العديد من عمليات التجسس الإلكتروني منها حملات روسية استمرت خمس سنوات تستغل يوم الصفر ثغرة أمنية في برامج Windows على أجهزة الكمبيوتر التي يستخدمها الناتو والاتحاد الأوروبي والحكومة الأوكرانية، وفي العام ذاته تم اختراق قرصنة في أوروبا الشرقية قطاعات الطاقة في الولايات المتحدة وإسبانيا وفرنسا وإيطاليا، ألمانيا وتركيا وبولندا في حملة تجسس إلكتروني كبرى⁽⁴²⁾.

10. البرامج الضارة على تطبيقات الجوال. الأجهزة المحمولة عرضة لهجمات البرامج الضارة تمامًا مثل أجهزة الحوسبة الأخرى. قد يقوم المهاجمون بتضمين البرامج الضارة في تنزيلات التطبيقات أو مواقع الويب للجوال أو رسائل البريد الإلكتروني المخادعة والرسائل النصية. بمجرد اختراق الجهاز المحمول، وفي آذار من عام 2013. تعرضت البنوك والمصارف التلفزيونية في كوريا الجنوبية للهجوم ببرامج ضارة (مصممة للتهرب من برنامج مكافحة الفيروسات الكوري الجنوبي الشهير) الذي يُعتقد أنه نشأ في كوريا الشمالية، وفي حزيران من عام 2011، تم اختراق شبكات صندوق النقد الدولي من قبل حكومة أجنبية باستخدام، رسائل البريد الإلكتروني الاحتيالية التي تحتوي على مرفقات برامج ضارة وكمية كبيرة من البيانات، بما في ذلك المستندات ورسائل البريد الإلكتروني "، وفي آذار من عام 2010. أعلنت Google أنها عثرت على برامج ضارة تستهدف مستخدمي الكمبيوتر الفيتناميين. وأكدت Google إن البرنامج الضار لم يكن معقدًا بشكل خاص وكان يُستخدم للتجسس على " عشرات الآلاف من المستخدمين الذين قاموا بتنزيل برامج لغة لوحة المفاتيح الفيتنامية "البرامج الضارة أطلقت أيضًا هجمات رفض الخدمة الموزعة ضد المدونات التي تحتوي على معارضة سياسية، على وجه التحديد، معارضة جهود تعدين البوكسيت في فيتنام⁽⁴³⁾.

ثالثاً: الحماية من التهديدات السيبرانية

لا توجد حالياً أي معاهدة دولية للدفاع الإلكتروني تنظم الفضاء الإلكتروني لذا من الضروري تطور كل دولة سياستها الدفاعية واستراتيجياتها الوطنية بالرجوع إلى تشريعاتها الخاصة. وهذا يتطلب ان تحدد الدول احتياجاتها وتوقعاتها وأنواع التهديدات التي تتعرض لها، فضلاً عن وسائل حماية نفسها وإصلاح ومنع الهجمات المستقبلية. تأتي المفاوضات السياسية

والدبلوماسية لتطوير العقائد المشتركة بالإضافة إلى القرارات والاتفاقيات ومدونات السلوك الجيد لتأمين الفضاء الإلكتروني والاتصالات في المرتبة الثانية. كل هذا يعتمد قبل كل شيء على رغبة الدول في التعاون مع الدول الأخرى من أجل إنشاء فضاء مشترك منظم وهناك خمسة من أبرز العناصر التي يجب أن تأخذ بنظر الاعتبار نظراً لأهميتها الجيو سياسية حول الأمن السيبراني وخاذ التدابير الرئيسية للحد منها أو لحماية المعلومات العامة والخاصة للدول والشركات والمؤسسات العامة والخاصة والافراد نظراً للجرائم وتزايد اعدادها خلال السنوات الماضية، منها(44) :-

1. تأثير وصول القراصنة وامكانية الوصول إلى مليارات السجلات الشخصية، حيث تم اختراق (14 مليون سجل) يومياً خلال عام 2016. وأدى ذلك إلى سرقة ما مجموعه (1.4 مليار) سجل خلال فترة قصيرة من العام ذاته، أذ تشير التوقعات إلى أنه من المتوقع أن يسرق مجرمو الإنترنت ما يقدر بنحو (33 مليار سجل) في عام 2023. حيث وجب على المستخدمين عبر الإنترنت تنقيف أنفسهم حتى يتمكنوا من اتخاذ قرارات ذكية وتحديد المخاطر المحتملة.
2. ارتفاع استهداف اجهزة الهاتف المحمول، من خلال البرامج الضارة ذكر تقرير اعد عام 2017 والصادر عن Verizon أن (18%) من الأشخاص الذين نقروا على الروابط الخبيثة فعلوا ذلك على الأجهزة المحمولة"، وأن مستخدمي المحمول "أكثر عرضة للخداع " من المستخدمين على واجهات أخرى. هذا يعني أن واحداً من كل خمسة مستخدمين للهاتف المحمول ينقر على الروابط الخبيثة، وأن متاجر تطبيقات الأجهزة المحمولة التابعة لجهات خارجية استضافت (99.9%) من جميع البرامج الضارة للأجهزة المحمولة.(45)
3. النقر فوق الروابط المجهولة عن طريق رسائل البريد الإلكتروني، اذ تشير البيانات إلى أن مستخدماً واحداً من بين (14 مستخدماً) قد تم خداعه بالنقر فوق ارتباط البرامج الضارة وأن (25%) من هؤلاء أصبحوا ضحايا لهجمات في المستقبل.
4. يمكن لأي شخص أن يكون هدفاً، وعدم الاستثناء بين الافراد والشركات او القطاعات الحكومية والعسكرية والمالية هي الأكثر تعرضاً للخطر. اذ يتم مهاجمة شركات رجال الأعمال الأمريكية المتوسطة و الشركات المالية المتوسطة ملايين المرات سنوياً، مما دعا الحكومة الأمريكية ان تخصص ميزانية قدرها (13 مليار دولار) للأمن السيبراني في عام 2016 من

أجل الاستعداد للتعامل مع الهجمات والاستثمار في الحلول الوقائية. ورصد ميزانية تقدر بـ 20 (مليار) للامن السيبراني لعام 2025.⁽⁴⁶⁾

5. تزايد وظائف الأمن السيبراني، نتيجة لتزايد الهجمات وخرق البيانات* او المشاكل الجيو سياسية الناتجة عن طريق الجريمة السيبرانية أزداد الطلب على خبراء الأمن السيبراني بنسبة (192%) منذ ايلول 2016، وتم الإعلان عن (1.5 مليون) وظيفة حتى كانون اول 2018. وفي دول العالم يبحث أصحاب العمل عن مجموعة واسعة للغاية من مجموعات المهارات التي تناسب هذا الطلب المتزايد.

كما "تنتشر مخاطر الأمن السيبراني في كل مؤسسة ولا تكون دائماً تحت السيطرة المباشرة لتقنية المعلومات. يمضي قادة الأعمال قدماً في مبادراتهم التجارية الرقمية، ويقوم هؤلاء القادة باختيارات المخاطر المتعلقة بالتكنولوجيا كل يوم. كما تعد المخاطر الإلكترونية المتزايدة أمراً حقيقياً - وكذلك حلول أمان البيانات"، اذ تتعامل حكومة الولايات المتحدة مع التهديدات الإلكترونية على محمل الجد، ولكن يبدو أنها تتحرك ببطء شديد للتخفيف من حدتها. كشف مكتب الإدارة والميزانية بالبيت الأبيض أنه من بين (96) وكالة فيدرالية قام بتقييمها، كانت (74%) إما "معرضة للخطر" أو "عالية الخطورة" للهجمات الإلكترونية. كانوا بحاجة إلى تحسينات أمنية فورية. ومع ارتفاع مخاطر الجرائم الإلكترونية في العديد من البلدان الأوروبية، اقترحت Aimée Ravacon من شركة Specops Software ثلاث نصائح متميزة لتقليل مخاطر الهجمات وقد تم تطبيقها فعلياً في اغلب دول اوربا الغربية فكانت اقلها عرضة للمخاطر الالكترونية اذ بلغت نسبة ضئيلة جداً لا تتجاوز (0,01% - 0,04%) وكما تم ذكره فقد انخفضت نسبتها من عام 2007 الى 2017، فكانت السويد متصدرة الدول في انخفاض نسبة الجريمة الالكترونية كما تم بيانه في الجدول (2)، وتمثلت تلك النصائح في (47):-

1. توقف عن إعادة استخدام كلمات المرور. عندما تعيد استخدام كلمات المرور الخاصة بك، فأنت بذلك تفتح على الجريمة الإلكترونية لأن المهاجمين يستخدمون معلومات تسجيل الدخول الخاصة بك من موقع ما لاستهداف موقع آخر.

2. استخدم المصادقة متعددة العوامل. تقدم العديد من الخدمات عبر الإنترنت الآن مصادقة متعددة العوامل، لكن عدداً قليلاً جداً من الأشخاص يستفيدون من طبقة الأمان الإضافية هذه. تستغرق هذه الخطوة البسيطة دقيقة واحدة فقط ولكنها يمكن أن تحميك من الوقوع ضحية.

3. لا تتقر على روابط غريبة. تم تصميم رسائل البريد الإلكتروني للتصيد الاحتيالي لتبدو حقيقية ويمكن أن تبدو وكأنها واردة من أشخاص تعرفهم. لكن النقر على الروابط في رسالة بريد إلكتروني للتصيد الاحتيالي يمكن أن يفتح باباً خلفياً للمهاجم". (48)

وأصبحت ضرورة حماية تلك المؤسسات العامة والخاصة تناط الى اشخاص من ذوي الخبرة منها فريق Talos المتكون من (250) شخص يدرسون التهديدات الجديدة والناشئة وكذلك استراتيجيات الهجوم السيبراني. وهي تحدد مواطن الضعف الجديدة، وتتقيف الجمهور حول أهمية الأمن السيبراني، وتعزز موثوقية أدوات المصادر المفتوحة. إن عمل هؤلاء المتخصصين يجعل الإنترنت أكثر أماناً لكل مستخدم.

فإن سوق الأمن يدخل عصر الحرب السيبرانية، حيث سيتم تطبيق جميع أساليب وترسانات الأموال من الحكومة والمجالات الاستخباراتية وبدأت الدول بالفعل تطبيقها على حد سواء في مجال المنافسة بين مختلف المنظمات والشركات، وبالرغم من أن الفضاء الإلكتروني أثبتت فعاليته في مواجهة الهجمات وغيرها من التأثيرات المدمرة، إلا أن المهاجمين شعروا دائماً بالراحة أكثر من المدافعين. هذا يشير إلى أن مثل هذه القدرة على البقاء مبالغ فيها، وأن التأثير على الفضاء الإلكتروني او الفضاء السيبراني قد يكون أكثر ضرراً بمرور الوقت .

رابعاً: ضمان الامن السيبراني

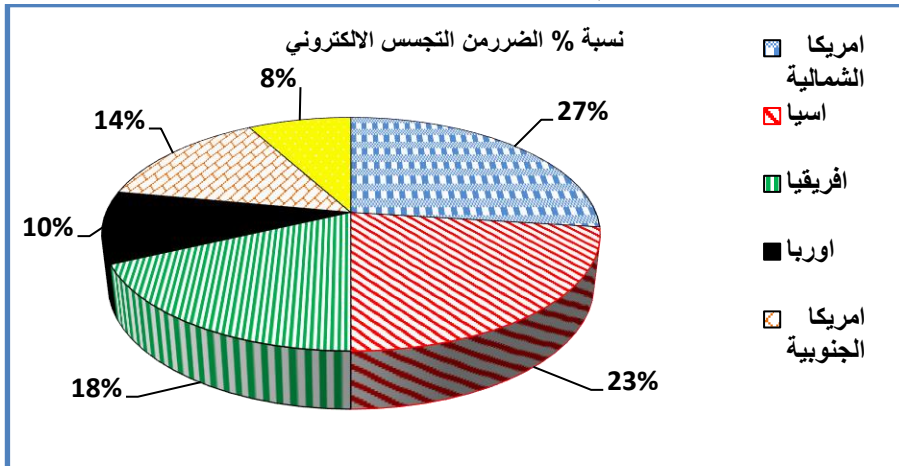
يعرف الهجوم الإلكتروني او الهجوم عبر الانترنت بأنه عمل خبيث ضد جهاز البيانات عبر شبكة عالم التحكم الآلي. يمكن أن يأتي الهجوم او التجسس السيبراني من أشخاص معزولين امثال "كيفن ميتنيك" ، الذي يعد من اشهر القراصنة، أو مجموعة من القراصنة، وفي الآونة الأخيرة عملت منظمات كبيرة ذات أهداف جيوسياسية على عمليات التجسس السيبرانية. (49) علماً أن تلك العمليات لم تعد حديثة عهد بل بدأت منذ عام 1982، (50) بعد ادخال المخابرات الامريكية خطأ في برمجيات إدارة خط أنابيب الغاز الكندي العابر لسيبيريا، مما تسبب في انفجار كبير في منطقة غير مأهولة. اذ لوحظ أن "التجسس عبر شبكات الكمبيوتر يمكن أن يكون فعالاً من حيث التكلفة، ويوفر نتائج فورية تقريباً ويستهدف مناطق معينة. ويشكل نسبة متباينة وفقاً لكل مستخدم لهذه الهجمات السيبرانية التي تمثل هجوماً اشبه بالهجوم البري او البحري او الجوي، وتشير ادواته الى أنه "عمل تطوعي، مسيء أو ضار، يتم إجراؤه عبر الفضاء الإلكتروني ويؤدي الى إتلاف المعلومات والأنظمة التي تعاملهم، وبالتالي القدرة على

ضرر بالأنشطة التي يدعمونها، ومن أجل ضمان الأمن السيبراني، يلزم بذل جهود منسقة عبر نظام المعلومات. تشمل:

- أمان التطبيق؛ أمن المعلومات وأمن الشبكات
- الأمن التشغيلي؛
- وعي المستخدم النهائي؛

أحد أكثر جوانب الأمن السيبراني إشكالية هو التطور المستمر والسريع للمخاطر الأمنية. كان النهج التقليدي هو تركيز معظم الموارد على مكونات النظام الهامة وحمايتها من التهديدات المعروفة الرئيسية. وهذا ينطوي على ترك بعض النظم الهامة بلا حماية والتخلي عن مكافحة بعض المخاطر الأقل أهمية. كما يحافظ الأمن السيبراني على سرية ونزاهة البيانات في الفضاء الإلكتروني. ويتضح أن جميع الدول تتعرض إلى أعمال أو عمليات تجسس إلكتروني يؤثر في الاقتصاد أو الأمن أو يلحق الضرر في الأجهزة الخاصة والشخصية، ويبين الشكل (7) نسبة الضرر الإلكتروني للدول وفقاً لقرارات العالم الأكثر تضرراً من قبل التجسس الإلكتروني إذ تنصدر أمريكا الشمالية المرتبة الأولى بعد أن بلغت نسبة الضرر السيبراني (27%)، فيما اتت القارة الآسيوية بالمرتبة الثانية بنسبة 23%، واتت القارة السمراء الأفريقية بنسبة 18%، اتت أوروبا بالمرتبة الرابعة 10%، أمريكا الجنوبية 8%، ثم استراليا بنسبة 14% (51).

شكل (7) نسبة الضرر السيبراني لقرارات العالم لعام 2017



الباحثة اعتماداً على

Cortada, James W. (November 6, 2007). The Digital Hand, Volume 3: How Computers Changed the Work of the American Public Sector Industries. USA: Oxford University Press

المبحث الثالث

الابعاد الجيو سياسية للجرائم السبرانية

اولاً: مخاطر الجريمة السبرانية

ثانياً: دوافع الجريمة السبرانية

ثالثاً: منشأ الهجمات السبرانية

رابعاً: تصنيف ومزايا الهجمات السبرانية

اولاً: مخاطر الجريمة السبرانية

عندما يكون الفضاء الإلكتروني مصدرًا أو أداة أو هدفًا أو مسرحًا للجريمة، تبرز مخاطر الهجمات الإلكترونية " او الجريمة السبرانية " وتكون اضرارها بأبعادها الجيو سياسية والجيو اجتماعية والجيو اقتصادية، ذات تأثير مباشر فى تدمير المستهدف. سواء كان الضرر مادياً او معنوياً.

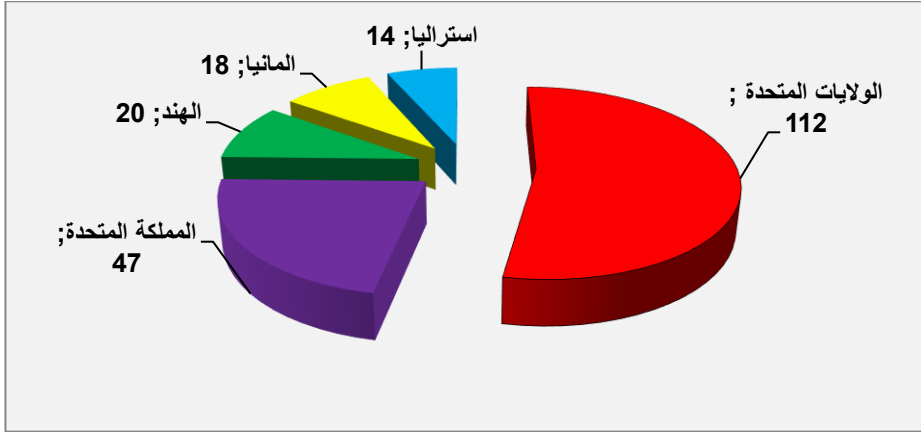
والذى سهل كثيراً للمتطفلين المحترفين بأرتكاب جرائم غير مرئية، سواء كانوا يعملون بمفردهم أو يعملون لدى الوكالات الحكومية أو الجيش، العثور على أنظمة كمبيوتر بها نقاط ضعف تغتر إلى برنامج الأمان المناسب. بمجرد العثور على هذه الثغرات الأمنية، يمكنها أن تصيب الأنظمة برمز خبيث ثم تتحكم عن بعد فى النظام أو الكمبيوتر عن طريق إرسال أوامر لعرض المحتوى أو لتعطيل أجهزة الكمبيوتر الأخرى. وهذا يعتمد على خلل فى النظام موجود مسبقاً داخل الكمبيوتر، مثل عدم وجود حماية ضد الفيروسات أو تكوين نظام معيب لكي يعمل الرمز الفيروسى بشكل صحيح ودقيق⁽⁵²⁾.

فأن الابتكار المستمر فى تكنولوجيا الاتصالات وزيادة فرص الاتصال فى الوقت الحقيقى دون حدود يجعل أمن الشبكة قضية معقدة عبر الوطنية. فمن الضرورى تقوية التعاون العالمى لضمان بيئة إنترنت آمنة. حيث قدرت شركة الأبحاث PWC ان حدوث 177,300 هجوماً إلكترونياً يومياً حول العالم. بعد ان ازدادت الجرائم الالكترونية بنسبة 66 ٪ سنوياً (فى المتوسط) وذلك عام 2007، فيما ارتفع عدد الجرائم بشكل كبير خلال عام 2014، مما تسبب فى (594 مليون)⁽⁵³⁾ ضحية بالغة فى جميع أنحاء العالم بمعدل (18 ضحية) بالغة فى الثانية، ومليون ونصف ضحية لجرائم الإنترنت يومياً للأشخاص. وفى عام 2017، بلغ

عدد الجرائم السيبرانية ما يقدر بنسبة (54 %) فضلاً عن ذلك، بلغ متوسط التكلفة السنوية للهجمات الإلكترونية (3.5) مليون دولار للعام ذاته.⁽⁵⁴⁾

وأصبحت جرائم الإنترنت الآن من الأعمال التجارية، حيث يتجاوز حجم الاحتيال عبر الإنترنت وسرقة الهوية وانتهاكات الملكية الفكرية وأعمال الفدية والتصيد ما يقدر بـ تريليون دولار سنوياً، مما يؤثر على ملايين الأشخاص حول العالم وعدد لا يحصى من الحكومات والشركات في مختلف البلدان. فهناك دولاً أصبحت عرضة للهجمات السيبرانية التي تأثرت بها مصالح اقتصادية وتم تعطيل بعض المصانع أو تأخير أعمال الشركات والمؤسسات المالية، وقد شهدت المملكة المتحدة وألمانيا والهند وأستراليا العديد من الهجمات الإلكترونية المهمة التي استهدفت الخدمات الحكومية والفيدرالية في السنوات الـ (10 الماضية)، ومع ذلك فإن وضعها كهدف يتضاءل مقارنةً بالولايات المتحدة، وفقاً لبحث جديد من Specops البرمجيات، حيث وقعت الولايات المتحدة ضحية لـ (112 هجوماً إلكترونياً منفصلاً) "هاماً" في الفترة ما بين تموز من عام 2007 وأيار من عام 2017. علماً أنها احتلت المرتبة الثانية في شنها الهجمات السيبرانية عام 2017، ومن أبرز الهجمات الكبيرة ((الاعتداءات على الوكالات الحكومية والإدارات الدفاعية وشركات التكنولوجيا الفائقة)) في الدولة، والتي تتميز بتنسيق هجمات أدت إلى خسائر اقتصادية تجاوزت المليون دولار، وهذا يعادل متوسط 9 هجمات إلكترونية هامة لا تحسد عليه يستهدف حكومتها أو البنى التحتية عالية القيمة كل عام. وللمقارنة مع سجلات الدول الأخرى، كانت الدولة الثانية في القائمة، انت المملكة المتحدة، هدفاً لـ (47 هجوماً) كبيراً في فترة الـ (10 أعوام) بين عامي 2007 - 2017،⁽⁵⁵⁾ فيما سجلت إحصاءات الهند وألمانيا وأستراليا (20 و 18 و 14) هجوماً على التوالي لم يقترب إجمالي الهجمات الإلكترونية خلال فترة العشر أعوام من إجمالي الهجمات التي تعرضت لها الولايات المتحدة، حيث سجلت في مجموعها (99)، هجوماً كبيراً شكل (8).

شكل (8) الهجمات السيبرانية الكبيرة التي تعرضت لها بعض الدول خلال المدة 2007-2017



Researcher acting on the source, Marina Magakia, 2019 , Cyber Security and Threat Policy: The United States' Efforts to Secure the Information Age. New York: Routledge, p468.

وهذا يؤكد ان الولايات المتحدة الامريكية من اكثر الدول عرضة للهجمات السيبرانية، ولا توجد دلائل على أن الهجمات الكبيرة على الوكالات الحكومية والأصول عالية القيمة ستوقف في أي وقت قريب. ومن ابرز الاحداث التي وقعت بها وأدت الأنشطة الضارة ضد أنظمة تكنولوجيا المعلومات إلى تعطيل قدرات الطاقة الكهربائية في الخارج. وقد أدى ذلك إلى انقطاع التيار الكهربائي لعدة مدن في مناطق متعددة. الحدث الثاني كان استغلال الخدمات المالية العالمية. في تشرين ثاني من عام 2008، كان لدى أحد البنوك الدولية معالج دفع مخترق يسمح بإجراء معاملات احتيالية في أكثر من (130 ماكينة صراف آلي) في (49 مدينة خلال 30 دقيقة). وكان الحدث الأخير هو الخسارة الشاملة للقيمة الاقتصادية للولايات المتحدة عندما قدرت الصناعة في عام 2008 خسائر بقيمة (1 تريليون دولار) في الملكية الفكرية لسرقة البيانات. أو حوالي (1.64٪) من الناتج المحلي الإجمالي العالمي. على الرغم من أن هذه الأرقام قديمة وتأتي من McAfee، وتمثل الشركة الثانية في العالم لبرامج مكافحة الفيروسات، إلا أنها تمثل معايير في هذا المجال، فأً 90٪ من الهجمات يتطلب تعاونًا دوليًا وموارد مالية كبيرة. وللقيام بذلك، يجب أن يؤدي الطموح السياسي للدول التعريف بالأمن السيبراني الوطني أو استراتيجيات الدفاع السيبراني إلى اتخاذ إجراءات واضحة ومتضافرة على

جميع مستويات صنع القرار - الوطنية والدولية والمحلية - لأن هذا الفضاء يشمل أنشطة أي فرد. المواطن وأي هيكل آخر، سواء كان عاما أو خاصا.⁽⁵⁶⁾

ففي شباط من عام 2014، وقعت المرافق الترفيهية في لاس فيجاس ساندز في الولايات المتحدة ضحية لهجوم سيبراني كبير بما في ذلك اختراق شبكة الكمبيوتر وسرقة البيانات الضخمة وإيقاف تشغيل جزء كبير من نظام المعلومات. وفي المملكة المتحدة اثرت الهجمات السيبرانية على عدد من المؤسسات منها في حزيران من عام 2012. حيث صرح رئيس دائرة الأمن في المملكة المتحدة أن شركة مسجلة في لندن فقدت ما يقدر ب(800 مليون جنيه إسترليني) أي ما يعادل (1.2 مليار دولار) نتيجة للهجمات الإلكترونية الحكومية. وفي نفس العام تعرضت الى حملة احتيال عالمية باستخدام إصدارات آلية من Zeus و SpyEye و Trojans، استهدفت الحسابات الشخصية والشركات عالية القيمة، وفي تشرين اول من عام 2010، ذكرت صحيفة وول ستريت جورنال أن المتسللين الذين يستخدمون برامج ضارة "زيوس"، متوفرة في الأسواق السوداء للجرائم الإلكترونية تقدر بحوالي (1200 دولار)، تمكنت من سرقة أكثر من (12 مليون دولار) من خمسة بنوك في الولايات المتحدة والمملكة المتحدة يستخدم زيوس روابط في رسائل البريد الإلكتروني لسرقة معلومات الحساب⁽⁵⁷⁾، والتي يستخدمها المتسللون بعد ذلك لتحويل الأموال إلى الحسابات المصرفية التي يسيطرون عليها، أو مجرمين منخفضي المستوى وتم القبض عليهم لفتح حسابات مصرفية بأسماء مستعارة نقل إليها المتسللون اموال مسروقة، وفي كانون ثاني من عام 2010. حذر جهاز الأمن MI5 في المملكة المتحدة من أن ضباط المخابرات السريين "من اتصال جيش التحرير الشعبي ووزارة الأمن العام في المملكة المتحدة برجال الأعمال في المعارض التجارية والمعارض مع عرض "هدايا" - كاميرات تحتوي على برامج ضارة توفر للصينيين إمكانية الوصول عن بُعد إلى أجهزة الكمبيوتر الخاصة بالمستخدمين".⁽⁵⁸⁾ وفي تشرين ثاني من عام 2008. اكتشفت الشرطة هجوم سلسلة التوريد متطورة للغاية حيث بطاقة الائتمان القراء المصنوعون في الصين والمستخدمون في المتاجر الكبرى في المملكة المتحدة لديهم جهاز لاسلكي تم إدخاله فيها يقوم الجهاز بنسخ بطاقة الائتمان عند إدخالها، وتخزين البيانات، ونقل البيانات التي جمعتها مرة واحدة يوميا عبر اتصال WiFi إلى لاهور في باكستان وتقدر الخسارة ب(50 مليون دولار) أو أكثر. ويمكن توجيه الجهاز لجمع أنواع معينة فقط من البطاقات (مثل البطاقات الذهبية)⁽⁵⁹⁾ . كما تعرضت الهند عام 2012. الى هجوم على شبكات الحكومة لأكثر من (10000) بريد

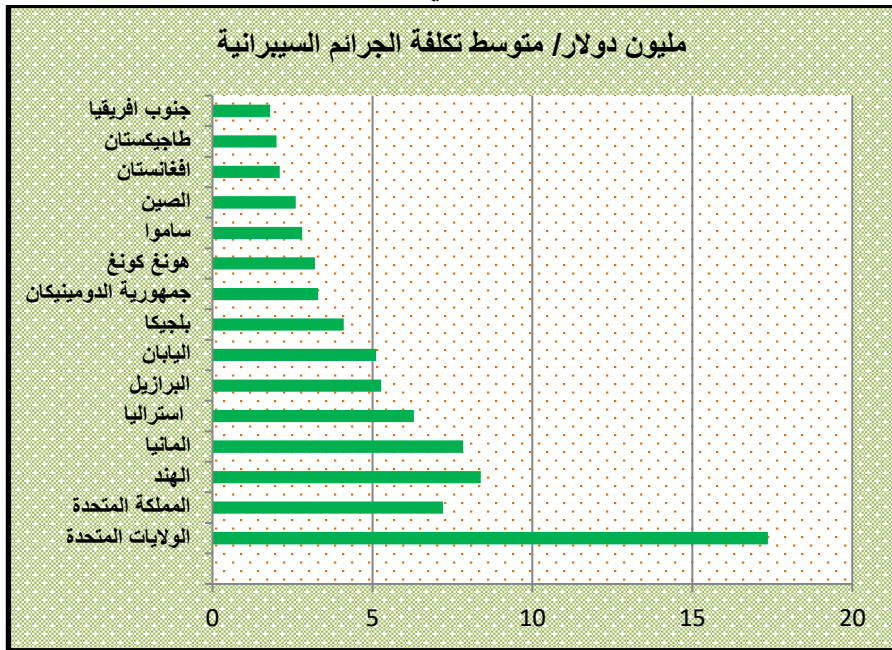
إلكتروني تم اختراق عناوين كبار المسؤولين في الحكومة الهندية، بما في ذلك المسؤولين منهم رئيس الوزراء مكتب الوزير، ووزارات الدفاع، والشؤون الخارجية، والداخلية، والمالية، وكذلك وكالة المخابرات الهندية، وفي كانون أول من عام 2010. تم اختراق موقع مكتب التحقيقات المركزي الهندي وبيانات (CBI)(cbi.nic.in) الحساسة، المخزونة على أجهزة الكمبيوتر ومحوها، علما ان الوصول اليها لم يكن سهلاً من خلال الانترنت، واتهمت الهند قرصنة باكستانيين، وفي عام 2008. توجهت اصابع الاتهام الى الصين حيث ذكرت صحيفة تايمز أوف إنديا أن مسؤولاً هندياً اتهم الصين بالاختراق أجهزة الكمبيوتر الحكومية. وكان جوهر الهجوم الصيني هو المسح ورسم خرائط لشبكات الهند الرسمية للوصول إلى المحتوى من أجل التخطيط لكيفية تعطيل الشبكات أثناء الصراعات الجيو سياسية العسكرية. وكان لألمانيا نصيب من الهجمات السيبرانية التي تعرضت لها، لاسيما عام 2014. تم اختراق قرصنة في أوروبا الشرقية قطاعات الطاقة في ألمانيا وعدد من الدول الأوروبية فضلاً عن الولايات المتحدة الأمريكية في حملة تجسس إلكتروني كبرى. وفي ايلول من عام 2014. قام مجرموا الانترنت باستخدام شهادة تم الحصول عليها عن طريق الاحتيال، وتمكنوا من الوصول إلى(300) من مواقع الويب الحكومية والشركات في ألمانيا والنمسا وسويسرا في عملية متعددة السنوات، ففي تشرين ثاني من عام 2014، تعرض المستشارون الماليون في شركات التعدين والموارد الطبيعية الاسترالية وما يرتبط بها من شركات قانونية لهجوم خلال مفاوضات تجارية حساسة، وفي ايلول من عام 2011، ذكرت إدارة إشارات الدفاع الاسترالية أن شبكات الدفاع تتعرض للهجوم بأكثر من (30 مرة) في اليوم، مع زيادة عدد الهجمات بأكثر من (350%) عما كانت عليه عام 2009، وفي عام 2010، أبلغت إدارة إشارات الدفاع الاسترالية عن زيادة هائلة في الهجمات الإلكترونية على الجيش، و كشف وزير الدفاع الأسترالي، جون فولكنر، عن وجود (2400 عنصر) من "حوادث الأمن الإلكتروني" على شبكات الدفاع عام 2009 وحوالي (5551) حادثة بين تموز واب عام 2010، تعرضت لها الحكومة الاسترالية، وفي عام 2013، تم اكتشاف متسلل صيني مزعوم يسرق المخططات الخاصة بمخابرات الأمن الاسترالية من مبنى المنظمة الجديد الذي قدر بـ (631 مليون دولار)، فضلاً عن مئات الهجمات السيبرانية الصغيرة ويبين لنا الجدول (4) والشكل (9) متوسط الكلفة المالية للجرائم التي تتعرض لها بعض الدول لعام 2017.⁽⁶⁰⁾

جدول (4) متوسط تكلفة الجرائم التي تعرضت لها الدول لعام 2017

ت	الدول	متوسط تكلفة الجرائم (مليون دولار)
1	الولايات المتحدة	17.36
2	المملكة المتحدة	7.21
3	الهند	8.39
4	المانيا	7.84
5	استراليا	6.3
6	البرازيل	5.27
7	اليابان	5.11
8	بلجيكا	4.1
9	جمهورية الدومينيكان	3.3
10	هونغ كونغ	3.2
11	ساموا	2.8
12	الصين	2.6
13	افغانستان	2.1
14	طاجيكستان	2
15	جنوب افريقيا	1.8

Source: Nazalt Sensen, 2019, Cybersecurity and its Impact on State Policy and Decision-making, Michkan, United States of America, Annual Cyber Monitor Reports, pp. 331-360.

شكل (9) متوسط تكلفة الجرائم التي تعرضت لها الدول لعام 2017



الباحثة : اعتماداً على الجدول (4)

ثانياً: دوافع الجريمة السيبرانية

ومن خلال التقرير السنوي الذي يصدر عن طريق Cybersecurity Ventures *، برعاية مجموعة Herjavec **، المتخصص بالجرائم الالكترونية لعام 2017، ذكر بأن الجريمة السيبرانية واحدة من أكبر المشكلات التي تواجه الدول او المؤسسات او الافراد ومن المتوقع بأن تلك الجرائم ستكلف العالم أكثر من (6 تريليونات دولار) سنوياً بحلول عام 2021، ارتفاعاً من 3 تريليونات دولار في عام 2015. ⁽⁶¹⁾ ويضيف التقرير أيضاً أن هذا يمثل أكبر تحويل للثروة الاقتصادية في التاريخ؛ لكونها تهدد الحوافز للابتكار والاستثمار، وستكون أكثر ربحية من التجارة العالمية لجميع المخدرات غير المشروعة الرئيسية مجتمعة. وقد سجل خبراء شركة Technologies بأن خطر الجريمة السيبرانية التي تعرضت لها (26 دولة) حول العالم عام 2017. قدرت نسبة الحوادث التي عرفت لدى الجمهور بـ (49%)، فيما بقي (51%) من

تلك الجرائم غير معروف. ويتم التعبير عن الضرر في انخفاض في الممتلكات أو في خسارة الدخل التي كان من الممكن الحصول عليها في حالة عدم وجود انتهاك (الربح المفقود)⁽⁶²⁾ قد يكون الضرر مادياً وقد يحدث للمالك أو للطرف المقابل، وأحياناً تكون الأضرار معنوية، أو خسارة جسدية، أو سمعة تجارية ضارة، ومنها أضرار بيئية، أو اجتماعية، وما إلى ذلك؛ ولابد من الحفاظ على بيئة المعلومات والتي تمثل مجموعة من الأجهزة والبرامج لتخزين ومعالجة ونقل المعلومات، وكذلك شروط تنفيذ عمليات المعلوماتية. والجريمة السيبرانية تكون على نوعين:

- النوع الأول: حيث تبرز الجريمة في اتساع انتشارها وسرعة زوالها (مثال ذلك دودة موريس، التي عطلت حوالي 10 ٪ من الإنترنت المبكر)؛
- النوع الثاني: وهو مركز للغاية يستغرق وقتاً طويلاً (مثل الهجوم على البرنامج النووي الإيراني).

وتتباين أهداف ودوافع التجسس السيبراني لدى المجرمين بين الدول جدول(5) كما يأتي:

جدول(5) الدوافع من وراء الجريمة السيبرانية

ت	النسبة المئوية	الدافع
1	71	المكسب المالي المادي
2	20	التجسس السيبراني
3	6	التطفل ا رهاب الكمبيوتر
4	3	الضرر بالمصالح السياسية

Source: Gooden, Dan (May 21, 2013). "China's hackers who breach Google Word are targeting confidential data." Ars Technica. Retrieved November 8, 2014.

ثالثاً: منشأ الهجمات السيبرانية

تستمر المخاطر التي تتعرض لها شبكات الإنترنت في التزايد لسبب وجيه وهو مهاجمة الفضاء الإلكتروني أسهل من عمليات الهجوم والدفاع التي تتم دون ذلك. تطورت هذه الديناميكيات تاريخياً لإيجاد السبل أو التقنيات التي من شأنها حماية تلك الشبكات من القرصنة أو الاختراق⁽⁶³⁾، للحفاظ على كل عقدة في الشبكة، وغلق جميع الاتصالات عند الانتهاء من العمليات الفاعلة الا ان المهاجم يبحث عن فجوة واحدة فقط في كل مرة لتحقيق هجوم ناجح، بينما يجب على المدافع إغلاق جميع النقاط الحساسة باستمرار*. ويبين الجدول(6) اعلى

الدول التي تمثل منشأ للهجمات الالكترونية السيبرانية عام 2014 و عام 2017، حيث تصدرت الصين بأنها البلد الاول في قيامها بأعمال التجسس الالكتروني والتصيد والاحتتيال وغيرها من العمليات السيبرانية وان انخفضت نسبتها من عام 2014 بعد ان كانت تبلغ (42%)، الى (20.56%) عام 2017، وقد احتلت الولايات المتحدة المرتبة الثانية بنسبة بلغت (15.08%)، وكما تراجع تايوان عام 2017، ظهرت روسيا بالمرتبة الثالثة بنسبة (10.07%)، كما ظهرت المملكة المتحدة بنسبة 8%، وهذه النسبة تمثل قفزة كبيرة في شنها الهجمات السيبرانية على الدول، بعد ان سجلت عام 2014 نسبة (1.1%)، و فرنسا بالمرتبة الخامسة بنسبة (7%)، تراجع الهند الى المرتبة الحادية عشر بنسبة (1%)، وظهر تأثير تراجعها في عام 2017 حيث احتلت المرتبة الاولى بين الدول الاكثر تعرضاً لبرامج دفع الفدية، كما احتلت ايران المرتبة السادسة عام 2017، للهجمات السيبرانية حيث بلغت نسبتها (3.3%)، وبعد ان كانت اندونيسيا تحتل المرتبة الثانية عام 2014 بنسبة (15%)⁽⁶⁴⁾ الا اننا لانجدها من الدول المتصدرة عام 2017، فضلاً عن تايوان وتركيا والبرازيل قد ضعف نشاطها السيبراني جداً ولم تظهر من الدول المتصدرة في عام 2017.

ت	الدولة	النسبة % من الهجمات 2014	ت	الدولة	النسبة % من الهجمات 2017
1	الصين	42	1	الصين	20.56
2	اندونيسيا	15	2	الولايات المتحدة	15.08
3	الولايات المتحدة	13	3	روسيا	10.07
4	تايلوان	3.7	4	المملكة المتحدة	8
5	الهند	2.1	5	فرنسا	7
6	روسيا	2	6	كوريا	4
7	البرازيل	1.7	7	ايران	3.3
8	ايران	1.6	8	سنغافورة	3
9	كوريا	1.4	9	اليابان	3
10	تركيا	1.4	10	فيتنام	3.06
11	المملكة المتحدة	1.1	11	المانيا	2.37
12	المانيا	1	12	الهند	1
13	دول اخرى	14	13	دول اخرى	19.56

Source: Nazalt Sensen, 2019, Cybersecurity and its Impact on State Policy and Decision-making, Michkan, United States of America, Annual Cyber Monitor Reports, pp. 331-360.

رابعاً: مزايا الهجمات السيبرانية

لا شك أن هناك مزايا رئيسية ستجذب قوى المجرمين والحكومات والمتسللين والأنشطة والإرهابيين للاستمرار في متابعة أدوات الهجوم السيبراني كجزء من جدول أعمالهم، مما يجعل الكثيرين عرضة للاستغلال أو ما هو أسوأ. سواء وافق المجتمع أو السياسيون أو الجيش أم لا على أن الحرب السيبرانية الحقيقية ستحدث في المستقبل، أو الإرهاب السيبراني سوف يكون هو الهاجس الأكبر للدول في كيفية الخلاص والتصدي له، إذ تمتلك الهجمات السيبرانية مزايا فريدة منها:- (65)

أ- أن الهجوم السيبراني يمكن أن يكون انتقائياً ويتم التحكم في التداعيات. ومثال ذلك يمكن للهجوم السيبراني أن يستهدف اقتصاداً كاملاً للدول دون أن يدمر بالضرورة البنية التحتية الأساسية الحرجة أو يمكن استخدامه لاستهداف البنية التحتية للدولة جنباً إلى جنب مع اقتصادها.

ب- أن الهجوم السيبراني يمكن أن ينفذ في "شكل غير مؤلم تماماً" للإرهابي لأنه يمكن شن هجوم بضغطة زر، ولا يحتاج إلى نشر العديد من العناصر، يتمتع هذا التكتيك بمزايا واضحة من حيث التكلفة والرؤية. وقد تتم برمجة هجوم على "نقرة زر" في وقت معين أو فقط في حالة استيفاء شرط منطقي معين. وهذا يعزز كلاً من مرونة وفرصة الهجوم مع زيادة غطاء النجاح المحتمل.

ت- التكلفة المنخفضة للهجوم السيبراني: حيث "يمكن الحصول على الروبوتات الآلية التي تبلغ 21000 آلة مقابل بضعة آلاف من الدولارات فقط، ومع ذلك تتسبب في حدوث ضرر وتعطل بسهولة تبلغ قيمتها مئات المرات." هذا يلغي تكلفة الأسلحة التقليدية والمخاطر التشغيلية.

وهذه المزايا هي عوامل جذب ملموسة وحقيقية وحيوية لمرتكبي الإنترنت، إلى جانب الجهات الفاعلة الحكومية وغير الحكومية على حد سواء، يتم ترسيخها بشكل خاص من خلال حقيقة أنه لا يمكن للحكومات التنسيق بشكل فعال فيما بينها أو غالباً، حتى داخلياً حول طبيعة أمن الفضاء الإلكتروني. مع الارتفاع الكبير في التكنولوجيا، من المرجح أن يرى المزيد والمزيد من

الممثلين فوائد الهجمات السيبرانية في العالم السيبراني الجديد في المستقبل وهناك ركائز اساسية لاتستطع الدول من خلالها القضاء او محاربة مرتكبيها وتتمثل في⁽⁶⁶⁾ :-

1. صعوبة الإسناد : الإسناد مشكلة رئيسية في الفضاء الإلكتروني. يمكن للمهاجمين تسوية الخوادم في أي جزء من العالم. ويمكنهم قصر أنشطتهم على يوم العمل في أي منطقة جغرافية. كما يمكنهم تحريك الكود باللغات الأجنبية. ويمكنهم إعادة استخدام مقتطفات الشفرة المستخدمة أولاً من قبل مجموعات اختراق مختلفة. يتم استخدام مثل هذا الاتجاه الخاطئ في (الأعلام الكاذبة) من قبل كل من ممثلي الدولة القومية ومجرمي الإنترنت.

2. سياسة الإنكار: عندما يكون من المستحيل إثبات الجاني علناً، يكون من السهل على المشتبه به أن ينكر ما قام به*.

3. التصعيد: نظراً لسهولة ونجاح هجمات الحرب الإلكترونية، فمن الطبيعي أن نرى تصعيداً في استخدامها. في المجالات السياسية والدبلوماسية والتجارية والعسكرية والبنية التحتية الحيوية ووسائل التواصل الاجتماعي. "الا ان التركيز بشكل عام في البداية كان ينصب على القرصنة المجهولة، وبعد قيام تلك القرصنة المجهولة بأختراق الحسابات الكترونية وسحب كل ما تجده مناسب وضروري للاشهار او التجسس على المنظمات بتشويهه و إنزال مواقع الويب الخاصة بالمنظمات أو الشركات التي اعترضت عليها* . يبدأ وجه الاتهام والتصعيد لجهات فاعلة او غير فاعلة.

أن تطبيق القانون والأمن السيبراني غير كافيين لحماية حدود الدولة الإلكترونية من هذا النوع من الهجمات. قد يتم إحباط هجوم DDoS من خلال ترقية الجدران النارية حتى الآن لا توجد دولة، باستثناء نظام شمولي للغاية، لديه حالياً السلطة القانونية لطلب مزودي خدمات الإنترنت، وشركات الاتصالات وغيرها من الشركات عبر الإنترنت لاتخاذ تدابير وقائية مثل تثبيت جدران الحماية، مما يجعل البلد عرضة للإنترنت الإرهاب.

رابعاً: دور المجتمع الدولي في الامن السيبراني

في تنسيق جهود المجتمع الدولي بشأن الأمن السيبراني كان للاتفاقية الأوروبية بشأن الجريمة السيبرانية، التي اعتمدها مجلس أوروبا في 23 تشرين ثاني من عام 2001 تم توقيعها في بودابست، والتي تحتوي على تصنيف لجرائم الكمبيوتر، والتوصيات المقدمة إلى السلطات التشريعية والتنفيذية للدول بشأن مكافحة الجريمة السيبرانية .

لاحظ أن هذه الاتفاقية تم توقيعها من قبل 39 دولة من دول الاتحاد الأوروبي، وكذلك الولايات المتحدة الأمريكية وكندا واليابان وجنوب إفريقيا. دخلت الاتفاقية حيز التنفيذ في 1 يوليو 2004، وهي حتى الآن الآلية الدولية الوحيدة الملزمة قانوناً في مجال الأمن السيبراني، وهي عبارة عن مجموعة من المبادئ الأساسية لأي دولة لتنظيم وتعزيز حماية الفضاء الإلكتروني، وتشكيل وتطوير التشريعات الوطنية وسياسات الدولة للحد من الجريمة السيبرانية والأمن السيبراني في البلاد. وكما لاحظنا من خلال ما طرح ان دول اوربا الاقل تعرضاً عن بقية دول العالم للجرائم السيبرانية. ومن العناصر الرئيسية للأمن السيبراني في العالم هي:-

1. حماية قنوات نقل البيانات من الضروري ضمان أمن موارد حزمة الإنترنت، وأمن الشبكات المفتوحة والعامّة وبيانات المستخدم.
2. حماية البنى التحتية للاتصالات السلكية واللاسلكية يلزم التحسين المستمر للبنية التحتية لشبكات الاتصالات: الهواتف المحمولة والاتصالات الساتلية وشبكات البث الأخرى وأجهزة الميكروويف.
3. الأمن حماية الفضاء المكون العالمي
4. حماية أجهزة الكمبيوتر ضمان أمن الخوادم وأجهزة الكمبيوتر من المستخدمين النهائيين من كسر المتسللين والمتطفلين، حل مشكلة موثوقية مكافحة الفيروسات وغيرها من وسائل مكافحة العناصر الضارة.
5. حماية التطبيقات لزيادة كفاءة وموثوقية تطبيقات الإنترنت، وخاصة البريد الإلكتروني، لحل مشكلات الأمان المتعلقة بحماية البريد الإلكتروني من الرسائل غير المرغوب فيها وغيرها من الإجراءات غير القانونية لموضوعات الفضاء.
6. حماية البيانات توفير حماية شاملة لبيانات المشاركين في الفضاء السيبراني - القانوني والتقني والاجتماعي، إلخ، للحفاظ على السرية.
7. حماية الخدمات الأساسية ضمان أمن الخدمات الأساسية في الفضاء الإلكتروني، وفعالية شبكات البيانات وتشغيل الخدمات الهامة.
8. حماية هوية المواطنين: لضمان صحة مستخدمي الإنترنت، وتنظيم العمل على مبادئ الثقة والإدارة الآمنة للبيانات الشخصية، ونظام موثوق به لحماية البيانات الشخصية والجوانب القانونية والسرية.

9. حماية مصالح الدولة - وضع وتنفيذ آليات وخطط عمل في الفضاء الإلكتروني لحماية مصالح الدولة.
10. حماية المصالح الوطنية: ضمان المصالح الوطنية في شبكة الإنترنت العالمية ككل في الفضاء الإلكتروني مع آليات الاستجابة السريعة.
11. حماية المصالح الإقليمية - تنسيق الجوانب الإقليمية وقضايا الأمن السيبراني.
12. حماية المصالح الدولية - المشاركة بنشاط في المساهمة في تحسين فعالية نظام الأمن السيبراني في العالم، إلخ.

الاستنتاجات

1. نظرًا إلى التهديدات البروتينية والمنتشرة في العديد من الدول والتي يصعب تحديدها، أدت إلى خسائر كبيرة منها قرصنة البنوك ومنها إيقاف البرامج الاستراتيجية في الجانب العسكري والتسلح النووي.
2. نتيجة التطور في مجال الأمن السيبراني أصبحت الحروب أكثر تطوراً وأقل خسارة كما كانت عليه في جيلها الأول والثاني والثالث واستخدامها إلى الأسلحة الحربية والنارية، بل أصبحت الحروب الإلكترونية شائعة.
3. لن تقتصر الهجمات السيبرانية على الدول أو المؤسسات الكبيرة أو البنوك والشركات العامة والخاصة بل أصبح التعرض إلى البيانات الشخصية للأفراد من خلال الأجهزة النقالة أو الموبايل أو جهاز الحاسوب الخاص أكثر عرضة للهجمات من خلال البرامج الخبيثة وتؤدي إلى العديد من المشاكل ودفع HGTJDM والتهديد إلى آخره.
4. ان تطور الأنشطة والممارسات في الفضاء الإلكتروني. ساهمت في تكثيف جهود التعاون الدولي والوطني لزيادة فرص تحقيق الهدف المتمثل في تأمين نظم المعلومات التي تعتبر ضرورية.
5. أدى الطموح السياسي للدول في تحديد استراتيجيات الأمن السيبراني والدفاع السيبراني إلى اتخاذ إجراءات واضحة ومتضافرة على جميع مستويات صنع القرار (المحلي والوطني والدولي)، حيث يشمل الفضاء السيبراني أنشطة الجميع الفردية وأي هيكل، سواء كانت عامة أو خاصة.

المقترحات :

1. يجب أن يكون البحث والتعاون الدولي وتبادل المعلومات متميزين. ينبغي تعزيز تقنيات التعرف على المهاجمين وإثبات الاكتشاف وإمكانية التتبع لضمان حماية أفضل للفضاء الإلكتروني.
2. في ظل هذه الظروف، يلزم مراجعة تفصيلية وتحديد العوامل والأسباب الرئيسية التي تدفع هجمات المتسللين إلى تطوير آليات جديدة وأكثر فعالية وأكثر عملية في مكافحة المتسللين والمهاجمين وآفات بيئة الفضاء الإلكتروني والبنية التحتية. علاوة على ذلك، في سياق العولمة والتوسع السريع في جغرافية هجمات القراصنة، والأفعال الإجرامية لمجرمي الإنترنت والمهاجمين، من الضروري تنسيق وتعبئة الموارد العقلية والفكرية والعلمية والبشرية ضد مكافحة الجرائم السيبرانية في جميع أنحاء العالم. يجب أن تكون جميع هذه العناصر والآليات والمكونات فعالة وكافية للمشاكل اليومية الناتجة في الفضاء الإلكتروني.
3. ينبغي أن تتخذ كل دولة تدابير لتعليم مواطنيها الوعي بالأمن السيبراني، فضلاً عن مواءمة أنشطة إدارة المخاطر وتكنولوجيا المعلومات وتنظيم المؤسسات الخاصة والعامة من أجل الامتثال.
4. ينبغي أن تتعاون البلدان مع بعضها البعض من أجل الحصول على فضاء آمن عبر الإنترنت والسماح بالطلبات المشروعة لتسليم المجرمين الموجودين في الخارج.
5. يجب على المؤسسات والأوساط الأكاديمية والرابطات الصناعية مثل ISACA بناء وصيانة الموارد البشرية الماهرة في مجال الأمن السيبراني.
6. ينبغي أن تبني البلدان قدرات قوية في مجال الكشف والردع في الفضاء الإلكتروني، فضلاً عن وجود آلية قوية للاستجابة للحوادث.
7. يجب أن تتبع الشركات إطار NIST للأمن السيبراني وإرشادات ISACA لتقييم أفضل الممارسات.

8. أخيرًا، ينبغي لجميع البلدان أن تشجع حرية الإنترنت وتتبع نموذجًا متعدد أصحاب المصلحة للحكومة، فضلاً عن تعزيز البنية التحتية للاتصالات القابلة للتشغيل المتبادل والموثوق بها والاتصال بالإنترنت. سيؤدي ذلك إلى اقتصاد قوي للمعلومات والمعرفة، والذي بدوره سيؤدي إلى اقتصاد عالمي مزدهر.

الهوامش:

- 1- Carlos Exk, 2017, The World Evolves, Copenhagen, translation, Raffi Adorard, 2018, p. 339.
- 2- Christian Agrum, 2010 Words for Understanding Cyber Security: Enjoying a Calm Internet, Editions, October 1, 2010, p. 217.
- 3 - Carlos Exk, 2017, previous source, p. 342.
- 4 - Carlos Exek, 2017, The World Evolves, Previous source, P.418..
- 5- Myriam Kimner and Jean-Paul Bente, Cyber Security for Economic Actors: Legal and Legal Risks and Responses, Hermes Scientific Publications, coll. "Cybercrime and Cybercrime," 13 December 2012, p. 21.
- 6- Christian Agrum, 2010, previous source, p. 220
- 7- Daniel Venter, 2017, "A Future and Strategic Study - Changes in Cybersecurity: Factors Constraints, and Variables," Naples, p. 175.
- 8- S. Helmreich, 2000، "الإصابات المرنة: فيروسات الكمبيوتر، الأجسام البشرية، الدول القومية، الرأسمالية التطورية"، العلوم والتكنولوجيا، والقيم الإنسانية، المجلد 25، <http://dx.doi.org/10.1177/016224390002500404> العدد 4، ص 472-491.
- 9 - Myriam Kimner and Jean-Paul Bente, Cyber Security for Economic Actors, Previous source, p.43
- 10 - Daniel Venter, 2017, previous source, p. 179.
- 11 للاتحاد الدولي للاتصالات ITU-T X.1205 - وتعرف التوصية
- 12 -Christian Agrum, previous source, p. 280.
- 13- Gooden, Dan (September 25, 2012). "The Trade Group reveals 100,000 passwords for Google and Apple engineers." Ars Technica.

Retrieved November 8, 2014. -

https://en.wikipedia.org/wiki/List_of_cyberattacks

¹⁴- <https://cyberleninka.ru/article/n/kiberbezopasnost-kak-osnovnoy-faktor-natsionalnoy-i-mezhdunarodnoy-bezopasnosti-hh-veka-chast-1>

¹⁵ - Christian Agrum, previous source, p. 282.

¹⁶ - Ravikumar Ramachandrani, 2018, considered cybersecurity and its crucial role in the global economy, Cambridge, London, 2018, p. 44.

¹⁷ - Daniel Venter, 2017, previous source, p. 186.

¹⁸ - Daniel Venter, "A Future Study and Strategy of Changes in Cybersecurity: Factors Constraints, and Variables" on defense.gouv.fr, June 2015. Framework for Improving Vital Cybersecurity Infrastructure, Air Force, Center for Strategic Aerospace Studies, Ministry of Defense Reflections On cyberspace, 2015, 33rd.

¹⁹ - Ravikumar Ramachandrani, 2018, previous source, p. 51.

²⁰ - Daniel Venter, 2017, previous source, p. 190.

²¹ - <https://statesassembly.gov.je/assemblyreports/2017/r.124-2017.pdf>, p.2-3.

²²- Ignatius, David (2017). "Russia's New Radical Strategy for Information War." Washington Post. 2017, p. 316.

²³- Ravikumar Ramachandrani, 2018, previous source, p. 67.

²⁴ - Daniel Venter, 2017, previous source, p126.

²⁵- Yaner Bendrath, 2010. "Debating Electronic Warfare: Perception and Policy in Protecting Critical Infrastructure in the United States," Information and Security, Volume 7, pages 65-73.

²⁶- A. mbtsquet, 2016 Network Warfare "The Internet" New York: Columbia University Press.p. 118

²⁷- Ignatius, David (2017). Previous source,p.183.

²⁸- [https://akhbarelyom.com/news/newdetails/2912272/1/-](https://akhbarelyom.com/news/newdetails/2912272/1/)

²⁹ - Yaner Bendrath, 2010. Previous source,p.97.

³⁰- Cebrowski and J. Garstka, 2013. "Grid-Centered Warfare: Its Origin and Future," Proceedings of the American Naval Institute, Vol. 124, No. 1, p. 78.

³¹- Ignatius, David (2017). Previous source,p190.

- ³².- Ernst, Delly, 2018, Previous source,p. 148.
- ³³- A. mbtsquet, 2016, , Previous source,p. 97.
- ³⁴- A. mbtsquet, 2016, , Previous source,p.102.
- ³⁵ - Ernst, Delly, 2018, Electronic Information Warfare, China, Hong Kong, translated by Serzy Pardo, 2019, p201.
- ³⁶ - Ignatius, David (2017). Previous source,p.110.
- ³⁷- Ernst, Delly, 2018, Previous source,p.153.
- ³⁸- A. mbtsquet, 2016 Network Warfare "The Internet" New York: Columbia University Press, pp. 96-114.
- ³⁹- Ernst, Delly, 2018, Previous source,p 88.
- ⁴⁰- Cebrowski and J. Garstka, 2013. Previous source, p. 91.
- ⁴¹- Friedman, 2018, The Evolution of Cybersecurity. Second Edition. New York: St. Martin's Press, p. 48.
- ⁴²- Friedman, 2018 ,Same source, p.96.
- ⁴³ - Ernst, Delly, 2018, Previous source,p 109.
- ⁴⁴ - Uncle Pattashi, 2019, cybercrime in European and American countries and the ranges of profitability expansion, translation removed by Badush, New York, p. 469
- ⁴⁵ - Friedman, 2018, Previous source,p 90.
- ⁴⁶ - Friedman, 2018, Previous source,p.98.
- * - يبلغ متوسط تكلفة خرق البيانات لشركة في ج5مئيع أنحاء العالم 3.86 مليون دولار. كما ان متوسط الوقت الذي يستغرقه تحديد خرق البيانات هو 196 يومًا.
- ⁴⁷- M. Cooper, 2006 "ظهور الإجهاض الوقائي : المنعطف البيولوجي في الحرب على الإرهاب"، النظرية والثقافة والمجتمع، المجلد 23، العدد 4، الصفحات 113-135. <http://dx.doi.org/10.1177/0263276406065121>
- ⁴⁸- Cebrowski and J. Garstka, 2013. Previous source, p. 93.
- * - مستشار أمن الحاسوب، يهودي أمريكي، من أكبر الهاكرز في العالم، وهو أحد أشهر مخترقي الأنظمة. تم اعتقاله لأول مرة من قبل مكتب التحقيقات الفدرالي الأمريكي في 15 شباط/ فبراير 1995. تم تجريمه بالتلاعب الإلكتروني واختراق أنظمة الحاسوب لدى كل من فوجيتسو وموتورولا ونوكيا وصن مايكر وسيستمز.
- ⁴⁹ - Cortada, James W. (November 6, 2007). The Digital Hand, Volume 3: How Computers Changed the Work of the American Public Sector Industries. USA: Oxford University Press.

Foreign sources

- ⁵⁰ - Ignatius, David (2017). Previous source, P. 330.
- ⁵¹ - Marina Magakia, 2019, Cybersecurity and Threat Policy: U.S. Efforts to Secure the Information Age. New York: Routledge, pp. 441-448.
- ⁵² - <https://en.wikipedia.org/wiki/Cyberattack>
- ⁵³ - Stephen Lyman, Angelo, "Crime as a Commercial-CIAL Cyberspace," in Criminality, 2009.p.82.
- ⁵⁴ - Marina Magakia, 2019, previous source, p. 460
- ⁵⁵ - Marina Magakia, 2019, previous source, p. 480
- ⁵⁶ - Marina Magakia, 2019, previous source, p. 469.
- ⁵⁷ - R. Clark, 2011. "China's Cyber Attack on America," The Wall Street Journal (June 15), at <http://online.wsj.com/article/SB10001424052702304259304576373391101828876.html>, accessed June 18, 2012.
- ⁵⁸ - R. Clark, 2011. Previous source, P.76.
- ⁵⁹ - Mastra Robot HW, 2018, China and Piracy, University of California, pp. 55-62.
- ⁶⁰ - Mastra Robot HW, 2018, Previous source, p.78.
- هو برنامج تسريع الأمن السيبراني الدولي الذي تنظمه Cybersecurity Ventures *
، من خلال معهد التنافسية Castilla y Leon بالتعاون مع الحكومة الإقليمية في INCIBE
León (ILDEFE.) ومعهد التنمية والتدريب والتوظيف في Castilla y León التجارية في
- ** - وهي شركة تكامل كندية لبرامج أمان الإنترنت، الآن واحدة من أكبر شركات تكنولوجيا
عام 2003. Herjavec المعلومات وأمن الكمبيوتر في كندا، تأسست مجموعة
- ⁶¹ - Arkan Adam, 2017, "Cybersecurity and its Impact on Economy and Politics," Rome, Hasora Nerni translation, p. 338.
- ⁶² - Susan Nana, Samara Johnny, 2018, previous source, p. 421.
- ⁶³ - Gooden, Dan (May 21, 2013). "China's hackers who breach Google Word are targeting confidential data." Ars Technica. Retrieved November 8, 2014.
- * - تجتذب العديد من الشركات أو تحتفظ ب "فريق أحمر" - مجموعة من المتخصصين
المشاركين في اختبارات الاختراق.

⁶⁴ - Gooden, Dan (May 21, 2013). Previous source

⁶⁵ - Warwick Ashford, Previous source.

⁶⁶ - T. Gjeltén، 2010، "مد قانون الحرب ليشمل الفضاء الإلكتروني"،

<http://www.npr.org/templates/story/story.php?storyId=130023318> ،

بالرجوع إليه في 18 يونيو 2012.

* - ومثال ذلك الاتهام المتكرر لروسيا للتورط في الانتخابات الأمريكية عام 2016، والنفي الحازم بعدم الاشتراك بعمليات سيبرانية في الانتخابات الأمريكية أو تزويرها، بذكر فلاديمير بوتين أخيراً أنه كان يمكن أن يكون "قراصنة روسيين وطنيين".

* - تبع ذلك سلسلة من اختراقات حسابات وسائل التواصل الاجتماعي من قبل الجيش السوري (، الذي استخدم الحسابات لنشر وجهات النظر المؤيدة للأسد - وغالباً SEA الإلكتروني) ما يقال، من خلال استخدام الفكاهة. لقد تطور هذا الآن إلى صناعة "أخبار وهمية" كاملة وآلية. تحليلاً لهذه الصناعة. التلاعب بالناخبين متاح Trend Micro في يونيو 2017، نشرت "، يقوم بتسويق نفسه ليكون قادرًا على معالجة أي نظام Siguldin للسعر. يقول التقرير، "المصدر، IP تصويت تقريباً على الإنترنت وتجاوز عمليات التحقق من الأمان مثل عنوان ، وآليات المصادقة في وسائل التواصل الاجتماعي والرسائل النصية القصيرة Captcha والبريد الإلكتروني وكذلك على تسجيل الموقع من بين أمور أخرى. "