جـامعة قــاصدي مربـاح ورقلــة

كليــة الحقوق والعلـوم سياسية

قسم :العلوم السياسية

مذكرة تخرج مكملة في إطار متطلبات نيل شهادة الماستر في ميدان الحقوق والعلوم السياسية

شعبة: العلوم سياسية

تخصص: دراسات أمنية واستراتيجية

فعالية الأنظمة الأمنية الأمريكية في مواجهة التهديدات السيبرانية – دراسة حالة للهجوم على شركة SolarWinds "Sunburst Attack"

إعداد الطالب: كحلال محمد رفيق

اشراف الأستاذ: محمد خميس

أعضاء لجنة المناقشة:

الدكتور: عبد الكريم باسماعيل	رئيسـا
الدكتور: محمد خميس	مشرفا ومقررا
الأستاذ : حسين بهاز	مناقشا

السنــة الجامعية: 2021/2020

جـامعة قــاصدي مربـاح ورقلــة

كليــة الحقوق والعلـوم سياسية

قسم :العلوم السياسية

مذكرة تخرج مكملة في إطار متطلبات نيل شهادة الماستر في ميدان الحقوق والعلوم السياسية

شعبة: العلوم سياسية

تخصص: دراسات أمنية واستراتيجية

فعالية الأنظمة الأمنية الأمريكية في مواجهة التهديدات السيبرانية – دراسة حالة للهجوم على شركة SolarWinds "Sunburst Attack"

إعداد الطالب: كحلال محمد رفيق

اشراف الأستاذ: محمد خميس

أعضاء لجنة المناقشة:

الدكتور: عبد الكريم باسماعيل	رئيسـا
الدكتور: محمد خميس	مشرفا ومقررا
الأستاذ: بهاز حسين	مناقشا

السنــة الجامعية: 2021/2020

Acknowledgment

I would like to extend my deepest gratitude to my supervisor, Prof. Khemis Mohammed, for his unwavering support, passion, and immense expertise throughout the journey of my dissertation. His patience, rigorous guidance, and constructive insights have been instrumental in shaping my understanding and bringing this project to completion. I am profoundly grateful for his dedication and encouragement.

I am equally indebted to my family, whose unconditional love, unwavering encouragement, and constant reassurance have been my greatest source of strength and inspiration. Their support and belief in me have been profoundly motivating throughout this journey. Your encouragement has been instrumental in helping me reach this milestone.

الملخص:

تطرقت هذه الدراسة إلى موضوع فعالية الأنظمة الأمنية الأمريكية في مواجهة التهديدات السيبرانية، وهذا عبر التطرق إلى الإستراتجيات والقوانين التي أقرها الرئيس باراك أوباما خلال فترة حكمه، ووصولا الى الإستراتجيات التي نهجها خلفه دونالد ترامب، كما تم إبراز الجيهات الحكومية المكلفة بتنفيذ هذه الإستراتجيات لحماية الفضاء السيبراني داخل الولايات المتحدة من أي تهديدات.

وفي الفصل الثاني، تم التطرق الى دراسة حالة للهجوم السيبراني الذي إستهدف شركة سولارويندز الأمريكية المختصة في تطوير برامج إدارة الشبكات والأنظمة والبنيات التحتية لتكنولوجيا المعلومات، والتي تمتلك عملاء في العديد من دول العالم، في القطاع العام والخاص. الهجوم الذي استهدف عبره العديد من الوكالات الفيدرالية للحكومة الأمريكية، والشركات التكنولوجية الكبرى، والذي خلف موجهة من الردود خلال فترة الانتخابات الأمريكية الأخيرة، حول مدى فعالية السياسات السيبرانية المعمول بها والمنتهجة اتجاه الأمن السيبراني داخل البلاد. وقد مس الإختراق مجموعة واسعة من جيهات الحكومية داخل البلد، ومن أبرزها كان:

– وزارة الخزانة الأمريكية، الإدارة الوطنية للاتصالات والمعلومات، وزارة الخارجية، المعاهد الوطنية للصحة (جزء من وزارة الصحة الأمريكية) ، وزارة الأمن الداخلي (DHS) ، وزارة الطاقة (DOE) ، الإدارة الوطنية الأمريكية للأمن النووي (NNSA) ، بعض الولايات الأمريكية (ولايات معينة غير معلنة).

كما مس الإختراق العديد من الشركات الأمريكية التي تنشط في المجال التكنولوجي وكان من أبرزها:

– شركة FireEye و المختصة في الأمن الإلكتروني وكشف الهجمات السيبرانية، والتي كانت أول من إكتشف الإختراق ، شركة ميكروسوفت " Microsoft" ، وشركة شركة في إم وير VMware وهي شركة تقوم بتوفير برمجيات الحوسبة السحابية ومحكاة أنظمة التشغيل.

الكلمات المفتاحية:

الأمن السيبراني ، الهجومات السيبرانية ، سولارويندز ، الولايات المتحدة ، التهديدات السيبرانية ، الإختراق ، الإختراق السيبراني ، الهجمات الإلكترونية ، الهجمات الإلكترونية ، استراتيجيات الدفاع السيبراني ، إدارة المخاطر السيبرانية.

Abstract

This study touched on the issue of the effectiveness of American security systems in facing cyber threats, and this by addressing the strategies and laws that President Barack Obama approved during his tenure, and to the strategies pursued by his successor Donald Trump, as well as the government agencies in charge of implementing these strategies to protect cyberspace. Within the United States from any threats.

In the second chapter, a case study of the cyber attack that targeted the American company, SolarWinds, specialized in developing programs for managing networks, systems and information technology infrastructures, which has clients in many countries of the world, in the public and private sector, is covered. The attack, which targeted many federal agencies of the US government, and major technology companies, which left a wave of responses during the recent US election period about the effectiveness of the cyber policies in place and adopted towards cybersecurity within the country. The penetration affected a wide range of government agencies inside the country, the most prominent of which were:

- US Department of the Treasury, National Communications and Information Administration, State Department, National Institutes of Health (part of the US Department of Health), Department of Homeland Security (DHS), Department of Energy (DOE), US National Nuclear Security Administration (NNSA), some US states (Certain undeclared states).

The hack also affected many American companies that are active in the technology field, the most prominent of which were:

- FireEye, a company specialized in cybersecurity and cyber attack detection, which was the first to discover the hack, Microsoft, and VMware, a company that provides cloud computing software and simulating operating systems.

Key words: Cyber Security, Cyber Attacks, United States, Cyber Threats, SolarWinds. Cyber Risk Management, Cyber Defense Strategies, Hacking.

Résumé :

Cette étude a abordé la question de l'efficacité des systèmes de sécurité américains face aux cybermenaces, en examinant les stratégies et les lois approuvées par le président Barack Obama pendant son mandat, et en poursuivant avec les stratégies adoptées par son successeur, Donald Trump, mises en œuvre par les agences gouvernementales chargées de cette mission. La mise en œuvre de ces stratégies pour protéger le cyberespace aux États-Unis contre toute menace a également été soulignée.

Dans le deuxième chapitre, une étude de cas sur la cyberattaque qui a visé la société américaine SolarWinds, spécialisée dans le développement de programmes de gestion de réseaux, de systèmes et d'infrastructures informatiques, et qui a des clients dans de nombreux pays du monde, notamment dans les secteurs public et privé, a été discutée. L'attaque, qui a visé plusieurs agences fédérales du gouvernement américain et de grandes entreprises technologiques, a suscité une vague de réactions lors des récentes élections américaines, concernant l'efficacité des cyberpolitiques en place et l'orientation de la cybersécurité dans le pays. Le piratage a touché un large éventail d'agences gouvernementales du pays, dont les plus importantes étaient :

- Le Département du Trésor des États-Unis, la National Telecommunications and Information Administration, le Département d'État, les National Institutes of Health (qui font partie du Département américain de la Santé), le Département de la Sécurité intérieure (DHS), le Département de l'Énergie (DOE), l'Administration nationale de la sécurité nucléaire des États-Unis (NNSA), et certains États américains (certains États ne sont pas déclarés).

Le piratage a également touché de nombreuses entreprises américaines actives dans le domaine technologique, parmi lesquelles les plus importantes étaient :

- FireEye, société spécialisée dans la sécurité électronique et la détection des cyberattaques, qui a été la première à découvrir le hack, Microsoft, et VMware, société qui fournit des logiciels de cloud computing et d'émulation de systèmes d'exploitation.

Mots clés : Cybersécurité, Cyberattaque, SolarWinds, États-Unis, Menaces Cybernétiques, Piratage, Gestion Des Risques Cybersécurité, Cyberstratégie.

الفهرس

مقدمة

1) –تقديم الموضوع:

يحظى جانب الأمن بإختلاف تقسيماته و أنواعه بأهمية عالية لدى كل الأطراف والفواعل الدولية ، نظرا لما لكونه حاجة أساسية للمجتمع الإنساني ومؤشرا على الاستقرار و الإزدهار والتقدم الشعوب، ومع تطور الدول ومرور السنين ، تطور مفهوم الأمن وانسقم إلى العديد من المفاهيم والسياقات ليكتسب دقة أكثر بحسب المجال الذي يعرف من خلاله ووفق التهديدات التي يدرس من خلالها.

ومع تطور التكولوجي والتوجه الدول إلى تعميم الإستخدامات الإلكترونية ، تزايدت التهديدات و الهجومات السيبرانية بهدف التجسس على البيانات الحساسة للمؤسسات الحكومية و الشركات التي تزودها بتكنولوجيا و البرامج التي يتم استخدامها في تخزين وتبادل و جمع البيانات الحكومية ، ومن بين أبرز الهجومات السيبرانية التي شهدتها الولايات المتحدة في سنة 2020 ، كان الهجوم الذي إستهدف شركة سوولاروبندز SolarWinds، والتي من خلالها تم إختراق العديد من الشركات التكنولوجية الأمريكية و المؤسسات الحكومية الرسمية ، والتي كان من أبرزها وزارة الخزانة الأمريكية ، الإدارة الوطنية للاتصالات والمعلومات الأمريكية ، وزارة الخارجية الأمريكية، المعاهد الوطنية للصحة (جزء من وزارة الصحة الأمريكية) ، وزارة الأمن الداخلي الأمريكية (DHS) ، وزارة الطاقة الأمريكية (DOE) ، الإدارة الوطنية الأمريكية للأمن النووي (NNSA) ، بعض الولايات الأمريكية (ولايات معنية غير معلنة). إستغرق الإختراق الذي مس مراكز البيانات الأمريكية لأكثر من 9 أشهر بحسب التحقيقات التي أجريها الفريق المشترك الأمني للشركات والمؤسسات الحكومية المتضررة FireEye، Microsoft، Cisco، مكتب التحقيق الفيدرالي. خلص التحقيق على ان الهجوم تقف من وراءه دولة متمكنة في جانب الهجومات السيبرانية وتم ترجيح أن روسيا أو الصين هم من يقفوا وراء الهجمة.

وعلى الرغم من قيام الولايات المتحدة بتخصيص ميزانيات و إستراتجيات للحد من الهجومات السيبرانية ، إلا أن ذلك لم يكن فعال بدرجة مكتملة وهذا إلا غاية أواخر سنة 2020 ، وفي هذا السياق سيتم دراسة مثال للأنشطة العدائية التي تستهدف الولايات المتحدة وتأثيرها في الفواعل وبنية العلاقات التي تربطها بدول منافسة لها ، وهذا عن طريق استهداف لأمن البنية التحتية لمراكز تخزين المعلومات الأمريكية ، والإستراتجيات المعمول بها من قبل الولايات المتحدة للحد من هذه التهديدات وفعالية الأنظمة الأمنية الأمريكية في هذا الصدد ، و في أخير سيتم دراسة حالة الهجوم السيبراني الذي إستهدف شركة سوولاروبندز SolarWinds.

2) -أهمية ومبررات اختيار الموضوع:

تسعى هذه الدراسة إلى توضيح ما يلي:

أ- تهدف هذه الدراسة إلى تسليط الضوء على أحد أبرز المواضيع الحديثة على الساحة الدولية ، وهو الأمن السيبراني كونه أحد أبرز القضايا و ركائز الدراسات الإستراتجية و الأمنية التي تعمل الدول الكبرى على تمكن فيه و توفير بنيات معلوماتية محصنة و غير قابلة للإختراق وهذا مايضفي أهمية بالغة للدول الكبرى.

ب- تزايد أهمية جانب حماية الفضاء السيبراني الذي توليه الولايات المتحدة ، خصوصا مع تزايد التهديدات والإختراقات السيبرانية التي تستهدف المراكز تخزين البيانات الحساسة التابعة للأجهزة الأمنية والحكومية.

ت- التعرف على الأسباب والدوافع من وراء الهجومات السيبرانية التي تستهدف الولايات المتحدة.

ث- البحث في الإستراتجيات والخطط الإستباقية المنتهجة من طرف الولايات المتحدة للحد من تأثير التهديدات السيبرانية.

أسباب اختيار الموضوع

*أ- أسباب الذاتية:

- تزايد اهتمامي بالمواضيع المتعلقة بتكنولوجيا و الأمن و الحماية السيبرانية ، ورغبة مني لفهم أعمق لكيفية تنفيذ الهجومات السيبرانية و الثغرات الأمنية التي يتم إستغلالها لتنفيذ الإختراق.

- إهتمامي بما يجري في الساحة الدولية وما يحدث من تغيرات وتحولات على مستوى الإستراتجيات الأمنية للدول ، وخاصة ما تعمل عليه الولايات المتحدة الأمريكية في الجانب التكنولوجي و الأمن السيبراني.

- المساهمة في إثراء مكتبة الجامعة بعمل يتطرق إلى موضوع مستجد على الساحة الدولية ، نظرا للأهمية الأمن السيبراني العلمية و السياسية في مجال الدراسات الأمنية و الاستراتيجية.

***ب- أسباب الموضوعية:**

- السعي لتعمق و الفهم العلمي الموضوعي لكيفية توفير الحماية الأمنية من طرف الولايات المتحدة فيما يخص البيانات الحكومية و الإستراتجيات المعمول بها لتصدي للهجومات السيبرانية و الحد منها.

- تسليط الضوء على الثغرات الأمنية في البرامج و البرمجيات التي تستخدم من طرف الولايات المتحدة، والتي من خلالها يتم إيجاد ثغرات تأدي الإختراق و التجسس على البيانات والمراسلات الحساسة لدولة الأمريكية.

- تبيان حجم الخطر من وراء الإختراقات السيبرانية و ما قد ينجر عنها من إنعكاسات على العلاقات الدولية و أداء وسير المؤسسات الحكومية ، والإقتصادية.

- طبيعة تخصصنا في مجال الدراسات الأمنية و الإستراتجية يقتضي التعامل مع مثل هذه المواضيع لفهم أعمق لها.

3)- أهداف الدراسة:

تهدف هذه الدراسة الى ما يلي:

- تبيان أهمية الأمن و الحماية السيبرانية في سياسات والإستراتجيات القوى العظمى وهذا مع تزايد التهديدات و المخاطر التكنولوجية في الفضاء السيبراني.

- إبراز الإستراتجيات المعمول بها من قبل الولايات المتحدة لتصدي للهجومات السيبرانية و الحد من مخاطرها.

- تبيان أنواع التهديدات و الهجومات السيبرانية و كيفية العمل للحد منها.

- محاولة إبراز الجانب الأخر لتهديدات الحديثة التي تواجهها الولايات المتحدة الأمريكية.

4)- إشكالية الدراسة:

إن التطور التكنولوجي الذي يشهده العالم واستعمالاته المتزايدة في حياتنا اليومية أدى إلى اعتماد الولايات المتحدة الأمريكية إلى تعميم استعمال أنظمة التخزين المعلومات والبيانات ومبادلات المعلومات الحساسة للأفراد والمؤسسات الحكومية و هذا ما أدى إلى تحول هذه البيانات إلى هدف لدى جيهات ودول منافسة للولايات المتحدة مما ساهم في تنامي التهديدات والهجومات بغية تنفيذ الإختراقات السيبرانية تأدي إلى تسريب معلومات

سرية للمرسالات بين سياسيين و المؤسسات الحكومية الأمريكية ، وانطلاقا مما سبق نحاول في هذه الدراسة التعرض إلى النقاش الدائر حول فعالية الأنظمة الأمنية الأمريكية في التصدي و مواجهة هذه التهديدات السيبرانية ، وهذا بطرح الإشكالية التالية:

– ما مدى فعالية الإستراتجيات الأمنية المعتمدة من طرف الولايات المتحدة الأمريكية للتصدي للتهديدات و الهجومات و الإختراقات السيبرانية ؟

وبناء على هذه الإشكالية نطرح مجموعة من التساؤلات الفرعية:

– ماهي الإستراتجيات التي أقرتها الولايات المتحدة للحد من التهديدات التي تستهدف أمنها في الفضاء السيبراني ؟

– ما مدى فعالية الإستراتجيات الأمنية في الجانب السيبراني في إكتشاف ووقف الهجومات السيبرانية ؟

– هل البرامج المستخدمة من طرف المؤسسات الحكومية الأمريكية أمنة من التعرض لإختراقات ؟

– من هي الجيهات المسؤولة على تنفيذ الإستراتجيات الأمنية وحماية الفضاء السيبراني للولايات المتحدة ؟

– ما هي أبرز التحديات في جانب الأمن السيبراني التي تواجه الولايات المتحدة الأمريكية ؟

5) –<u>فرضيات الدراسة:</u>

– تشكل المكانة والقوة الولايات المتحدة هدفا وتحدي للدول المنافسة لها بهدف جمع البيانات عن طريق تنفيذ عمليات اختراق سيبرانية للتجسس على مسؤولون سياسيون و مراسلات حكومية السرية.

– بقدر ما كانت الإسترتجيات الأمنية الأمريكية في الجانب السيبراني متماسكة وصعبة الإختراق بقدر ما يشكل ذلك تحدي للجيهات التي تسعى الى تنفيذ الإختراقات السيبرانية.

– تنامي اعتماد الولايات المتحدة الأمركية للإستعمال مراكز تخزين البيانات و المعاملات الكترونية ، جعلها عرضة الهجومات السيبرانية.

– اعتماد المؤسسات الحكومية الأمريكية على استخدام برامج للأطراف ثالثة الممثلة في القطا ع الخاص ، مكن الهاكرز من إيجاد ثغرات تمكنهم اختراق البرامج الوصول الى البيانات الحكومية.

6) -أدبيات الدراسة:

حظى موضوع الأمن السيبراني والإستراتجيات التي تتبناها الدول في هذا السياق بإهتمام كبير من الدارسين و الباحثين في السنوات الأخيرة فالكثير منهم اهتموا بدراسة وتعمق في هذا الموضوع وقد تناولوا هذا الموضوع في العديد من الجوانب المتعددة منه، وفي ما يلي مجموعة من الدراسات التي لها علاقة بموضوع دراستنا بطريقة مباشرة أو غير مباشرة:

1- وثيقة تحت عنوان "**الأمن السيبراني: منهج مرجعي عام**" تم إعداد هذه الوثيقة بواسطة فريق متعدد الجنسيات من الأكاديميين و الممارسين ، وتهدف هذه الوثيقة الى تزويد حلف الناتو والدول الشريكة بالأهداف التعليمية المتعمقة والدعم المنهجي اللازم للدورات الأكاديمية الخاصة بالأمن السيبراني بوجه عام.[1]

2- دراسة جوزيف ناي "**Cyber Power القوة السيبرانية**" ، والتي تطرق فيها جوزيف ناي الى مفاهيم القوة و النمو السريع للفضاء السيبراني كسياق جديد مهم في السياسة العالمية، بحيث تطرق فيه لإنخفاض تكلفة الدخول و إخفاء الهوية وعدم تناسق يمكن الجهات الفاعلة الصغيرة من ممارسة قوة الصلبة والناعمة في الفضاء الإلكتروني مقارنة بالعديد من المجالات التقليدية للسياسة العالمية، كون المجال السيبراني هو بيئة جديدة ومتقلبة من صنع الإنسان يصعب فيها على القوى الكبرى من السيطرة على هذا المجال بقدر مالديها من القوة أخرى مثل البحر و الجو، لكن الفضاء الالكتروني يوضح أيضا النقطة التي مفادها أن انتشار السلطة لا يعني المساواة في السلطة أو كون الحكومات كأقوى الجهات الفاعلة في السياسة العالمية.[2]

3- مقالة لدكتور بارة سمير بعنوان "**الدفاع الوطني للأمن السيبراني (Cyber Security)**" والتي تعالج التوجه الدولي نحو الحكومة الإلكترونية و قضية الأمن المعلوماتي السيبراني من التحديات الكبرى على الصعيدين الإقليمي و العالمي، والذي تطرق فيها لدور الدفاع الوطني في تحقيق الأمن السيبراني في الجزائر أمام التحديات الوطنية والعالمية التي يفرضها الفضاء السيبراني.[3]

---

[1] موقع حلف الناتو، **الأمن السيبراني: منهج مرجعي عام**، تم الإطلاع:04/17/2021 على الرابط
https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_10/20170908_1610-cybersecurity-curriculum-a.pdf

[2] Joseph S. Nye, JR **" Cyber Power"** Harvard Kennedy School, Cambridge, 2010, p1

[3] بارة سمير، **الدفاع الوطني للأمن السيبراني**، المجلة الجزائرية للأمن الإنساني، ص426، العدد 2، الجزائر،2017

4- مقالة بعنوان **تدعيات الحرب الإلكترونية على العلاقات الدولية: دراسة في الهجوم الإلكتروني على إيران "فيروس ستكنست"** ، من إنجاز غريب حكيم وشرقي صبرينة، والتي تناولت موضوع تداعيات الحرب الإلكترونية على العلاقات الدولية دراسة في الهجوم الإلكتروني الذي استهدف إيران ، وتطرقت الدراسة إلى إبراز الأنماط التوظيفية المتعددة التي سطعت مع تحول الفضاء الإلكتروني إلى ساحة للتفاعلات الدولية و الإستخدمات ذات الطبيعة المدنية و العسكرية الأمر الذي جعل الفضاء مجال للصراعات المختلفة سواء من قبل الفاعلين من الدول أو من غير الدول لحيازة أكبر قدر ممكن من النفوذ والتأثير السيبراني، حيث تهدف الدراسة إلى بيان مدى تأثير خطورة الحروب الإلكترونية على العلاقات الدولية.[4]

ودراستنا هذه ستتناول مدى فعالية الإستراتجيات الأمنية للولايات المتحدة الأمريكية في المجال السيبراني وفق دراسة حالة للهجوم السيبراني الذي إستهدف شركة سولارويندزSolarWinds و خلفيات هذا الإختراق و الأساليب المستعملة والتقنيات المستعملة في اختراق برنامج SolarWinds Orion و الذي من خلاله تمكن الفريق المهاجم من تمرير البرمجيات وتلاعب فيها للوصول لإختراق الجيهات الحكومية الرسمية في الولايات المتحدة و شركات القطاع الخاص.

7) -النظريات والمقاربات النظرية المستخدمة في الدراسة:

اعتمدت هذه الدراسة على مجموعة من النظريات من أجل دراسة أليات والإستراتجيات التي انتهجتها الولايات المتحدة لرفع من قدراتها الدفاعية والأمنية في الفضاء السيبراني و حماية قواعد بياناتها من الإختراقات ومنها:

* **نظرية الحروب اللاتماثلية:** الحرب الغير متكافئة ، تعتمد على إستراتجيات وتكتيكات غير تقليدية ، يتبناها طرف عندما تكون القدرات العسكرية للقوى المتحاربة غير متكافئة، وتختلف قوة و وسيلة و الطريقة تنفيذ الهجمات عن طرف الثاني [5]، ويتم استغلال نقاط ضعف وثغرات العدو لتنفيذ الهجوم معتمدا على وسائل وتقنيات من الصعب توقعها وكشف عنها.

[1] غريب حكيم، شرقي صبرينة، **تدعيات الحرب الإلكترونية على العلاقات الدولية: دراسة في الهجوم الإلكتروني على إيران (فيروس ستكنست)**، دفاتر السياسة و القانون، المجلد:12/ العدد 02 ص 92، 2020.

[2] موسوعة بريطانيكا، مفهوم الحرب غير متكافئة ، ت الإطلاع: 04/18/2021 على موقع: https://www.britannica.com/topic/asymmetrical-warfare

* **النظرية الواقعية الجديدة:** الواقعية الجديدة هي ثمرة للنظريات التقليدية لتوازن القوى "أو الواقعية" للعلاقات الدولية وقد أوضحها كينيث والتز لأول مرة في عامي 1975–1979 في كتابه نظرية السياسة الدولية ، والادعاء النظري الأساسي لها هو أنه في السياسة الدولية ، الحرب هي احتمال[6].

* **نظرية القوة الناعمة:** هو مفهوم صاغه جوزيف ناي على أنه القدرة على الحصول ما تريد من خلال الإقناع وليس الإكراه، وفي الأونة الأخيرة تم إستخدام المصطلح للتأثير على الرأي العام و الظغط من خلال المنظمات السياسية والغير السياسية ، وهو ما يتم استغلاله في الأونة الأخيرة في الجانب السيبراني ، وهذا عن طريق اختراق حواسيب المنشئات نووية لدول و إتلاف البيانات والنتائج المتوصل اليها وهذا ، بدون استخدام القوة التقليدية للقيام بذلك ، ومثال ذلك هجوم Stuxnet.

8) -المناهج المعتمدة في الدراسة:

اعتمدت الدراسة على مجموعة من المناهج وهي:

* **المنهج الوصفي:** تم الإعتماد على هذا المنهج لوصف الطريقة وحيثيات تنفيذ عملية الإختراق لشركة سولاروينذز و من بعده التمكن من تنفيذ الإختراق الثاني الذي إستهدف الشركات الأمريكية و المؤسسات الحكومية الرسمية الامريكية التي تستخدم برنامج **Orion** المقدم من طرف شركة **SolarWinds**.

* **منهج دراسة الحالة:** يعرف منهج دراسة حالة بأنه المنهج المعتمد على دراسة حالة معينة بهدف جمع معلومات متعمقة عنه و هو فعال في إعطاء معلومات لا يمكن الحصول عليها بأساليب أخرى و منهج دراسة حالة يكون مناسبا للإستخدام عندما يكون تركيز البحث على ظاهرة معاصرة ضمن سياق الحياة الواقعي ، كذلك فإنه يفضل استخدامه عندما تكون هناك رغبة في دراسة حالة تحتوي على العديد من المتغيرات والعوامل المرتبطة مع بعضها البعض[7] ، اعتمدت عليه بإعتباره المنهج المناسب لدراسة الموضوع الذي نحن بصدد البحث فيه ، من خلال التعمق في في حيثيات الإختراق و الجوانب التي سبقت إكتشاف الثغرات المستغلة من طرف الجيهات المهاجمة لشركة سولاروينذز **SolarWinds**، و إكتشاف الإختراق من طرف شركة الأمن السيبراني **FireEye**، والتي بدورها قامت بإطلاع الجيهات الحكومية الأمريكية ، بحيث سيساعدنا هذا المنهج في المتابعة و التدقيق في تطورات الأحداث التي طرأت بعد إكتشاف هذا الإختراق وكيف كانت ردود أفعال الأطراف الأمريكية التي تم استهدافها من خلال هذا الإختراق.

---

[6] Donnelly, Jack. Realism and International Relations. Themes in International Relations. Cambridge, UK: Cambridge University Press, 2000. https://www.oxfordbibliographies.com/view/document/obo-9780199743292ت الإطلاع: 2021/18/4 على الموقع :

[7] سماء راضي حسين أحمد ، **دور كود التشكيل العمراني في تحقيق مجتمعات عمرانية مستدامة بمصر**، مذكرة لنيل شهادة دكتوراه، جامعة المنصورة ، قسم الهندسة المعمارية ، مصر، 2013.

9) – مصطلحات الدراسة:

*– **الأمن السيبراني:** هو فن حماية الشبكات و الأجهزة و البيانات من الوصول الغير مصرح به أو الإستخدام الإجرامي وممسارة ضمان السرية و النزاهة وتوافر المعلومات [8] من أي هجمات رقمية تسعى إلى إستغلال المعلومات الحساسة للإستعمالات الغير قانونية.

*– **قواعد البيانات (Database):** هي مجموعة بيانات أو معلومات يتم تنظيمها خصيصا للبحث والإسترجاع بواسطة الكمبيوتر، او سيرفرات لشركات تكنولوجية أو حكومية ، يتم تخزين فيها البيانات و المعلومات.

*– **الإختراق السيبراني:** هي العملية التي يتم فيها البحث عن الثغرات في الأنظمة التكنولوجية و البرامج الحاسوبية وإستغلالها لتنفيذ إختراق الضحية سواء كانت فرد أو مجموعة من أفراد، بهدف التجسس أو الإستلاء على البيانات الخاصة.

*– **التهديدات السيبرانية:** هو عمل ضار يسعى إلى إتلاف البيانات أو سرقة البيانات أو تعطيل الحياة الرقمية بشكل عام، تشمل الهجمات الإلكترونية تهديدات مثل فيروسات الكمبيوتر وهجمات رفض الخدمة DDos وغيرها من طرق.[9]

10) – حدود الدراسة:

– **الحدود المكانية:** في الفضاء السيبراني ، يعالج موضوع الدراسة فعالية الأنظمة والإستراتجيات الأمنية الأمريكية في مواجهة التهديدات السيبرانية وكدراسة حالة تم تناول الهجوم الذي استهدف سولارويندز وعملاءها في القطاعات الحكومية و القطاع الخاص ، و الذي اكتشافه في سنة 2020.

– **الحدود الزمانية:** في ما يخص الإستراتجيات المنتهجة من قبل الولايات المتحدة ، سيتم بداية التطرق لها بداية من سنة 2008 لحم جورج بوش ، وبداية الفترة الرئاسية للرئيس باراك أوباما و السياسة والقوانين السيبرانية التي أقرها في فترة حكمه ، وصولا الى نهاية فترته في سنة 2016 ، وبداية حكم دونالد ترامب والإستراتجيات السيبرانية التي انتهجتها ادارته خلال 4 سنوات ، الى غاية نهاية سنة 2020. كما سنتطرق في دراسة الحالة الى مراحل التي صاحبت اختراق شركة سولارويندز و المؤسسات الحكومية الأمريكية في بداية سنة 2020 وإلى غاية اكتشاف الإختراق من طرف شركة FireEye في شهر ديسمبر ، مرورا بكرونولوجيا الأحداث التي عقبت الحادث الى غاية 2021.

[8] **What is Cybersecurity?**موقع وكالة الأمن السيبراني وأمن البنية التحتية الأمريكية: https://us-cert.cisa.gov/ncas/tips/ST04-001 ت الإطلاع: 04/19/2021 على موقع:

[9] **What Are Cyber Threats and What to Do About Them** ت الإطلاع: 04/19/2021 على موقع: https://preyproject.com/blog/en/what-are-cyber-threats-how-they-affect-you-what-to-do-about-them/

11) – خطة الدراسة:

تم تقسيم هذه الدراسة إلى فصلين بحيث يتم تناول في الفصل الأول الإطار النظري والمفاهيمي للأمن السيبراني و الجيهات المسؤولة على توفيره استراتجياته في الولايات المتحدة الأمريكية ، بدءا بتعريف بالأمن السيبراني و أنواع الهجومات و التهديدات السيبرانية و أهداف و أهمية الأمن السيبراني ، وتبيان الإستراتجيات التي أقرها الرئيس باراك أوباما و دونالد ترامب خلال رئاستهم للولايات المتحدة للتصدي للهجومات و التهديدات السيبرانية. أما الفصل الثاني نتطرق فيه إلى حيثيات الهجوم ، وكرونولوجيا الأحداث التي صحبت اكتشاف الإختراق ، وصولا الى الكيفية التي تمت بها تلغيم التحديثات لـ برنامج SolarWinds Orion ، وفي الأخير نتطرق إلى الجهة المتهمة بتنفيذ الهجوم.

12) – صعوبات الدراسة:

– لقد واجهتنا العديد من الصعوبات في هذه الدراسة خاصة في ما يتعلق بالمعلومات الأكاديمية الدقيقة المتعلقة بعملية الإختراق ، خصوصا و أن الإختراق حديث الإكتشاف " أواخر سنة 2020 " وكذا سرية التحقيقات و المعلومات المسربة عن الحادثة بما أن إختراق مس مؤسسات سيادية أمريكية عملت على التحفظ على إبلاغ عن الأضرار الفعلية التي مست أنظمتها والبيانات التي من المرجح تم إستلاء عليها.

الفصل الأول:

الإطار المفاهيمي و النظري للدراسة

الفصل الأول: الإطار المفاهيمي و النظري للدراسة

أمام ما يعيشه العالم من تطور تكنولوجي هائل ومتواصل و انتشار أوسع للإستعمالات الرقمية ووسائل الإتصال الإلكترونية بين الأفراد و الشركات و حكومات الدول ، ومع ظهور لبرامج و أدوات الحماية ، تباين للكثيرين أن لا شيئ يشكل تهديد للإستخدماتهم داخل هذا الفضاء السيبراني الجديد ، فرغم كل ذلك يبقى هذا الفضاء عرضة للإختراقات والهجومات السيبرانية التي تستغل الثغرات ، أمام كل هذا يمكن القول أننا في أفضل ما يمكن وصفه بأنه أزمة إلكترونية عالمية و المستقبل لا يبدو واعدا ، ففي تقرير لمركز الدراسات الإستراتجية والدولية الصادر في يونيو 2014 تم تقدير أن التأثير العالمي للجرائم الإلكترونية يتراوح بين 375 و 575 مليار دولار نظرا لأن الحوادث السيبرانية لا يتم اكتشافها في الكثير من الأحيان ولا يتم الإبلاغ عنها بشكل متكرر ، فمن الصعب الوصول إلى فهم أكثر دقة لمدى الجريمة السيبرانية ، فأفضل تقدير يمكن حصره في 445 مليار دولار ، وهذا بالنظر إلى أن الإقتصادات الأربعة الأكبر ، الولايات المتحدة الأمريكية و الصين و اليابان و ألمانيا مجتمعة تمثل 200 مليار دولار.[10]

[10] Dominec Antonucci, **The Cyber Risk Handbook**, Wiley Finance Series, United States, 2017, p23

المبحث الأول: مفهوم التهديدات السيبرانية و الأنظمة الأمنية.

يستخدم الخبراء مجموعة متنوعة من التعريفات والمفاهيم عندما يتعلق الأمر بالأمن السيبراني ، وهذا بسبب التفسيرات الموسعة وتعدد المفاهيم المتعلقة بالفضاء السيبراني وهذا راجع لتنامي وبروز تهديدات جديدة مع التطور التكنولوجي المتسارع وارتباطها بالأمن السيبراني[11] ، تم ممارسة الأمن السيبراني في الدوائر العسكرية لأكثر من عقد. و في السنوات الأخيرة ظهر المصطلح في مجموعة متنوعة من السياقات ، مع إختلاف البيئة التي يعرف ويدرس من خلالها المصطلح[12]، من شركات تكنولوجية ، المنظمات غير الحكومية ، الأفراد ، المنظمات الإرهابية ، المجموعات الإفتراضية (الهاكرز) ، الدول ، أو مجموعات التي ترعاها دولة وتمولها لتنفيذ هجومات سيبرانية ضد جيهات حكومية أو دولة اخرى ، او معارضين سياسيين بغية التتبع و التجسس عليهم، وأمام هذه الأخطار والتهديدات التي تشكلها هذه الجيهات ، سعت الدول الى بناء استراتجيات تمكنها من توفير الحماية و الأمن السيبراني لبيناتها و الوثائق السرية والمراسلات الحكومية من أي إختراق، وفي هذا السياق عملت الولايات المتحدة على تحقيق أمنها السيبراني ، خصوصا كونها كانت عرضة للهجومات السيبرانية في العديد من المرات.

المطلب الأول: مفهوم الأمن السيبراني.

تتعدد التعريفات للمفاهيم المرتبطة بالأمن و الفضاء السيبراني ، فيعد تحديد وظبط التعريفات ضرورة لإنشاء وتنفيذ السياسة السيبرانية ، وتحقيقا لهذه الغاية، فإن **الأمن السيبراني** هو الجهد المبذول لحماية المعلومات والإتصالات والتكنولوجيا من أي أذى يحدث إما عن طريق الخطأ أو عن قصد ، فالأمن السيبراني هو الجهد المبذول لضمان السرية و النزاهة وحماية البيانات والموارد والعمليات من خلال إستخدام الظوابط الإدارية و المادية و الفنية.[13]

ويعرف **الأمن السيبراني** كذلك: بكونه العملية و الإجراءات التكنولوجية التي تم تصميمها لحماية الشبكات، البيانات و الأنظمة من الجرائم السيبرانية بفعالية الأمن السيبراني، كما يمكن تقليل مخاطر الهجمات الإلكترونية

[11] Jan Trobisch, **Challenges in the Protection of US Critical Infrastructure in the Cyber Realm,** School of Advanced Military Studies United States Army Command and General Staff College Fort Leavenworth, Kansas, 2014,p9
[12] Darko Galinec, Darko Možnik & Boris Guberina, **Cybersecurity and cyber defence: national level strategic approach,** Automatika: Journal for Control, Measurement, Electronics, Computing and Communications, p273, 2017 : To link to this article: https://doi.org/10.1080/00051144.2017.1407022
[13] Amos N. Guiora, **Cybersecurity : geopolitics, law, and policy**, Routledge, United States, 2017, p17

وحماية الكيانات و الأفراد و المؤسسات من خلال إستغلال التكنولوجيات و الأنظمة و الشبكات أكثر تعقيدا من الناحية الأمنية.[14]

يبقى الأمن السيبراني كمصطلح يستخدم على نطاق واسع غير أنه في بعض الأحيان غامض وغير مضبوط ، ومثل العديد من جوانب النظام العدالة الجنائية يتم تعريف الأمن السيبراني في الكثير من الأحيان وفق الفرد أو الكيان الذي يعرف هذا المصطلح ، تختلف هذه التعريفات بإختلاف المؤسسات الحكومية ، الدول القومية والأكاديميين والقطاع الخاص ، مما يؤدي إلى وجود اختلافات حول ما يشكله الأمن الإلكتروني في الواقع ، فبعض التعريفات تركز أكثر على تعريف الفضاء الإلكتروني ، بينما يركز الاخرون بشكل أكبر على الأمان ، وكثيرا ما يتم إستخدام مصطلح الأمن السيبراني في عناوين السياسة و دراسات الأكاديمية وفي ما يلي بعض التعريفات الأخرى لهذا المصطلح:[15]

تم تعريف **الأمن السيبراني** في قانون التحسين المقدم إلى مجلس الشيوخ الأمريكي لسنة 2014 المقدم من طرف السيناتور Jay Rockefeller على أنه: تسهيل ودعم تطوير مجموعة من المعايير الطوعية القائمة على الإجماع التي تقودها الصناعة وفق المبادئ التوجيهية وأفضل الممارسات و المنهجيات و الإجراءات لتقليل المخاطر الإلكترونية للبنية الأساسية.[16]

كما عرف **الأمن السيبراني** كل من Dan Craigen, Nadia Diakun-Thibault, Randy Purse على أنه تنظيم و جمع الموارد و العمليات والهياكل المستخدمة لحماية الفضاء السيبراني وتمكين الفضاء السيبراني من الأحداث التي لا تتوافق بحكم القانون مع واقع حقوق الملكية[17]، وتعرف وزارة الأمن الداخلي الأمريكية (DHS) الأمن السيبراني على انه النشاط أو العملية أو القدرة أو الحالة التي يتم بموجبها توفير حماية للمعلومات و إتصالات الأنظمة من أي ضرر.

يرى **جوزيف ناي** أن التفكير في الأمن السيبراني في الوقت الحالي هو مشابها للتفكير في أمن الطاقة النووية في الخمسينيات عندما كانت الأسلحة جديدة ، و المفاهيم الكامنة وراء التفاعلات العدائية كانت قيد التطوير،

[14] Harry Colvin, **Cyber Security for Beginners: Everything You Need to Know About it**, CreateSpace Independent Publishing Platform, 2017, p2
[15] Janine Kremling, Amanda M. Sharp Parker, **Cyberspace, Cybersecurity, and Cybercrime**, SAGE Publications, United States, 2018, p61
[16] Same ref : p63
[17] Same ref:p63

ويعرف كلمة سايبر Cyber على أنه إختصار يشير إلى الأنشطة الإلكترونية المتعلقة بالحاسوب[18]، ويعرف الأمن على أنه: عدم وجود تهديد للقيم الإنسانية ، بحيث ينطوي الأمن على أبعاد عديدة تتجاوز مجرد عدم وجود ضرر مادي أو أذى جسدي وهذا ما يعني القدرة على العيش وفقا للقيم الدستورية والإنسانية التي تعتبر مركزية لهويتنا.[19]

ومنه فإن الأمن السيبراني هو الضمانات و الإجراءات التي يمكن إستخدامها لحماية المجال السيبراني، في كل من المجالات المدنية والعسكرية من التهديدات التي قد تضر بترابطه، يتكون الأمن السيبراني من ثلاث خصائص أساسية ومهمة وهي ضمان المعلومات والخدمات والبنى التحتية لتكنولوجيا المعلومات و المعروفة باسم الثالوث CIA = Confidentiality, Integrity, and Availability أي السرية والنزاهة والتوافر وبالتالي فإن تأمين نظام المعلومات يعني منع كيان غير مصرح له من الوصول إلى بيانات الكمبيوتر أو خدمات الحوسبة أو البنية التحتية للحوسبة و تعديل عليها. [20]

المطلب الثاني: أنواع الهجمات والتهديدات السيبرانية.

تختلف وتتعدد طبيعة و طرق التي يتم من خلالها تشكيل التهديدات سيبرانية و تنفيذ الهجمات وعمليات الإختراق السيبرانية وهذا بإختلاف المهاجم و الهدف و الضحية من وراء العملية المنفذة، ويعرف دكتور كمال جبور التهديدات السيبرانية على انها " الدافع و النية من الجهات الفاعلة" ، هذه الدوافع و النوايا هي "الشهرة" للمتسللين و المخترقين ، و المنفعة المالية للمجرمين ، و المكاسب الإديولوجية للإرهابيين ، و الأفضلية والقوة السياسية و العسكرية للدول القومية ، ويوجد دافع اخر للهاكرز والذين يعملون بشكل مستقل عن الحكومات ، هؤلاء الهاكرز يقدمون أنفسهم على أنهم وطنيين يقومون بأنشطة التي لا تستطيع الحكومة التي يدعمونها من تنفيذها أو القيام بها.[21]

[18] Joseph S. Nye, Jr, **Power and National Security in Cyberspace**, America's Cyber Future Security and Prosperity in the Information Age, June 2011, p8

[19] Interview with Joseph Nye by José Luis Valdés–Ugalde, **Approaching Power and Understanding Leadership through The Lens of Joseph Nye**, jun. 2008, seen on 4/21/2021.
http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-35502008000100007

[20] **Cybersecurity:** Current challenges and Inria's research directions, White Book N3, INRIA, Publication date: January 2019, p24-25

[21] Robert T. Bridges, **USCYBERCOM**, A Research Report Submitted to the Faculty
In Partial Fulfillment of the Graduation Requirements; AIR COMMAND AND STAFF COLLEGE
AIR UNIVERSITY, April 2009, p4

فتعريف الهجوم السيبراني من وفق موضوع المذكرة هو: مجموعة من الإجراءات عبر الفضاء الإلكتروني التي تستهدف إستخدام لشبكات الكمبيوتر من طرف منظمات وشركات ، ومؤسسات حكومية لغرض تعطيل أو تدمير أو الكشف و التحكم في البنية الحاسوبية التحتية دون إذن ، وهذا بهدف إتلاف أو سرقة البيانات والمراسلات أو منع الوصول إليها.

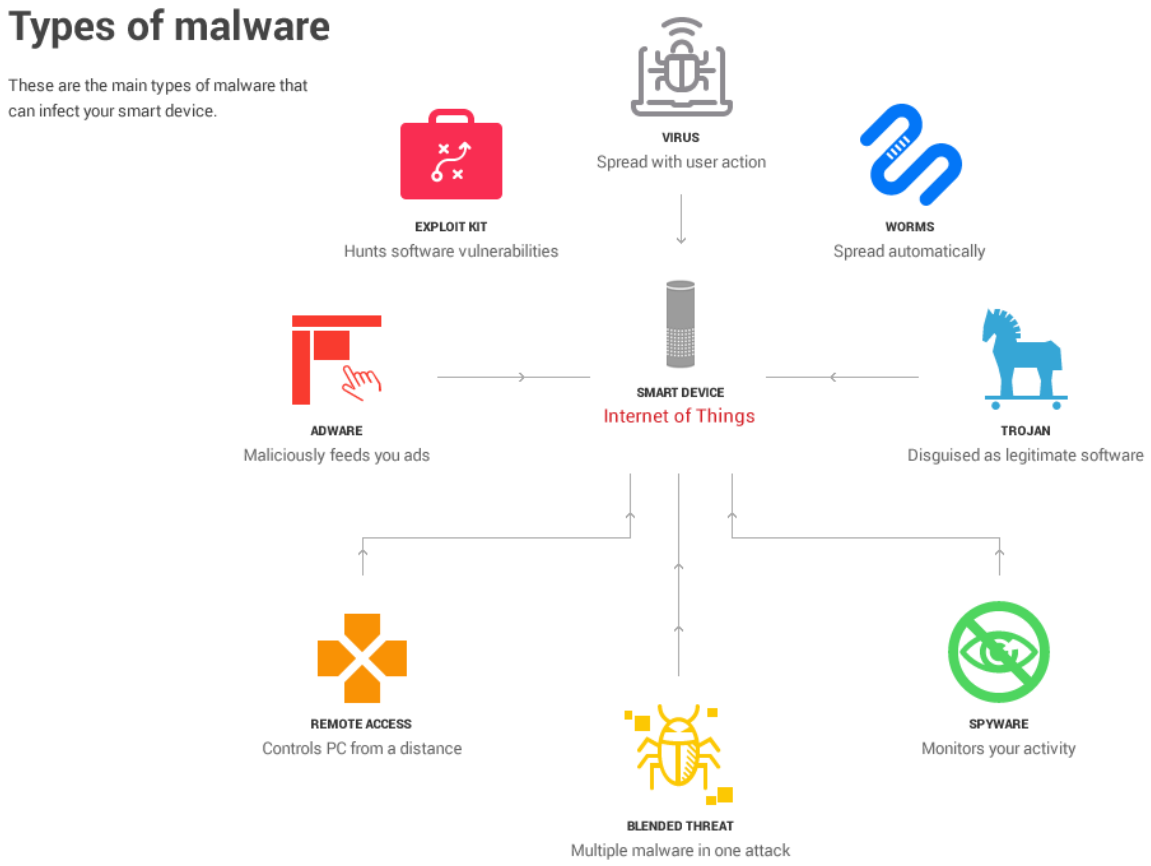
وفي ما يلي أبرز أنواع الهجمات و التهديدات السيبرانية التي تعاني من الشركات التكنولوجية ، و الأفراد ، و الحكومات و الدول و رجال السياسة في الفضاء السيبراني.

1- **البرمجيات الخبيثة / البرامج الضارة (Malware):** هو المصطلح الشامل لمجموعة متنوعة من التهديدات السيبرانية يتم برمجتها لإستهداف وظائف أي جهاز أو حاسوب أو شبكة قابلة للبرمجة بهدف إلحاق الضرر وتدميرها او لسرقة البيانات وهذا بإستهداف نظم الحماية للحاسوب وتخطيها للتحكم فيها.[22]

ويتم استعمال البرمجيات الخبيثة Malware لأسباب عديدة ، مثل: خداع الضحية لتقديم بيانات شخصية لسرقة الهوية ، سرقة بيانات بطاقة ائتمان المستعمل أو البيانات المالية الأخرى ، أو فرض السيطرة على أجهزة كمبيوتر متعددة لشن هجومات رفض الخدمة " Denial-of-Service (DoS) attack " ضد الشبكات الأخرى، أو إصابة أجهزة الكمبيوتر و استخدامها لتعدين البيتكوين أو العملات المشفرة الأخرى.[23]

وهناك أنواع عديدة وأصناف التي تنتمي الى عائلة البرمجيات الخبيثة Malware ومنها:

[22] **What is malware?**, seen on 4/21/2021 : https://www.mcafee.com/en-us/antivirus/malware.html
[23] Same prev ref



مخطط توضيحي لأنواع البرامج الضارة Malware من إنجاز الطالب.

– **الفيروسات Viruses:** أحد أشكال البرامج الضارة Malware والتي غالبا ما تعلق نفسها بملف مضيف أو MBR "Master Boot Record" أي سجل التمهيد الرئيسي كملف طفيلي ، و عند الوصول إلى الملف المضيف فإنه ينشط الفيروس ويمكنه من إصابة أمكان مختلفة من الجهاز، تنتشر معظم الفيروسات من خلال النشاط البشري داخل وبين أجهزة الكمبيوتر، وعادة ما يتم تصميم الفيروس لإتلاف البيانات ، وتختلف معدلات وسرعات وأهداف تنفيذ الهجوم من فيروس للأخر ، فبعض الفيروسات تعمل على تدمير الملفات الموجودة على الجهاز بأسرع وقت ممكن في حين يفعل الأخرون ذلك ببطئ على مدار ساعات او أيام، وقد يستهدف الاخرون الصور و المستندات (.doc/.docx). فقط.[24]

[24] Simplicity VoIP, **The A to Z of Cybersecurity Glossary**, seen on 4/21/2021 www.globalknowledge.com

– **دودة الحاسوب Worm:** هي جزء مستقل من البرامج الضارة التي تستنسخ نفسها وتنتشر من كمبيوتر للأخر[25] ، وهي تختلف عن الفيروسات بحيث أنها لا تتطلب تدخلا بشريا للتنقل عبر الشبكة و الإنتشار من الجهاز المصاب إلى الشبكة بأكملها، يمكن أن تنتشر الديدان إما عبر الشبكة بإستخدام ثغرات نظام التشغيل أو عبر البريد الإلكتروني ، ويؤدي تكرار و انتشار الدودة عبر الشبكة إلى استهلاك موارد الشبكة مثل مساحة التخزين وسرعة الأنترنت.[26]

– **الباب الخلفي Backdoor:** في مجال الأمن السيبراني ، يشير الباب الخلفي إلى أي طريقة يمكن من خلالها للمستخدمين المصرح او غير مصرح لهم الإلتفاف على إجراءات الأمان العادية و الحصول على وصول عالي المستوى على نظام الكمبيوتر أو شبكة أو تطبيق برمجي، وقد كانت الأبواب الخلفية كرابع أكثر التهديدات شيوعا في عام 2018 لكل من المستخدمين العاديين والشركات.[27]

– **الوصول عن بعد بواسطة حصان طروادة Remote Access Trojan:** يعد أحد أخطر التهديدات الأمنية التي تواجهها المؤسسات في الوقت الحاضر ، في السنوات الأخيرة أصبح التهديد المستمر المتقدم Advanced Persistent Threat (APT) كأخطر هجوم إلكتروني يسرق المعلومات السرية أو يقوض نظام المعلومات من منظمة أو الشركة المستهدفة ، وهذا كونه من البرامج الضارة ذات زمن انتقال عال ومخفي للغاية مما يسبب أضرار جسيمة بالجهة المتضررة ، يمنح هذا النوع من الهجوم للجهة المنفذة وصولا تفاعليا إلى كمبيوتر الضحية لسرقة البيانات السرية ، ويتم غالبا تضمينه في النظام عن طريق البريد الإلكتروني ، أو ذاكرة USB أو في حزمة الملفات، ومن الصعب على المستخدمين العاديين ، وكذلك الأمر مع المسؤولون ذوي الخبرة في إدارة السرفيرات إكتشاف والعثور على مثل هذه البرامج الضارة.[28]

– **روتكيت Rootkit:** روتكيت هي مجموعة من الأدوات (مثل ملفات الثنائية و البرامج النصية وإعدادات الملفات) التي تسمح للمتطفلين بإخفاء نشاطهم على جهاز الكمبيوتر حتى يتمكنوا من مراقبة النظام والتحكم فيه سرا لفترة طويلة ، الروتكيت الذي يتم تصميمه بطريقة جيدة ومحترفة سيجعل الجهاز المخترق يبدو كما لو لم يكن هناك خطأ أو إختراق ، مما يسمح للمهاجمين بالحفاظ على قاعدة لوجستية مباشرة تحت انظار مسؤول

[25] Josh Fruhlinge, **Malware explained: How to prevent, detect and recover from it**, Seen on 4/22/2021: https://www.csoonline.com/article/3295877/what-is-malware-viruses-worms-trojans-and-beyond.html

[26] Jeetendra Pande, **Introduction to Cyber Security**, Uttarakhand Open University, Haldwani, 2017, p20

[27] Backdoor computing attacks, Seen on 4/22/2021: https://www.malwarebytes.com/backdoor/

[28] Chun Guo, , Zihua Song, Yuan Ping, Guowei Shen, Yuhei Cui, and Chaohui Jiang, Article: **PRATD: A Phased Remote Access Trojan Detection Method with Double-Sided Features,** Guizhou Provincial Key Laboratory of Public Big Data, College of Computer Science and Technology, Guizhou University, College of Cybersecurity, Sichuan University, Chengdu, China, 2020, p1

النظام طالما رغبوا في ذلك [29]، يقول Bill Blunden أن روتكيت Rootkits الذي قام بتشريحهم وتحقيق فيهم كانوا كلهم في المجال العام أي انها كانت عبارة عن قرصنة وهجوم ممول وبرعاية دولة ، وقد جاء في تقرير لعام 2008 للكونغرس المتعلق بالإقتصاد والأمن بين الولايات المتحدة والصين ، أنه قد لاحظت لجنة المراجعة ان " قدرة العمليات السيبرانية للصين الحالية متقدم جدا" مما يمكنهم من المشاركة في أشكال من الحرب السيبرانية شديدة التعقيد قد تكون الولايات المتحدة غير قادرة على مواجهة أو حتى الكشف عن هذه الجهود." و وفقا للتقرير ، انه كان هناك حوالي 250 مجموعة من الهاكرز التي تتسامح معهم الحكومة الصينية (وهذا ان لم يتم تشجعيهم ودعمهم في السر).[30]

– **رانسوم وير أو برنامج الفدية Ransomware**: هي شكل خبيث من أشكال البرمجيات الضارة " Malware" والتي تعمل على منع وتقيد وصول الفرد إلى جهاز الكمبيوتر الخاص به وهذا عن طريق تشفير بيانتهم والملفات والمطالبة بالدفع " بعملة رقمية مشفرة: كا البيتكوين او غيرها من العملات المشفرة" مقابل إستعادت الإمكانية عملها و الوصول اليها و ، ويعود أول هجوم موثق لبرامج الفدية إلى عام 1989 ، وظلت برامج الفدية غير شائعة نسبيا حتى منتصف العقد الأول من القرن الحادي و العشرين ومنذ ذلك الوقت ارتفعت ألية وإحترافية تنفيذ الهجوم وقدرت أضرارها بمئات ملايين الدولارات في السنة ، وعلى سبيل المثال تسبب نوع واحد من برامج الفدية " CryptoWall3 " في خسائر بقيمة 320 مليون دولار في عام 2015 فقط.[31] ، تستخدم برامج الفدية نموذجية التشفير RSA 2048 لتشفير الملفات ، وهي خوارزمية تشفير جد معقدة وقوية ، هذا ويقدر معدل الكمبيوتر المكتبي لكسر تشفير RSA 2048 بحوالي 6.4 كوادريليون سنة لكسر هذا التشفير.[32]

– **برامج التجسس Spyware**: يستخدم هذا المصطلح لوصف أي تقنية كمبيوتر تقوم بجمع المعلومات حول شخص أو مؤسسة دون علمهم أو موافقتهم ، يمكن تثبيت برامج السرية على جهاز الكمبيوتر أو الهاتف من خلال عدة وسائل سرية ، بما في ذلك كجزء من برنامج يحتوي على فيروس ، أو نتيجة إضافة برنامج أو تطبيق على الهاتف الذكي او الكمبيوتر المستهدف ، وكملاحظة ، يتم إستخدام مصطلحات Spyware– Keylogger– Adware – Stealware لوصف نفس التعليمات البرمجية الضارة أو أنواع مماثلة لها ، وقد

[29] Reverend Bill Blunden, **The Rootkit Arsenal: Escape and Evasion: Escape and Evasion in the Dark Corners of the System,** Jones & Bartlett Learning; 1st edition, United States of America, 2009, p10-11
[30] Same ref, p14
[31] Camelia Simoiu, Christopher Gates, Joseph Bonneau, Sharad Goel, a study: **"I was told to buy a software or lose my computer. I ignored it": A study of ransomware**, Stanford University, 2019, direct link: https://web.stanford.edu/~csimoiu/doc/ransomware.pdf
[32] RANSOMWARE Hostage Rescue Manual: What You Need to Know To Prepare and Recover from a Ransomware Attack, KnowBe4, 2018, p2

عملت مقاطعات أمريكية كا يوتا ، و كاليفورنيا ، نيويورك على تشريع لحظر برامج التجسس أو السيطرة عليها وإضافة إلى ذلك عمل الكونغرس الأمريكي على قوانين جديدة في هذا الموضوع ، وتستعمل برامج التجسس لجمع المعلومات تسجيل الضغطات المفاتيح لسرقة كلمات المرور ، أو قائمة المواقع التي يزورها المستخدم أو التطبيقات ، وأيضا جمع أسماء وأرقام وبيانات بطاقات الإئتمان.[33]

– **أدوير Adware أو برمجية الإعلانات المدعومة:** عبارة عن برنامج يعرض الإعلانات على الكمبيوتر أو الهاتف الذكي للمستخدم بشكل تلقائي[34] ، وتستخدم هذه التعليمات البرمجية الخبيثة لجمع المعلومات حول مستخدمي الكمبيوتر و الهواتف الذكية ومراقبة المواقع التي يزورها المستخدم و منه يمكن تخزين المعلومات حول المواقع التي تم زيارتها في قواعد بيانات واستخدامها لتحديد نوع اللافتات أو الإعلانات التي يتم عرضها على المستخدم.[35]

2– التصيد أو الخداع الإلكتروني Phishing:

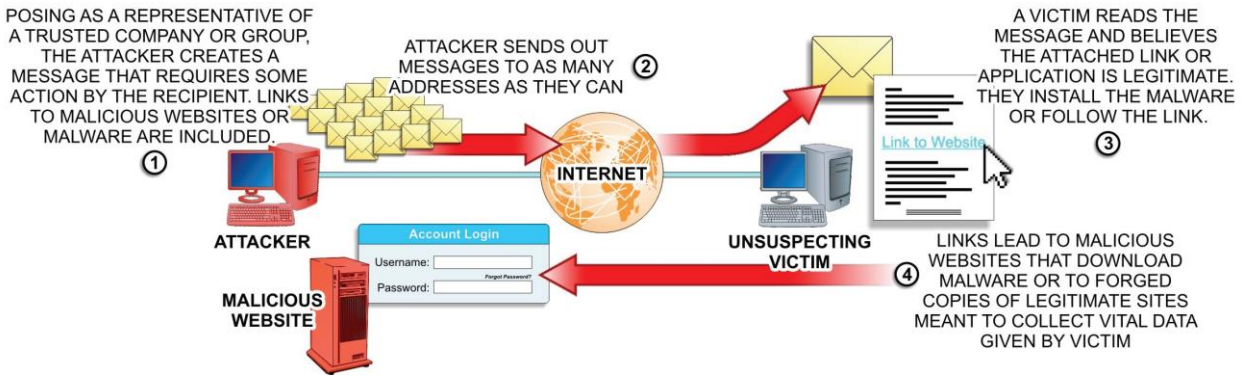
يعتمد الخداع الإلكتروني على تقنية الهندسة الاجتماعية عن طريق محاولة التمكن من اكتساب معلومات حساسة وعادة ما تكون بيانات اعتماد تسجيل الدخول أو بيانات بطاقة الإئتمان وهذا عن طريق التنكر في هيئة منظمة جديرة بالثقة ، وتستعمل بشكل عام هذه النوعية من الهجمات رسائل البريد الإلكتروني والتي توجه المستخدم لموقع ويب مزيف يشبه الموقع الحقيقي ، وتطلب هذه المواقع من المستخدم إدخال البيانات ومعلوماته، مما يمكن من سرقة هويته وبياناته الحساسة.[36]

[33] Michael Erbschloe, **Trojans, Worms, and Spyware: A Computer Security Professional's Guide to Malicious Code**, Elsevier Butterworth–Heinemann, United States of America 2004, p25-26

[34] Jun Gao, Li Li, Pingfan Kong, Tegawendé F. Bissyandé, Jacques Klein, **Should You Consider Adware as Malware in Your Study?**, University of Luxembourg, Luxembourg and Monash University, Australia: Published in: 2019 IEEE 26th International Conference on Software Analysis, Evolution and Reengineering (SANER), Date of Conference: 24-27 Feb. 2019.

[35] Same ref: p26-27

[36] Charles J . Brooks, Christopher Grow, Philip Craig, Donald Short, **CYBERSECURITY ESSENTIALS**, John Wiley & Sons, Inc, 2018, p600



رسم تمثيلي عن عملية هجوم التصيد "Phishing Attack"

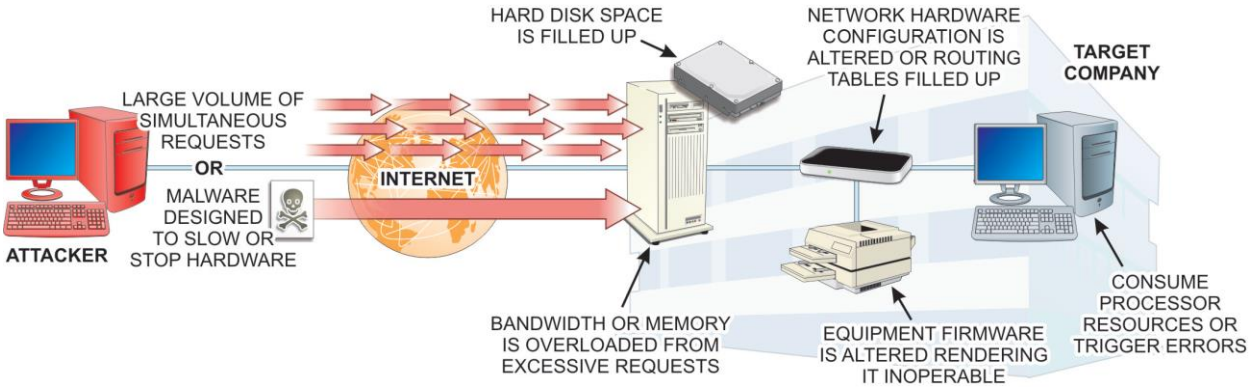
مصدر: Charles J . Brooks, Christopher Grow, Philip Craig, Donald Short, CYBERSECURITY ESSENTIALS, John Wiley & Sons, Inc, 2018, p601

3- هجمات تعطيل الخدمة Denial of Service (DoS- DDoS) Attacks:

هجوم رفض الخدمة هو محاولة لتعطيل عمل الخدمة أو السيرفيرات ما يعني عدم القدرة على الوصول إلى الموقع و توقفه ، ويتم في هذا الهجوم الإعتماد على شبكات مختلفة وكثيرة لتنفيذ الهجوم ويشار إليها باسم الروبوتات "Botnets" وعادة ما تكون الأنظمة والأجهزة الكمبيوتر المتسخدمة في الهجوم مصابة بأحد أحصنة طراودة Trojan" ويتم إستعمال في هذا الهجوم مئات أو حتى ألاف الكمبيوترات ، مما يصعب من عملية توقيف مثل هذا الهجوم ، كون أن الحل لن يقتصر على حظر عنوان IP واحد فقط ، ومن السهل جدا تنفيذ هجمات DDoS بإستخدام سكريبتات تسهل الأمر على المنفذ ، مثل إستخدام script kiddie[37] ، وكمثال للهجومات تعطيل الخدمة DDoS التي عانت منها الدول ومؤسسات حكومية نجد الهجوم الذي وقع في سنة 2007-2008 والذي إستهدف دولة إستونيا و جورجيا على توالي، أدى الهجوم على إستونيا في 2007 إلى تدمير مواقع الويب البرلمانية وتعطيل خدمات الحكومية والمصرفية مع قطع الإتصال بالشبكات وتعطيل عمل وسائل الإعلام والحكومة بسبب عدة موجات من هجمات DoS attacks ، وتصل المعاملات المالية في إستونيا عبر الأنترنت الى نسبة 90 بالمئة ، مما كان تأثير ذلك معوقا على البلد. وفي مثال أخر وفي أوائل عام 2013 اندلعت توترات بين الفلبين و تايوان بعد مقتل صياد تايواني مما خلق موجة توتر بين البلدين، مما قاد "ناشطو القرصنة" التايوانيون على شن هجمات واسعة النطاق على مواقع الويب الحكومية الفيليبنية وألحقوا أضرار مباشرة بالإقتصاد.[38]

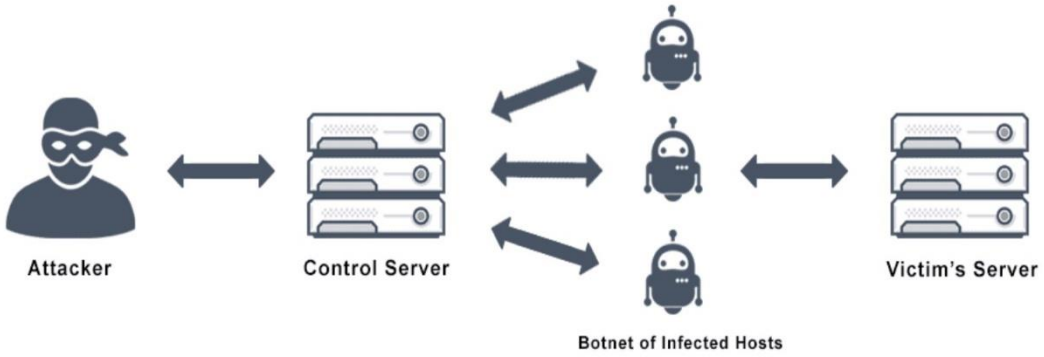
[37] Charles J . Brooks, Christopher Grow, Philip Craig, Donald Short, **CYBERSECURITY ESSENTIALS**, John Wiley & Sons, Inc, 2018, p607

[38] PUBLIC DATA AT RISK: CYBER THREATS TO THE NETWORKED GOVERNMENT, APRIL 2015,p17



رسم تمثيلي لعملية تنفيذ الهجوم تعطيل الخدمة Dos Attack

Charles J . Brooks, Christopher Grow, Philip Craig, Donald Short, CYBERSECURITY ESSENTIALS, John Wiley & Sons, Inc, 2018, p608



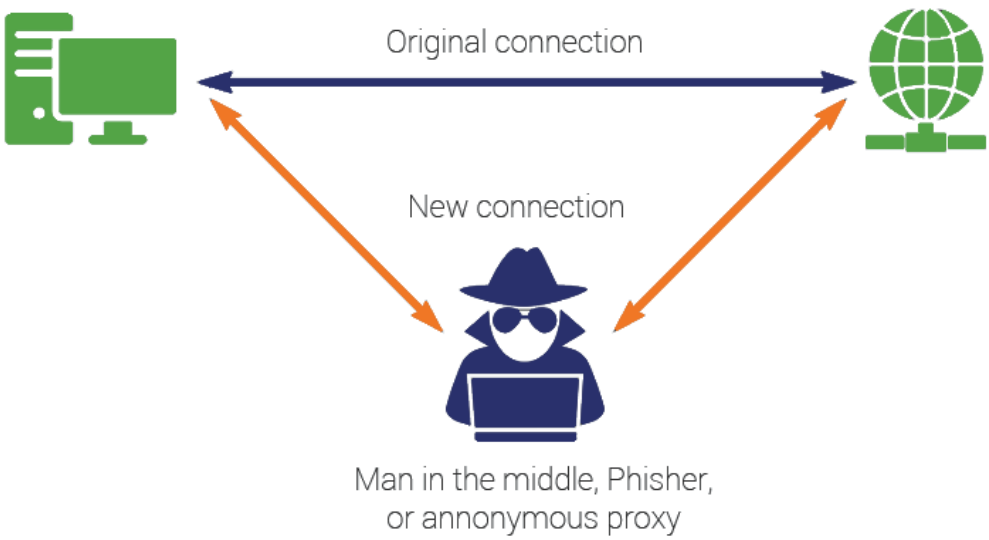
رسم توضيحي لعملية تنفيذ هجوم تعطيل الخدمة DDoS Attack

مصدر الصورة: https://avinetworks.com/glossary/ddos-attack/

4- هجوم الوسيط Man in the Middle Attack:

في التشفير وأمن الكمبيوتر الشخصي، يعتبر هجوم " الوسيط ، أو الرجل في الوسط " a man-in-the-middle attack (MITM)، هجومًا ينقل فيه المهاجم سرا وربما يغير المراسلات بين الطرفين يثقان في أنهما يتواصلان بشكل مباشر مع بعضهما البعض، هجوم الوسيط هو مصطلح عام عندما يضع الجاني نفسه في مناقشة بين طرفين للإستماع بطريقة سرية لمحادثتهم ، أو لتقليد أحد الأطراف عبر مراسلات الكترونية مما يجعله يظهر كما لو أن تداولًا عاديًا للمعلومات قيد التقديم لطرف الأخر ، الهدف من هذا الهجوم هو الحصول على معلومات فردية على سبيل المثال: الإهتمامات المستهدف من العملية ، وعادة ما يكون المستهدفين من

مثل هذه العمليات ، مستعملي التطبيقات ومواقع أعمال والمال و هذا للحصول على المعلومات التي يتم إستخدامها في عملية إحتيال[39] ، ومنه فإن هذا النوع من الإختراقات يتسلل فيه المهاجم بين متحاورين في الشبكة دون علم كل منهما حيث يقوم بإعتراض الإتصال الحقيقي وعمل اتصال ثاني يمر من خلال جهازه وهذا بإستخدام مجموعة من البرامج الخاصة.



رسم توضيحي لعملية هجوم الوسيط Man in the Middle Attack

مصدر الصورة: https://www.kaymera.com/how-does-the-man-in-the-middle-attack-work/

5- هجمات حقن قواعد البيانات (SQL Injection):

(Structured Query Language) و المعروفة إختصارا ب SQL وهي لغة الإستعلامات البنائية أو لغة قواعد البيانات ، وهي لغة برمجة غير إجرائية ، تستعمل للتعامل والتحكم مع قواعد البيانات، ويعد حقن SQL بأكواد برمجية أحد أكثر نقاط ضعف تدميرا التي تؤثر على الأعمال التجارية أو مراكز بيانات حكومية ، حيث تؤدي الى كشف عن جميع المعلومات الحساسة المخزنة في قواعد البيانات ، كأسماء المستخدمين ، وكلمات المرور والأسماء والعناوين وأرقام الهواتف و بطاقات الإئتمان ، ومنه فإن هجمات حقن قواعد البيانات هي ثغرة

[39] Avijit Mallik, **MAN-IN-THE-MIDDLE-ATTACK: UNDERSTANDING IN SIMPLE WORDS**, Cyberspace: Jurnal Pendidikan Teknologi Informasi, Volume 2, Nomor 2, Oktober 2018, p109-110

أمنية التي تمنح المهاجم القدرة على التأثير على لغة الإستعلام الهيكلية (Structured (Query Language "SQL" من خلال القدرة على التأثير على ما يتم تمريره إلى قاعدة البيانات.[40]

الصورة تمثل الكيفية التي يتم إستعمالها في حقن قواعد البيانات SQL Injection

مصدر الصورة: https://cybercoastal.com/sql-injection-introduction-for-beginners/

6- الهندسة الإجتماعية (Social Engineering):

هي القدرة على على الحصول على معلومات حساسة وسرية عن طريق التلاعب بعقول الأشخاص بأساليب انتحال الشخصية للحصول على ثقة الضحية بشكل تدريجي ، بمعنى أنها تساعد على اختراق الأنظمة ، والشركات أو الحكومات ، من خلال التلاعب بالبشر وليس من خلال البرمجيات، وهذا عن طريق تزويدهم بمعلومات صحيحة و دقيقة عنهم أو عن نشاطهم ، مما يوقع الضحية في الفخ للإعتراف بمعلومات أو عمليات سرية ، ومثال لمثل هذه العملية ، هو ما قام به المعارض وناشط السياسي الروسي أليكسي نافالني بعد عملية تسميمه من طرف المخابرات الروسية ، وتحقيق الذي قام به هو وفريق مساعد له لتثبيت وتوريط منفذي العملية من قادة وعملاء في مديرية المخابرات الرئيسية الروسية GRU ، تستخدم الهندسة الاجتماعية لتلاعب النفسي لخداع المستخدمين لإرتكاب أخطاء أمنية أو الكشف عن معلومات حساسة.

[40] Justine Clarke, **SQL Injection Attacks and Defense: 2nd Edition**, Elsevier, United States, 2012, p1

7- هجوم كلمات المرور (Password Attack- Brute Force Attack):

هو نوع من أنواع الهجمات الذي يعتمد على تخمين وكسر وتغيير كلمات المرور واستغلالها للدخول الغير مصر به الى النظام ، أو حساب ، يعتمد هذا الهجوم على تخمين كلمات ، الحروف أو الأرقام المرور المتوقعة وهذا بإستعمال برنامج الي (Automated Software) وهذا مايسهل الأمر للهاكر، ومن بين أشهر البرامج التي تستخدم في فك التشفير :Aircrack-ng – Hashcat – L0phtCrack.

8- المخترق الداخلي(Internal Attacker):

يحدث الهجوم الداخلي عندما يسعى فرد أو مجموعة من العمال بإختراق المنظمة أو الشركة التي ينتمون إليها، فيقوم المخترق الداخلي بتواطئ مع الجيهات التي تسعى إلى الوصول الى قواعد البيانات للمؤسسة أو الشركة التي ينتمي إليها ، وهذا بدوافع و أسباب مختلفة ، منها الإنتقام ، الإبتزاز ، كسب المال.

يتم اللجوء إلى إستعانة بالمخترق الداخلي الذي ينتمي الى الشركة المستهدفة ، عندما يصعب على المخترقين كسر أنظمة الحماية للشركة المستهدفة ، ومنه يتم البحث عن وسيط ينتمي ويشتغل داخل الشركة الهدف ، ومحاولة إغراءه ماليا ليسهل لهم عملية الإختراق.

يتم في خلال مثل هذه العمليات إستهداف الموظفون ذو المهارات العالية مثل (مسؤولي النظام وقواعد البيانات و المبرمجين)[41] ، وتسهل المهمة إذ كان الموظفون المستهدفون ساخطون أو يعانون من مشاكل داخل الشركة ، أو من أجور ضعيفة ، أو عدم إخلاصهم ونزاهتهم لشركة.

[41] Internal Attack, Seen on 4/24/2021, Website link: https://www.techopedia.com/definition/26218/internal-attack

جدول يوضح أنواع المهاجمين و الهجومات السيبرانية: مصدر: *Mark Ciampa, Security Awareness: Applying Practical Security In New World, United States, 2015, p23*

نتيجة الهجوم Sample attack	المستهدف Typical target	الهدف Objective	الفئة المهاجمة Attacker category
سرقة معلومات بطاقة الائتمان	المستخدمين ، الشركات ، الحكومات	المال ، والشهرة ، إبتزاز	مجرمو الأنترنت Cybercriminals
محو البيانات	الشركات ، المستخدمين	الشهرة ، الإثارة والسرور	Script kiddies سكريبتات الصبيانية
العثور على نقاط الضعف والثغرات في نظام التشغيل	أي جهة	بيع الثغرات لمن يدفع أعلى سعر	Brokers الوسطاء
سرقة الملفات لنشر المعلومات الحساسة	الشركات ، الحكومات	الإنتقام من صاحب العمل أو الحكومة	Insiders المهاجم الداخلي
تعطيل وشل أنظمة التشغيل	الشركات، الحكومات ، منشئات عسكرية	التسبب في الاضطراب والذعر	Cyberterrorists الإرهاب السيبراني
تعطيل مواقع مالية	الحكومات ، الشركات	تصحيح التصور الخاطئ ضدهم	Hacktivism هاكتيفيزم / المتسللين
إطلاع على رسائل الإلكترونية للسياسين.	المستخدمين ، الحكومات	التجسس على الشعوب ، تعطيل أنظمة تشغيل لحكومة	State-sponsored attackers المهاجمون برعاية دولية

المطلب الثالث: أهداف وأهمية الأمن السيبراني.

يعد الأمن السيبراني في غاية الأهمية في الوقت الحالي ، خصوصا مع انتقال الإستعمالات اليومية للأفراد و الحكومات والقطاعات الاقتصادية الى العالم الرقمي ، من إستخراج وثائق حكومية للمواطنين ، والدفع الإلكتروني للضرائب أو الفواتير ، أو عمليات التسوق والشراء ، وهذا الذي شهد انتشارا بعد جائحة كورونا، وتم تسجيل ارتفاع في نسب التسوق الإلكتروني. و أمام هذه التغيرات ، يفرض الأمن السيبراني نفسه أمام تزايد الهجمات السيبرانية التي تستغل الثغرات للإيقاع بضحايا عن طريق الإحتيال و النصب ، أو عن طريق تنفيذ هجمات مثل : Ransomware برامج الفدية ، أو Phishing Attack التصيد ، او هجوم تعطيل الخدمة DDoS Attack.

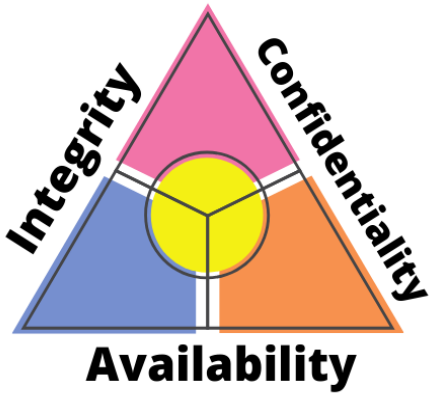
الهدف من الأمن السيبراني هو حماية المعلومات من السرقة أو الإختراق أو الهجوم الذي يؤدي إلى وقف وتعطيل عمل قواعد البيانات ، ويمكن قياس فعالية الأمن السيبراني عبر تحقيق الأهداف التالية:

1- التوفر Availability: تعزيز سير توفر الخدمات و البيانات للمستخدمين المصرح لهم، وإمكانية الوصول اليها أو إستخدامها أو تشغيلها عند الطلب ، وعدم توقفها.

2- النزاهة أو الموثوقية وسلامة المحتوى Integrity: حماية البيانات والمعلومات من أي تعديلات غير مشروعة، أو الإطلاع أو إتلاف أو فقدان غير مصرح به.

3- السرية Confidentiality: توفير الخصوصية و السرية للمعلومات و البيانات المستخدمين وحمايتها من أي إطلاع.

و تتشكل هذه الأهداف في شكل ثالوث: السرية ، النزاهة و التوافر معروف ب CIA والذي هو اختصار ل confidentiality, integrity, availability. هذا النموذج هو مصمم لتوجيه السياسات الخاصة بأمن المعلومات داخل المؤسسة أو الشركة ، يتم العمل وفق هذه المعايير عند إنشاء تطبيقات أو قاعدة بيانات ، للعمل على ضمان الأمن ووصول إلى البيانات. [42]



وللوصول إلى إثبات وتحقيق هذه الأهداف نحتاج إلى أدوات عملياتية تقدم لكل الأطراف الأمان والرضى والتي تتمثل في:

- أدوات ووسائل تحقيق خاصية التوفر Availability:

* الحماية المادية: المقصود بالحماية المادية هو القدرة على الإحتفاظ بالمعلومات حتى في حالة وجود تحديات وأخطار ، وهذا بضمان وجود المعلومات الحساسة عن طريق حفظها في مناطق آمنة من أي وصول أو إختراق.

[42] William Stallings, **Effective Cybersecurity: A Guide to Using Best Practices and Standards**, Addison-Wesley Professional; 1st edition, 2018, p 4-5

* التكرار الحسابي Computational redundancies: يتم تطبيق هذه العملية على السيرفرات لتحمل الأخطاء المحتملة أو أخطاء الغير مقصودة.

- أدوات ووسائل تحقيق خاصية النزاهة Integrity:

* النسخ الإحتياطي Backups: وهو ضمان الأرشفة الدورية للبيانات ، لإستخدامها في حالة فقدان البيانات الأصلية أو إتلافها ، كما يتم استخدامه أيضا لعمل نسخ لأغراض تاريخية ، مثل الدراسات الطويلة أو الإحصائيات أو السجلات التاريخية أو لتلبية سياسة الإحتفاظ بالبيانات.

* التحقق الجمعي أو التدقيق المجموع Checksum: وهي عملية تستخدم للتحقق من سلامة الملف أو عملية نقل البيانات، بمعنى آخر ، هو حساب الدالة الذي يقوم بتعيين محتويات الملف إلى قيمة عددية. تُستخدم عادةً لمقارنة مجموعتين من البيانات للتأكد من أنها متطابقة.

* تصحيح أكواد ورموز البيانات Data Correcting Codes: تستخدم هذه الطريقة لتخزين البيانات بطريقة يمكن من خلالها إكتشاف التغييرات الصغيرة بسهولة وتصحيحها تلقائيا.

- أدوات ووسائل تحقيق خاصية السرية Confidentiality:

* التشفير Encryption: التشفير هو طريقة لتحويل المعلومات لجعلها غير قابلة للقراءة للمستخدمين غير المصرح لهم باستخدام خوارزمية ، يتم إسخدام مفتاح تشفير بحيث لا يمكن قراءة البيانات وإطلاع عليها وهذا لحماية البيانات الحساسة مثل أرقام بطاقات الإئتمان أو رسائل و المحادثات وهذا عن طريف تشفير البيانات لتصبح على شكل نص مشفر غير قابل للقراءة.

* المصادقة Authentication: هي عملية تضمن وتؤكد هوية المستخدم ، وهذا بإستعمال رسالة كود إلى الهاتف ، أو البريد الإلكتروني ، أو بصمة الأصبع ، أو كلمة مرور ثانوية تم حفظها مسبقا من طرف المستخدم.[43]

المبحث الثاني: الأنظمة الأمنية المستعملة لتصدي للهجومات السيبرانية

أمام كل التهديدات السيبرانية التي تواجه الدول و الأفراد في الفضاء السيبراني ، وفي ظل ارتفاع في معدلات الجريمة الإلكترونية ، وتنوع الهجمات والأساليب المستخدمة ، تعمل شركات الأمن المعلوماتي و الأمن السيبراني على تطوير أدوات ووسائل وإستراتجيات عمل بهدف تعطيل وكشف الإختراقات و الهجمات السيبرانية وتوفير

[43] **Cyber Security Goals**, Article, Seen on 4/24/2021, Website link: https://www.javatpoint.com/cyber-security-goals

الحماية للبيانات ، وفي هذا الصدد و من خلال ما تم التطرق إليه في المطلب الثاني من المبحث الأول حول أنواع الهجمات و التهديدات السيبرانية سيتم التطرق في هذا المبحث إلى أليات التي تعمل على كشف وتجنب والحماية من الهجومات السيبرانية و للحد منها، بالإضافة الإستراتجيات المتقدمة التي تقدمها الشركات المختصة في الأمن المعلوماتي و السيبراني لتوفير أقصى حماية للمنظمات و الشركات و الحكومات المتعاقدة معها ، برغم من أن الأمر يبقى معقد وصعب التحقيق بصورة دائمة وثابتة ، إلا أن الدفاع هو وسيلة حتمية أمام هذه التهديدات.

المطلب الأول: الوسائل المستعملة لتعطيل الهجومات السيبرانية.

– كيفية تجنب **البرمجيات الخبيثة / البرامج الضارة (Malware)**:

- عدم ظغط وفتح النوافذ المنبثقة و الروابط المشكوك فيها على المتصفح.
- عدم زيارة المواقع التي من المحتمل على أنها مصدر للبرمجيات و محتوى ضار.
- عدم فتح الملفات ذات امتداد مثل: (.bat,.com, .exe, .pif, .vbs) بحيث مثل هذه الملفات من المحتمل على انها مرتبطة ببرمجيات ضارة.
- عدم توقيف وتعطيل عمل أليات التحكم الأمني مثل: (برامج مكافحة الفيروسات وبرامج وأدوات الكشف عن التجسس ، جدار الحماية الشخصي.)
- تجنب إستخدام خاصية الأمر بتشغيل البرامج أو النظام على مستوى المسؤول (using administrator–level).
- تجنب إستخدام البرامج المسروقة أو المعدلة ، أو البرامج الغير معروفة المصدر و القديمة الغير محدثة.[44]
- القيام بعمل النسخ الإحتياطي للبيانات بشكل دائم في محيط معزول عن الشبكة التي يتم العمل بها.
- القيام بعمل تحديثات روتينية لنظام التشغيل المعمول به مثل: الماك ، ويندوز ، اللينكس.
- أخذ كل الحيطة في فتح الإيميلات ، أو الرد عليها، وعدم تقديم معلومات حساسة بدون التحقق من الطرف الذي يتم تراسل معه.

[44]Murugiah Souppaya, Karen Scarfone, **Guide to Malware Incident Prevention and Handling**, Computer Security Division (Information Technology Lab) NIST, 2015, p3

- التحقق من الروابط التي يتم دخول لها ، وقبل كتابة أي كلمة سر ، أو معلومات حساسة ، وهذا لتجنب الإصابة بهجمات التصيد(phishing).

وفي ما يلي بعض أنواع الهجمات وكيفية التصدي لها:

- **الفيروسات و دودة الحاسوب Worms-Viruses:**
  - إستخدام برامج المدفوعة ضد الفيروسات Antivirus و البرمجيات الخبيثة Antimalware
  - تقليل إستخدام الذاكرة الفلاشية USB flash drives ، وهذا كون الفيروساتViruses و دودة الحاسوب Worm ينتشران بصورة سريعة بإستعمال الذاكرات الفلاشية.
  - فحص الملفات الواردة عبر البريد الإلكتروني قبل أي فتح.

- **هجوم حصان طروادة Trojan Horse:**
  - إستخدام برامج ضد البرامج الخبيثة Antimalware مثل Malwarebytes.
  - تفعيل و تنصيب التحديثات بصورة روتينية للبرامج وأنظمة التشغيل.
  - تحميل الملفات فقط من مصادر ومواقع موثوقة.
  - الحذر عند وعدم فتح البريد الإلكتروني بسهولة في صندوق البريد الوارد.
  - استخدام جدار حماية الشبكة.[45]

- **برامج التجسس و برمجية الإعلانات المدعومة Adware-Spyware:**
  - عدم إستخدام البرامج المجانية ، وتأكد المصدر البرنامج قبل تنصيبه على نظام التشغيل.
  - إستخدام برامج مسح ضد برامج التجسس.
  - التأكد من مصدر أي USB flash drive أو Smartphone cable connector قبل ربطه بجهاز الكمبيوتر، وهذا لكون هذه الأدوات من الممكن استخدامهم لإختراق الكمبيوتر وتجسس عليه بواسطة

[45] Zhu Zhenfang, **Study on Computer Trojan Horse Virus and Its Prevention**, International Journal of Engineering and Applied Sciences (IJEAS), Volume-2, Issue-8, August 2015, p95

برمجيات خبيثة منصبة فيهم مسبقا. ومثال ذلك USB Ninja Cable والذي يتم استخدامه في عمليات التجسس واختراق أنظمة التشغيل.

- **برامج الفدية Ransomeware:**

- إستخدام النسخ الإحتياطية للبيانات Data Backups
- توقيف عمل التطبيقات الخارجية مثل: (Dropbox, Google Drive) واستخدامهم فقط أثناء الحاجة اليهم.
- تشغيل التحديثات لكل البرمجيات الحماية ، بإضافة الى إضافات وملحقات المتصفح (Browser addons).
- عدم الظغط وفتح رسائل البريد الإلكتروني العشوائية (Spam e-mail)، أو الروابط المشكوك فيها.
- إستخدام برنامج حماية ضد الفيروسات.
- إستخدام شبكة افتراضية خاصة (VPN) أثناء استعمال شبكة أنترنت عامة (Public Wi-Fi).

- **هجمات تعطيل الخدمة Denial of Service (DoS- DDoS) Attacks:**

- توفير طاقة إستعابية كبيرة ومضاعة للعدد المتوقع لزوار الموقع (traffic bandwidth).
- تطوير خطة لإستجابة لهجوم رفض الخدمة وهذا بناءً على تقييم أمني شامل، وهذا بكتابة أفضل الخطوات التي يجب اتخاذها من طرف الفريق المسؤول على الأمن السيبراني، التي تتضمن:
  - مراجعة الأنظمة المعمول بها Systems checklist
  - تحديد مسؤوليات أعضاء الفريق الرئيسيين لضمان رد فعل منظم للهجوم فور حدوثه.
  - تحديد إجراءات الإخطار والتصعيد. و التأكد من أن أعضاء الفريق الأمني على دراية بالضبط بمن يتصلون في حالة وقوع هجوم.[46]
- تأمين البنية التحتية لشبكة المعمول بها ، وهذا بإستخدام برمجيات الجدار وشراء أنظمة حماية من هجمات DDoS والتي تكون عبارة عن Hardwire يتم ربطه بشبكة.
- التعامل مع شركات مختصة في توفير الحماية من الهجومات تعطيل الخدمة DDoS مثل: Akamai, CloudFlare, Fastly.

[46] Tactics To Prevent DDoS Attacks & Keep Your Website Safe, Seen on 4/28/2021 at: https://phoenixnap.com/blog/prevent-ddos-attacks

- **هجوم كلمات المرور Brute Force Attacks:**

- إستخدام كلمات مرور قوية التركيب، التأكد من ان كلمة المرور المستخدمة تحتوي على 12 حرف كحد أدنى وتتضمن أرقام ورموز و الأحرف الصغيرة والكبيرة.
- أن لا تكون الكلمات المستعملة موجود في القاموس، وتجنب إستخدام كلمات مرور التي تحتوي على معلومات شخصية تخصك والتي قد تكون معروفة للمهاجم، مثل تاريخ الميلاد.
- تقييد عدد المرات التي يحاول فيها المستخدم تسجيل الدخول ، بعد خمس محاولات خاطئة على أقل.
- إستخدام حروف التحقق "الكابتشا" CAPTCHA كواجهة أولية قبل كتابة كلمة المرور وهذا لمنع البرامج التي تستخدم في الهجوم بمحاولة كتابة كلمة المرور بشكل أوتوماتيكي متكرر.
- ربط خاصية الإنذار إلى الهاتف أو الإيميل لتنبيه صاحب الحساب من أن حسابه يتعرض لمحولات تسجيل الدخول خاطئة ومتكررة.
- تفعيل خاصية توثيق ذو عاملين (FA2) Two Factor Authentication / أو الاستيثاق بعوامل عدة، وهذا عن طريق استقبال كود تفعيل قبل الدخول للحساب على الهاتف أو البريد الإلكتروني أو مكالمة هاتفية.

- **التصيد أو الخداع الإلكتروني Phishing:**

- إستخدام email filters مثل: MailWasher Pro – MailCleaner – SpamTitan ، وهذا لتحييد وحذف أوتوماتيكي للإيميلات الغير مرغوب فيها والتي تحتوي على روابط مزيفة.
- اليقظة ، وهذا عن طريق التأكد من الروابط جيدا قبل القيام بإدخال كلمة المرور او معلومات وأرقام بطاقة الإئتمان ، وغير ذلك.

- **هجوم الوسيط Man in the Middle Attack:** يتطلب حظر هجمات الوسيط مجموعة من تقنيات التشفير والتحقق للتطبيقات بالنسبة للمستخدمين ، وكذا توفير بنيات حماية إزدواجية لشبكة الأنترنت ومثال ذلك إستخدام تقنية (DMZ– Demilitarized zone) منطقة منزوعة السلاح، وهو جدار أمني يفصل الشبكة الداخلية و الشبكة الخارجية ويكون هذا بإستخدام جهاز روتر Router أو بإستخدام جدار ناري Firewall ، ويتم تقديم هذه تقنيات الحماية من طرف شركات مثل: Microsoft –Cisco وفي مايلي كيفية توفير حماية من هجوم الوسيط:

- تجنب الدخول على نقاط واي–فاي WiFi الغير مشفرة بكلمة مرور.
- إيلاء الاعتبار فيما يتعلق بتحذيرات المتصفح التي تشير إلى أن الموقع غير آمن.
- عدم استخدام أجهزة الكمبيوتر المقدمة من طرف (مثل المقاهي أو الفنادق) عند إجراء التبادلات المالية الحساسة.
- بالنسبة لمسؤولي المواقع، تساعد اتفاقيات المراسلات الأمنة بما في ذلك (HTTPS SSL–TLS) في تخفيف هجمات الانتحال عن طريق تشفير المعلومات المنقولة والمصادق عليها.[47]
- إستعمال الشبكة الإفتراضية الخاصة (VPN) للتواصل بشبكات أخرى خارجية وهذا من أجل ضمان أن تكون البيانات المتناقلة بين الأطراف مؤمنة ومحمية من أي اختراق أو تعديل فيها.

– **هجمات حقن قواعد البيانات SQL Injection:** أفضل الطرق التي بإمكانها صد هذه الهجمة هو التحكم في مدخلات المستخدم والتحقق منها لمراقبة أنماط الهجوم ، كما يمكن للمطورين و المبرمجين أيضا تجنب الثغرات الأمنية من خلال تطبيق أساليب الوقاية التالية:

- Input validation التحقيق من صحة الإدخال: وهذا عن طريق التأكد من كل الإضافات التي يتم القيام بها مع مراقبة دورية للأكواد البرمجية الموجودة وتأكد من حالتها.
- Parameterized queries: الاستعلامات ذات المعلمات هي وسيلة لتجميع جملة SQL مسبقًا بحيث يمكنك بعد ذلك توفير المعلمات من أجل تنفيذ العبارة. تتيح هذه الطريقة لقاعدة البيانات التعرف على الكود وتمييزه عن بيانات الإدخال.[48]
- إستخدام جدار الحماية المخصص للحماية من هذه الهجمات.

المطلب الثاني: كيفية تفعيل ورفع من درجات الحماية لتجنب الإختراقات السيبرانية.

في هذا المطلب سيتم التطرق إلى الأساليب و الإستراتجيات الأكثر فعالية وأمان في توفير الحماية و الدفاع ضد التهديدات السيبرانية ، والتي يتم اعتماد عليها واستخدامها من طرف خبراء الأمن المعلوماتي و السيبراني للشركات و المنظمات و الحكومات ، لتشفير البيانات ، و المراسلات ووصول إلى البرامج.

[47] Avijit Mallika, Abid Ahsanb, Mhia Md. Zaglul Shahadata, Jia-Chi Tsou, **Man-in-the-middle-attack: Understanding in simple words**, International Journal of Data and Network Science 3, 2019, p85

[48] How to prevent SQL injection attacks, Seen on 4/29/2021 at: https://www.ptsecurity.com/ww-en/analytics/knowledge-base/how-to-prevent-sql-injection-attacks/

1- التشفير Encryption:

خلال استخدامنا للكمبيوتر و التطبيقات والبرامج والمواقع على أنترنت، سيكون المستعمل في حاجة إلى الإحتفاظ بسرية المعلومات والملفات الخاصة به مثل: الصور ، جدول البيانات، الرسائل الصوتية أو المكتوبة، وغير ذلك. ويعتبر هذا مشكل أساسي لأمن الكمبيوتر في سبيل الحفاظ على سرية الملف، ولمواجهة هذا المشكل ، يتم استخدام التشفير Encryption لتحويل الملف المرسل الى تنسيق جديد غير قابل للقراءة ، الى غاية ان يتم استخدام فك التشفير للتمكن من إعادة الملف الى النموذج الأصلي (حتى لو لم يكن الملف نصا) والملف المشفر هو نص مشفر.[49]

ومنه فإن التشفير هو الإجراء الذي يتم من خلاله تحويل و إخفاء المعلومات للحفاظ على سريتها.

Encrypt = En + Crypto

En = Make

Crypto = Hidden/ Secret

ويعتمد التشفير على استخدام مفتاح (Key) لتحويل المعلومات والبيانات الى حالة مشفرة والسرية(Cipher).

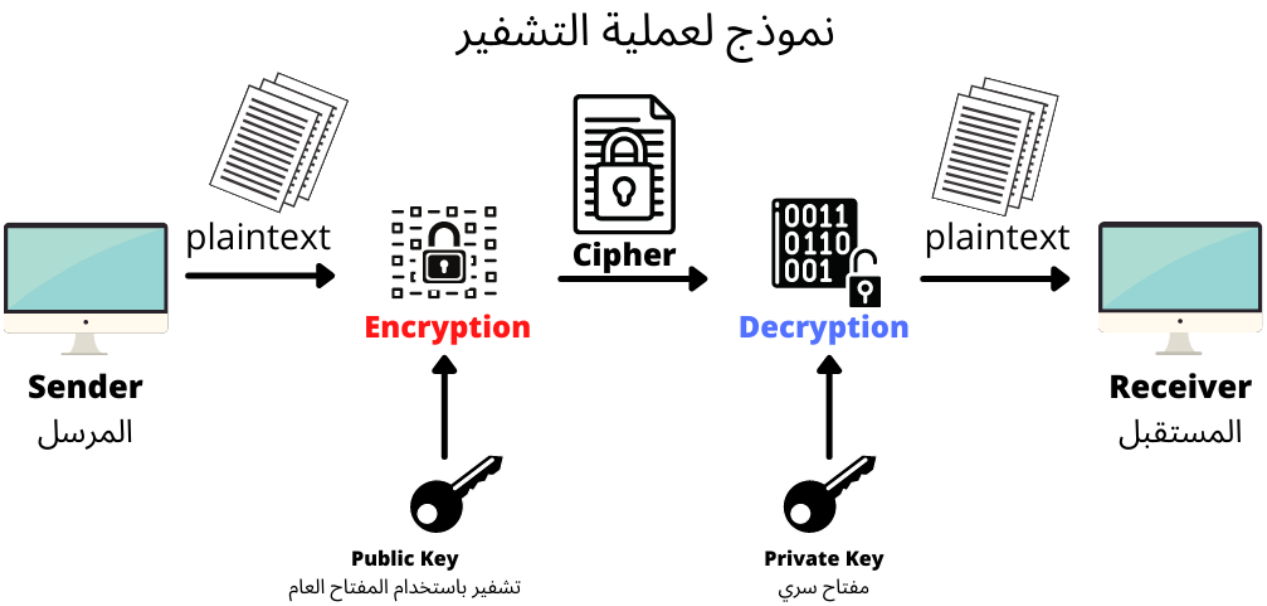
والمقصود بالشفرة (Cipher/ Ciphertext): هي الطريقة التي يتم من خلالها تشفير البيانات.

التشفير Cryptography: هو دراسة التقنيات الرياضية المتعلقة بجوانب أمن المعلومات مثل السرية وتكامل البيانات ومصادقة عليها. [50]

فك التشفير Decryption: هي العملية التي يتم من خلالها جعل المعلومات والبيانات المشفرة قابلة للقراءة مرة أخرى.

[49] Jean-Philippe Aumasson, **Serious Cryptography: A Practical Introduction to Modern Encryption**, No Starch Press Publishing company, San Francisco, 2017, p27

[50] Cheng-Jing Kuo, **Cryptography**, Graduate Institute of Communication Engineering National Taiwan University, Taipei, Taiwan, ROC, p2



ويوجد نوعان يتم استعمالهم في التشفير ، الأول هو التشفير الغير المتماثل "Asymmetric Encryption" والثاني هو التشفير المتماثل "Symmetric Encryption" .

يعتمد التشفير الغير المتماثل Asymmetric Encryption على إستعمال نوعان مختلفان للمفاتيح للتشفير وفك الشفرة ، وهما تشفير بإستخدام المفتاح العام Public key to encrypt و مفتاح سري لفك التشفير Secret key to decrypt. في حين يعتمد التشفير المتماثل Symmetric Encryption على استخدام مفتاح واحد لفك التشفير.

نماذج الهجوم و أهداف الأمان للتشفير الغير المتماثل هي تماما مثل التشفير المتماثل، بإستثناء اذا كان المفتاح المستخدم في التشفير عام(Public Key) فإن أي مهاجم بإمكانه إجراء استعلامات تشفير بإستخدام المفتاح العام للتشفير، فالتشفير المتماثل و الغير متماثل هما النوعان الرئيسيان من التشفير، وعادة ما يتم دمجهما لبناء أنظمة إتصالات آمنة من أي اختراقات. [51]

[51] Jean-Philippe Aumasson, **Serious Cryptography: A Practical Introduction to Modern Encryption**, No Starch Press Publishing company, San Francisco, 2017, p48

يوجد أنواع وتقنيات أخرى متعددة للقيام بتشفير البيانات والمراسلات، التي تنتمي الى Asymmetric Encryption و Symmetric Encryption.

- **التشفير الغير متماثل Asymmetric Encryption:**

- خوارزمية التشفير RSA = Rivest – Shamir – Adleman آر إس إيه ، والتي تم تطويرها واطلاقها في سنة 1976 من طرف Ron Rivest – Adi Shamir – Leonard Adleman، وسميت بإسمائهم ، تم إعلان عن هذه الخوارزمية من طرفهم في جامعة « MIT » Massachusetts ، كون الفريق الذي عمل على هذه الخوارزمية يشتغلون كأستاذة في الجامعة.[52]

- **التشفير المتماثل Symmetric Encryption:**

- معيار تشفير البيانات Data Encryption Standard (DES): تم تطوير هذه الخوارزمية من طرف الشركة الأمريكية International Business Machines Corporation (IBM) ، والتي اهتمت بتقنيات التشفير وعملت على انشاء وتطوير خوارزمية جديدة تستعملها في منتجاتها ومعملاتها ، وفي سنة 1977 تم الإعلان على هذه الخوارزمية ، والتي قدمت تشفيرا مناسبا للحماية البيانات من هجمات التشفير " cryptographic attacks ".
- معيار التشفير المتقدم Advanced Encryption Standard (AES): في سنة 2001 تم المصادقة على استخدام هذه الخوارزمية من طرف وزارة التجارة الأمريكية ، وفي شهر ماي من سنة 2002 أصبحت هذه الخوازمية (AES) معيارا رسميا في تعاملات الحكومة الفيدرالية الأمريكية ، وهذا لما تضمنه من تعقيد وتشفير قوي للبيانات.[53]

[52] Joshua Holden, **The Mathematics of Secrets: Cryptography from Caesar Ciphers to Digital Encryption**, Princeton University Press and Oxford, United Kingdom, 2017, p216

[53] Robert Ciesla, **Encryption for Organizations and Individuals Basics of Contemporary and Quantum Cryptography**, Apress; 1st ed. Edition, 2020, p31-32

- القياس الحيوي/القياسات الحيوية- البيومترية Biometrics:

تمثل القياسات الحيوية أحد أكثر الأشكال قوة وموثوقية لتحديد هوية الإنسان في الأمن المادي والسيبراني ، ولقد شهد العقد الماضي تطورات هائلة في تكنولوجيات الإستشعار وتقنيات وخوارزميات معالجة البيانات ، وقد أدى ذلك إلى تعزيز من تقنيات وتكنولوجية القياسات الحوية التقليدية، مثل: بصمات الأصابع و الوجه وقزحية وشبكية العين والصوت ، وديناميكيات ضغط على المفاتيح " Keystroke Dynamics " ، وظهور تقنيات جديدة أخرى. وقد أدى التقاء الأسواق الإستهلاكية واحتياجات الأمن القومي الى زيادة الطلب على المنتجات والخدمات البيومترية ، وعلى سبيل المثال، أدى دمج أجهزة الإستشعار "Biometric Sensors" في الهواتف الذكية واستخدام هذه التكنولوجيات في الخدمات المصرفية للبنوك عبر الأنترنت إلى تعزيز الإعتماد على استخدام تقنيات القياس الحيوية لدى الجماهير.

تحمل القياسات الحيوية "Biometrics" قدرة قوية على تحديد ما اذا كان الفرد حقيقيًا أم محتالً ، مثل هذه القدرة الدقيقة على التعرف على الأفراد بشكل موثوق الى جانب الصعوبة الشديدة لتزوير البيانات البيومترية جعلت منها الشكل الأكثر موثوقية لتحديد هوية الإنسان ، وفقًا لدراسة لشركة Research and Markets Ltd ، وهي شركة أبحاث السوق، سيصل سوق المقاييس الحيوية العالمية الى 42.4 مليار دولار بحلول عام 2021 ، نظرا للتقدم في المشهد التكنولوجي والفهم الأفضل له من طرف الناس ، تستخدم تقنيات القياسات الحيوية الأن في مختلف القطاعات بما في ذلك الحكومة والدفاع ، تطبيق القانون، التمويل والتجارة الإلكترونية والتعليم ، كما بدأت بعض البلدان في استخدام القياسات الحيوية لمنع تزوير الهوية أثناء الانتخابات أو في إدارة الرعاية الاجتماعية وتوفيرها. [54]

- ماهي القياسات الحيوية " البيومترية " Biometrics:

هي العملية التي يتم من خلالها اكتشاف السمات الجسدية وغيرها من السمات الفريدة للشخص وتسجيلها بواسطة جهاز أو نظام إلكتروني كوسيلة لتأكيد الهوية.[55]

- أو ، هي آلية أمان تستخدم للمصادقة وتوفير الوصول بناءً على التحقق من الخصائص المادية للشخص ، وهذا تحت فكرة أن كل شخص هو فريد بطريقة أو بأخرى ، سواء كان ذلك بصوته أو بصمات الأصابع أو العين ، أو الطريقة التي يمشي بها أو غير ذلك.

[54] Issa Traore, Mohammad S. Obaidat, Isaac Woungang, **Biometric-Based Physical and Cybersecurity Systems**, Springer International Publishing, Switzerland, 2018, p7

[55] Online dictionary Dictionary.com : Biometrics, Seen on 4/30/2021, link: https://www.dictionary.com/browse/biometrics#

و هناك نوعان الأكثر شيوعا من معرّفات القياسات الحيوية (Biometric Identifiers) وهما:

- الخصائص الفيزيولوجية " Physiological Characteristics" والتي تعود شكل الوجه ، هندسة وشكل اليد ، وتفاصيل وبصمة الأصابع والعين وملامح الوجه وتركيبة الجسم، والحمض النووي DNA [56].
- الخصائص السلوكية " Behavioral Characteristics" و التي تتضمن نبرة وشفرة الصوت ، الإيماءات والحركات ، طريقة المشي، الإمضاء.

ومن خلال هذا فإن القياسات البيومترية بصفة عامة ستشمل جمع وتخزين البيانات البيومترية بهدف المقارنة مع الشخص تم أخذ قياساته البيومترية مسبقا للسماح له بالمرور أو إستخدام أي وسيلة تتطلب تعريف بيومتري التي تشمل ما تم ذكره من خصائص سلوكية و فيزيولوجية ، فإذ تم حدوث توافق فهذا يعني أنه الشخص الحقيقي المسموح له بتفعيل الخدمة ، أما اذ تعذر القبول والسماح من طرف الأجهزة البيومترية للشخص ، فهذا يعني ان الشخص هو متنكر أو متحايل.

- الإستثاق بعوامل متعددة Factor Authentication Methods :

تُعرف طريقة المصادقة التقليدية باسم المصادقة أحادية العامل (SFA/Single-factor authentication) وهي عملية أمان يتم فيها استخدام عامل واحد فقط (عادةً كلمة مرور) لتأكيد هوية المستخدم التي يدعيها، تعتبر هذه الطريقة غير آمنة بشكل كافٍ للعديد من التطبيقات ذات أهمية أمنية. مثل الخدمات المصرفية عبر الأنترنت ، أو عمليات تسجيل الدخول إلى الحسابات الشخصية أو غير ذلك ، ففي عام 2016 تم تسجيل 63% من عمليات اختراق البيانات بسبب كلمات المرور الضعيفة و الحسابات الغير مؤمنة بطرق متعددة. ولهذا يتم اللجوء إلى استعمال المصادقة الثنائية (FA2) كحل لتعزيز أمان الوصول من خلال طريقتين للتحقق من هوية المستخدم ، بحيث تجعل طبقة الأمان الإضافية صعوبة على المهاجمين للوصول الى أجهزة الشخص أو الحسابات على الأنترنت.[57] أما Multi-Factor Authentication (MFA) فهو نهج متعدد الطبقات لتأمين البيانات والتطبيقات وهذا عن طريق تقديم أكثر من بيانات اعتماد للتحقق من هوية المستخدم لتسجيل الدخول مثل: كلمة المرور + كود رسالة هاتفية + بصمة الأصبع أو الصوت.

[56] Anil K. Jain, Arun A. Ross, Karthik Nandakumar, **Introduction to Biometrics**, Springer Science & Business Media, Germany, 2011, p273.

[57] Niklas Tellini, Fredrik Vargas, **Two-Factor Authentication: Selecting and implementing a two-factor authentication method for a Digital Assessment Platform**, Bachelor's Thesis, KTH Royal Institute of Technology, School of Information and Communication Technology (ICT), 2017, p17

عوامل المصادقة Authentication Factors:

- عوامل المعروفةKnowledge Factors : مثل كلمات المرور ، كلمة المستخدم ، الإيميل ، رقم الهاتف.
- عوامل الحيازة Possession Factors: مثل الهاتف الذكي ، رمز سري "token" ، أو بطاقة الكترونية.
- عوامل الوراثية Inherence Factor: مثل القياسات الحوية " البيومترية " مثل شفرة الصوت ، أو أو بصمة العين أو الأصابع.
- عامل الجغرافي والزماني Time and Location: يتم استعمال هذا في عملية المصادقة بعوامل متعددة " Multi Factor Authentication (MFA) ، وهذا بإضافة عوامل أخرى مثل الوقت و المكان ، للمستخدم ، وإلزامه بتواجد في مكان محدد وتوقيت محددا ليتمكن من الحصول على الدخول.

- **الجدار الناري Firewall:**

ليس كل مصادر الزيارات التي تتلقاها الشبكة وأنظمة التشغيل تأتي من مصدر سليم ومرخص له، لذا يجب الا يتم السماح لهم بالدخول الى الشبكة أو مغادرتها، ولهذا يجب تعطيل كل هذه المصادر ومنعها من الوصول للشبكة، كل هذه الإحتياطات الأمنية ، هي وظيفة جدار الحماية أو الجدار الناري، يعمل الجدار الناري Firewall ، كبوابة حماية و أمان لأنظمة التشغيل ضد أي تهديدات خارجية ، جدار الحماية هو جهاز تصفية يفرض سياسة أمان الشبكة ويحمي الشبكة من الهجمات الخارجية ، جدار الحماية هو أداة مصممة لإيقاف أي ضرر خارجي محتمل ممكن أن يقوم بتوغل في البيانات أو المراسلات في مراكز البيانات.[58] و منه فإن جدار الحماية هو جهاز أمان يراقب حركة المرور الشبكة الواردة و الصادرة.

وتتعدد الإستخدامات الجدار الأمني ، فمن الجانب الخارجي يمكن أن تمنع جدران الحماية الموظفين من إرسال بيانات معينة خارج الشبكة مثل الرسائل الإلكترونية ، ومن الجانب الداخلي يمكن أن يمنع جدار الحماية الموظفين من الدخول لبعض المواقع مثل: الفايسبوك Facebook، يوتوب Youtube.

ومن خلال ما سبق ، سنشرح الطريقة التي يعمل وفقها الجدار الناري في توقيف وترصد أي تهديدات وهجومات سيبرانية تستهدف إختراق الشبكة وإلحاق ضرر بها ، وهذا عن طريق ثلاث إستراتجيات ، الأولى تسمى ب

[58] James Michael Stewart, **Network Security, Firewalls and VPNs, 2nd Edition, Jones & Bartlett Learning**, United States, 2014, p: unkown

حزمة التصفية (Packet Filtering) ، والثانية خدمات الوكيل (Proxy Service) والثالثة التفتيش الجليل (Stateful Inspection).

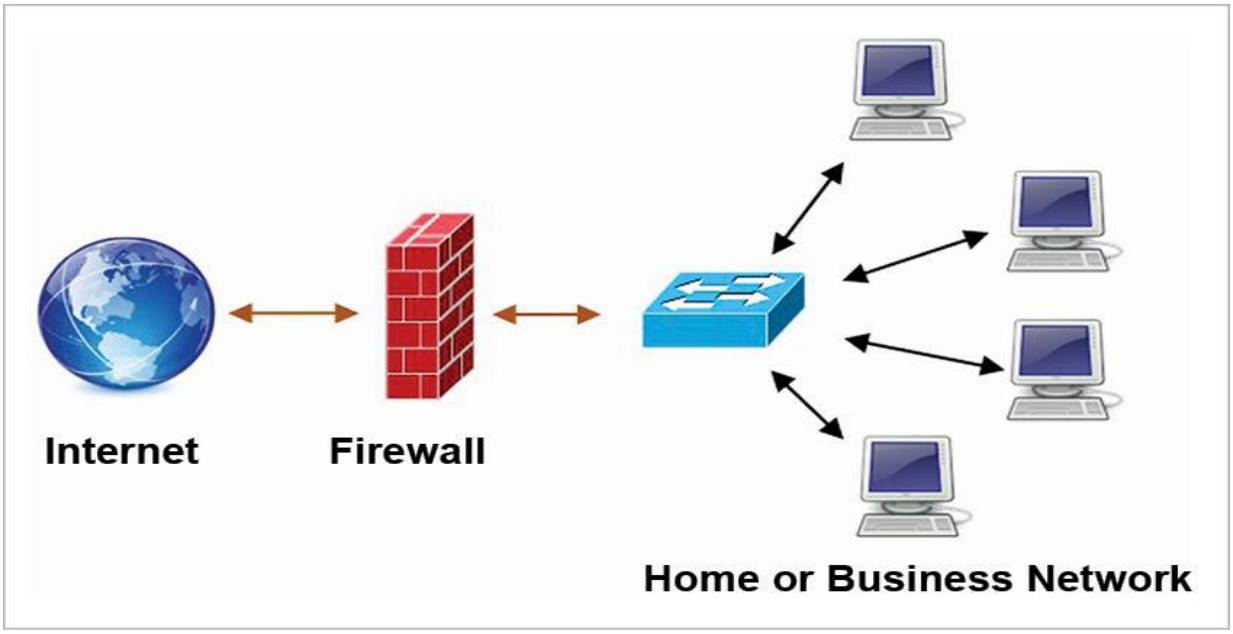
- حزمة التصفية(Packet Filtering): تستخدم معظم جدران الحماية من الجيل الأول تصفية الحزمة الأساسية ، والتي تعمل على فحص محتويات الأوامر الموجهة لنظام وشبكة التشغيل وهذا بسماح أو برفض الخدمة المطلوبة ، وهذا بإعتماد على نوع التصفية وطبقة أو تركيز بروتوكول التصفية والحماية[59]. تعتمد التصفية على فحص جميع البيانات التي تمر على الشبكة وقيام بفلترتها.
- خدمة الوكيل(Proxy Service): يتم إستخدام الخوادم الوكيلة بشكل عام في طبقة التطبيق the application layer ، ويتم برمجتها لإعطاء أكثر سرية ولعدم الكشف عن هويتها للعملاء الذي يصلون إلى مزودي الخدمة على نطاق أوسع[60] ، ويعمل الوكيل على إخفاء الهوية وكجدار حماية بين الأنظمة و الشبكات.
- التفيش الجليل (Stateful Inspection): يعمل جدار الحماية في هذه الحالة الى تتبع العيوب المحددة ، ويسمح لجميع الحزم الى التدفق في كلا الإتجاهمين بعبور جدار الحماية[61] ، بحيث يعمل الجدار الحماية على تتبع حالة الإتصال بين الأنظمة بحيث يقوم بتحقق من نوع البيانات Data التي تمر عبر الشبكة والنظام ، ويقوم بتتبع ومعرفة عناوين البروتوكلات " IP address " لكل الأجهزة التي يتم تعامل معها ونوع الأجهزة التي تتصل ببعضها.

وتتعدد أنواع الجدار الأمني الىScreening Routers والتي تقوم بغربلة وتصفية مدخلات الشبكة وكواجهة أولية لحماية الشبكة ، الأجهزة Hardware ، أو برامج كمبيوتر Software :

- أجهزة جدران الحماية Hardware Firewalls: يتم عزل أجهزة الحماية من الكمبويتر ، وهذا في حالة تم تعرض أجهزة الأمن لضرر ، سيكون الكمبويتر محمي من طرف جدران الحماية الثانية على شكل برامج مثبتة مثبتة مسبقا[62]، وتتمثل أجهزة جدران الحماية في: شكل أجهزة توجيه Routers، و مبدل (شبكات) Network Switch.

[59] Same prev ref. p: unkown
[60] Avinash Kak, **Lecture 19: Proxy-Server Based Firewalls: Lecture Notes on "Computer and Network Security"** , Purdue University: Indiana, United States, March 30, 2021
[61] Avishai Woo, **Packet Filtering and Stateful Firewalls**, School of Electrical Engineering, Tel Aviv University, Isreal, p6
[62] Mark Ciampa, **Security Awareness: Applying Practical Security In New World**, Cengage Learning; 5th edition United States, 2015, p95

- برنامج جدار الحماية Software: والتي تكون عبارة على برامج تثبت على الكمبيوتر وتوفر حماية للجهاز من الشبكة الخارجية، وعادة ما يتم دمج ذلك مع برنامج مضاد للفيروسات Antivirus.



رسم يوضح ويشرح كيفية عمل الجدار الأمني لحماية الشبكة وأجهزة الأنترنت من التهديدات الخارجية

– وعاء العسل" Honeypots و DMZ:

Honeypot، أو مصيدة الهاكرز ، هو نظام حماية مخادع يحاكي شبكة كاملة لجذب المهاجمين وهذا من خلال التنكر مع نقاط الضعف الشائعة لجذب المهاجمين لدراسة ومراقبة وتحليل أنشطتهم ، والثغرات التي يتم استغلالها والطريقة التي ينفذ بها الإختراق والأدوات المستعملة من طرفهم [63]، كل هذا عن طريق الخداع ، والخداع هو أسلوب قديم قدم الصراع ، فقبل 800 قبل الميلاد قال **صن تزو Sun Tzu** في كتابه فن الحرب " الحروب تقوم على الخداع" ، ومن الأمثلة البارزة على استخدامه في الحرب نجد عملية الحارس الشخصي خلال الحرب العالمية الثانية ، عندما استخدمت قوات الحلفاء الخداع وجعلت الألمان يعتقدون ان الهجمات قادمة من اتجاه اخر[64]، ومنه جاءت الفكرة لإستخدام وتطوير تقنيات من طرف خبراء الأمن المعلوماتي والسيبراني لتتبع الثغرات الموجودة في الشبكات وأنظمة تخزين البيانات ودراسة الطرق التي يعمل بها الهاكرز من أجل الحد والتصدي لهم. فا Honeypot هي تكنولوجيا وتقنيات تعمل على جمع المعلومات والثغرات حول

[63] Chee Keong Ng · Lei Pan · Yang Xiang, **Honeypot Frameworks and their Applications: A New Framework**, Springer, Singapore, 2018, p1

[64] Allen Harper, Daniel Regalado, Branko Spasojevic, Chris Eagle, Stephen Sims, Ryan Linn, Shon Harris, Gray Hat **Hacking: The Ethical Hacker's Handbook, Fifth Edition**, McGraw-Hill Education, 2018, p594

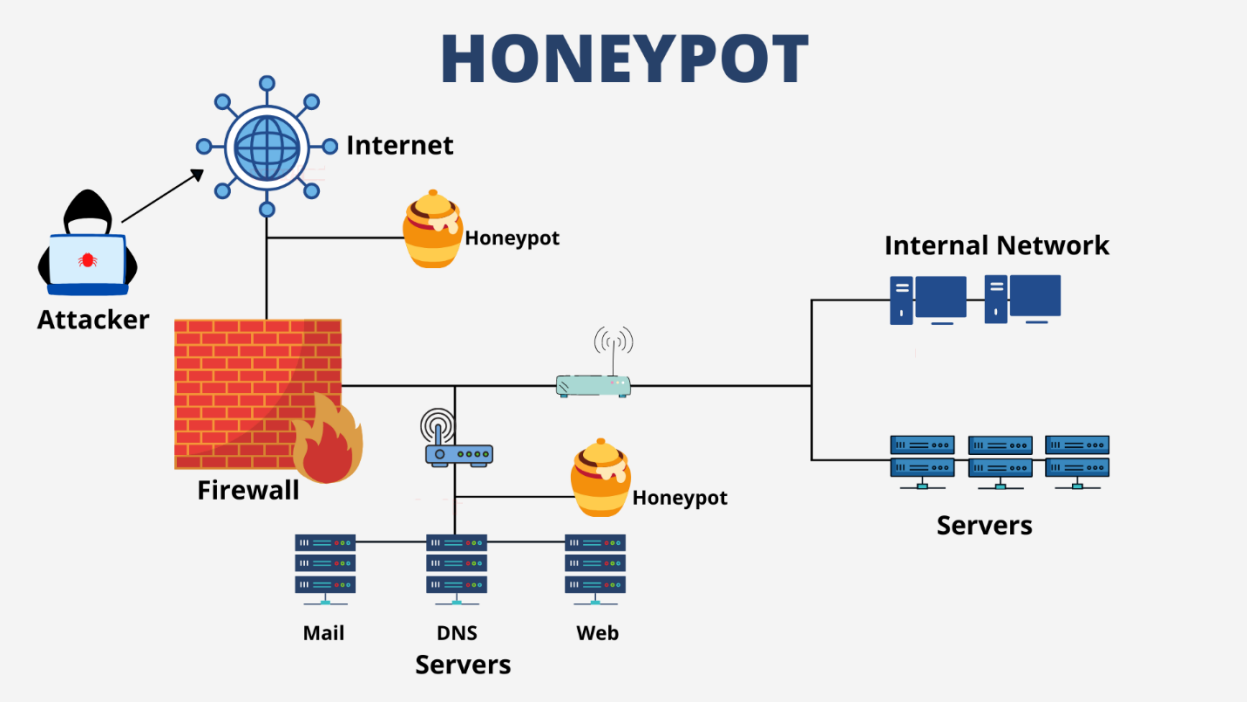
الهجمات من خلال استدراج المتسللين لتنفيذ الهجوم أو عمل ضار، وهي بمثابة طعم يغري المستخدمين سواء كانوا يعملون داخل المؤسسة أو خارجها لكشف ورصد وتحليل تحركات المهاجم المشتبه بهم.[65]

ويوجد نوعان ل Honeypots ، وهما مصيدة الإنتاج (Production Honeypot) ، و Research Honeypot، ويكمن الفرق بينهم في توجيهات وأهداف الإستخدام:

- Research Honeypot: تُستخدم هذه للبحث في التهديدات التي تواجهها المنظمات وكيفية توفير حماية أفضل لتهديدات ، يركز هذا النوع بشكل أكبر على البحث في تصرفات المتسلل بإستخدام عدد من من التقنيات الطرق المختلفة لجذب المهاجم ، لا تضيف هذه التقنية قيمة مباشرة الى المنظمة، و بدلاً من ذلك يتم استخدامها للبحث في التهديدات وكيفية الحماية بشكل أفضل من تلك التهديدات ، وتستخدم النتائج المحصل عليها للبحث في مخاطر الأمنية والكيفيات التي ينبغي تفعيلها لتجنب وتوفير حماية أفضل للشبكة ، ويتم استعمال هذه التقنية من طرف الجامعات ، والحكومات ، المخابر الأمن السيبراني للجيوش ، ومنظمات و الشركات التي تعمل في الأمن المعلوماتي والسيبراني.[66]

- Production Honeypot: تركز هذه التقنية على الجانب الدفاعي ، ويتم نصب هذه المصيدة خلف جدار الحماية ويتم اخفاءه داخل شبكة الإنتاج والهدف منه هو إبعاد المهاجم عن النظام الفعلي ، بحيث يخلق تصور وبيئة وهمية بأن المهاجمين يهاجمون النظام الفعلي والرئيسي ، ومنه يتم تنبيه لمدير النظام والفريق المكلف بحماية وأمن الشبكة من هذا الإختراق[67]. يتم تنصيب Honeypot في هذه الحالة مع بقية السيرفرات الحقيقية و يتم وضع بيانات حقيقية عليها لكي يتم استدراج المهاجم ، لتنفيذ الهجوم.

[65] R. C. Joshi, Anjali Sardana, **Honeypots: A New Paradigm to Information Security**, Published by Science Publishers, United States, 2011, p2
[66] Same prev ref : p15
[67] Chee Keong Ng · Lei Pan · Yang Xiang, **Honeypot Frameworks and their Applications: A New Framework**, Springer, Singapore, 2018, p8



صورة تمثيلية لطريقة عمل Honeypot

مصدر الصورة: https://cyberfishnews.com/comprehensive-guide-on-honeypots-14925.html

المبحث الثالث: الإستراتجيات الولايات المتحدة الأمريكة للتصدي للهجومات السيبرانية

غالبا ما ظهرت الولايات المتحدة الأمركية على أنها وراء موجة التهديدات السيبرانية والهجومات التي تستهدف أمنها الوطني ، وحتى وان كان أمن الأنترنت يمثل مشكلة حاسمة في الولايات المتحدة ، فقد إستغرق الأمر وقتا حتى تتخذ السلطات إجراءات فيدرالية لمكافحة الهجمات الإلكترونية في الفضاء السيبراني ، ومن خلال معالجة الأمن السيبراني بإعتباره أمرًا بالغ الأهمية للأمن القومي الأمريكي والسلامة العامة والخصوصية الشخصية والحريات المدنية ، قرر الرئيس الأمريكي أوباما تحويله الى قضية حيوية لكل من الأمة والمواطنين في عام 2009، فشرعت إدارة أوباما في صياغة إستراتيجية للأمن السيبراني من أجل مواجهة التهديدات والتي شبهها الرئيس بـ "أسلحة الدمار الشامل". [68]

وفي هذا الخصوص قال **الرئيس أوباما** في سنة 2013:

"يعتمد الإزدهار الاقتصادي لأمريكا والأمن القومي وحرياتنا الفردية على إلتزامنا بتأمين الفضاء السيبراني والحفاظ على أنترنت مفتوح وقابل للتشغيل المتبادل و وآمن وموثوق. لا تزال بنيتنا التحتية الحيوية معرضة للخطر من التهديدات في الفضاء السيبراني ، ويتضرر اقتصادنا من سرقة ملكيتنا الفكرية ، على الرغم من أن التهديدات خطيرة وتتطور باستمرار ، أعتقد أنه إذا تعاملنا معها بشكل فعال ، يمكننا ضمان بقاء الإنترنت محركًا للنمو الاقتصادي ومنصة للتبادل الحر للأفكار." [69] **الرئيس أوباما(البيت الأبيض2013)**

و قبل أوباما ، أطلقت إدارة بوش مبادرة الحكومة الوطنية الشاملة للأمن السيبراني (CNCI) في عام 2008 تحت غطاء من السرية مما أدى إلى انتقادات حادة من مجموعات الخصوصية والحريات المدنية. تضمنت المبادرة 12 توجيهًا تغطي الشبكات العسكرية والمدنية والحكومية وأنظمة البنية التحتية الحيوية ، لكن بالنسبة للنقاد لم تتمكن من تقديم ضمانات كافية بأن السعي وراء الأمن السيبراني لن يشمل مراقبة شبكات القطاع الخاص وحركة الإنترنت. [70] ، وكان هدف إدارة بوش من إنشاء المبادرة الوطنية الشاملة للأمن السيبراني هو تفعيل الإستجابة و التعامل بشكل إستباقي مع الكيانات التي ترغب في سرقة أو تلاعب بالبيانات المحمية على الأنظمة الفيدرالية الأمنة. [71]

---

[68] Marianne STONE, **Obama's Cybersecurity Plan**, Columbia University, School of International and Public Affairs SECURITY TECHNOLOGY POLICY PAPERS SERIES 1, 1 (Spring 2010), New York, p2

[69] Anthony J. Masys (Editor), **Exploring the Security Landscape: Non-Traditional Security Challenges**, Springer International Publishing, Switzerland, p46

[70] Same prev ref, p2

[71] John W. Rollins, Anna C. Henning**, Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations**, Congressional Research Service, Report#: R40427, March 10, 2009, p2

وتعد الولايات المتحدة الأمريكية من بين أكبر الجهات الفاعلة واستخداما للفضاء السيبراني ، وعلى سبيل المثال ، أنظمة شبكات الكمبيوتر هي مسؤولة على وظائف هامة مثل " إدارة وتشغيل محطات الطاقة النووية و السدود وشبكة الطاقة الكهربائية ونظام مراقبة الحركة الجوية والبنية التحتية المالية ، علاوة على ذلك تلعب أنظمة شبكات الكمبيوتر دورًا أساسيًا في العمليات اليومية للحكومة والمنظمات و الشركات من خلال إدارة كشوف المرتبات وإجراء البحث والتطوير وإجراء وتتبع المبيعات وحركة البضائع " ، وفي ظل هذا الإعتماد الكبير والمتزايد للدولة على أنظمة شبكات الكمبيوتر و الإعتماد المتبادل بين المواطنين العاديين ، تظل البيانات والمعلومات الحساسة عرضة للهجوم والإستغلال ، وبالتالي يظل أمن الفضاء السيبراني أولوية للقطاعين العام والخاص في البلاد. [72] ومنه عمل الرئيس السابق للولايات المتحدة دونالد ترامب مع الإدارة التي اشتغلت معه على تعزيز وحماية الأمن السيبراني من خلال تقديم الإستراتجية السيبرانية الوطنية في سبتمبر من سنة 2018 و التي تتناول أهمية القانون الدولي و "القواعد" لتنظيم النشاط السيبراني، وكذا تم في نفس السنة إصدار الاستراتيجية السيبرانية لوزارة الدفاع ، هذه الوثيقة الخاصة بوزارة الدفاع تؤطر أدوار الجيش فيما يتعلق بالفضاء السيبراني. وفي هذا السياق كتب **الرئيس دونالد ترامب:**

" إن حماية الأمن القومي لأمريكا وتعزيز رخاء الشعب الأمريكي هما على رأس أولوياتي. يعد ضمان أمن الفضاء الإلكتروني أمرًا أساسيًا لكلا المساعدين. يعد الفضاء الإلكتروني جزءًا لا يتجزأ من جميع جوانب الحياة الأمريكية ، بما في ذلك اقتصادنا ودفاعنا. ومع ذلك ، لا تزال كياناتنا الخاصة والعامة تكافح لتأمين أنظمتها ، وقد زاد الخصوم من وتيرة وتعقيد أنشطتهم الإلكترونية الضارة. أنشأت أمريكا الإنترنت وشاركتها مع العالم. الآن ، يجب أن نتأكد من تأمين الفضاء الإلكتروني والحفاظ عليه للأجيال القادمة. في الأشهر الـ 18 الماضية ، إتخذت إدارتي إجراءات لمواجهة التهديدات السيبرانية ، لقد فرضنا عقوبات على الجيهات الفاعلة السيبرانية الخبيثة. لقد وجهنا لائحة اتهام ضد أولئك الذين ارتكبوا جرائم سيبرانية لقد نسبنا نشاطًا ضارًا بشكل علني إلى الخصوم المسؤولين وأصدرنا تفاصيل حول الأدوات التي استخدموها. لقد طلبنا من الإدارات والوكالات إزالة البرامج المعرضة لمخاطر أمنية مختلفة. لقد اتخذنا إجراءات لمساءلة رؤساء الإدارات والوكالات عن إدارة مخاطر الأمن السيبراني للأنظمة التي يسيطرون عليها ، مع تمكينهم من توفير الأمن الكافي " [73]. **(مقدمة الرئيس دونالد ترامب في الإستراتجية السيبرانية الوطنية)**

[72] Kayla Morency, **CYBERSECURITY FINALLY TAKES CENTER STAGE IN THE U.S**, Journal of High Technology Law, 2014, p193-194

[73] NATIONAL CYBER STRATEGY of the United States of America SEPTEMBER 2018. Link: https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

المطلب الأول: إستراتيجية الأمن السيبراني في فترة باراك أوباما.

في الوثيقة للإستراتيجية الأمن القومي (NSS) الأمريكي لسنة 2010 ، وهي وثيقة يتم اعدادها بشكل دوري من قبل الفرع التنفيذي للولايات المتحدة والتي يتم فيها سرد مخاوف الأمن القومي وكيف تخطط الإدارة للتعامل معها ، أشارة إدارة باراك أوباما بدقة إلى نهجها في عدد من المجالات الرئيسية:

- **التدخل العسكري:** حيث كانت إدارة أوباما مترددة في شن عمليات عسكرية كبيرة في الخارج ،على غرار ما حاول سلفه في أفغانستان و العراق خلال فترة جورج بوش.
- **العراق:** أوضحت الإستراتيجية الأمن القوي أن الولايات المتحدة ستنسحب من العراق، وهو أمر استمرت في القيام به بشكل شامل، واستخدمت أمريكا بعد ذلك العمل العسكري المباشر في العراق بتردد كبير.
- **إيران/ الإنتشار النووي:** أشارت الإدارة إلى نيتها في متابعة التقارب الدبلوماسي والحل التفاوضي إذا كان ذلك ممكنًا.
- **مكافحة الإرهاب:** اتبعت الإدارة استراتيجية استباقية لمكافحة الإرهاب ، والتي تضمنت برنامج القتل المستهدف ، وزيادة استخدام ضربات الطائرات بدون طيار.[74]

ستبقى المواضيع المذكور أعلاه ذات مركزية لاستراتجية للإدراة أوباما ، وعندما يتم اطلاق الإستراتجية القادمة ، ستبقى من المرجح أن تبرز ثلاث مجالات في ضوء التحديات الناشئة منذ عام 2010 ، وفي هذا الخصوص قدم الرئيس أوباما مراجعة فيما يخص سياسة الفضاء السيبراني وهذا نظرا الى التهديدات المتزايدة التي تستهدف الولايات المتحدة ، وهذا " لتقييم السياسات والهياكل الأمريكية للأمن السيبراني" وتمثل المراجعة الخطوة الأولى من تعهد الرئيس بقيادة جهد والعمل مع القطاع الخاص ومجتمع البحث والمواطنين لبناء بنية تحتية إلكترونية جديرة بالثقة وخاضعة للمساءلة تتسم بالمرونة وتحمي الميزة التنافسية لأمريكا وتعزز أمننا القومي والوطني. وقد ركزت مراجعة السياسة على عدد من القضايا التي تؤثر على الأمن السيبراني أو تتأثر به ، بدءًا من الخطط القصيرة إلى المتوسطة الأجل ، كما تحاول الوثيقة المقدمة من طرف إدارة أوباما إعادة تنظيم النهج المعمول به في السابق ، من طرف إدارة جورج بوش ، من خلال مبادرة الوطنية الشاملة للأمن السيبراني "Comprehensive National Cybersecurity Initiative (CNCI)". التي يرى فريق المكلف من طرف

[74] Adam Quinn, **Obama's National Security Strategy Predicting US Policy in the Context of Changing Worldviews**, Chatham House the Royal Institute of International Affairs, Research Paper: US Project January 2015, p2-3

الرئيس أوباما على انها بحاجة الى الكثير من التحسين. ومن من بين الأهداف التي أقرتها المراجعة المقدمة من طرف الرئيس أوباما:

- **القيادة من الأعلى:** يكون البيت الأبيض مسؤولاً عن اتخاذ زمام المبادرة لتحديث قدرة الدولة على التعامل مع التهديدات السيبرانية فضلاً عن القضايا الأخرى ذات الصلة مثل القواعد القانونية.
- **بناء القدرات لأمة رقمية:** على الرغم من أن الأمن السيبراني كان على رادار الحكومة لبعض الوقت ، إلا أن عامة الناس ليس لديهم وعي كافي بالمسألة ، لذا ستساعد زيادة هذا الوعي عند الأمريكيين على اتخاذ خيارات أكثر ذكاءً وإدارة المخاطر بطريقة أكثر كفاءة.
- **تقاسم المسؤولية الأمن السيبراني:** قضية الأمن السيبراني هي قضية عالمية. لذلك يجب ان يشارك كل من القطاعين العام والخاص والجهات الفاعلة الوطنية والدولية في العملية حتى تنجح ، كما ينبغي تطوير هذا التعاون بين القطاعات وكذلك على المستوى الدولي.
- **إنشاء مشاركة فعالة للمعلومات والاستجابة للحوادث:** يجب أن تتمركز جهود الاستجابة حول مسؤول الأمن السيبراني المعين من قبل الرئيس. يجب أن يكون إطار الاستجابة واضحًا وموحدًا مع تعزيز تبادل المعلومات لتحسين القدرات.
- **تشجيع الإبتكار:** تعزيز تطوير التقنيات الجديدة والمحسّنة من خلال البحث والتطوير المبتكر الذي يمكن أن يساهم في زيادة أمان الفضاء السيبراني. يجب أن يقترن هذا بتقنية المصادقة الجديدة " authenticating technology" (أي إدارة الهوية والقياسات الحيوية) لضمان أن تبادل البيانات جدير بالثقة وأكثر أمان وحماية. [75]

كما قد تم التطرق الى الإستراتجيات العمل وتطوير أليات الحماية للفضاء السيبراني في تقرير مراجعة الدفاع الرباعي (QDR) لسنة 2010 ، وهذا بالعمل على تمكين القوات العسكرية البرية و الجوية والبحرية على محاربة صراعات المحدودة وواسعة النطاق وردعها ، وكذا تمكين هذه القوات من من خلال القدرات السيبرانية والفضائية وتعزيزها ضد التحديات التي تطرحها الجماعات الحكومية والغير حكومية[76]. كما تم توجيه أوامر بالعمل بفعالية في الفضاء السيبراني ، كون أن البيئة الأمنية تتطلب قدرات محسنة لمواجهة التهديدات في الفضاء السيبراني ، كون أنه في القرن الحادي والعشرين ، لا تستطيع القوات المسلحة

[75] Marianne STONE, Obama's Cybersecurity Plan, Columbia University, School of International and Public Affairs SECURITY TECHNOLOGY POLICY PAPERS SERIES 1, 1 (Spring 2010), New York, p 2-3
[76] Quadrennial Defense Review Report, February 2010 p: v
https://archive.defense.gov/qdr/QDR%20as%20of%2029JAN10%201600.pdf

الحديثة التصرف ببساطة بدون شبكات معلومات واتصالات مرنة وموثوقة و وصول مضمون الى الفضاء السيبراني، لذا يجب على على وزارة الدفاع الأمريكية برفع الحماية الدفاع بن شبكتها ، ومنه تتخذ وزارة الدفاع عدة خطوات لتعزيز القدرات في الفضاء السيبراني وتتمثل في:

- تطوير نهج أكثر شمولاً لعمليات وزارة الدفاع في الفضاء السيبراني.
- تطوير قدر أكبر من الخبرة والوعي السيبراني.
- انتهاج خطط مركزية لقيادة العمليات السيبرانية ، وتعزيز الشراكات مع الوكالات والحكومات الأخرى.[77]
- كما سيتم تحسين قدرات ومرونة وقوة القوات الأمريكية في جميع المجالات من خلال نشر أنظمة تمكين أكثر وأفضل ، بما في ذلك نظام مراقبة الاستخبارات والمراقبة والاستطلاع ، وقدرات الهجوم الإلكتروني ، وشبكات الاتصالات ، والبنية التحتية الأساسية الأكثر مرونة ، والدفاعات الإلكترونية المحسنة.[78]
- تمكين القوات من خلال قدرات الفضاء السيبراني وتعزيز قدرات الجيش لحرمان الخصوم من أهدافهم من خلال الدفاع الصاروخي الباليستي ، كما تواصل وزارة الدفاع جهودها في تحسين قدرتها ردع هجمات أسلحة الدمار الشامل و الفضاء السيبراني ، وتحميل المعتدين المسؤولية وحرمانهم من القدرة على تهرب من الكشف من خلال استخدام وكلاء.[79]

و كملخص لما جاء في تقرير لسنة 2010 في ما يخص الفضاء و الأمن السيبراني ، توجيهات بالعمل بشكل فعال في الفضاء السيبراني وهذا من خلال اتخاذ وزارة الدفاع عددًا من الخطوات لتعزيز قدراتها في الفضاء السيبراني ومتمثلة في:

- **تطوير نهج شامل لعمليات وزارة الدفاع في الفضاء السيبراني.**
- **تطوير قدر أكبر من الخبرة والوعي بالفضاء السيبراني.**
- **مركزية قيادة عمليات الفضاء الإلكتروني.**
- **تعزيز الشراكات مع الوكالات والحكومات الأخرى.**[80]

[77] Quadrennial Defense Review Report, February 2010 p: i x- x
https://archive.defense.gov/qdr/QDR%20as%20of%2029JAN10%201600.pdf
[78] Same prev ref, p x
[79] Same prev ref p14-15.
[80] Same prev ref p37 - 38

وفي استراتيجية الأمن القومي المقدمة من طرف إدارة الرئيس باراك أوباما في شهر ماي سنة 2010 ، تم التطرق الى موضوع تأمين الفضاء السيبراني " Secure Cyberspace " ، كون أن تهديدات الأمن السيبراني تمثل أحد أخطر تحديات الأمن القومي والسلامة العامة والإقتصادية التي تواجه الولايات المتحدة كأمة ، وقد تم الإشارة الى ان التقنيات ذاتها التي تمكّننا من القيادة والإبداع تعمل أيضًا على تمكين أولئك الذين قد يعطّلون ويدمرون مصالح الأمريكية ، بحيث تساهم التقنيات و التكنولوجيا من تفوق العسكري ، في حين تشكل الشبكات الحكومية الغير سرية تخضع دائما لمحاولات اختراق وهجومات من طرق المتسللين ، تعتمد حياتنا اليومية وسلامتنا العامة على الطاقة والشبكات الكهربائية ، لكن الخصوم المحتملين يمكنهم استخدام الثغرات السيبرانية لتعطيلها على نطاق واسع. الإنترنت والتجارة الإلكترونية هما عاملان ومفتاحان أساسيان في قدرتنا التنافسية الاقتصادية ، لكن مجرمي الإنترنت كلفوا الشركات والمستهلكين مئات الملايين من الدولارات وقد تسببوا في خسائر وأضرار للملكية الفكرية للولايات المتحدة ، وتتراوح التهديدات التي تواجه الولايات المتحدة من المتسللين المجرمين كأفراد ، وصولا الى الجماعات الإجرامية المنظمة من الشبكات الإرهابية الى الدول القومية المتقدمة ، و يتطلب الدفاع ضد هذه التهديدات لأمننا وازدهارنا وخصوصيتنا الشخصية على على تعزيز شبكات للوصول الى نتائج آمنة ومرنة وجديرة بالثقة ، وبالتالي ، فإن بنيتنا التحتية الرقمية هي أحد الأصول الوطنية الإستراتيجية ، وحمايتها – مع الحفاظ على الخصوصية والحريات المدنية – هي أولوية للأمن القومي. سنقوم بردع الاختراقات والهجمات السيبرانية ومنعها و العمل على التعافي بسرعة من الاختراقات والهجمات السيبرانية عن طريق:

- **الاستثمار في الأفراد والتكنولوجيا:** لتحقيق هذا الهدف ، نعمل عبر الحكومة ومع القطاع الخاص لتصميم تكنولوجيا أكثر أمانًا تمنحنا القدرة على حماية أفضل وتحسين مرونة الأنظمة والشبكات الحكومية والصناعية الهامة ، كما سنواصل الاستثمار في أحدث الأبحاث والتطوير الضروريين للابتكار والاكتشاف اللذين نحتاجهما لمواجهة هذه التحديات.
- **تعزيز الشراكات:** كون أن لا الحكومات ولا القطاع الخاص ولا المواطنين بإمكانهم مواجهة هذا التحدي بمفردهم ، سنقوم بتوسيع طرق عملنا معًا كما سنعمل على تعزيز شراكاتنا الدولية بشأن مجموعة من القضايا ، بما في ذلك وضع معايير للسلوك المقبول في الفضاء السيبراني ؛ القوانين المتعلقة بالجرائم الإلكترونية ؛ حفظ البيانات وحمايتها وخصوصيتها ؛ وأساليب دفاع الشبكة والاستجابة للهجمات

السيبرانية ، والعمل على الصعيدين الوطني والدولي للتحقيق في التطفل السيبراني ولضمان استجابة منظمة وموحدة للحوادث السيبرانية المستقبلية.[81]

وفي 16 ماي سنة 2011 ، أصدرت إدارة أوباما استراتجيتها الدولية للفضاء السيبراني " الرخاء والأمن والإنفتاح في عالم متصل بالشبكات ، صرح الرئيس أوباما ان الإستراتجية الدولية تمثل " المرة الأولى التي تضع فيها أمتنا نهجًا يوحد مشاركتنا مع الشركاء الدوليين بشأن النطاق الكامل للقضايا السيبرانية." وهذا لتشكيل وبناء نهج لتعظيم فوائد الفضاء السيبراني والتخفيف من التهديدات لإستخدامه الموسع ، وأكدت إدارة أوباما على الحاجة إلى بناء " سيادة القانون" من خلال قواعد والعمليات الدولية ، ويدل هذا على البصيرة الإستراتيجية والدور الذي توليه إدارة أوباما للقانون الدولي في رؤيتها لمستقبل الفضاء السيبراني.[82]

وعليه فقدت تضمنت الإستراتجية الدولية للفضاء السيبراني ، النهج الإستراتيجي الذي ستتبناه وتعمل عليه الولايات المتحدة ، وهذا كون السياسة الدولية للفضاء السيبراني هو الإعتقاد بأن التقنيات الشبكية لها إمكانات هائلة لأمتنا وللعالم ، فقد شهدت الولايات المتحدة على العقود الثلاثة الماضية تقنيات أحدثت ثورة في اقتصاد الأمريكي ، وكما شهدت أيضًا تحديات غير متصلة بالإنترنت تنتقل الى الأنترنت مثل الإستغلال و العدوان ، وفي هذا السياق ستنتهج الولايات المتحدة سياسة دولية للفضاء السيبراني تعمل على تمكين الإبتكار الذي يقود الاقتصاد الأمريكي و يحسن الحياة هنا و في الخارج ، وفي كل هذا العمل و الجهود ستركز الولايات المتحدة على مبادئ أساسية لسياستها الخارجية و لمستقبل الأنترنت ، وهذا وفق الإستراتجيات التالية:

1- البناء على النجاحات: بحيث تلتزم الولايات المتحدة بالحفاظ على فوائد الشبكات الرقمية لمجتمعاتنا واقتصاداتنا وتعزيزها.

2- التعرف على التحديات: بحيث تقر الولايات المتحدة بأن نمو هذه الشبكات يجلب معه تحديات جديدة لأمننا القومي والاقتصادي وأمن المجتمع العالمي.

3- الإرتكاز على المبدأ: وفي هذا السياق ستواجه الولايات المتحدة هذه التحديات مع الحفاظ على مبادئها الأساسية. و المتمثلة في:

- **الحريات الأساسية:** وهذا بإلتزام بالحرية التعبير، وجميع الحريات المدنية.

[81] National Security Strategy, May 2010 , p27-28 , direct link: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/national_security_strategy.pdf

[82] David P. Fidler, **International Law and the Future of Cyberspace: The Obama Administration's International Strategy for Cyberspace**, American Society of International Law (ASIL), June 08, 2011. Direct link: https://www.asil.org/insights/volume/15/issue/15/international-law-and-future-cyberspace-obama-administration%E2%80%99s

- **الخصوصية:** تجمع الإستراتجية بين التزام بحماية المواطنين و المصالح الأمريكية والتزام بالخصوصية وتوفير الحماية من أي احتيال وسرقة أو تهديد لسلامة الشخصية.
- **التدفق الحر للمعلومات:** تلتزم الولايات المتحدة بتعزيز وحماية التدفق الحر للمعلومات. [83]

ولقد جاء في تقرير مراجعة الدفاع الرباعي (QDR) لسنة 2014 ، على أن الولايات المتحدة الأمريكية تواجه بيئة أمنية سريعة التغير وهذا في ظل بروز التقنيات ومراكز القوة الجديدة ، مما يجبر الولايات المتحدة للتركيز على التحديات الإستراتيجية وظبطها في وسط هذه المتغيرات ، والتي تشكل تهديدا للولايات المتحدة ، ولا سيما من الأنظمة في كوريا الشمالية و إيران ، وكما تستمر هذه الإضطرابات والعنف في أماكن أخرى مما يخلق بيئة خصبة للتطرف العنيف والصراع الطائفي ، لا سيما في الدول الهشة التي تمتد من الساحل إلى جنوب آسيا ، والتي تهدد مواطني الولايات المتحدة في الخارج ، وفي خلال هذه الأثناء ، تتطور الحرب الحديثة بسرعة ، مما يؤدي إلى تزايد نزاعات في المجالات الجوية والبحرية والفضائية ، وكذلك الفضاء السيبراني. وفي هذا الخصوص وفي ما يتعلق بالفضاء السيبراني ، ستعمل الولايات المتحدة على:

- تفعيل ورفع من نسق عمل القوة المشتركة واستعدادها لمحاربة الأعداء المتطورين والمتزايدين من خلال محاولتهم لحرمان القوات الأمريكية من المزايا التي تتمتع بها في الفضاء السيبراني، وهذا من خلال مواصلتنا للإستثمارات ذات الأولوية في العلوم والتكنولوجيا والبحث و التطوير داخل قطاع الدفاع وخارجه.
- تتخذ الإدارة خطوات لضمان استمرار التقدم في المجالات الأكثر أهمية لمواجهة التحديات المستقبلية مثل قدرات الفضاء السيبراني.
- العمل على تدعيم والحفاظ على توازن القوة المشتركة بحيث تظل حديثة وقادرة وجاهزة ، وفي هذا الصدد ستتخذ إدارة الرئيس أوباما خطوات إضافية التالية في ما يخص الفضاء السيبراني ، في الميزانية المالية لسنة 2015 ، وهذا بهدف الإستثمار في القدرات والإمكانات السيبرانية وهذا لتعزيز قدرتنا على إجراء العمليات في الفضاء السيبراني ودعم العمليات العسكرية جميع أنحاء العالم المنفذة من طرف القادة المقاتلين أثناء تخطيطهم وتنفيذ المهام العسكرية ، ومواجهة الهجمات الإلكترونية ضد الولايات المتحدة.
- مع نمو وتيرة التهديدات السيبرانية وتعقيدها ، سنستمر في إعطاء أولية عالية للدفاع السيبراني والقدرات السيبرانية ، بحيث ستقوم وزارة الدفاع بالردع تحت موافقة الرئيس أوباما وتوجيهات من وزير الدفاع ،

[83] INTERNATIONAL STRATEGY FOR CYBERSPACE: Prosperity, Security, and Openness in a Networked World, May 2011, p 4-5, Direct link: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

فإنها ستعطل وتحرم العدو من اجراء عمليات في الفضاء السيبراني التي من شأنها ان تهدد مصالح الولايات المتحدة ، وللقيام بذلك يجب أن نكون قادرين على الدفاع عن سلامة شبكاتنا وحماية أنظمتنا الرئيسية من أي استهداف أو عمليات سيبرانية، و دفاع عن الأمة من أي هجوم سيبراني مدمر للمصالح الحيوية للولايات المتحدة.[84]

- يتطلب ردع التهديدات السيبرانية ودحرها تحالفًا قويًا متعدد أصحاب المصلحة التي تتيح التطبيق القانوني للسلطات والحكومة ، و الحلفاء و الشركاء الدوليين، كما سنواصل دعمنا لفريق الأمن السيبراني للحكومة الفيدرالية وسنواصل العمل مع وزارة الأمن الداخلي (DHS) ، لتحسين الأمن السيبراني للبنية التحتية الحيوية ، ومع وزارة الأمن الداخلي ومكتب التحقيقات الفيدرالي لدعم تطبيق القانون ، كما ستظل وزارة الدفاع ملتزمة بالعمل الشركاء الدوليين أيضا ، وهذا من خلال مشاركة معلومات التهديد والقدرات لحماية البنية التحتية للولايات المتحدة والدفاع عنها وهذا كدورنا كوكالة خاصة بالقطاع للقاعدة الصناعية الدفاعية. [85]

في 6 فبراير من سنة 2015 أصدرت إدارة أوباما استراتيجية جديدة للأمن القومي (NSS) ، وكانت هذه الوثيقة الثانية التي تنشرها إدارة رئيس باراك أوباما ، بحيث نُشرت الوثيقة الأولى في شهر ماي من سنة 2010 ، وقد نصت الوثيقة الجديدة لسنة 2015 على ان الغرض منها هو " تحديد المبادئ والأولويات لتوجيه استخدام القوة و التأثير الأمريكي في العالم". وقد أكدت الوثيقة لعام 2015 على دور القيادة الأمريكية في السياق الدولي ، و يحتفظ تقرير سنة 2015 بالكثير من الأفكار الأساسية لإصدار سنة 2010 ، ومع ذلك ، يبدو ان تركيزها يتحول بعيدًا نحو العمل مع المؤسسات الدولية على ترسيخ القيادة المشتركة وهذا على المستوى الثنائي أو من خلال تسهيل التعاون بين الدول. كما أنها تتطلب خطاً أكثر صرامة مع كل من الصين وروسيا ، مع التأكيد على الرغبة في التعاون مع كليهما.[86] ، وقد تطرقت الوثيقة الى خطط الأمن بصفة عامة في مختلف المجالات الحساسة ، و إلى الأمن السيبراني بصفة خاصة من خلال مايلي:

- تم الإشارة للمجهودات التي قامت بها إدارة أوباما خلال 6 سنوات الماضية ، من خلال إشارة الى الدور الذي لعبته ادارته لوقف الأزمة المالية وتحفيز وإنعاش النمو الاقتصادي ، كما تم تعزيز ميزتنا

[84] Quadrennial Defense Review 2014, Department of Defense, p III – VII – 14 – 15, Direct link: https://archive.defense.gov/pubs/2014_quadrennial_defense_review.pdf
[85] Same prev ref, p15
[86] Nathan J. Lucas, Coordinator, Kathleen J. McInnis, **The 2015 National Security Strategy: Authorities, Changes, Issues for Congress**, Congressional Research Service, United States, January 30, 2017, p2. Direct link: https://www.everycrsreport.com/files/20170130_R44023_4c1b6b64f4dd43684f8f751370f551d7d0d45ae0.pdf

التنافسية وريادتنا في مجالات التعليم و الطاقة والعلوم والتكنولوجيا والبحث والتطوير والرعاية الصحية ، كما قد تم تحقيق تحولًا في مجال الطاقة في أمريكا الشمالية ، كما أننا نقوم بتحصين بنيتنا التحتية الحيوية ضد جميع المخاطر ، وخاصة التجسس والهجومات السيبرانية ، كما أكدت الوثيقة على ان إدارة الرئيس أوباما تعمل بجد لحماية الحريات المدنية وتعزيز الأمن.[87]

- يرتبط ويتصل العالم بالمساحات المشتركة ، كأنترنت والفضاء والجو والمحيطات والتي تتيح التدفق الحر للأشخاص والسلع والخدمات والأفكار وفي هذا الشأن ، ستعمل إدارة أوباما على ضمان الوصول الآمن الى هذه المساحات المشتركة ، بإعتبارها شرايين الاقتصاد العالمي والمجتمع المدني ، والوصول إليها معرض للخطر بسبب المنافسة المتزايدة والسلوكيات الإستفزازية ، لذلك سنستمر في في تعزيز قواعد السلوك المسؤول مع التأكد من أن لدينا القدرات اللازمة لضمان الوصول الى هذه المساحات المشتركة.
- بصفتنا مهد الأنترنت ، تتحمل الولايات المتحدة مسؤولية خاصة لقيادة عالم متصل بالشبكات ، كما يعتمد الازدهار والأمن بشكل متزايد على توفر إنترنت مفتوح وقابل للتشغيل المتبادل وآمن وموثوق، كما يرتبط اقتصادنا وسلامتنا وصحتنا من خلال البنية التحتية الشبكية التي تستهدفها الجهات الحكومية الخبيثة والإجرامية والأفراد الذين يحاولون التهرب وانكار مسؤوليتهم عن الخروقات القانونية التي يقومون بها من خلال استهدافهم لمنشئاتنا والبنيات التحتية و مراكز البيانات لأهداف تخريبية ، او التجسس ، وإعتمادا على اطار العمل في ما يخص الأمن السيبراني ، نحن نعمل على تأمين الشبكات الفيدرالية ونعمل مع القطاع الخاص والمجتمع المدني وأصحاب المصلحة الآخرين لتعزيز أمن ومرونة البنية التحتية الحيوية للولايات المتحدة ، كما اننا سنواصل العمل مع الكونغرس لمتابعة إطار تشريعي يضمن معايير عالية من الأمان الحماية للفضاء السيبراني ، كما أننا سندافع عن أنفسنا بما يتفق مع القانون الأمريكي والقانون الدولي ، ضد الهجمات السيبرانية ونفرض تكاليف على الجهات الفاعلة السيبرانية الضارة بما في ذلك من خلال مقاضاة النشاط السيبراني غير القانوني ، كما أننا سنساعد البلدان الأخرى على تطوير القوانين التي تمكن من اتخاذ إجراءات قوية ضد التهديدات التي تنشأ من بنيتها التحتية. و على الصعيد العالمي ، يتطلب الأمن السيبراني التمسك بمعايير السلوك الدولي الراسخة لتشمل حماية الملكية الفكرية وحرية الإنترنت واحترام البنية التحتية المدنية وإدارة الإنترنت كمسؤولية

[87] NATIONAL SECURITY STRATEGY, FEBRUARY 2015, p3 , Direct link: https://obamawhitehouse.archives.gov/sites/default/files/docs/2015_national_security_strategy_2.pdf

مشتركة بين الدول والقطاع الخاص مع المجتمع المدني ومستخدمي الإنترنت كأصحاب مصلحة رئيسيين.[88]

ومن خلال هذا يتبين حجم المجهودات التي بذلتها وعملت لأجلها إدارة الرئيس السابق أوباما في كل ما يخص الفضاء السيبراني و التهديدات التي تستهدف أمن الولايات المتحدة من خلال الإختراقات من الجهات المدعومة من طرف الدول والجيهات المناهضة للولايات المتحدة.

المطلب الثاني: إستراتيجية الأمن السيبراني في فترة دونالد ترامب.

في أكتوبر 2016 ، اتهمت الولايات المتحدة روسيا باختراق المنظمات السياسية المشاركة في الانتخابات الأمريكية ، وتسريب المعلومات المسروقة للتأثير على النتيجة ، وفي ديسمبر فرض الرئيس أوباما عقوبات على القرصنة والأعمال الغير قانونية التي قامت بها روسيا خلال حملة الانتخابية للمترشح دونالد ترامب ، وهيلاري كلينتون. وقد أثرت هذه الحادثة بإرث الرئيس أوباما في مجال الأمن السيبراني و القوانين و الخطط التي أقرها وعمل وفقها خلال السنوات السابقة لحكمه ، وقد شكل " الإختراق وتسريب المعلومات " إخفاق ومشاكل لما عمل من أجله الرئيس أوباما في ما يخص القوانين و القواعد الردعية المستحدثة في إستراتجياته الأمنية في ما يتعلق بالأمن السيبراني.

وبرغم من هذا الإختراق الإنتخابي الذي مس الولايات المتحدة ، إلا ان الرئيس المنتخب دونالد ترامب لم يُظهر إلا القليل من الاهتمام بهذا الشأن كونه لا يقدم أولوية للقيم الديموقراطية أو القانون الدولي في ما يخص معايير سياسة الأمن السيبراني ، وعكس ذلك كان الرئيس المنتخب ترامب قد استخف بتقارير حول التورط الروسي في عمليات اختراق وأبدى تقبله للنتائج ، ورغبته في تحسين العلاقات مع روسيا ، مما يعني ان هذا الحادث الذي مس الانتخابات الأمريكية لن يؤدي الى تعزيز وخلق نهج رادع في الأمن السيبراني بخصوص سياسات دونالد ترامب نحو روسيا. [89] وبينما دعا الرئيس المنتهية عهدته أوباما وأعضاء مجلس الشيوخ الجمهوريون البارزون مثل جون ماكين John McCain ، و ليندسي جراهام Lindsey Graham الى إتخاذ إجراءات صارمة ضد

[88] Same prev ref, p12-13

[89] David P. Fidler, **Cybersecurity and the Changing International Law of Data: The U.S. Election Hacks, Cybersecurity, and International Law**, American Journal of International Law: Volume 110, The American Society of International Law and David P. Fidler, Published online by Cambridge University Press: 15 February 2017.

روسيا ، صرح الرئيس المنتخب دونالد ترامب أن دور روسيا في الهجوم واختراق الانتخابات غير واضح ، و أن الإنتقام غير مناسب.[90]

وفي 18 ديسمبر 2017 أصدر الرئيس دونالد ترامب أول إستراتيجية للأمن القومي لإدارته وهذا وسط ضجة كبيرة في الفترة التي سبقت الإصدار من خلال ما تعرضت له سياسة ترامب الخارجية من عداء كبير وانتقادات التي صدرت في اتجاه إدارته على أساس خيانته للأممية الليبرالية الأمريكية و عمل على وفق أجندته المعلنة سابقا " أمريكا أولاً – America First ". بحيث كانت الردود الأولية على الخطاب الذي ألقاه ترامب خلال تقديمه للإستراتيجية من جانب الكثير من المجتمعات السياسية و الأكاديمية متناقضة[91]

في أحسن الأحوال ، حيث انتقد المحللون " الإطار الواقعي " للإستراتيجية ، وتركيزها على منافسة القوى "قوى عظمى" أو "دول كبيرة" ، والإعتماد المفرط الذي يبدو على الأدوات العسكرية لفن الحكم. [92] وقد تصورت وثيقة الإستراتيجية على ان العالم مقبل على منافسة شديدة في الأفق ومختلف جداً عما كان عليه في العقود الماضية كما نصت الوثيقة على أن الولايات المتحدة يجب أن تكون مستعدة للمنافسة في أفضل الظروف ، وقد ركزت الوثيقة على أربع أعمدة للإستراتيجية التي ستنتهج من إدارة الرئيس ترامب (مجالات المصلحة الوطنية) وهي:[93]

- **حماية الشعب الأمريكي ، و الوطن ، وطريقة حياة الأمريكيين:** بحيث تم تركيز في هذا العمود ، على أمن الحدود و المنطقة ، والدفاع ضد أسلحة الدمار الشامل ، و **مكافحة التهديدات البيولوجية والأوبئة** (والملاحظ في هذه النقطة هو تلميح و تطرق إستراتيجية دونالد ترامب الى موضوع التهديدات البيولوجية والمخاطر التي قد تنجم من المخابر " Biosafety level 4 laboratories – مخابر السلامة الحيوية من درجة 4 " ، وهذا من خلال العمل مع البلدان الأخرى لإكتشاف وتخفيف حالات تفشي الأمراض مبكرًا ومنع انتشارها ، وتشجيع البلدان الأخرى على الإستثمار في أنظمة الرعاية الصحية و تعزيز الأمن الصحي العالمي للإنسان والحيوان وهذا لمنع تفشي الأمراض المعدية ، عن طريق العمل مع الشركاء اخرين لتأكد من أن المختبرات التي تتعامل مع مسببات الأمراض الخطيرة كالفيروسات ، لديها تدابير السلامة والأمان الكافية) ، كل هذا كان في أواخر ديسمبر من سنة 2017 ، أي قبل ظهور فيروس كورونا بقرابة 3 سنوات. وكما تم التطرق الى الى تعزيز مراقبة الحدود و

[90] Sarah Kreps and Debak Das, **Warring from the virtual to the real: Assessing the public's threshold for war over cyber security**, Research and Politics, April-June 2017, p1

[91] Emma Ashford, Joshua R. Itzkowitz Shifrinson, **Trump's National Security Strategy: A Critics Dream**, Texas National Security Review: Volume 1, Issue 2 (March 2018) , p139

[92] Same prev ref

[93] Carlota García Encina, **The Trump Administration's National Security Strategy**, Real Instituto elcano (Royal Institute), Working Paper 14/2018: 13 July 2018, Spain, p3

سياسة الهجرة. و التصدي ومكافحة تهديدات الجهاديين الإرهابيين وتفكيك المنظمات الإجرامية ، والحفاظ على أمن أمريكا في عصر الأنترنت و تعزيز المرونة الأمريكية ، وهذا من خلال تأمين الشبكات والمعلومات الفيدرالية والبنية التحتية الحيوية لأمتنا ومكافحة الجرائم الإلكترونية.

- **تعزيز الرخاء الأمريكي:** ويركز هذا العمود على تجديد وإنعاش الإقصاد المحلي ، وتعزيز العلاقات الاقتصادية الحرة و العادلة و المتبادلة ، و الريادة في البحث والتكنولوجيا والابتكار والاختراع ، وتعزيز وحماية قاعدة ابتكار الأمن القومي الأمريكية.[94]

- **الحفاظ على السلام من خلال القوة:** وهذا من خلال التركيز على السياسة الدفاعية عبر تجديد المزايا والقدرات التنافسية لأمريكا ، بما في ذلك تحسين القدرة الفتاكة للقوة المشتركة ، وتوضيح المصالح الأمريكية في مناطق مختلفة حول العالم ، بالإضافة إلى طرق تعزيز المصالح الأمريكية باستخدام الوسائل الدبلوماسية والاقتصادية ، وقد تم التطرق في هذا السياق الى الفضاء و الفضاء السيبراني ، وهذا من خلال تعبير على إستخدام جهات فاعلة حكومية و غير حكومية للهجمات الإلكترونية للإبتزاز ، حرب المعلومات ، والتضليل و أكثر من ذلك تلحق هذه الهجمات ضرر بأعداد كبيرة من الأشخاص والمؤسسات وهذا بأقل قدر من إستثمار فيها نسبيًا ، وانكار تام من طرفهم لتورطهم في هذه الهجمات. بحيث تنظر العديد من الدول الآن إلى القدرات السيبرانية على أنها أدوات تأثير لإسقاط النفوذ ، ويستخدم البعض الأدوات السيبرانية لحماية و توسيع أنظمتهم الإستبدادية " أوتوقراطية – Autocratic regimes ، بحيث أصبحت الهجمات السيبرانية سمة رئيسية للصراع الحديث ، وفي هذا الصدد ستعمل الولايات المتحدة على ردع الجيهات الفاعلة الخبيثة التي تستخدم قدرات الفضاء السيبراني ضد الولايات المتحدة.
- **تعزيز النفوذ الأمريكي:** وهذا من خلال تحسين قدرة الولايات المتحدة على تحقيق النتائج المرجوة في المحافل متعددة الأطراف و أيضا توسيع دائرة مجتمع الدول و الحلفاء الذي التي تتشارك وتتعامل معهم الولايات المتحدة ، وفي هذا الصدد ستوفر الولايات المتحدة القيادة و التكنولوجيا لتشكيل وإدارة المجالات المشتركة كالفضاء ، والفضاء السيبراني ، والجوي ، و البحري ، وهذا في إطار القانون الدولي.[95]

[94] NATIONAL SECURITY STRATEGY of the United States of America, DECEMBER 2017
Direct link: https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf
[95] Same prev ref : NATIONAL SECURITY STRATEGY of the United States of America, DECEMBER 2017
Direct link: https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf

ويمكن تلخيص أهم ما جاء بخصوص تعزيز الأمن السيبراني وكل ما يرتبط بحماية الفضاء السيبراني من التهديدات في الإستراتيجية الأمن القومي لإدارة الرئيس دونالد ترامب في مايلي:

– تعتمد الإستراتيجية على الأمر التنفيذي للرئيس ترامب " تعزيز الأمن السيبراني للشبكات الفيدرالية و البنية التحتية الحيوية " والذي تم توقيعه في ماي 2017.

– كما ستعمل الإستراتيجية السيبرانية التي قدمتها إدارة ترامب على حماية الشبكات الأمريكية من خلال تأمين الشبكات ومكافحة الجرائم السيبرانية وتحسين عملية الإبلاغ عن الحوادث.

– ستعمل الإستراتيجية السيبرانية على تعزيز الاقتصاد الرقمي المرن و الحيوي ، كما ستعمل على حماية البراعة الأمريكية من التهديدات مثل سرقة الملكية و الفكرية.

– العمل على تطوير قوة عاملة متفوقة في مجال الأمن السيبراني من خلال التعليم و التوظيف.

– ستواجه الإستراتيجية السيبرانية السلوك المزعزع للإستقرار في الفضاء السيبراني من خلال تعزيز السلوك المسؤول بين الدول القومية والعمل على وجود عواقب للسلوك السيبراني غير المسؤوول.

– إطلاق مبادرة دولية للردع السيبراني.

– فضح و مواجهة التأثير الخبيث والحملات الإعلامية على الأنترنت.

– كما ستعمل الإستراتيجية السيبرانية الوطنية للرئيس دونالد ترامب على تعزيز الإنترنت آمن ومفتوح وهذا من خلال: تشجيع الدول على تعزيز حرية الإنترنت ، النهوض بنموذج أصحاب المصلحة المتعددين لحوكمة الإنترنت ، تعزيز البنية التحتية للاتصالات المفتوحة والقابلة للتشغيل المتبادل والموثوقة والآمنة ، بناء وتطوير القدرات السيبرانية الدولية.

– تقدم الإستراتيجية أولوية للحفاظ على أمن أمريكا في عصر الإنترنت.

– أصدرت إدارة ترامب عددًا من الاستراتيجيات الخاصة بالوكالات التي تؤكد على أهمية الأمن السيبراني.[96]

في جانفي من سنة 2018 ، أصدر وزير الدفاع الأمريكي " جيم ماتيس – Jim Mattis " استراتيجية الدفاع الوطني لعام 2018 National Defense Strategy (NDS) ، بتفويض من الكونغرس ، وقد حلت استراتيجية الدفاع الوطني محل مراجعة الدفاع التي كانت تجرى كل أربع سنوات " Quadrennial Defense Review " ، و الملاحظ هو أنه قد تم إستبدال QDR باستراتيجية الدفاع الوطني (NDS) في فترة رئاسة

[96] **President Donald J. Trump is Strengthening America's Cybersecurity**, September 20, 2018, Direct link: https://trumpwhitehouse.archives.gov/briefings-statements/president-donald-j-trump-is-strengthening-americas-cybersecurity/?utm_source=twitter&utm_medium=social&utm_campaign=wh

دونالد ترامب. [97] وقد أعادت الإستراتيجية الصادرة عن البنتاغون تعريف التحديات الجيوسياسية التي تواجه الولايات المتحدة واعترف بـ "عودة ظهور المنافسة الاستراتيجية طويلة المدى" مع الصين وروسيا كأولوية قصوى لوزارة الدفاع (DoD) ، قد أصدرت الإستراتيجية تحذيرًا خطيرًا من أن الميزة العسكرية النسبية للولايات المتحدة على خصومها قد "تآكلت" ومن أجل عكس هذا الاتجاه وتدارك الأوضاع يجب العمل على التحقق من طموحات منافسيها ، كما يجب على الدولة ، الإستثمار في تحديث القدرات الأساسية من خلال ميزانيات مستدامة يمكن التنبؤ بها ، كما ركزت الوثيقة على أهداف أساسية " كخلق قوة أكثر فتكًا تتميز بالاستعداد المعزز ، والمفاهيم التشغيلية المبتكرة.[98]

وفي هذا السياق تضمنت الوثيقة ، التوجيهات والإستراتجيات التي ستعمل وفقهم وزارة الدفاع في كل ما يخص الفضاء السيبراني ، و التهديدات التي تواجه الأمن القومي الأمريكي ، والتكنولوجيات التي ستعتمد عليها كل الجيهات الأمنية المسؤولة عن الدفاع السيبراني داخل الولايات المتحدة الأمريكية ، وهذا قد أقرت الوثيقة على أن الدول هي الجهات الفاعلة الرئيسية على المسرح العالمي ، لكن الجهات الفاعلة غير الحكومية تهدد أيضًا البيئة الأمنية بقدرات متطورة بشكل متزايد ، بحيث أحدث الإرهابيون والمنظمات الإجرامية العابرة للحدود و قراصنة الأنترنت و غيرهم من الجيهات الفاعلة الخبيثة من غير الدول تحولًا في الشؤون العالمية مع زيادة قدرات على شن وإحداث اضطرابات شاملة للدول ، بحيث لا يمكن إنكار الآن أن الوطن لم يعد ملاذاً آمن ، مع سعي الإرهابيين نحو استهداف ومهاجمة مواطنينا ، فالنشاط السيبراني الضار ضد البنية التحتية التجارية أو الشخصية أو الحكومية أو التخريب السياسي والمعلوماتي يظهر مدى التهديدات الجديدة للإستخدامات التجارية و العسكرية التي تستهدف أمننا في الفضاء السيبراني ، فمع تزايد الإتصال الرقمي لجميع جوانب الحياة و الأعمال والحكومة والجيش ، أدى ذلك الى ظهور وخلق نقاط ضعف وثغرات كبيرة في الأنظمة الحماية السيبرانية ، ومنه فإن أثناء النزاع يجب توقع الهجمات ضد البنيات التحتية الدفاعية والحكومية و الاقتصادية.[99] وفي سبيل التصدي وتحقيق تفوق عسكري على الخصوم والمنافسين فإن الإستراتيجية الأمنية العسكرية The National Military Strategy (NMS) ، لسنة 2018 دعت الى العمل المتشارك وتناسق بين القوة المشتركة وقادتها للقتال في الفضاء أو الفضاء السيبراني كما هو الحال في المجالات التقليدية الثلاثة

[97] Mara Karlin, **How to read the 2018 National Defense Strategy**, January 21, 2018, Direct link: https://www.brookings.edu/blog/order-from-chaos/2018/01/21/how-to-read-the-2018-national-defense-strategy/

[98] Seamus P. Daniels, **Show Me the Money: Assessing the Fiscal Reality of the National Defense Strategy's Ambitions**, Center for Strategic and International Studies, Washington, D.C., United States, p1

[99] Summary of the **National Defense Strategy National Defense Strategy**: Sharpening the American Military's Competitive Edge 2018. p3, Direct link: https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf

الأخرى وهي الأرض ، البحر ، الجو.[100] وقد دعت الإستراتيجية الدفاع الوطني ، وإستراتيجية السيبرانية لوزارة الدفاع الأمريكية خلال فترة إدارة الرئيس دونالد ترامب إلى :

- **في مجال الفضاء و الفضاء السيبراني** ، ستقدم الوزارة الأولوية للإستثمارات في المرونة وإعادة البناء والعمليات لضمان قدراتنا الفضائية ، كما سنستثمر أيضا في الدفاع السيبراني والمرونة ، والتكامل المستمر للقدرات السيبرانية والتفوق في كل المجالات والوحدات القتالية للقواتنا المشتركة ، البرية و البحرية و الجوية وفي الفضاء السيبراني.
- **وفي مجال القيادة والسيطرة والاتصالات وأجهزة الكمبيوتر والاستخبارات والمراقبة والاستطلاع (C4ISR)** ، سيتم تقديم الأولوية للإستثمارات لتطوير شبكات مرنة وموحدة وقابلة للصمود ، [101] وكما ستقدم الإستثمارات أيضًا الأولوية للقدرات للحصول على المعلومات واسغلالها ، وحرمان المنافسين من نفس المزايا ، والتي تمكننا من تقديم الإسناد أثناء الدفاع ضد الجهات الفاعلة الحكومية أو غير الحكومية ومحاسبتها أثناء الهجمات السيبرانية.
- تعزيز القوة المشتركة من خلال إجراء عمليات في الفضاء السيبراني والتي تعزز المزايا العسكرية الأمريكية.
- الدفاع على البنية التحتية الحيوية للولايات المتحدة ضد النشاط السيبراني الضار الذي يمكن أن يتسبب بمفرده أو كجزء من حملة ما ، في وقوع حادث سيبراني كبير.
- تأمين معلومات وأنظمة وزارة الدفاع ضد النشاط السيبراني الضار ، بما في ذلك معلومات وزارة الدفاع على الشبكات غير المملوكة لوزارة الدفاع ، وتوسيع التعاون السيبراني مع الوكالات و الصناعة والشركاء الدوليين.[102]

المطلب الثالث: الجيهات المسؤولة على تنفيذ الإستراتجيات السيبرانية الأمريكية.

في سبيل تحقيق الأهداف والإستراتجيات التي تصدر من وزارة الدفاع الأمريكية و البيت الأبيض في مجال الأمن السيبراني ، فهذا يأدي بنا الى البحث عن هذه الجيهات المكلفة بتأمين الفضاء السيبراني و الأمن

[100] **The National Military Strategy: The Joint Staff of 2018 – United States**, p2, Direct link: https://www.jcs.mil/Portals/36/Documents/Publications/UNCLASS_2018_National_Military_Strategy_Description.pdf

[101] Same prev ref: Summary of the NDS. P6

[102] CYBER STRATEGY SUMMARY, DEPARTMENT OF DEFENSE, 2018. p3, Direct link: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

القومي الأمريكي ، كل هذا يتم عبر القيادات العسكرية التابعة لوزارة الدفاع الأمريكية والمتمثلة في القيادة السيبرانية للولايات المتحدة " United States Cyber Command – و التي تعرف إختصارا بـ: USCYBERCOM " ، و أيضا تعمل وكالة الأمن القومي " NSA – National Security Agency " وهي هيئة مخابرات تابعة للحكومة في جانب التحقيقات ومعالجة المعلومات ورصد التهديدات السيبرانية و التحقيق فيها مع كافة الشركاء ، وكما تعمل أيضا وزارة الأمن الداخلي في الولايات المتحدة " The United States Department of Homeland Security (DHS) " رفقة الأجهزة التابعة لها مثل وكالة الأمن السيبراني و أمن البنية التحتية " Cybersecurity and Infrastructure Security Agency (CISA) " على حماية الولايات المتحدة من الداخل من الهجمات الإرهابية والكوارث بإضافة الى مهام تحسين الأمن السيبراني عبر جميع مستويات الحكومة والتنسيق مع الجيهات الحكومية والعسكرية ضد المتسللين و الهجمات و الإختراقات من الدول و الأفراد.

1- القيادة السيبرانية للولايات المتحدة (U.S. Cyber Command):

في شهر جوان من سنة 2009 أعلن وزير الدفاع الأمريكي روبرت قايتس Robert Gates ، عن إنشاء القيادة السيبرانية الأمريكية (USCYBERCOM) ، وهي قيادة موحدة فرعية يقودها مدير وكالة الأمن القومي (NSA)[103] ، وتهدف جهود القيادة السيبرانية الأمريكية وتخطيطها إلى ضمان قيام وزارة الدفاع بكل ما في وسعها لردع الخصوم وتخفيف التهديدات ومعالجة نقاط الضعف و الثغرات في الفضاء السيبراني.

و تواجه القيادة السيبرانية تحديات خطيرة في الفضاء السيبراني ، ويعكس تأسيسها حاجة وزارة الدفاع لها في إدارة المخاطر السيبرانية وتأمين حرية العمل وضمان القدرات المتكاملة ، وتهدف القيادة للتغلب على التحديات التي تواجهها من خلال الجهود المتضافرة لتنفيذ استراتيجية المعتمدة للفضاء السيبراني[104].

وتعمل القيادة السيبرانية مع فروع تابعة لها ، للإنجاح مهامها في البر أو الجو أو البحر أو في الفضاء والفضاء السيبراني وهي:

- القيادة السيبرانية للجيش الأمريكي " United States Army Cyber Command ".
- قيادة الأسطول السيبراني " U.S. Fleet Cyber Command ".
- سلاح الجو السادس عشر " The Sixteenth Air Force (16 AF) ".

[103] Wesley R. Andrues, REPORT: **What U.S. Cyber Command Must Do**, Joint Force Quarterly: 4th Quarter 2010, Issue 59, p115, Direct link: https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-59.pdf

[104] Keith B. Alexander, **Building a New Command in Cyberspace**, Air University Press, Strategic Studies Quarterly , Vol. 5, No. 2 (SUMMER 2011), p7 , Direct link: https://www.jstor.org/stable/10.2307/26270554

– قيادة الفضاء السيبراني لقوات المشاة البحرية." Marine Corps Forces Cyberspace Command [105].

وفي ما يلي الأهداف التي تركز وتسعى القيادة السيبرانية لتحقيقها:

- تركز القيادة على ثلاث مجالات رئيسية: الدفاع وحماية شبكات المعلومات التابعة لوزارة الدفاع الأمريكية.
- تقديم الدعم للقادة المقاتلين لتنفيذ مهامهم حول العالم.
- تعزيز قدرة الولايات المتحدة على الصمود و الرد على الهجومات السيبرانية.
- كما توحد القيادة اتجاه العمليات التي تجرى في الفضاء السيبراني وتقوي قدرات وزارة الدفاع في الفضاء السيبراني ، وتعمل على دمج وتعزيز القدرات السيبرانية لوزارة الدفاع وتحسينها ، كما تعمل القيادة أيضًا بشكل وثيق مع الشركاء المشتركين بين الوكالات والشركاء الدوليين في تنفيذ هذه المهام الحاسمة.[106]

2– وكالة الأمن القومي (NSA – National Security Agency):

تقود وكالة الأمن القومي وشريكها العسكري وجهاز الأمن المركزي حكومة الولايات المتحدة في علم التشفير الذي يشمل كلاً من منتجات وخدمات وعمليات استخبارات الإشارات (SIGINT) وضمان المعلومات (IA) ، ويمكّن عمليات شبكة الكمبيوتر (NCO) من أجل الحصول وكسب ميزة إتخاذ القرار للأمة و حلفاء الولايات المتحدة تحت كل الظروف ، وتعتبر وكالة الأمن القومي NSA كجزء تابع لوزارة الدفاع الأمريكية ، ويعمل بها مزيج من الأفراد المدنيين والعسكريين. توفر خدمة الامن المركزي (CSS) دعمًا مشفرًا ودقيقًا ومساعدة لمجتمع التشفير العسكري ، وهو ما يعزز الشراكة الكاملة بين وكالة الأمن القومي NSA و العناصر المكلفة بالتشفير التابعة للقوات المسلحة وكبار القادة العسكريين والمدنيين لمعالجة القضايا الحرجة المتعلقة بالجيش التصرف بشأنها لدعم أهداف الإستخبارات الوطنية والتكتيكية. كما تنسق خدمة الأمن العسكري CSS و تطور السياسات والتوجيهات بشأن مهام عملياتية ل " استخبارات الإشارات SIGINT " وهذا بهدف تأمين المعلومات الخاصة بـ NSA / CSS لضمان التكامل العسكري.

و تعمل مديرية استخبارات الإشارات على جمع ومعالجة ونشر المعلومات من الإشارات الأجنبية المرصودة ، وهذا لأغراض إستخباراتية ومكافحة التجسس ولدعم العمليات العسكرية ، وتعمل المديرية تحت سلطة وزير

[105] U.S. Cyber Command History, Direct link: https://www.cybercom.mil/About/History/
[106] Same prev ref.

الدفاع ، وتضمن توافر ونزاهة ومصادقة وسرية المعلومات " availability, integrity, authentication, confidentiality ".

وتعمل وكالة الأمن القومي للتحري لكشف وتوصيف التهديدات السيبرانية ولتوفير الوعي الظرفي لمشغلي الشبكات والمدافعين عنها. [107] ، و الدفاع عن الشبكات الحيوية وتعزيز أهداف الولايات المتحدة وتحالفاتها ، وكون وكالة الأمن القومي هي الرائدة عالميا في علم التشفير وفن وعلم صنع الأكواد التشفيرية و كسرها ، فإن هذه الخبرة المكتسبة من تكنولوجياتنا وشعبنا ، تسمح لنا بتحقيق أهدافنا وإكتشاف أسرار الخصوم وحماية أسرار الولايات المتحدة والتغلب على خصومنا في الفضاء السيبراني.[108]

3- وزارة الأمن الداخلي Department of Homeland Security (DHS) :

تم إنشاء وزارة الأمن الداخلي في عام 2002 ، وهذا عقب الهجومات التي إستهدفت نيويورك في 11 سبتمبر سنة 2001 ، وتضم 22 إدارة ووكالة فيدرالية مختلفة في وكالة وزارية موحدة ومتكاملة. تعمل وزارة الأمن الداخلي على قيادة وتوحيد الجهود لتأمين الولايات المتحدة من خلال منع الهجومات الإرهابية وردعها والتصدي للتهديدات و المخاطر ، وتظم الوزارة الأمن الداخلي وكالة تابعة لها تختص في كل ما يتعلق بالفضاء والتهديدات السيبرانية و التي تم إنشائها في فترة رئاسة دونالد ترامب وبقرار منه في سنة 2018، والمتمثلة في وكالة الأمن السيبراني وأمن البنية التحتية – Cybersecurity and Infrastructure Security Agency (CISA) " ، وتتولى الوزارة ووكالة الأمن السيبراني التابعة لها مسؤولية تنفيذ الإستراتجيات التالية:

- تعزيز فهم التهديدات من خلال التحليل الاستخباراتي.
- جمع المعلومات والاستخبارات المتعلقة بأمن الوطن.
- تبادل المعلومات اللازمة للعمل من الجيهات والوكالات الإستخباراتية المتعاونة مع وزارة الأمن الداخلي.
- إدارة المعلومات الاستخبارية لمؤسسة الأمن الداخلي[109]
- تقييم مخاطر الأمن السيبراني المتطورة.
- حماية أنظمة معلومات الحكومة الفيدرالية.
- حماية البنية التحتية الحيوية.
- منع وتعطيل الاستخدام الإجرامي للفضاء السيبراني.

[107] U.S. National Intelligence - An Overview 2013, P17-18 Direct link: https://www.dni.gov/files/documents/USNI%202013%20Overview_web.pdf
[108] What We Do: Article. Direct link: https://www.nsa.gov/what-we-do/
[109] Same prev ref.

- الاستجابة الفعالة للحوادث السيبرانية.
- تعزيز أمن وموثوقية النظام السيبراني.
- تحسين إدارة أنشطة الأمن السيبراني لوزارة الأمن الداخلي.[110]

المطلب الرابع: إبرام عقود مع الشركات توفير الحماية الأمنية السيبرانية.

كل الشركات التكنولوجية والمؤسسات الحكومية للدول هي مستهدفة ومعرضة للهجومات السيبرانية ، وتتغير الحلول المحددة لمواجهة هذه التهديدات والثغرات يوميًا ، ومع ذلك تواجه الشركات والحكومات نقص في القدرة على التعرف واكتشاف الثغرات الأمنية التي تستعمل من طرف الهاكرز والتي تستغل للوصول الغير مصرح للشبكات وأنظمة تشغيل البرامج ومراكز تخزين البيانات الخاصة بالحكومات أو الشركات ، فمن خلال إكتشاف الثغرات على البرامج أو أنظمة التشغيل وإستغلالها من طرف الهاكرز ، يتمكن المهاجمون من تشغيل تعليمات برمجية ضارة وتثبيت برامج تجسس وسرقة وتحويل البيانات الحساسة ، ومن خلال هذا تعمل الجيهات الحكومية في الولايات المتحدة على توقيع شراكات وعقود مع شركات مختصة في الأمن السيبراني ، أو شركات تعمل على تزويد الجيهات الحكومية بأدوات وبرامج تسيير البنيات التحتية والمراكز تخزين البيانات و تأمين التواصل بين كل أطراف الحكومية مع الحفاظ على سريتها.

ففي السنوات الماضية كانت هناك العديد من التقارير الإخبارية حول دمج برامج تجسس وبرمجيات ضارة من قبل الحكومات في المنتجات التكنولوجية " مثل الحواسيب ، شاشات تلفاز الذكية ، ألعاب ، لوحات مفاتيح ، هواتف.. الخ ، وهذا ما يتم في بعض أحيان بتواطئ من الشركات المصنعة لهذه الوسائل مع بلدانها ضد بلدان أخرى ، وكمثال ، نستعرض هذه الحوادث التي تم إكتشافها في السنوات الأخير:

- في أواخر سنة 2016-2017 تصدرت دمية My Friend Cayla والتي يتم تنشيطها صوتيًا عناوين الأخبار لتقنيتها ، بحيث تستخدم الدمية تقنية التعرف على الكلام عن طريق ربطها بتطبيق هاتفي على Android أو iOS ، والتي يمكن إستخدامها لجمع المعلومات عن الأطفال أو أي شخص في الغرفة أو حتى التحدث مع الطفل ، وفي عام 2017 حظرت ألمانيا الدمية بدعوى أنها تحتوي على جهاز مراقبة ينتهك لوائح الخصوصية في البلاد.
- في سنة 2010 تم إكتشاف ستكوسنت Stuxnet وهي دودة حاسوبية خبيثة تصيب نظام الويندوز ، بدا تطويرها سنة 2005 بالشراكة بين الولايات المتحدة و إسرائيل ، والتي إستهدفت منشأة التخصيب

[110] CYBERSECURITY STRATEGY, U.S. DEPARTMENT OF HOMELAND SECURITY. P2, Direct link: https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Fact-Sheet.pdf

الواقعة في مدينة " نطنز – Natanz " بإيران ، وهاجمت البرمجية الخبيثة أنظمة التحكم الإشرافي وتحصيل البيانات لبرنامج إيران النووي ، مما سبب أضرار وخيمة على تطور الأبحاث والنتائج المتوصل لها. واستهدف ستوكسنت وحدات التحكم المنطقية القابلة للبرمجة Programmable Logic Controller (PLCs) المملوكة لشركة Siemens ، وهذا عن عبر زرع البرمجيات الخبيثة في أنظمة التحكم الصناعية التي تم شحنها إلى إيران والتي أدت الى تعطيل المشروع النووي. [111]

- وفي سنة 2019 وقعت خلافات وتوترات بين الولايات المتحدة و الصين بعد إمضاء الرئيس الأمريكي دونالد ترامب أمرا تنفيذيا يضع الشركة الصينية هواوي في القائمة السوداء Huawei في سوق الولايات المتحدة وهذا ما يعني أن الموردين والشركاء والمشترين الأمركيين لمنتجات وتقنيات شركة هواوي سيكونون بحاجة للحصول على إذن من وزارة التجارة الأمريكية لممارسة الأعمال التجارية مع هواوي ، وعلاوة على ذلك لن تسمح شركة Google للهواتف الذكية المصنعة من طرف هواوي بإستخدام تطبيقات الهواتف الذكية الشائعة مثل Gmail ، كما لن تسمح لهم بإستعمال متجر التطبيقات Google Play Store في هواتفهم الجديدة ، ويأتي قرار الرئيس ترامب ضد الشركة التي تحظى بدعم من الحكومة الصينية وسط تصاعد التوترات بين البلدين والمخاوف المتزايدة من احتمال قيام الحكومة الصينية بإستخدام أجهزة هواوي للتجسس على الولايات المتحدة ، وأيضا ثبوت أن الشركة شاركت في أنشطة تتعارض مع الأمن القومي للولايات المتحدة. [112]
- في 15 جوان 2020 وخلال الحملة الانتخابية الأمريكية قال مدير حملة الرئيس الأمريكي دونالد ترامب أن التجمع الذي سيتم عقده في مدينة تولسا في أوكلاهوما Tulsa, Oklahoma الأسبوع القادم ، قد تجاوزت طلبات التذاكر عليه مليون طلب ، وقد كان مبرمج هذا اللقاء في ملعب يتسع ل 19000 مقعد ، لكن أقل من 6200 حضروا التجمع ، وكان السبب في ذلك هو قيام المستخدمين على تطبيق الصيني TikTok بالتسجيل للحصول على تذاكر للتجمع ولكنهم لم يحضروا. [113]
- في سنة 2010 اندلع صراع بين الصين و الولايات المتحدة والمعروف باسم " عملية أورورا – Operation Aurora " ، بحيث بدأ الصراع بين الصين و شركة قووقل Google وهذا بعد إختراق حسابات النشطاء السياسيين البريدية Gmail ، وهذا بهدف التجسس عليهم ، الإختراق مس شركات

[111] Stuart Madnick, Simon Johnson, and Keman Huang, **What Countries and Companies Can Do When Trade and Cybersecurity Overlap**, Harvard Business Review: Working Paper CISL# 2019-03. 2019. P3

[112] Md Sajjad Hosain, **Huawei ban in the US: Projected consequences for international trade**, International Journal of Commerce and Economics, Volume 1; Issue 2; April 2019, p22

[113] Jack Bandy, Nicholas Diakopoulos, **TulsaFlop: A Case Study of Algorithmically-Influenced Collective Action on TikTok**, Northwestern University, 2019. P1, Direct link: https://arxiv.org/pdf/2012.07716.pdf

أمريكية أخرى وهي: ميكروسوفت – أدوبي – ياهوو ، تم إستعمال Malware لتنفيذ الإختراق والذي استغل ثغرة أمنية كانت على متصفح إكسبلور ، لشركة ميكروسوفت.

- حظرت الولايات المتحدة على الحكومة والجيش الأمريكي إستخدام برنامج مكافحة الفيروسات لشركة كاسبرسكي الروسية ، كما منعت إستخدام طائرات بدون طيار المصنوعة من قبل شركة DJI الصينية. وبدورها قامت الصين بإزالة معدات الشبكات Cisco Systems وبرامج الأمان لشركة McAfee الأمريكية.[114]

وفي من أجل توفير الحماية الأمنية للبرامج والتكنولوجيات المستعملة من طرف الحكومة والجيهات الأمنية الحساسة ، تم اللجوء إلى تعاقد مع شركات مختصة في الأمن السيبراني و توفير الحماية ضد الثغرات التي تستغل في إختراق الشبكات و الحواسيب للشركات ، ومن بين أبرز هذه الشركات الأمنية نذكر منها:

– FireEye: وهي شركة مختصة في الأمن السيبراني ، مقرها كاليفورنيا، شاركت في الكشف عن الهجمات السيبرانية الكبرى التي إستهدفت الولايات المتحدة ومنعها. توفر الشركة أجهزة و برامج وخدمات للتحقيق في الهجمات السيبرانية و الحماية من البرامج الضارة ، وتحليل مخاطر أمن تكنولوجيا المعلومات ، كما كانت الشركة أول من إكتشف الإختراق الذي مس شركة SolarWinds ، وتمتلك شركة FireEye عقود مع مؤسسات حكومية أمريكية.

– Darktrace: وهي شركة رائدة أمريكية مختصة في الأمن السيبراني ، تستخدم الذكاء الاصطناعي للكشف عن التهديدات الإلكترونية المعقدة ، من التهديدات الداخلية والتجسس الإجرامي ، إلى هجمات برامج الفدية وهجمات المدعومة من طرف دول. [115]

– Cisco Systems: هي شركة رائدة على مستوى العالم في مجال الربط الشبكي للأنترنت ، تأسست في 1984 من قبل اثنين من علماء الكمبيوتر من جامعة ستانفورد بحثًا عن طريقة أسهل لربط أنواع مختلفة من أنظمة الكمبيوتر ، وتقدم شركة سيسكو العديد من الخدمات في كل ما يتعلق بربط الشبكات وتأمين الشبكات من الإختراقات السيبرانية ، عن طريق برامج الحماية مقدمة من طرفهم ، كما تمتلك الشركة مراكز تخزين البيانات وتسييرها للجيهات الحكومية[116].

– CrowdStrike: هي شركة رائدة في مجال الأمن السيبراني تحمي العملاء من جميع التهديدات السيبرانية ، تم إنشاء الشركة في سنة 2011 ، هذا وقد أحدثت الشركة ثورة في أمان المؤسسات من خلال تكنولوجيتها في تأمين بواسطة Security Cloud ، تعمل الشركة على إدماج وتعزيز الذكاء الإصطناعي في أنظمتها

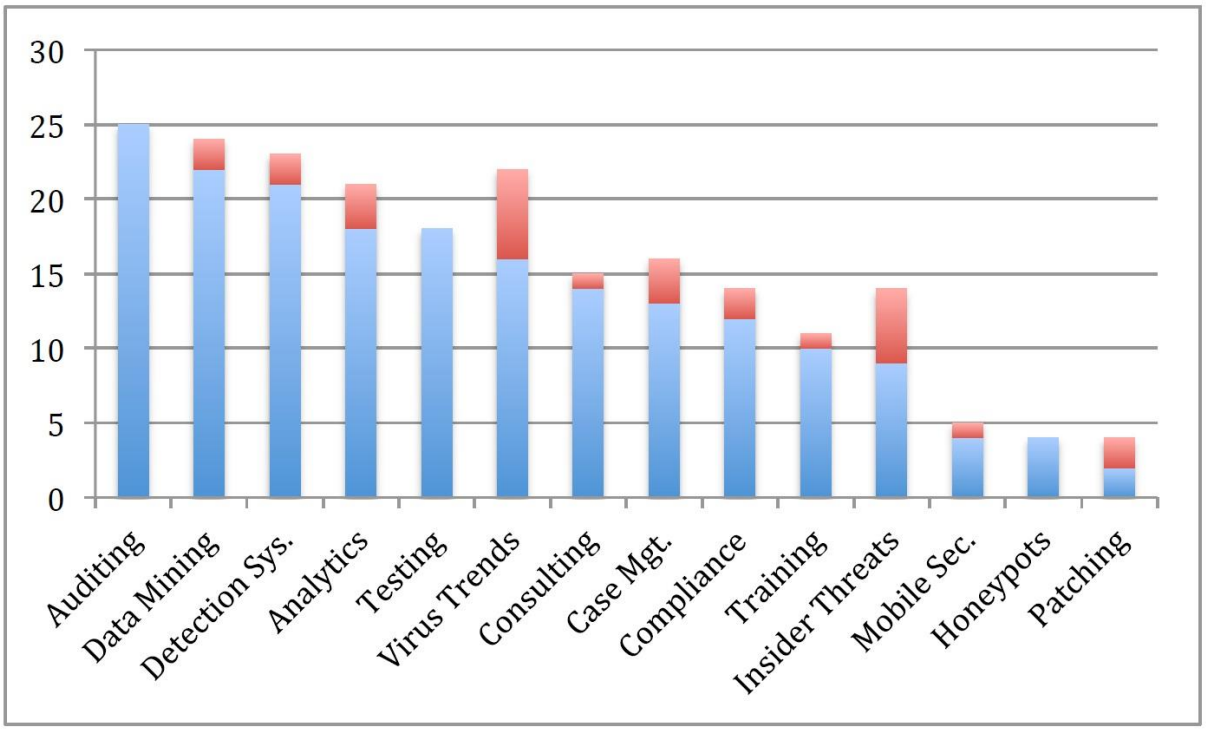
[114] Same prev ref. p4
[115] About us. Seen at 5/18/2021. Direct link: https://www.darktrace.com/en/
[116] Products, Solutions, and Services, Direct link: https://www.cisco.com/c/en_dz/products/index.html

الأمنية ، وقدمت الشركة خدمات حماية خلال الانتخابات الأمريكية ، وهذا بترصد والتحقيق التهديدات والأجواء التي سارت فيها الحملة الانتخابية ، بحيث تقدم الشركة خطط من شأنها تعزيز الوضع الأمني للكيانات الانتخابية و الحملات.[117]

- Palo Alto Networks: يقع مقر الشركة في كاليفورنيا ، وتم تأسيسها في سنة 2005 ، وهي شركة عالمية للأمن السيبراني ، تقدم خدماتها لأكثر من 54000 عميل في حوالي 150 دولة ، تساعد منصة التشغيل الأمنية الأساسية للشركة في إبعاد المتسللين عن طريق إستخدام التحليلات لتنفيذ المهام الروتينية ، تم تحسين وتطوير الخدمات المقدمة من الشركة ، لتشمل توفير الحماية وللبنوك والشركات المالية والرعاية الصحية ، كما توفر الشركة أمانًا سحابيًا وجدار حماية متقدمًا ، وإكتشاف التهديدات ومنعها.[118]

ولتوضيح المهام و الخدمات الحماية الإستباقية المقدمة من طرف الشركات الأمن السيبراني سنستعرض في هذا مسح ممارسات الأمن السيبراني للقطاع الخاص. وتمثل البيانات التالية في الجدول التقنيات المستخدمة من طرف الشركات الأمن السيبراني:

لمحة عن ممارسات الأمن السيبراني الاستباقية



[117] CrowdStire Services, Direct link: https://www.crowdstrike.com/services/
[118] Company informations from Palo Alto Networks: Direct link: https://www.paloaltonetworks.com/

يوضح الجدول البيانات المتاحة للخدمات وحلول الأمنية المقدمة للشركات التي تقدم وتروج لخدمات أو أبحاث في الأمن السيبراني ، يمثل الجانب الأيسر لرسم البياني ، الممارسات الأكثر انتشارا عبر الشركات الحماية السيبرانية ، بينما الخدمات الموجودة على الجانب الأيمن تعتبر أقل شيوعًا. و يمثل العمود المكدس الشركات التي تذكر بشكل جازم أنها تقدم منتج أو خدمة الأمن السيبراني ذات الصلة ويتبعها ، إن أمكن ، عمود إضافي (باللون الأحمر) ، والذي يوضح عدد الشركات التي من المحتمل أن تقدم هذا المنتج أو الخدمة بناءً على التفسيرات من المعلومات المتاحة على مواد التسويق على شبكة الإنترنت ووصف المنتج.[119]

شهدت ميدان الأمن السيبراني تغير وتزايد في مؤشرات الطلب على خدمات الحماية والأمن السيبراني ، في هذا عقب الإستعمالات المرتفعة التي شهدها العالم خلال الأزمة الوبائية للأنترنت في معاملات كالتجارة الإلكترونية والتي عرفت أرقام قياسية عقب الغلق والحجر الذي تم فرضته الحكومات في غالبية بلدان العالم ، مما زاد من ارتفاع نسب المبيعات و المعاملات على شبكة الأنترنت ، مثل الدراسة عن بعد التي إعتمدتها الجامعات ، والعمل عن بعد ، وغير ذلك. وخلال هذا االوضع الغير مسبوق ، استغله جيهات خبيثة و الهاكرز في تنفيذ عمليات احتيال وقرصنة للكثير من المواقع و الخدمات ، وإستهداف الشركات والأفراد عن طريق العديد من التقنيات والثغرات الأمنية ، وما يلي أبرز أنواع الهجومات التي تم تسجيلها خلال الجائحة:

أبرز أنواع الحوداث خلال الجائحة

		Specificity	
No	**Type of incident**	**Personal life changes**	**Professional environment changes**
1	Ransomware	To a small extent	To a large extent
2	Phishing	To a large extent	To a large extent
3	RDP attacks	No	Yes
4	Brute-force	No	Yes
5	Supply chain attacks	No	Yes
6	Web-skimming	Yes	Insignificant
7	Data exfiltration	To a small extent	To a large extent

Source: Tiberiu-Marian GEORGESCU, Study on how the Pandemic Changed the Cybersecurity Landscape p46

[119] Amanda N. Craig, Scott J. Shackelford, Janine S. Hiller, **PROACTIVE CYBERSECURITY : A COMPARATIVE INDUSTRY AND REGULATORY ANALYSIS**, p33 , direct link: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2573787

وقد كانت أهم تغيير خلال سنة 2020 ، هو تصاعد في هجمات برامج الفدية "Ransomware" وهذا لعدة أسباب ، ومن أبرزها هو انتقال والتغيير الذي مس بيئة العمل وتحول الكثير من العمال نحو الإشتغال من المنزل ، وقد كانت الفترة الحرجة الأولى خلال شهر مارس 2020 ، عندما اضطرت العديد من الشركات للإغلاق مكاتبهم بشكل عاجل وتحويل أنشطتهم نحو البيئة الرقمية ، الأمر الذي استغله الهاكرز في تنفيذ الهجمات بواسطة برامج الفدية ، التي تورط العمال والشركة وتجبرهم الوضعية السابقة نحو دفع المال للإستعادة القدرة على تشغيل الكمبيوترات. ومن أبرز الهجومات برامج الفدية التي شهدتها سنة 2020-2021 ، نذكر منها:

- الهجوم على شركة الاتصالات الفرنسية " Orange" والتي تعد رابع أكبر متعامل هاتفي في أوروبا ، ووقعت الشركة صحية لبرنامج فدية معروف ب " Nefilim Ransomware " ، وفي شهر أوت تعرضت جامعة يوتا University of Utah" لهجوم كلفها دفع 457.000$ لمجموعة من هاكرز. [120] وفي شهر ماي 2021 تعرضت الشركة الأمريكية Colonial Pipeline الى هجوم أوقف أجهزة تشغيل وتوزيع خط الأنابيب التي تنقل أكثر من 2.5 مليون برميل يوميا ، أي ما يعادل 45% من إمدادات الساحل الشرقي من الديزل و البنزين ووقود الطائرات. [121] وتم اعتبار هذا الهجوم على أنه الأكبر على إطلاق في نظام الطاقة الأمريكي ، بحيث تم إحداث عجز في محطات التوزيع وإرتفاع في الأسعار ، الأمر الذي أجبر الشركة على دفع 75 Bitcoin أي ما يعادل 5 مليون دولار لهاكرز ، لفك التشفير للأجهزة تشغيل المحطة.[122]
- وقد شهدت سنة 2020 ارتفاع في نسبة الهجومات على معلومات بطاقات الإئتمان من خلال " Phishing Attacks " و Web Skimming " والتي إستهدفت مجال التجارة الإلكترونية عن طريق النصب والمخادعة ، وارتفعت مثل هذه الهجومات بنسبة 26%. [123]

كل هذه الأحداث الطارئة ساهمت في تغيير السياسيات والإجراءات المتبعة من طرف الحكومات والشركات إتجاه الأمن السيبراني و الحماية ، وهذا من أجل التكيف مع الوضع وتقليل من حدة المخاطر و التهديدات السيبرانية التي تستهدفها ، ولقد تم ذلك عبر:

[120] Top Ransomware Attacks of 2020, Article, Direct link: https://usa.kaspersky.com/resource-center/threats/top-ransomware-2020
[121] Mary-Ann Russon, **US fuel pipeline hackers 'didn't mean to create problems**, Direct link: https://www.bbc.com/news/business-57050690
[122] Michael D. Shear, Nicole Perlroth and Clifford Krauss, **Colonial Pipeline Paid Roughly $5 Million in Ransom to Hackers**, Direct link: https://www.nytimes.com/
[123] Tiberiu-Marian GEORGESCU, **Study on how the Pandemic Changed the Cybersecurity Landscape**, Article: Informatică Economică vol. 25, no. 1/2021. p47

- **زيادة ميزانية الأمن السيبراني:** إلى غاية نهاية 2020 وبحسب 23 شركة ، تم زيادة الإنفاق والميزانيات الخاصة بالأمن السيبراني بنسبة 39% ، وهذا استجابة للضعف الذي عانت منه هذه الشركات في مواجهة الحوادث والتهديدات السيبرانية ، وسعت هذه الشركات في إبرام عقود مع شركات تقدم خدمات حماية وأمن سيبراني للحصول على مزيد من الحلول البرمجية للحماية شبكاتها وأنظمتها من الإختراق ، أو عن طريق الإستثمار في تدريب العمال للوقاية من الهجومات السيبرانية.[124]
- **إبرام عقود مع شركات التأمين ضد التهديدات السيبرانية:** وهذا لتخفيف من من الخسائر الناجمة عن الحوادث السيبرانية ، بما في ذلك إختراق البيانات ، وانقطاع الأعمال ، وإتلاف الشبكة.

وفي ما يلي جدول يوضح تباين أسعار أسهم الشركات الأمن وحماية السيبرانية ، من شهر فيفري 2020 مقارنة بشهر فيفري 2019، وعلى توالي شهر فيفري 2020 مقارنة بشهر فيفري 2021 وتم إختيار شهر فيفري كونه شهر مرجعي الأخير الذي لم تتأثر فيه الشركات بالقيود العالمية مصاحبة للجائحة سنة 2020.

Cybersecurity companies' stock price evolution

No.	Company name	Feb 2019-2020	Feb 2020-2021	Variation	Description
1	Palo Alto Networks	2.26%	39.09%	↗	Threat detection & prevention
2	Fortinet	37.78%	29.39%	↘	Security solutions
3	Splunk	23.55%	0.83%	↘	Big data security
4	Check Point Software	-4.10%	3.95%	↗	Unified threat management
5	Proofpoint	4.04%	6.25%	↗	Security-as-a-Service
6	Cloudflare	N/A	77.03%	-	Web performance and security
7	NortonLifeLock	-14.24%	6.92%	↗	Endpoint, cloud & mobile security
8	CrowdStrike	N/A	72.50%	-	Cloud delivered endpoint protection
9	FireEye	-10.68%	26.41%	↗	Advanced threat protection
10	Zscaler	-2.91%	35.64%	↗	Cloud security
11	Cisco Systems	-5.59%	0.83%	↗	Networking, and cybersecurity solutions
12	SecureWorks	-30.03%	-0.08%	↗	Managed security services
13	Vmware	-7.51%	-6.43%	↗	Cloud computing and virtualization software and services
14	SolarWinds	0.90%	-13.52%	↗	IT management software & monitoring tools
15	Okta	58.72%	52.36%	↘	Identity and access management

Source: Tiberiu-Marian GEORGESCU, Study on how the Pandemic Changed the Cybersecurity Landscape p52

[124] Same ref. 51

وكما هو ملاحظ فمن بين 15 شركة التي تمت دراستها لا توجد بيانات للإثنتين منها في الإطار الزمني الذي تم تحديده في 2019-2020 وهم Cloudflare و CrowdStrike. ومع ذلك فإن تطور أسعار أسهمها من فيفري 2020 إلى فيفري 2021 قد تجاوز 71% وهو ما يمكن إعتباره زيادة هائلة ، ومن بين الشركات 13 المتبقية سجلت تسع منها زيادة أكبر في الفترة 2020-2021 مقارنة بفترة 2019-2020.[125]

ومن الجدير بالذكر هو ان انخفاض الذي عانت منه شركة SolarWinds عائد إلى المشكلات الأمنية التي عانت منها عقب الإختراق الذي إستهدفها في النصف الثاني من سنة 2020 ، ومعروف باسم Sunburst، والذي سيتم التطرق له كدراسة حالة في الفصل القادم ، لدراسة هذا الحادث بكل تفاصيله.

[125] Same prev ref. p52

خلاصة الفصل الأول:

بعد إستعراض الفصل الأول بمباحثه و مطابله ، والذي ركزنا فيه من خلال الجانب النظري للدراسة من حيث أهمية الأمن السيبراني في الظل التهديدات المتزايدة التي تستهدف الشركات والدول ، مع إبراز أنواع الهجومات والتهديدات السيبرانية التي تستهدف الشركات و الأفراد والحكومات ، وطرق الحماية للحد من الحوادث السيبرانية ورفع من درجات الأمان والحماية للأنظمة التشغيل ، كما تطرقنا إلى الإستراتجيات للأمن القومي الأمريكي في خلال فترة رئاسة باراك أوباما ، و الرئيس دونالد ترامب ، هذه الإستراتجيات التي أولت إهتمام بالفضاء السيبراني وبالخطط التي سطرتها إدارة الرئيس أوباما وترامب للحد من التهديدات التي تواجه الولايات المتحدة من الجيهات المعادية والمنافسة لها، كما تم التطرق للجيهات الحكومية المسؤولة على تنفيذ هذه الإستراتجيات ، وفي الأخير تم إبراز العلاقة التي تربط القطاع الخاص والمتمثل في شركات الحماية و الأمن السيبراني والحكومات من خلال توقيع شراكات للعمل في سبيل تعزيز أمن الشبكات و الفضاء السيبراني ، ومنه سبق نستخلص:

1- تولي الولايات المتحدة وعلى مدار اكثر من 10 سنوات أهمية بالغة بأمنها في الفضاء السيبراني ، والذي أوضحته الإستراتجيات التي أقرتها إدارة باراك أوباما ودونالد ترامب على التوالي ، مما يؤكد على الجهود التي تم وضعها لحماية كل الفاعلين في من التهديدات والخروقات السيبرانية التي سجلت ارتفاع خلال السنوات الخمسة الأخيرة.

2- يشكل الفضاء السيبراني بيئة مواتية للمنظمات الإجرامية و المجموعات المدعمة من طرف الدول ، لتنفيذ العديد من العمليات إجرامية والغير قانونية ، وهذا بفضل إمكانية ترك أدلة تورط المنفذين ، الأمر الذي خلق صعوبة للولايات المتحدة فرض عقوبات درعية.

3- إن الصراعات العديدة التي تشهدها الولايات المتحدة مع دول منافسة أو معادية لها " مثل: كوريا الشمالية ، الصين ، روسيا ، إيران " ، أو من طرف جماعات إرهابية ، جعلها عرضة وهدفا للعديد من الهجومات السيبرانية ، الأمر الذي أدى بالولايات المتحدة إلى إستحداث أقسام ووكالات حكومية تعمل وتسعى لتحقيق وحماية الفضاء السيبراني و الشبكات البنيات التحتية.

4- شهد العالم عقب جائحة Covid19 والحجر الذي تم فرضها في دول العالم ، نمو في نسبة الهجومات واختراقات السيبرانية ، الأمر الذي أدى الى لجوء الحكومات والأفراد إلى الإستعانة بخبرات وبرامج شركات الحماية السيبرانية ، والذي بدوره ساهم في ارتفاع أسهمها وأرقام مبيعتها.

الفصـــل الثانـــي:

دراسة حالة للهجوم السيبراني على شركة SolarWinds (Sunburst Attack)

الفصل الثاني: دراسة حالة للهجوم السيبراني على شركة SolarWinds " Sunburst Attack "

أدى الإعتماد المتزايد على الشبكات وأنظمة التشغيل في المهام اليومية للشركات و الحكومات إلى زيادة الطلب على الشبكات و أنظمة التشغيل والبرامج الموثوقة والتي توفر أداء عالي وتحكم الكلي في تسيير البيانات ، وكجزء من تحقيق هذه الأهداف المتعلقة بتحقيق أداء عالي خلال مراقبة الشبكات للمساعدة في تحديد أخطاء الشبكة والوقاية منها ، ظهرت العديد من الأدوات والبرامج التي تساعد في مراقبة أداء الشبكات ، ويتم الإعتماد في هذا الصدد على أدوات شائعة للإدارة بروتوكول الشبكة و متمثل في " Simple Network Management Protocol " (SNMP) وهو بروتوكول لإرسال معلومات أداء الشبكة ونقلها على شبكات IP ، وتوجد أنواع أخرى من أدوات مراقبة أداء الشبكة والتي تحتوي على ميزات متقدمة وخدمات أكثر شمولية كالتي تقدمها شركة سيسكو Cisco بواسطة أداة المقدمة من طرفهم ومعروفة باسم " Cisco's NetFlow – flow monitoring tools" وأيضا أداة GlobalWatch والتي تقدمها شركة Webmetrics ، وصولا إلى الخدمة التي تقدمها الشركة SolarWinds والتي تقدم برنامج Orion والذي ينافس باقي الخدمات للشركات التي تم ذكرها [126]، وتعمل مثل هذه البرامج على إدارة الشبكة ومراقبة الأداء مراكز البيانات.

وفي دراستنا هذه سيتم التركيز على برنامج SolaWinds Orion والإختراق الذي استهدف التحديثات خلال بداية سنة 2020 ، تعتبر شركة سولارويندز من الموردين الرئيسيين لأكثر من 33000+ شركة وحكومة في العالم ، الأمر الذي جعلها هدف للهاكرز بهدف التوصل الى المعلومات الحساسة للحكومات وخاصة للجيهات الحكومية الحساسية في الولايات المتحدة الأمريكية ، وتم إكتشاف هذا الإختراق من طرف شركة الأمريكية للأمن السيبراني FireEye.

المبحث الأول: ماهي الخدمات التي تقدمها شركة SolarWinds و من هم عملائها ؟

تعتبر شركة SolarWinds أحد أبرز الشركات في مجال الشبكة ، أنظمة تسيير وتأمين البيانات ، و سيتم التطرق لكل الخدمات التي توفرها الشركة في المطلب الثاني بالتفصيل ، كما تمتلك الشركة قاعدة عملاء كبيرة ينقسم ما بين جيهات حكومية و قطاع خاص ، ويتجاوز 33000 عميل حول العالم ، المنتجات التي تقدمها الشركة تتمثل في مراقبة الشبكة ، ومراقبة الأنظمة ، مراقبة قواعد البيانات ، وبرامج حماية وأمن.

[126] Paul Moceri, **SNMP and Beyond: A Survey of Network Performance Monitoring Tools**, p1 , direct link: https://www.cse.wustl.edu/~jain/cse567-06/ftp/net_traffic_monitors2.pdf

المطلب الأول: تعريف بشركة SolarWinds.

تأسست شركة سولاروينذز رسميا في سنة 1999 في Tulsa, Oklahoma ، شارك في تأسيس الشركة دونالد يونسي والذي شغل منصب مدير التنفيذي سابقا في شركة Walmart وشقيقه ديفيد يونسي [127]، وكان هدف الشركة ومهمتها هي تسهيل تكنولوجيا المعلومات من خلال تقديم أدوات برمجية مصممة خصيصًا وبأسعار معقولة. أصدرت الشركة أول منتجاتها في سنة 1998 وهم Trace Route و Ping Sweep [128]، كما أصدرت أول تطبيق لها لمراقبة أداء الشبكة في سنة 2001 ومعروف باسم Orion.

و وفقًا لمايكل بينيت Michael Bennett الذي أصبح الرئيس التنفيذي للشركة في عام 2006، أن إختيار إسم SolarWinds تم من قبل أوائل الموظفين في الشركة ، وأن الشركة لا علاقة لها بالطاقة الشمسية أو طاقة الرياح ، وفي سنة 2006 نقلت الشركة مقرها الرئيسي أوستن ، تكساس Austin, Texas أين كان يتواجد حوالي 300 من إجمالي موظفي الشركة البالغ عددهم 450 موظفًا اعتبارًا من عام 2011.

خلال عام 2007 قامت شركة سوولاروينذز بجمع تمويلات من طرف Bain Capital, and Insight Venture Partners عن طرق بيع للأسهمها ، وتوصلت الشركة للحصول على 112.5 مليون دولار في سنة 2009 ، وتوقع المحللون والمسؤولون التنفيذيون في الشركة توسعًا مستمرًا بعد الاكتتاب العام. بما في ذلك العديد من عمليات الاستحواذ. في عام 2010 تقاعد مايكل بينيت Michael Bennett من منصبه كرئيس تنفيذي وحل محله الرئيس المالي السابق للشركة كيفن طومسون.

في سنة 2013 اعتبرت Forbes شركة سولاروينذز على أنها أفضل شركة صغير في أمريكا ، مستشهدة بالمنتجات عالية الأداء وتكاليفها المنخفضة ونمو الرائع الذي سجلته في السنوات الأخيرة ، وبحلول سنة 2014 ارتفع عدد موظفي الشركة الى حوالي 900 شخص.[129]

[127] SOLARWINDS COMPANY HISTORY TIMELINE, Seen on: https://www.zippia.com/solarwinds-careers-38741/history/
[128] Artcile: Thank you for growing with us. Direct link: https://www.solarwinds.com/20th-anniversary
[129] Same prev ref.

المطلب الثاني: الخدمات والبرامج المقدمة.

كما سبق تطرق إليه فشركة SolarWinds تقدم خدمات وأدوات وبرامج عديدة في كل ما يتعلق تسيير الشبكات ، وتسيير الأنظمة ، والأمن السيبراني ، وبرامج لتسيير قواعد البيانات ، وسنتطرق لكل هذه الخدمات في مايلي بتفصيل:

1- **The SolarWinds MSP Products**: برنامج سولارويندز وهو خدمة توفر منصة شاملة من الأدوات لمقدمي خدمات تكنولوجيا المعلومات التي يحتاجونها لمسعادتهم على توسيع عروض خدماتهم للفوز بأعمال جديدة والحفاظ على عملائهم ، وتحتوي هذه الخدمة الأدوات التالية:

- المراقبة والإدارة عن بعد " MSP- Remote Monitoring and Management ": توفر هذه الخدمة إدارة وتصحيح وإستكشاف أخطاء الخوادم ونقاط النهاية عبر مواقع متعددة وبكفاءة عالية.
- MSP Manager: إعداد تقارير وحلول.
- تأكيد الإيميل Mail Assure: الحماية من البريد العشوائي والبرامج الضارة بالإضافة إلى أرشفة البريد الإلكتروني.
- MSP Anywhere: الوصول عن بعد لاستكشاف الأخطاء وإصلاحها بسرعة.

2- **الخدمات السحابية SolarWinds Cloud Products**: وهي عبارة عن مجموعة منتقاة من منتجات المراقبة لتطبيقات السحابية ، و DevOps-oriented teams.

- PINGDOM: وهي أداة لمراقبة المواقع الإلكترونية و موثوق من طرف 850,000 مستخدم.
- PINGDOM SERVER MONITOR: يختص في مراقبة السيرفرات " مراكز تخزين البيانات " وهو موجه لـ DevOps professionals.
- أسطوانة الورق PAPERTRAIL: إدارة السجلات المستضافة على السحابة للمساعدة في استكشاف المشكلات وإصلاحها في البنية التحتية و التطبيقات.
- APPOPTICS: يوفر البرنامج مراقبة سلسة وعميقة للتطبيقات و البنيات التحتية ، كما يوفر رؤية شاملة حول التطبيق للإكتشاف الأخطاء وإصلاحها بشكل أسرع.
- LOGGLY: مراقبة السجلات المستضافة على Cloud وحصول على تحليلات لنشاطها.[130]

[130] SolarWinds Product Overview Guide, Simple, powerful, and affordable monitoring software IT pros love, Direct link: https://www.solarwinds.com/-/media/solarwinds/swresources/datasheet/swi-ov-brochure-print.ashx?rev=04da25ab90ce4b08ae6e4e07d962f036

3- أدوات سولارويندز SolarWinds Tools:

- Web HELP DESK: تسهيل عمليات وإدارة الوصول.
- DAMEWARE REMOTE SUPPORT: أدوات التحكم عن بعد وإدارة الأنظمة.
- مجموعة أدوات المهندس " ENGINEER'S TOOLSET ": تحتوي المجموعة على 60 أداة لا غنى عنها لتحري وتشخيص الخلل في الشبكة وإصلاحه.
- KIWI SYSLOG SERVER: إضفاء الطابع المركزي على إدارة رسائل السجل وتبسيطها عبر أجهزة الشبكة والخوادم ومراقبة السيرفرات للإيجاد الثغرات وإصلاح الأخطاء البرمجية.
- NETWORK TOPOLOGY MAPPER: يمكن هذا البرنامج من رسم الشبكات تلقائيا وبطريقة سريعة ، ويسمح البرنامج برسم خرائط طوبولوجيا للشبكة بطريقة شاملة ومفصلة.
- MOBILE ADMIN: تبسيط إدارة تكنولوجيا المعلومات وتسييرها من الأجهزة المحمولة.
- SERV-U MANAGED FILE TRANSFER: نقل وإرسال الملفات بأمان داخل وخارج شبكات المؤسسة أو الشركة.

4- برامج الحماية SolarWinds Security Products:

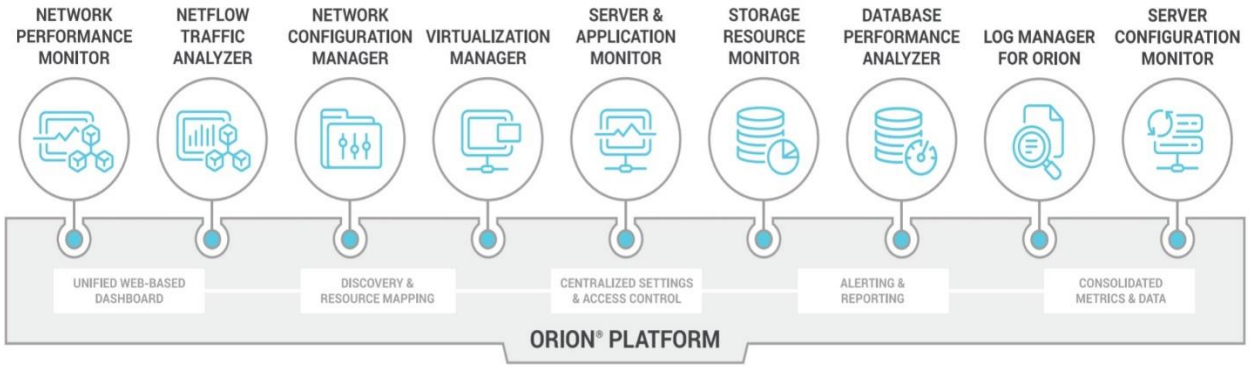
- LOG & EVENT MANAGER
- BACKUP حفظ نسخ إحتياطة للبيانات.
- RISK INTELLIGENCE: تحديد موقع البيانات الحساسة عبر الشبكات وحمايتها من أي إتلاف.
- SERV-U: يعمل البرنامج على تأمين الملفات.
- PATCH MANAGER: برنامج إدارة التصحيح مصمم لمعالجة الثغرات الأمنية في البرامج بسرعة.
- NETWORK CONFIGURATION MANAGER: يمكن من تقليل التكلفة وتوفير ساعات العمل والبقاء متوافقًا مع إدارة تكوين الشبكة التلقائية والنسخ الاحتياطي.
- MAIL ASSURE: تأكيد الإيميلات و الحماية من الهجومات والإختراقات عبر البريد الإلكتروني.
- LOG MANAGER FOR ORION: التحقيق في مشكلات تكنولوجيا المعلومات وتحري في بيانات الدخول وتسجيل وحل مشكلات الشبكة بسرعة وكفاءة والمنع من حدوثها في مستقبل.
- THREAT MONITOR: أداة معلومات الأمان وإدارة الأحداث ، تتيح الأداة لموفري الخدمات من إكتشاف التهديدات في الشبكات المدارة. [131]

[131] Same prev ref.

5- Orion Platform:

تعد Orion كمنصة قوية تعمل على تسهيل مراقبة و تحليل وإدارة مجموعة كبيرة للتكنولوجيات والبرامج و الأدوات الكاملة في مكان واحد ، عبر منصة شاملة ، منصة Orion هي عبارة عن بنية برمجية معيارية ، تم تصميمها لتزويد أقسام تكنولوجيا المعلومات برؤية موحدة ، وقابلية للتوسع في المؤسسة ، مع توفير سهولة في الإستخدام في وحدة تحكم واحدة قابلة للتوسع في مهام بشكل كبير.

الأدوات التي تظمها منصة Orion



وتظم المنصة العديد من الأدوات التي تسهل من مهام الشركات و الحكومات في تسيير مراكز تخزين البيانات و إدارة الشبكات والمتمثلة في:

NETWORK PERFORMANCE MONITOR

Fault, availability, and performance monitoring for networks of all sizes

- Speeds troubleshooting, resolves network outages, and helps reduce downtime
- Customizable network topology and dependency-aware intelligent alerts
- Wireless heat maps, automated capacity forecasting, alerting, and reports

solarwinds.com/NPM

NETFLOW TRAFFIC ANALYZER

Network traffic and bandwidth utilization in an easy-to-view dashboard

- Monitor interface-level network bandwidth and traffic patterns with up to one-minute granularity
- Bandwidth use by user, application, protocol, and IP address group
- Analyze traffic patterns over months, days, or minutes by drilling down into any network element

solarwinds.com/NTA

NETWORK CONFIGURATION MANAGER

Centralized network device change and configuration management software

- Automated configuration backups, comparisons, and rollback
- Real-time configuration change detection and audits for compliance management
- Bulk deploy configuration changes

solarwinds.com/NCM

IP ADDRESS MANAGER

Easy-to-use IP address management software

- Automated IP address tracking, alerting, and reporting
- Integrated DHCP, DNS, and IP address management
- IP detail and history tracking

solarwinds.com/IPAM

NETWORK OPERATIONS MANAGER

Unified network management software for on-premises, cloud, and hybrid

- Network performance monitoring and troubleshooting
- Traffic, bandwidth, and WAN monitoring
- User and device tracking

solarwinds.com/NOM

NETWORK AUTOMATION MANAGER

Unified network automation and operations management software

- Advanced network monitoring and troubleshooting
- Traffic, bandwidth, and WAN monitoring
- Change and configuration management
- High availability

solarwinds.com/NAM

SERVER & APPLICATION MONITOR

Manage, troubleshoot, and resolve app performance and availability issues

- Deep visibility into applications, database, host server, virtualization, and storage systems on-premises as well as in the cloud
- Support for over 200 applications out of the box, including Exchange™, SQL Server®, and more
- Software asset inventory and capacity planning

solarwinds.com/SAM

DATABASE PERFORMANCE ANALYZER

Solve complex database issues and optimize application response times

- See exactly what is impacting performance inside your database and get expert resolution advice
- Correlate response time with VM resources, host, and storage I/O with history and baselines
- Agentless architecture ideal for test/dev and production, on-premises, or in the cloud

solarwinds.com/DPA

VIRTUALIZATION MANAGER

Performance, troubleshooting, capacity, and sprawl management from VM to datastore

- Deep visibility into usage and performance of VMs, hosts, clusters, and datastores
- Enhanced actionable intelligence allows for single-click multiple-steps remediation of active and predicted VM performance and resource allocation
- Power off idle VMs, adjust over- and under-allocated resources, help fix co-stop issues typically in minutes

solarwinds.com/VMAN

STORAGE RESOURCE MONITOR

Multi-vendor storage capacity and performance monitoring

- Provides real-time performance visibility to SAN and NAS array LUNs, RAID groups, volumes, disks, and more
- Automated storage capacity planning to identify hot spots, peak hours, and potential outages
- Identify LUN contention and other difficult storage performance issues

solarwinds.com/SRM

WEB PERFORMANCE MONITOR

Measure user experience and troubleshoot latency issues for web applications

- Visibility into end-user experience for web and SaaS application transactions
- Monitor performance for applications behind the firewall from multiple geographic locations
- Built-in integration with Orion Platform shows infrastructure dependencies for fast troubleshooting

solarwinds.com/WPM

SERVER CONFIGURATION MONITOR

Easy to use Windows® system and application change monitoring

- Asses Windows system and application changes against custom baselines
- Correlate performance incidents against configuration changes
- Detect and track changes over time

solarwinds.com/SCM

Source: SolarWinds Product Overview Guide, Simple, powerful, and affordable monitoring software IT pros love, Link: https://www.solarwinds.com/-/media/solarwinds/swresources/datasheet/swi-ov-brochure-print.ashx?rev=04da25ab90ce4b08ae6e4e07d962f036

المطلب الثالث: أبرز عملاء شركة SolarWinds

تسعى الشركات و الحكومات في سبيل تعزيز كفاءة وأداء خدماتها الرقمية الى التعامل مع الشركات الكبرى ذات خبرة في تسيير أنظمة تشغيل ومراكز تخزين البيانات وتوفير برامج و المنصات برمجية التي تسهل تسيير وتخزين المعلومات والمراسلات الحكومية وللقطاع الخاص ، وفي هذا مجال تحظى منتجات شركة سولارويندز بثقة وإستعمال جهات عديدة في العالم وفي الولايات المتحدة بالخصوص ، لما تقدمه أداء وكافة عالية ، وفي أعقاب الإختراق الذي إستهدف الشركة والعملاء الكبار لها عبر منصتها Orion ، سارعت شركة سولارويندز إلى إخفاء وحذف المعلومات على موقعها حول الشركات والمؤسسات الحكومية التي تستعمل برامجها وهذا للحفاظ سمعة وسرية الجيهات المتضررة من العملية[132]. إلا أن المعلومات وصفحة التي تحتوي على عملاء الشركة بقت متاحة وهذا عبر أرشفة التي يقدمها موقعWayback Machine والذي يتبع موقع Internet Archive الذي يقدم خدمة أرشفة وحفظ الصفحات ومحتويات المواقع، وذكرت شركة سولارويندز على أن منتجاتها وخدماتها تستخدم من طرف أكثر 300000 عميل في جميع أنحاء العالم ، بما في ذلك القطاع العسكري ، والشركات الأمريكية الكبرى " Fortune 500 " والوكلات الحكومية و المؤسسات التعليمية والمتمثلة في:

- أكثر من 425 شركة من قائمة US Fortune 500.
- جميع الشركات 10 الكبرى الأمريكية في اتصالات داخل الولايات المتحدة.
- جميع الفروع الخمسة للجيش الأمريكي ، والمتمثلة في : الجيش والبحرية والقوات الجوية ومشاة البحرية وخفر السواحل.
- وزارة الدفاع الأمريكية ، وزارة الخارجية ، وكالة ناسا ، وكالة الأمن القومي ، الخدمة البريدية ، الإدارة الوطنية للمحيطات والغلاف الجوي (NOAA) ، وزارة العدل ، ومكتب رئيس الولايات المتحدة.
- كل من خمس أكبر شركات محاسبة في ولايات المتحدة.
- مئات الجامعات والكليات حول العالم. [133]

وفي ما يلي قائمة لأبرز العملاء داخل الولايات المتحدة :

[132] Russell Brandom, **SolarWinds hides list of high-profile customers after devastating hack**, Article from THE VERGE website: posted on: Dec 15, 2020 , Direct link: https://www.theverge.com/2020/12/15/22176053/solarwinds-hack-client-list-russia-orion-it-compromised
[133] SolarWinds' Customers, Original link: https://www.solarwinds.com/company/customers
Back link from Wayback Machine: https://web.archive.org/web/20201214065921/https://www.solarwinds.com/company/customers

الشركة / الجهة الحكومية	الشعار	المهام
USA VISA		تقديم التأشيرات للدخول للولايات المتحدة ، إصدار جوازات سفر ، وبطاقات إقامة للأجانب
US Secret Service		الخدمة السرية و التحقيقات الجنائية ، وحماية القادة السياسين الأمريكيين و وعائلاتهم وحماية زيارة رؤساء الدول و الحكومات وغير ذلك.
The Federal Reserve		جهاز حكومي فيدرالي، يعمل في الولايات المتحدة عمل البنوك المركزية في الدول الأخرى من العالم.
The Department of Justice		وزارة العدل ، تسيير الشؤون القانونية وإصدار والفصل في الأحكام.
The Office of the President of the United States		مكتب الرئيس الأمريكي ، تسيير شؤون وسياسات الولايات المتحدة.
The Department of Defense		وزارة الدفاع مسؤولة عن توفير القوات العسكرية اللازمة لردع الحرب وحماية أمن البلاد.
Department of Energy /Los Alamos National Laboratory		هي المسؤولة عن النهوض بالطاقة (DOE) وزارة الطاقة والبيئة والأمن النووي للولايات المتحدة ؛ تشجيع الابتكار العلمي والتكنولوجي لدعم تلك المهمة ؛ رعاية البحوث الأساسية في العلوم الفيزيائية ؛ وضمان التنظيف البيئي لمجمع الأسلحة النووية في البلاد.
National Security Agency		تقود وكالة الأمن القومي الحكومة الأمريكية في مهام التشفير للمنتجات وخدمات استخبارات الإشارات وضمان المعلومات وتمكن عميات شبكة الكمبيوتر وحماية ضد التهديدات السيبرانية.
Centers for Disease Control and Prevention		بصفتها وكالة حماية الصحة العامة في البلاد ، فإن مراكز مكافحة الأمراض والوقاية منها لديها سلطات معينة لتنفيذ اللوائح المتعلقة بحماية أمريكا من تهديدات الصحة والسلامة ، سواء الخارجية أو داخل الولايات المتحدة ، وزيادة أمن الصحة العامة.

The US Army, Marine Corps, Navy, Air Force, and Coast Guard		حماية الولايات المتحدة ، في البحر والجو و البر ، والحفاظ على سلامة و أمن السواحل الأمريكية.
NASA		الأبحاث الفضائية
The Department of Homeland Security		تتمثل مهمة وزارة الأمن الداخلي في ضمان وطن آمن ومأمون وقادر على الصمود ضد الإرهاب والمخاطر الأخرى.
Microsoft		تمكين كل شخص ومنظمة على تحقيق المزيد ، من خلال برامج والخدمات التكنولوجية المقدمة من طرف الشركة.
Cisco		تطوير وبيع أجهزة الشبكات والاتصالات السلكية واللاسلكية المتطورة في جميع أنحاء العالم. تبلغ قيمة الشركة أكثر من 500 مليار دولار مما يجعلها من بين أكبر 100 شركة تقنية في جميع أنحاء العالم.
Yahoo!		محرك ومزود خدمات الويب ، توفر الشركة محرك بحث وخدمات ذات صلة بذلك.
AT&T		مصنفة في المركز الأول كأكبر شركة اتصالات في العالم، وفي المركز الثاني كأكبر مزود لخدمات الهاتف المحمول وتقنيات وتكنولوجيات الإتصلات.
Mastercard		تعمل الشركة على ربط وتعزيز اقتصاد رقمي شامل يستفيد منه الجميع في كل مكان من خلال جعل المعاملات آمنة وبسيطة وذكية ويمكن الوصول إليها وهذا باستخدام البيانات والشبكات الآمنة
Visa		هي الشركة الرائدة عالميًا في مجال المدفوعات الرقمية. مهمتنا هي ربط العالم من خلال شبكة الدفع الأكثر ابتكارًا وموثوقية وأمانًا – تمكين الأفراد والشركات والاقتصادات من الازدهار .
FireEye		توفير الحماية والأمن من الهجومات والإختراقات السيبرانية.

المبحث الثاني: حيثيات الهجوم على SolarWinds

يعتبر الهجوم السيبراني الذي إستهدف شركة Solarwinds كأحد أبرز الهجومات السيبرانية التي تم تنفيذها ، كون أن تأثيرات الهجوم كانت واسعة محليا ودوليا، ربما يكون الجانب الأكثر أهمية للهجوم هو اتساع نطاق آثاره ، والتأثير على كل من المنظمات الحكومية و التجارية والذي خلق تأثيرات تاريخية من المرجح أن تحدد الالتزامات والتوقعات المستقبلية لمجموعة واسعة من الجهات الحكومية والخاصة.

ولهذا يتوجب على الجيهات المتضررة " الحكومية و الشركات " العمل على فهم طبيعة الحادث وتأثيره [134] ، لتجنب أي إختراقات مشابهة. خلال الهجوم الذي تأثرت به سولارويندز تم إعتماد على نوع جد متقدم وصعب في تنفيذ الهجوم و المعروف بـ " هجوم سلسلة التوريد – Supply chain attack " و الذي يعتمد على إستهداف الطرف الثالث الذي يزود ويتعامل مع الجيهة الرئيسية المستهدفة من الإختراق ، وهذا من خلال اكتشاف الثغرات ونقاط الضعف المتواجدة في برامج وخدمات في سلسة التوريد الثانوية للضحية المستهدفة ، إمكانية حدوث هجوم سلسلة مطروحة في أي شركة أو جهة حكومية تستخدم خدمات ومنصات برمجية للأطراف ثانية ، وعادة ما يتم استهداف في مثل هذه الهجومات " القطاع المالي ، الشركات التي تنتمي للقطاع الطاقوي و البترول أو القطاع الحكومي ، ويتم ذلك بتلاعب الهاكرز بعملية تصنيع المنتج عن طريق تثبيت برمجيات خبيثة ، في حالة التي استهدفت SolarWinds قام المهاجمون بزرع " Backdoors " في ملفات DLL في حزم التحديث الخاصة بـ SolarWinds Orion من مارس حتى يونيو من عام 2020 والتي تم استخدامها بعد ذلك لخرق العملاء الذين قاموا بالترقية إلى الإصدارات المتأثرة.

المطلب الأول: كرونولوجيا إختراق SolarWinds Orion

في 8 ديسمبر 2020 ، أعلنت شركة FireEye أنها عثرت على أدلة للإختراق الشبكة الخاصة بها وأن الجهة المهاجمة قامت بسرقة "Red Team Tools" الخاصة بالشركة ، وكون الشركة تقدم خدمات حماية سيبرانية ، فهي تمتلك أدوات وبرامج خاصة بها تستخدمها في اختبار شبكات وبرامج العملاء ، وهذا ما تم إكتشاف انه تم سرقته ، وفي في ظل هذه الهجمة المكتشفة ، فتحت شركة FireEye تحقيق في الحادثة ،

[134] Evan D. Wolff, Kate M. Growley, Maida O. Lerner, Matthew B. Welling, Michael G. Gruden, Jacob Canter, **Navigating the SolarWinds Supply Chain Attack**, The Procurement Lawyer, Volume 56, Number 2, Spring 2021, p3

وفي 11 ديسمبر أعلنت على أن شركة SolarWinds كانت جزء من الهجوم وأنه كان فيه ملف في إحدى تحديثات سولارويندز على منصة Orion يحتوي على ملف ملغوم وضار من خلال تثبيت Backdoor.

وبعد الحادثة وتصريحات الشركة ، تم عقد اجتماع في البيت الأبيض على مستوى " مجلس الأمن القومي الطارئ – Emergency National Security Council ". وهي أعلى جهة في قضايا الأمن الوطني داخل الولايات المتحدة ، وهذا مما يدل على توقع أن عواقب وأضرار هذا الإختراق ستكون كبيرة. وفي تاريخ 13 ديسمبر أصدرت وكالة الأمن السيبراني وأمن البنية التحتية CISA توجيهًا طارئًا (Emergency Directive) لكل الجيهات الحكومية لتحقق من الشبكات الداخلية وفصل أو إيقاف تشغيل منتجات SolarWinds Orion[135]. وفي سياق ذلك عرف نفس اليوم أول إفصاح وتقرير من طرف شركة SolarWinds حول الحادثة ، بحيث قدمت تفصيل حول البرامج المتأثرة بإختراق واستطاعت معرفة النسخ المتأثرة بـ Malware واعتبرت أن هذا الهجوم كان جد متطور ومتقدم من حيث من حيث الكفاءة وتقنيات عالية في التنفيذ العملية " supply chain attack".[136]

وفي تاريخ 14 ديسمبر قامت شركة سولارويندز بإفصاح رسمي ومباشر لـ " هيئة الأوراق المالية والبورصات الأمريكية – SEC– U.S. Securities and Exchange Commission " وهي وكالة تابعة للحكومة الأمريكية والمسؤولة على تنفيذ القوانين الفيدرالية للأوراق المالية واقتراح قوانين و تنظيم قطاع الأوراق المالية ، هذا جاء التبليغ جاء بعد يوم واحد من إفصاح الشركة عن الحادث للعملاء ، وجاء ابلاغ SEC لكون شركة سولارويندز مطروحة في سوق الأسهم وبالتالي مجبرة بإفصاح عن أي حادث يؤثر على الشركة ، وتم تقديم في المراسلة بيانات مهمة و المتمثلة في:

- أن الشركة لديها 300000 عميل ، و 10% منهم ما يقارب 33000 هم من يمتلكون برنامج Orion المتضرر من الإختراق ، و13000 هم من قاموا بتحميل النسخة التي كان مصابة ومخترقة.[137]

[135] CISA ISSUES EMERGENCY DIRECTIVE TO MITIGATE THE COMPROMISE OF SOLARWINDS ORION NETWORK MANAGEMENT PRODUCTS, Original release date: December 13, 2020 | Last revised: December 14, 2020, Direct link: https://www.cisa.gov/news/2020/12/13/cisa-issues-emergency-directive-mitigate-compromise-solarwinds-orion-network

[136] **SolarWinds Security Advisory**, Information about SUNBURST, Direct link: https://www.solarwinds.com/sa-overview/securityadvisory

[137] CURRENT REPORT, **SOLARWINDS CORPORATION: SEC FILING**, PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934. December 14, 2020, Direct link: https://www.sec.gov/ix?doc=/Archives/edgar/data/1739942/000162828020017451/swi-20201214.htm

- إعتبرت الشركة ان الهجوم كان جد متطور محترف على أنظمتنا أدى إلى إدخال ثغرة في منتجات Orion Platform الخاصة بنا ، واعتبر الخبراء ان اختراق كان جد مستهدف ومعقد للغاية.
- تم التعرف على الثغرة الأمنية فقط في تحديثات التي تم تسليمها بين شهر مارس و يونيو 2020 ، ولكن التحقيقات لا تزال جارية.
- خلال البيان المرسل لهيئة الأوراق المالية والبورصات الأمريكية ، كان يتضمن تصريح غريب من الشركة ، والمتمثل في كونها تستعمل برنامج Microsoft Office 365 ، ولم تفصل في ذكرها لهذا ، ولكن وبحسب الخبراء انه وخلال عملية الاختراق قام المهاجمون بإستخدام ثغرة في هذا البرنامج.
- كما ذكرت الشركة ، أنها وعقب اكتشاف الحادث دخلت في تعاون مع خبراء الأمن السيبراني للعديد من الشركات الرائدين في المجال لمساعدتنا في إيجاد حلول للحادث ، وكما اننا نتعاون بنشاط مع شركائنا والعملاء ووكلات إنفاذ القانون والإستخبارات في العالم.[138]

وفي تاريخ 15 ديسمبر دخلت جهة جديدة على خط التحقيقات و المتمثلة في الجهة التشريعية ، وهذا بطلب الكونغرس من مكتب التحقيقات الفيدرالي FBI، وCISA وكالة الأمن السيبراني وأمن البنية التحتية ، بتحقيق رسميا وإبلاغ الكونغرس بعدة نقاط حول الحادث ، وتم هذا بطلب من أعضاء الكونغرس وهم: Jerry Moran – Roger Wicker – John Thune – Cantwell Maria – Richard Blumenthal – Jeanne Shaheen ، وهم قادة لجنة مجلس الشيوخ الأمريكي للتجارة والعلوم والنقل واللجنة الفرعية لشؤون التجارة والعدل والعلوم والوكلات ذات ، وكان الطلب يتضمن تقديم تقرير حول مدى الهجوم السيبراني لسلسة التوريد على حكومة الولايات المتحدة الذي نفذته جيهات روسية.[139]

وفي نسخة المراسلة الرسمية ، تم توجيه وذكر الجهة المتوقع تنفيذها للإختراق وهي " Cozy Bear " أو المعروفة أيضا بـ "Advanced Persistent Threat" APT29 وهي جهة معروفة و مصنفة مسبقا لدى الحكومة الفيدرالية الأمريكية كمجموعة هاكرز روسية تعمل ومرتطبة بوكلات الإستخبارات الروسية ، وتضمن طلب أعضاء الكونغرس في:

- إحصاء الجيهات الحكومية المتضررة من الحادثة ، والوكلات التي تستعمل SolarWinds Orion

[138] Second report, Date: December 17, 2020, Direct link: https://www.sec.gov/Archives/edgar/data/1739942/000162828020017620/swi-20201217.htm
[139] Senators Request Information from FBI, CISA on Reports of Russian Cyberattack Against the U.S. Government, Dec 15 2020, Direct link: https://www.moran.senate.gov/public/index.cfm/2020/12/senators-request-information-from-fbi-cisa-on-reports-of-russian-cyberattack-against-the-u-s-government

- ماهي البيانات التي تم سرقتها خلال الإختراق.
- هل الجيهات المتأثرة كانت نتيجة عدم إلتزامها بالأنظمة الحكومية في أمن المعلومات ، أو ما يطلق عليه بـ FISMA – Federal Information Security Modernization و هو قانون وإجراءات تقر بأهمية أمن المعلومات للمصالح الاقتصادية والأمن القومي للولايات المتحدة.
- وأيضا تم توجيه أسئلة حول ماذا ستقدم FBI و CISA للشركات المتأثرة ، وما نوع البيانات التي يمكن للحكومة الأمريكية مشاركتها مع الشركات لمساعدتها للتعافي والتعاون مع هذه الحادثة.[140]

في 16 ديسمبر ، وكما سبق الذكر ، أن شركة SolarWinds هي مطروحة في سوق الأسهم تم إكتشاف أن أكبر ملاك للأسهم في الشركة وما يطلق عليهم Private Equity و هم: Thoma Bravo و Silver Lake Partners أنهم قاموا ببيع جزء من أسهم الخاصة بهم على صندوق التقاعدي في كندا في يوم 9 ديسمبر ، أي بيوم واحد بعد إعلان شركة FireEye عن اكتشاف الإختراق ، وقد ثارت شكوك حول بيع حصة بما يقارب 315 مليون دولار[141] وهذا فقط قبل أيام من إعلان الشركة عن إختراقها بالهجمة والذي خلف نزول سعرها وخسائر في قيمتها ، فكانت تدور عليهم شبهة. وصرحت بعد ذلك الشركة ان بيع لم يكن له علاقة مع الهجوم.

في تاريخ 17 ديسمبر نشرت CISA وMicrosoft بيانات أكثر حول الجيهات المصابة بالهجوم و الطريقة والتقنيات التي تم استعمالها في تنفيذ الإختراق ، وتم تسجيل جيهات جديدة حساسة في الحكومة وفي القطاع الخاص والتي تجاوزت 40 جيهة[142]، مثل:

- وكالة الطاقة النووية وهي المسؤولة على الأسلحة النووية الأمريكية، ومختبر لوس ألموس الوطني وهو مختبر يتبع وزارة الطاقة الأمريكية نُظم في بادئ الأمر إبان الحرب العالمية الثانية لإجراء أعمالٍ سريةٍ تتضمن تصميم الأسلحة النووية كجزء من مشروع مانهاتن ، قد تم إختراقهم.
- وزارة الأمن الداخلي في الولايات المتحدة أو جهاز الأمن الداخلي " Department of Homeland Security –DHS" وهي المسؤولة على CISA ووكالات أمنية أخرى ، تم إختراقها.

[140] Letter from senators, United States Senate, WASHIGTON, DC20510, December 15, 2020. Direct link: https://www.moran.senate.gov/public/_cache/files/e/d/ed2078ad-8f58-460a-ab54-5ffe570bfd23/9E2CFEA30538117FF470015EBAD88368.12.15.2020---letter-to-cisa-and-fbi-re-solarwinds---final-signed.pdf

[141] Drew Harwell, Douglas MacMillan, **Investors in breached software firm SolarWinds traded $280 million in stock days before hack was revealed**, Seen on 5/23/2021. Direct link: https://www.washingtonpost.com/technology/2020/12/15/solarwinds-russia-breach-stock-trades/

[142] TTP Table for Detecting APT Activity Related to SolarWinds and Active Directory/M365 Compromise, https://us-cert.cisa.gov/ncas/current-activity/2021/03/17/ttp-table-detecting-apt-activity-related-solarwinds-and-active

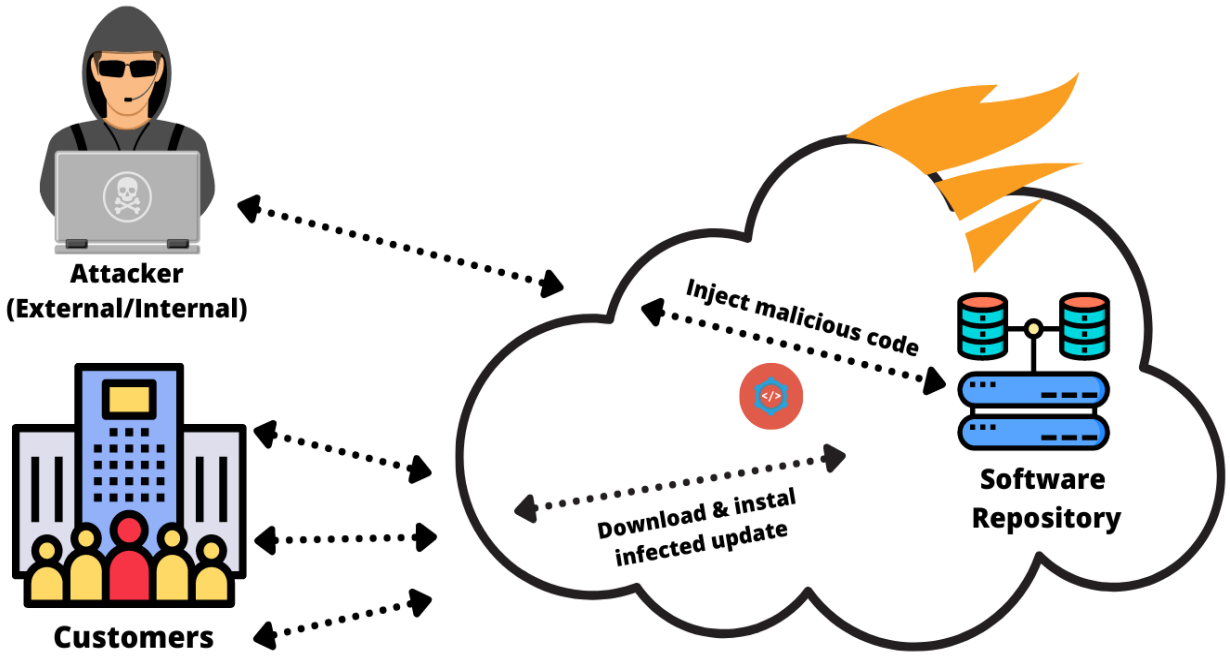
- وزارة المواصلات المسؤولة على الطيران و التنقلات والقطارات.
- وزارة التجارة ، والعديد من جيهات الأمريكية الحساسة الأخرى.[143]

وخلال التحقيق تم الوصول لكون أول ظهور للتحديث المصاب بـ backdor والمخترق لمنصة SolarWinds Orion كان في شهر مارس 2020 ، ما يعني أن بين الفترة التي اخترقت فيها الشركة واكتشاف الاختراق كانت بحوالي أكثر من 9 أشهر. وهذا الذي قاد خبراء الأمن السيبراني مكلفون بتحقيق لتسائل ، إذ اختراق تم شهر مارس 2020 ، فعملية زرع الملف الملغم والقيام بـ Digital signature بحيث ما يكون ظاهر ستأخذ فترة أطول لصعوبة تفيذ هذه الخطوات ، الأمر الذي رجحته شركة SolarWinds الى شهر أكتوبر 2019 ، بحيث صرحت ان لاحظت تغير في الأكواد البرمجية بداية من تلك الفترة ، ومنه يتبين ان الجهة المهاجمة تمكنت من دراسة وفهم طريقة عمل شركة SolarWinds بداية من شهر أكتوبر 2019 الى مارس 2020 لتنقيذ عملية الإختراق.

[143] Prev same ref.

المطلب الثاني: كيفية تنفيذ الهجوم

العملية المنفذة من مجموعة الهاكرز الروس Cozy Bear أو APT29 كما هي معروفة عند الحكومة والمخابرات الأمريكية ، كانت جد صعبة ومعقدة في تنفيذها ، مما يؤكد على المستوى العالي للفريق المهاجم واحترافيته العالية ، والدعم والموارد الكبيرة المخصصة لهم في إنجاح مثل هكذا عمليات تجسس. وفي الصورة التمثيلية التالية سيتم تبسيط الطريقة التي تم من عبرها تنفيذ الاختراق:



وتمثل السحابة في الصورة مراكز تخزين البيانات لشركة SolarWinds ، وكون الشركة تقدم برامج وأدوات ، فهي تمتلك Software Repository وهو عبارة على مستودع برمجيات لتخزين البرامج والتحديثات المقدمة للعملاء ، بحيث يمكن للعملاء الوصول له وتنزيل البرنامج او التحديثات.

الجهة المهاجمة والتي نفذت الإختراق تمكنت من الوصول الى داخل الشبكة الخاصة بشركة SolarWinds وتمكن من التحكم واختراق Software Repository ، وبعد ما تمكن الجهة المهاجة من الوصول ، تم تلغيم البرنامج والتحديثات لشهر مارس بـ أكواد برمجية خبيثة " Malicious Code ".

ومن خلال ذلك قام المستعملون للبرنامج SolarWinds Orion بتحميل التحديثات الملغة عبر الموقع الرسمي للشركة ، وتم اختراقهم عبر ذلك.

وقد تم تسمية الـ Malware المستعمل في العملية بـ SUNBURST من طرف شركة سولارويندز ، وهو عبارة عن (DLL) digitally–signed backdoor والذي احتوى عليه التحديث نسخات Orion. وتم تسميته من طرف الهاكرز في التحديث بـ SolarWinds.Orion.Core.BusinessLayer.dll

وقد مر الهجوم والإختراق بعدة مراحل للوصول الى الجيهات المستهدفة والتي قدرت بـ 18000 ضحية ، والتي من أكيد أن الجهة التي تقف وراء هذا العمل كانت تستهدف جيهات محددة وهي المؤسسات الحكومية للولايات المتحدة. والمراحل المتمثلة في:

1- Delivery of Supply Chain Attack: يتم في هذه الحالة تجميع معلومات حول الجهة التي حملت ونصبت التحديث الذي يحتوي على الإصابة ، وهذا عن طريق تجميع active directory local domain name ، ويتم إرساله للمهاجم بطريقة مشفرة وهذا بطريقة Domain generation algorithms بحيث يصبح ارسال مشفر وغير واضح لأي أحد ، ويرسل للمهاجم ، وبعدها يقرر المهاجم إذ كان يريد مواصلة في اختراق الجهة التي حملت التحديث او يتوقف.

2- Command And Control: في خطوة الثانية من الإختراق يقوم المهاجم بـ بإرسال وتنصيب Malware الثاني الذي سمي بـ Teardrop والذي يحتوي على أداة CobaltStrike تستخدم من طرف المهاجمين و من طرف Red Team (" الفريق الأحمر: هو مجموعة تلعب دور العدو أو المنافس ، وتوفر ملاحظات أمنية من هذا المنظور. يتم استخدام الفرق الحمراء في العديد من المجالات ، لا سيما في الأمن السيبراني وأمن المطارات والجيش ووكالات الاستخبارات[144].") وهدا خلال العمليات التحقق الأمني او تنفيذ الإختراقات ، والذي يميز هذه الأداة انها تعطي صلاحيات وطرق كثيرة وسهلة جدا للمهاجم عندما يخترق أي جهة ، ويتوصل للأهدافه بسهولة.[145][146]

3- الحركة الجانبية Lateral Movement: في هذه المرحلة وبعد ان توصل المهاجم الى قواعد بيانات شركة SolarWinds وتمكن من تنفيذ الإختراق بنجاح ، فالأكيد ان المعلومات التي يبحث عنها غير موجودة

[144] Jeremiah Talamantes, **What is Red Teaming And Why Do I Need It?,** https://www.redteamsecure.com/blog/what-is-red-teaming-and-why-do-i-need-it-2
[145] SUNBURST,Article, Seen on 5/23/2021, https://attack.mitre.org/software/S0559/
[146] **Tracking UNC2452-Related Reporting**, Seen on5/23/2021, Direct link: https://github.com/center-for-threat-informed-defense/public-resources/blob/master/solorigate/README.md

على SolarWinds Servers[147]. مما يضطر انه يذهب إلى أجهزة وأنظمة ثانية للعملاء ، وكون برنامج Orion هو برنامج مراقبة " monitoring " فقد سهل ذلك على هاكرز للإتصال بأنظمة كثيرة داخل الشركة و القيام بـ Forging SAML Authentication Tokens وهي عملية تزوير لإذن بدخول بعدد مرات غير متناهية ، والتي عادت ما تكون محدد بساعة واحدة من طرف الشركة للمستخدمين.[148]

4- التهريب "Exfiltration": ينتهي الهجوم بإستخراج البيانات التي يستهدفها المهاجم ، مثل الرسائل البريدية ، عبر أوامر البريد بواسطة PowerShell ، أو الملفات المحفوظة المحمية بكلمة مرور والتي تحتوي على بيانات حساسة من سيرفرات الضحية.[149] [150]

المطلب الثالث: الجيهات المتهمة بتنفيذ الإختراق

في 17 ديسمبر تعهد الرئيس المنتخب جو بايدن بالإرتقاء بالأمن السيبراني باعتباره "أمرًا حتميًا" عندما يتولى منصبه ، وقال انه لن "يقف مكتوف الأيدي" في مواجهة الهجمات والسيبرانية وهذا بعد خرق هائل أثر الذي استهدف وأثر على الحكومة الأمريكية. هذا و لم يعلق الرئيس ترامب علنًا على الهجوم.[151] وتم تصريح وإبلاغ في نفس اليوم على ان الإختراق مس أيضا الإدارة الوطنية للأمن النووي وهذا عن طريق الوصول الى الأنظمة التي تحتفظ بمخزون الأسلحة النووية الأمريكية. كما نشرت شركة ميكروسوفت على ان حوالي 40 من عملائها تم إستدافهم عبر الإختراق.

وفي 5 جانفي 2021 اتهمت مجموعة من وكالات الإستخبارات الأمريكية رسميًا روسيا بالارتباط بالاختراق الذي تم اكتشافه مؤخرًا لشركة SolarWinds ، بحيث أرجع مكتب التحقيقات الفيدرالي ، ومكتب مدير الاستخبارات الوطنية (ODNI) ، ووكالة الأمن القومي (NSA) ووكالة الأمن السيبراني وأمن البنية التحتية (CISA) هذا الإختراق إلى روسيا.[152]

---

[147] **SUNBURST: How it Happened and How to Minimize the Risk of Future Nation-State Attacks**, 12/23/2020, Direct link: https://securityboulevard.com/2020/12/sunburst-how-it-happened-and-how-to-minimize-the-risk-of-future-nation-state-attacks/

[148] Forge Web Credentials: SAML Tokens, https://attack.mitre.org/techniques/T1606/002/

[149] Same prev ref.

[150] Patrick Orzechowski, Greg Genung, Threat Report: **SolarWinds Attack - Part II - Is MITRE ATT&CK Falken's Maze?**, Published date: 02.18.21, Seen on 5/23/2021. Direct link: https://www.deepwatch.com/blog/solarwinds-mitre-attck-falkens-maze/

[151] MORGAN CHALFANT AND MAGGIE MILLER, **Biden vows to make cybersecurity 'imperative' following massive hack**, 12/17/20. Seen on 5/23/2021. Direct link: https://thehill.com/policy/cybersecurity/530706-biden-vows-to-make-cybersecurity-imperative-following-massive-hack

[152] MAGGIE MILLER, **US intel agencies blame Russia for massive SolarWinds hack**, Seen on 5/23/2021. Direct link: https://thehill.com/policy/cybersecurity/532756-us-intel-agencies-blame-russia-for-massive-solarwinds-hack

وفي 22 جانفي قام الرئيس جو بايدن بتعين واستعانة بمجموعة من قدامى الخبراء في مجال الأمن السيبراني من ذوي الخبرة السيبرانية العميقة للمساعدة في التعافي من عمليات الاختراق التي مست القطاعات الحكومية الحساسة المنسوبة لوكالات تجسس الروسية. [153] و في بداية الشهر فيفري توصلت مؤسسة إخبارية دولية رويترز Reuters ، ومن جيهات مقربة من التحقيق للإمكانية تورط الصينيين في الهجوم السيبراني ، وهذا ما رفضت الوكالة الفيدرالية للأمن والتحقيقات FBI تأكيده أو نفيه.[154]

وفي 23 فيفري ذكر مستشار الأمن القومي للولايات المتحدة جيك سوليفان Jake Sullivan ، على ان إدارة جو بايدن تستعد لفرض عقوبات وتدابير أخرى لمعاقبة موسكو على حملة التي تجاوزت حد التجسس السيبراني واختراق SolarWinds ووصول إلى غاية تسميم للمعارض الروسي أليكسي نافالني Navalny Alexei. [155]

وفي هذا السياق ، الجهة الروسية التي عادت ما كان يتم توجيه الإتهام لها من الولايات المتحدة في حوادث إختراق عديدة ، يطلق عليها تسميات عديدة ، منها: Cozy Bear – APT29 – Dark Halo – SolarStorm وعديد من التسميات الأخرى ، وهي مجموعة تجسس روسية تتمتع بموارد جيدة ومتفانية ومنظمة للغاية ويعتقد انها تعمل لصالح روسيا منذ سنة 2008 ، لجمع المعلومات الإستخباراتية لدعم صنع القرار في السياسة الخارجية و الأمنية. وتستهدف مجموعة Cozy Bear بشكل أساسي الحكومات الغربية والمنظمات ذات صلة بها. مثل الوزارات والوكالات الحكومية ومراكز الفكر السياسي – Political Think Tanks وغير ذلك. كما شملت أهدافهم حكومات أعضاء كومنولث "رابطة الدول المستقلة". والحكومات الآسيوية والأفريقية والشرق أوسطية. المنظمات المرتبطة بالتطرف الشيشاني ، والناطقين باللغة الروسية ضالعين في الاتجار غير المشروع بالمواد الخاضعة للرقابة والمخدرات.

ومن المعروف أن الفريق هجومي الروسي يمتلك ويستخدم ترسانة كبيرة من مجموعات أدوات البرمجيات الخبيثة مثل: MiniDuke, CosmicDuke, OnionDuke, CozyDuke, CloudDuke, SeaDuke, HammerDuke, PinchDuke, and GeminiDuke.[156]

[153] Christopher Bing, Joseph Menn, **After big hack of U.S. government, Biden enlists 'world class' cybersecurity team**, Seen on 5/23/2021. Direct link: https://www.reuters.com/article/us-usa-biden-cyber/after-big-hack-of-u-s-government-biden-enlists-world-class-cybersecurity-team-idUSKBN29R18I

[154] Christopher Bing, Jack Stubbs, Raphael Satter, Joseph Menn, **Exclusive: Suspected Chinese hackers used SolarWinds bug to spy on U.S. payroll agency – sources**, https://www.reuters.com/article/us-cyber-solarwinds-china-exclusive/exclusive-suspected-chinese-hackers-used-solarwinds-bug-to-spy-on-u-s-payroll-agency-sources-idUSKBN2A22K8

[155] Biden administration preparing to sanction Russia for SolarWinds hacks and the poisoning of an opposition leader. Seen onM 5/23/2021. Direct link: https://www.nationthailand.com/news/30402990

[156] **Threat Group Cards: A Threat Actor Encyclopedia**, Thailand Computer Emergency Response Team (ThaiCERT)

وقد قامت Cozy Bear بالعديد من اختراقات ، وأبرزها:

– في مارس 2014 تم العثور على Malware (Trojan.Cozer) في شبكة معهد أبحاث خاص الواقع في واشنطن ، وفي شهر جوان تم اكتشاف اختراق للشبكات الحكومية الأمريكية ، وفي صيف 2014 تسلل عملاء رقميون لجهاز المخابرات والأمن العام الهولندي وتم اكتشاف ان الهاكرز هم روس وكانوا يستهدفون الحزب الديمقراطي الأمريكي ووزارة الخارجية والبيت الأبيض.

– في شهر أوت تم ربط Cozy Bear بهجوم السيبراني ضد نظام البريد الإلكتروني للبانتاغون مما تسبب في إغلاق نظام البريد الإلكتروني لهيئة الأركان المشتركة ووصول الى انترنت اثناء التحقيق.

– في سنة 2016 تم تنفيذ اختراق مشترك لمجموعة الروسية Cozy Bear و Fancy Bear ضد الحزب الديمقراطي الأمريكي.

– بعد الانتخابات الأمريكية في 2016 ارتبط ذكر Cozy Bear بسلسلة من الحملات التصيد ضد مراكز الأبحاث و المنظمات غير الحكومية داخل ولايات المتحدة.

– في 2020 تم اتهام Cozy Bear من قبل NSA– National Security Agency و National Communications Security Establishment و NCSC– Cyber Security Centre UK CSE–CANADA بمحاولة سرقة البيانات الخاصة باللقاحات والعلاجات الخاصة بـ COVID–19 التي يتم تطويرها في المملكة المتحدة والولايات المتحدة وكندا.

– وفي 2020–2021 تم اتهام Cozy Bear بتنفيذ الاختراق ضد شركة SolorWins.[157]

Electronic Transactions Development Agency, Direct link: https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=UNC2452%2C%20Dark%20Halo%2C%20SolarStorm

[157] Cozy Bear, From Wikipedia; seen on 5/23/2021, Direct link: https://en.wikipedia.org/wiki/Cozy_Bear

خلاصة الفصل الثاني:

وفي نهاية الفصل الثاني ، نستخلص ما يلي:

– شكلت قائمة عملاء شركة SolarWinds هدفا لفريق الإختراق الروسي Cozy Bear لتنفيذ الإختراق عبر برنامج Orion ، لإحتوائها على جهات حكومية حساسة.

– في مثل هذه الحادثة ، يذكرنا الإختراق أن جميع أنظمة الكمبيوتر والبرامج ، هي معرضة لخطر القرصنة وتجاوز كل الإستراتجيات الأمنية الموضوعة للحماية ، بحيث يمكما اختراق أي شيئ متصل بالإنترنت " وفي الكثير من الأحيان سيتم اختراقه اذ كانت فيه نية ورغبة من جهة محترفة لتنفيذ ذلك " ، فالطريقة الوحيدة لتكون أي جهة حكومية أو شركة خاصة مقاومًا للاختراق بنسبة 100% هي عدم إستخدام نظام الكمبيوتر وأي شيئ متعلق بشبكات الأنترنت ، وهذا ما يستحيل تنفيذه خلال هذا العصر ، بحيث ترتبط حياة كل الشركات و الحكومات والشعوب بشبكات الأنترنت و الكمبيوتر وكل ما يتعلق بتكنولوجيات الجديدة.

– يقوم الأمن المعلومات و الأمن السيبراني على تقييم و إدارة وتقليل المخاطر التي تتعرض لها أنظمة الكمبيوتر و الشبكات الخاصة بها بشكل كبير . ولكنهما لا يلغيان إمكانية حدوث إختراق.

– في هذا السياق ومع تنامي التهديدات والهجومات السيبرانية ، يجب على الجيهات المسؤولة على حماية البيانات وتوفير الأمن في الفضاء السيبراني أن تنتهج خطط وإستراتجيات وبناء أنظمة مرنة وسريعة لتسيير الحوادث السيبرانية ، عبر تسطير خطة إدارة وإصلاح الحوادث والتعافي منها في أسرع وقت ممكن ، لتفادي أي تعطيل في تزويد بالخدمات ، مما قد يولد خسائر إقتصادية لجيهات عديدة.

– يعد الأمن على أنه أكثر من مجرد تقنية ومن هذا المنطلق فإن الأمن لا يقتصر فقط على التكنولوجيا فحسب ، بل بتعلق بالحوكمة والسياسات العمليات والأشخاص ، ومنه فإن الأشخاص هم الجزء الأكثر أهمية في هذه المعضلة ، لأنهم هم الذين يتعين عليهم نشر وتهيئة أحدث التقنيات واتباع جميع السياسات وإجراءات الأمنية داخل جميع بيئات العمل التي ترتبط بحماية أمن المعلومات والفضاء السيبراني.

– يجب أن يصبح الأمن جزءا من ثقافتنا ، بحث يجب ان يكون الموظفون على دراية بخطط الإستجابة للحوادث ، وكيفية رصد واكتشاف أي خلل بنظام والشبكات وتبليغ عنها للفريق المختص ، لكبح أي اختراق.

الـخـاتـمـة

الخاتمة

قامت إشكالية الدراسة الأساسية على رصد و البحث في الإستراتجيات الأمنية المنتهجة من طرف الولايات المتحدة الأمريكية في الفضاء السيبراني للحد من الهجومات و التهديدات السيبرانية ، وهذا من أجل فرض الخطط والقوانين الردعية التي تحمي الفضاء السيبراني ومصالح الولايات المتحدة من أي تهديد ، وقد قمنا بتركيز في الفصل الأول على الجانب المفاهيمي والنظري للدراسة عبر التطرق للأبرز أنواع الهجومات السيبرانية التي يتم عبرها إختراق الأنظمة التشغيل والشبكات ومراكز تخزين البيانات ، كما تطرقنا إلى كيفية الرفع من درجات الحماية ضد الهجومات السيبرانية وهذا بهدف ضمان الامان للمعلومات الحساسة المرتبطة بشبكات الانترنت ومراكز تخزين البيانات.

كما قامت الدراسة بتطرق الى الإستراتجيات السيبرانية المتبعة من طرف الولايات المتحدة بداية من سنة 2009 ووصولا الى سنة 2020 ، خلال فترة حكم الرئيس باراك أوباما و دونالد ترامب ، خلال بحثنا أبرزنا كل الإستراتجيات الأمنية التي تم تبنيها للوقوف ولصد أي اختراقات او تهديدات للفضاء السيبراني ، مع إقرار فرض عقوبات ردعية في وجه الجيهات المهددة للأمن الأمريكي.

وقد تم ابراز التحديات والتهديدات التي تواجهها الولايات المتحدة في فضائها السيبراني والجيهات التي تشكل مصدر تهديد لها ، كما سعت الولايات المتحدة الى انشاء وكالات وأقسام حكومية أمنية تعمل على تتبع والتحقيق في الإختراقات والحوادث السيبرانية وهذا ما تم تطرق له في الفصل الأول ، مع توضيح المهام المخولة لهذه الوكالات والملحقات التابعة لها ، وفي نهاية الفصل تم التطرق الى الشركات الأمن السيبراني التي تتعامل معها جيهات عديدة في الولايات المتحدة والعالم ، وإبراز اثار جائحة كورونا على الأمن السيبراني عبر الصعود الذي سجلته أسهم هذه الشركات في ظل ارتفاع الجريمة الإلكترونية خلال فترة الحجر الصحي التي اقرتها الدول مع تنامي وانتشار الفيروس Covid19 وتزايد اقبال العديد من الجيهات على خدمات الحماية السيبرانية التي تقدمها العديد من الشركات.

وفي الفصل الثاني تناولنا فيه دراسة حالة حول الهجوم والإختراق الذي شهدته العديد من الجيهات الحكومية و الشركات الخاصة في الولايات المتحدة من مجموعة الهاكرز APT29 التي تتبع أجهزة المخبارات الروسية ، وهذا عبر استهدافهم لشركة سولارويندز المختصة في برامج رصد الشبكات والأنظمة وتسيير مراكز تخزين البيانات ، كما تم استعراض كرونولوجيا التي صاحبت عملية الإختراق وإكتشاف الهجوم ، وتم عرض للأبرز الخدمات المقدمة من طرف شركة سولارويندز مع التركيز على منصة التي تم عبرها استهداف العملاء "SolarWinds Orion" ، و كما قمنا بتقديم قائمة للأبرز عملاء الشركة من القطاع الخاص و العام ، كما

قمنا بتفصيل في الطريقة التي مكنت الهاكرز من تنفيذ الإختراق والأساليب التي استعملت للإنجاح العملية ، وفي الأخير قدمنا نبذة عن الجيهة التي اتهمتها و حملتها الولايات المتحدة مسؤولية الحادث.

وبناء على ما سبق نستنتج:

– أثبتت الإستراتجيات السيبرانية المنتهجة من الولايات المتحدة عدم فعالتيتها في حماية الفضاء السيبراني من التهديدات وخروقات المتكررة التي تمارسها الجيهات والقوى المنافسة لأمريكا.

– رغم توفر العديد من الأجهزة والوكالات الحكومية المكلفة بحماية الفضاء السيبراني من أي هجومات واختراقات ، إلا ان ذلك لم يمنع من اجهاض وكبح العمليات المتكررة في استهداف الولايات المتحدة.

– ان المشكل الذي تعاني منه الولايات المتحدة في الأمن السيبراني ، هو صعوبة تحديد الجيهات الفاعلة التي تشكل خطر وتستهدف الوكالات الحكومية ، وهذا لصعوبة تقديم ادلة وإثباتات تجرم الفاعلين عبر أنشطتها في الفضاء السيبراني ، وهذا لسهولة طمس الأدلة وتهرب من المسائلة القانونية.

– أثبتت عملية الإختراق التي مست شركة سولارويندز ، على انه يمكن للمهاجمين اختراق سلسلة توريد البرامج وتعديل الملفات التنفيذية ، وهذا تحت اشراف ودعم الدولة التي ترعى هذه الجيهات الفاعلة ، وكل ذلك يتم عبر محاكاة حركة مرور البروتوكول لتجنب الإكتشاف أو ترك أدلة تورط الجهة الفاعلة. ومنه فإن شركات البرمجيات مثل سولارويندز وخاصة تلك التي تعمل في مجال الأمن السيبراني ، تحتاج الى تصميم ضوابط وصول ذات امتيازات وقائية في عملية DevOps الخاصة بها وتقويتها باستخدام ضوابط قائمة على اكتشاف سريعة وفعالية ، لتجنب أي اختراق.

– يجب على المؤسسات الحكومية الأمريكية العمل على تطوير برمجيات خاصة بها وغير تابعة لشركات أخرى ، مما قد يعقد ويصعب الأمر على جيهات التي تسعى الى اختراق أنظمتها عبر هجومات سلسلة التوريد.

– عدم تحصين وفرض استراتجيات سيبرانية محكمة ، يأدي الى عرضتها الى الهجومات والتهديدات السيبرانية وشل اقتصادها وتسبيب خسائر لها ، والذي ينعكس سلبيا على أمنها القومي.

– كشف الإختراق الذي مس شركة سولارويندز عن وجود ثغرات أمنية وبرمجية التي اذ لم يتم تداركها ، من الممكن تأدي الى المزيد من الحوادث المشابهة.

– أولت الإدراة باراك أوباما و دونالد ترامب أهمية بالغة بالفضاء السيبراني للولايات المتحدة عبر الإستراتجيات والقوانين التي تحمي الشركات والمواطنين من أي تهديدات وخروقات سيبرانية ، إلا أن ذلك لم يكن كافي لوقف كبح محاولات الأطراف المعادية من اختراق وتنفيذ تستهدف الأمن السيبراني للبلاد.

– في ظل تنامي التهديدات و الاختراقات السيبرانية ، فلابد من العمل على استحداث استراتجيات وخطط اكثر فعالية و تماشيا مع الأساليب التي يستحدثها الهاكرز ، ما يعني الخروج من قواعد توظيف العمال المكلفين بالحماية السيبرانية التقليدية ، و توجه الى جلب هاكرز فعليين و توظيفهم في مراكز ومؤسسات حكومية من اجل مجابهة كل التهديدات الأمنية المستحدثة ، و لعل من أبرز الملتقيات و التجمعات التي يمكن من خلالها إيجاد و توظيف هاكرز متمكنيين " DEF CON " و هو واحد من أكبر المؤتمرات الهاكرز والذي يعقد كل عام في لاس فيغاس، نيفادا. فمن أجل تجنب وتحصين الأنظمة الأمنية والبيانات من الهجومات و الاختراقات السيبرانية ، يتم انتقاء أفضل الهاكرز خلال مثل هذه الملتقيات و توظيفهم مباشرة لوضع خطط عمل اكثر فعالية لكبح التهديدات السيبرانية المستحدثة ، كون هاذ الهاكرز هم اكثر شغف بالمجال الأمني و على دراية بكافة المستجدات و طرق الاختراق التي يبتكرها الهاكرز من امثالهم ، وهذا يأدي الى رفع مستوى الحماية داخل المؤسسات الحكومية و الشركات الخاصة.

قائمة المراجع

Les Références

المراجع

Bibliography: **Les Références:** **قائمة المراجع:**

Books: 1/ الكتب:

1- Dominec Antonucci, **The Cyber Risk Handbook**, Wiley Finance Series, United States, 2017.

2- Amos N. Guiora, **Cybersecurity : geopolitics, law, and policy**, Routledge, United States, 2017.

3- Harry Colvin, **Cyber Security for Beginners: Everything You Need to Know About it**, CreateSpace Independent Publishing Platform, 2017.

4- Janine Kremling, Amanda M. Sharp Parker, **Cyberspace, Cybersecurity, and Cybercrime**, SAGE Publications, United States, 2018.

5- Reverend Bill Blunden, **The Rootkit Arsenal: Escape and Evasion: Escape and Evasion in the Dark Corners of the System,** Jones & Bartlett Learning; 1st edition, United States of America, 2009.

6- RANSOMWARE Hostage Rescue Manual: What You Need to Know To Prepare and Recover from a Ransomware Attack, KnowBe4, 2018.

7- Michael Erbschloe, **Trojans, Worms, and Spyware: A Computer Security Professional's Guide to Malicious Code**, Elsevier Butterworth–Heinemann, United States of America 2004.

8- Charles J . Brooks, Christopher Grow, Philip Craig, Donald Short, **CYBERSECURITY ESSENTIALS**, John Wiley & Sons, Inc, 2018.

9- Justine Clarke**, SQL Injection Attacks and Defense: 2nd Edition**, Elsevier, United States, 2012.

10- *Mark Ciampa, **Security Awareness: Applying Practical Security In New World**, United States, 2015.*

11- William Stallings, **Effective Cybersecurity: A Guide to Using Best Practices and Standards**, Addison-Wesley Professional; 1st edition, 2018.

12- Jean-Philippe Aumasson, **Serious Cryptography: A Practical Introduction to Modern Encryption**, No Starch Press Publishing company, San Francisco, 2017.

المراجع

13- Joshua Holden, **The Mathematics of Secrets: Cryptography from Caesar Ciphers to Digital Encryption**, Princeton University Press and Oxford, United Kingdom, 2017.

14- Robert Ciesla, **Encryption for Organizations and Individuals Basics of Contemporary and Quantum Cryptography**, Apress; 1st ed. Edition, 2020.

16- Issa Traore, Mohammad S. Obaidat, Isaac Woungang, **Biometric-Based Physical and Cybersecurity Systems**, Springer International Publishing, Switzerland, 2018.

17- Anil K. Jain, Arun A. Ross, Karthik Nandakumar, **Introduction to Biometrics**, Springer Science & Business Media, Germany, 2011.

18- James Michael Stewart, **Network Security, Firewalls and VPNs, 2nd Edition, Jones & Bartlett Learning**, United States, 2014.

19- Mark Ciampa, **Security Awareness: Applying Practical Security In New World**, Cengage Learning; 5th edition United States, 2015.

20- Chee Keong Ng · Lei Pan · Yang Xiang, **Honeypot Frameworks and their Applications: A New Framework**, Springer, Singapore, 2018.

21- Allen Harper, Daniel Regalado, Branko Spasojevic, Chris Eagle, Stephen Sims, Ryan Linn, Shon Harris, Gray Hat **Hacking: The Ethical Hacker's Handbook, Fifth Edition**, McGraw-Hill Education, 2018.

22- R. C. Joshi, Anjali Sardana, **Honeypots: A New Paradigm to Information Security**, Published by Science Publishers, United States, 2011.

23- Chee Keong Ng · Lei Pan · Yang Xiang, **Honeypot Frameworks and their Applications: A New Framework**, Springer, Singapore, 2018.

24- Anthony J. Masys (Editor), **Exploring the Security Landscape: Non-Traditional Security Challenges**, Springer International Publishing, Switzerland.

Government documents: الوثائق الحكومية الرسمية:

25- Murugiah Souppaya, Karen Scarfone, **Guide to Malware Incident Prevention and Handling**, Computer Security Division (Information Technology Lab) NIST, 2015.

26- John W. Rollins, Anna C. Henning**, Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations**, Congressional Research Service, Report#: R40427, March 10, 2009.

27- NATIONAL CYBER STRATEGY of the United States of America SEPTEMBER 2018. Link: https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

28- Quadrennial Defense Review Report, February 2010

https://archive.defense.gov/qdr/QDR%20as%20of%2029JAN10%201600.pdf

29- National Security Strategy, May 2010, direct link: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/national_security_strategy.pdf

30- INTERNATIONAL STRATEGY FOR CYBERSPACE: Prosperity, Security, and Openness in a Networked World, May 2011, Direct link: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

31- Quadrennial Defense Review 2014, Department of Defense, Direct link: https://archive.defense.gov/pubs/2014_quadrennial_defense_review.pdf

32- Nathan J. Lucas, Coordinator, Kathleen J. McInnis, **The 2015 National Security Strategy: Authorities, Changes, Issues for Congress**, Congressional Research Service, United States, January 30, 2017. Direct link: https://www.everycrsreport.com/files/20170130_R44023_4c1b6b64f4dd43684f8f751370f551d7d0d45ae0.pdf

33- NATIONAL SECURITY STRATEGY, FEBRUARY 2015, Direct link: https://obamawhitehouse.archives.gov/sites/default/files/docs/2015_national_security_strategy_2.pdf

34- NATIONAL SECURITY STRATEGY of the United States of America, DECEMBER 2017

Direct link: https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf

35- **President Donald J. Trump is Strengthening America's Cybersecurity**, September 20, 2018, Direct link: https://trumpwhitehouse.archives.gov/briefings-statements/president-donald-j-trump-is-strengthening-americas-cybersecurity/?utm_source=twitter&utm_medium=social&utm_campaign=wh

36- Summary of the **National Defense Strategy National Defense Strategy**: Sharpening the American Military's Competitive Edge 2018, Direct link: https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf

37 - **The National Military Strategy: The Joint Staff of 2018 – United States**, Direct link: https://www.jcs.mil/Portals/36/Documents/Publications/UNCLASS_2018_National_Military_Strategy_Description.pdf

38- CYBER STRATEGY SUMMARY, DEPARTMENT OF DEFENSE, 2018. Direct link: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

39- Wesley R. Andrues, REPORT: **What U.S. Cyber Command Must Do**, Joint Force Quarterly: 4th Quarter 2010, Issue 59, Direct link: https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-59.pdf

40- U.S. National Intelligence - An Overview 2013, Direct link: https://www.dni.gov/files/documents/USNI%202013%20Overview_web.pdf

41- CYBERSECURITY STRATEGY, U.S. DEPARTMENT OF HOMELAND SECURITY. Direct link: https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Fact-Sheet.pdf

42- CISA ISSUES EMERGENCY DIRECTIVE TO MITIGATE THE COMPROMISE OF SOLARWINDS ORION NETWORK MANAGEMENT PRODUCTS, Original release date: December 13, 2020 | Last revised: December 14, 2020, Direct link:

https://www.cisa.gov/news/2020/12/13/cisa-issues-emergency-directive-mitigate-compromise-solarwinds-orion-network

43- CURRENT REPORT, **SOLARWINDS CORPORATION: SEC FILING**, PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934. December 14, 2020, Direct link: https://www.sec.gov/ix?doc=/Archives/edgar/data/1739942/000162828020017451/swi-20201214.htm

44- Second report, Date: December 17, 2020, Direct link: https://www.sec.gov/Archives/edgar/data/1739942/000162828020017620/swi-20201217.htm

45- Letter from senators, United States Senate, WASHIGTON, DC20510, December 15, 2020. Direct link: https://www.moran.senate.gov/public/_cache/files/e/d/ed2078ad-8f58-460a-ab54-5ffe570bfd23/9E2CFEA30538117FF470015EBAD88368.12.15.2020---letter-to-cisa-and-fbi-re-solarwinds---final-signed.pdf

Academic journals and articles: المجلات والمقالات الأكاديمية:

46- Darko Galinec, Darko Možnik & Boris Guberina, **Cybersecurity and cyber defence: national level strategic approach,** Automatika: Journal for Control, Measurement, Electronics, Computing and Communications, 2017. link to this article: https://doi.org/10.1080/00051144.2017.1407022

47- Joseph S. Nye, Jr, **Power and National Security in Cyberspace**, America's Cyber Future Security and Prosperity in the Information Age, June 2011.

48- **Cybersecurity:** Current challenges and Inria's research directions, White Book N3, INRIA, Publication date: January 2019.

49- Simplicity VoIP, The A to Z of Cybersecurity Glossary, seen on 4/21/2021 www.globalknowledge.com

50- Jeetendra Pande, **Introduction to Cyber Security**, Uttarakhand Open University, Haldwani, 2017.

51- Chun Guo, , Zihua Song, Yuan Ping, Guowei Shen, Yuhei Cui, and Chaohui Jiang, Article: PRATD: A Phased Remote Access Trojan Detection Method with Double-Sided Features, Guizhou Provincial Key Laboratory of Public Big Data, College of Computer Science and Technology, Guizhou University, College of Cybersecurity, Sichuan University, Chengdu, China, 2020.

52- Camelia Simoiu, Christopher Gates, Joseph Bonneau, Sharad Goel, a study: **"I was told to buy a software or lose my computer. I ignored it": A study of ransomware**, Stanford University, 2019, direct link: https://web.stanford.edu/~csimoiu/doc/ransomware.pdf

53- Jun Gao, Li Li, Pingfan Kong, Tegawendé F. Bissyandé, Jacques Klein, **Should You Consider Adware as Malware in Your Study?**, University of Luxembourg, Luxembourg and Monash University, Australia: Published in: 2019 IEEE 26th International Conference on Software Analysis, Evolution and Reengineering (SANER), Date of Conference: 24-27 Feb. 2019

54- PUBLIC DATA AT RISK: CYBER THREATS TO THE NETWORKED GOVERNMENT, APRIL 2015.

55- Avijit Mallik, **MAN-IN-THE-MIDDLE-ATTACK: UNDERSTANDING IN SIMPLE WORDS**, Cyberspace: Jurnal Pendidikan Teknologi Informasi, Volume 2, Nomor 2, Oktober 2018.

56- Zhu Zhenfang, **Study on Computer Trojan Horse Virus and Its Prevention**, International Journal of Engineering and Applied Sciences (IJEAS), Volume-2, Issue-8, August 2015.

57- Avijit Mallika, Abid Ahsanb, Mhia Md. Zaglul Shahadata, Jia-Chi Tsou, **Man-in-the-middle-attack: Understanding in simple words**, International Journal of Data and Network Science 3, 2019.

58- Cheng-Jing Kuo, **Cryptography**, Graduate Institute of Communication Engineering National Taiwan University, Taipei, Taiwan, ROC.

59- Avinash Kak, **Lecture 19: Proxy-Server Based Firewalls: Lecture Notes on "Computer and Network Security"** , Purdue University: Indiana, United States, March 30, 2021

60- Avishai Woo, **Packet Filtering and Stateful Firewalls**, School of Electrical Engineering, Tel Aviv University, Isreal,

61- Marianne STONE, **Obama's Cybersecurity Plan**, Columbia University, School of International and Public Affairs SECURITY TECHNOLOGY POLICY PAPERS SERIES 1, 1 (Spring 2010), New York.

62- Kayla Morency, **CYBERSECURITY FINALLY TAKES CENTER STAGE IN THE U.S**, Journal of High Technology Law, 2014.

63- Adam Quinn, **Obama's National Security Strategy Predicting US Policy in the Context of Changing Worldviews**, Chatham House the Royal Institute of International Affairs, Research Paper: US Project January 2015.

64- David P. Fidler, **International Law and the Future of Cyberspace: The Obama Administration's International Strategy for Cyberspace**, American Society of International Law (ASIL), June 08, 2011. Direct link: https://www.asil.org/insights/volume/15/issue/15/international-law-and-future-cyberspace-obama-administration%E2%80%99s

65- David P. Fidler, **Cybersecurity and the Changing International Law of Data: The U.S. Election Hacks, Cybersecurity, and International Law**, American Journal of International Law: Volume 110, The American Society of International Law and David P. Fidler, Published online by Cambridge University Press: 15 February 2017.

66- Sarah Kreps and Debak Das, **Warring from the virtual to the real: Assessing the public's threshold for war over cyber security**, Research and Politics, April-June 2017.

67- Emma Ashford, Joshua R. Itzkowitz Shifrinson, **Trump's National Security Strategy: A Critics Dream**, Texas National Security Review: Volume 1, Issue 2 (March 2018).

68- Carlota García Encina, **The Trump Administration's National Security Strategy**, Real Instituto elcano (Royal Institute), Working Paper 14/2018: 13 July 2018, Spain.

69- Seamus P. Daniels, **Show Me the Money: Assessing the Fiscal Reality of the National Defense Strategy's Ambitions**, Center for Strategic and International Studies, Washington, D.C., United States.

70- Keith B. Alexander, **Building a New Command in Cyberspace**, Air University Press, Strategic Studies Quarterly , Vol. 5, No. 2 (SUMMER 2011) , Direct link: https://www.jstor.org/stable/10.2307/26270554

71- Stuart Madnick, Simon Johnson, and Keman Huang, **What Countries and Companies Can Do When Trade and Cybersecurity Overlap**, Harvard Business Review: Working Paper CISL# 2019-03. 2019.

72- Md Sajjad Hosain, **Huawei ban in the US: Projected consequences for international trade**, International Journal of Commerce and Economics, Volume 1; Issue 2; April 2019.

73- Jack Bandy, Nicholas Diakopoulos, **TulsaFlop: A Case Study of Algorithmically-Influenced Collective Action on TikTok**, Northwestern University, 2019. Direct link: https://arxiv.org/pdf/2012.07716.pdf

74- Amanda N. Craig, Scott J. Shackelford, Janine S. Hiller, **PROACTIVE CYBERSECURITY : A COMPARATIVE INDUSTRY AND REGULATORY ANALYSIS**, direct link: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2573787

75- Tiberiu-Marian GEORGESCU, **Study on how the Pandemic Changed the Cybersecurity Landscape**, Article: Informatică Economică vol. 25, no. 1/2021.

76- Paul Moceri, **SNMP and Beyond: A Survey of Network Performance Monitoring Tools** , direct link: https://www.cse.wustl.edu/~jain/cse567-06/ftp/net_traffic_monitors2.pdf

77- Evan D. Wolff, Kate M. Growley, Maida O. Lerner, Matthew B. Welling, Michael G. Gruden, Jacob Canter, **Navigating the SolarWinds Supply Chain Attack**, The Procurement Lawyer, Volume 56, Number 2, Spring 2021.

Theses: الأطروحات والمذكرات:

78- Jan Trobisch, **Challenges in the Protection of US Critical Infrastructure in the Cyber Realm,** School of Advanced Military Studies United States Army Command and General Staff College Fort Leavenworth, Kansas, 2014.

79- Robert T. Bridges, **USCYBERCOM**, A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements; AIR COMMAND AND STAFF COLLEGE AIR UNIVERSITY, April 2009.

80- Niklas Tellini, Fredrik Vargas, **Two-Factor Authentication: Selecting and implementing a two-factor authentication method for a Digital Assessment Platform**, Bachelor's Thesis, KTH Royal Institute of Technology, School of Information and Communication Technology (ICT), 2017.

Websites: المواقع الإلكترونية:

81- Interview with Joseph Nye by José Luis Valdés–Ugalde, **Approaching Power and Understanding Leadership through The Lens of Joseph Nye**, jun. 2008, seen on 4/21/2021. http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-35502008000100007

82- **What is malware?**, seen on 4/21/2021 : https://www.mcafee.com/en-us/antivirus/malware.html

83- Josh Fruhlinge, **Malware explained: How to prevent, detect and recover from it**, Seen on 4/22/2021: https://www.csoonline.com/article/3295877/what-is-malware-viruses-worms-trojans-and-beyond.html

84- Backdoor computing attacks, Seen on 4/22/2021: https://www.malwarebytes.com/backdoor/

85- Internal Attack, Seen on 4/24/2021, Website link: https://www.techopedia.com/definition/26218/internal-attack

86- **Cyber Security Goals**, Article, Seen on 4/24/2021, Website link: https://www.javatpoint.com/cyber-security-goals

87- Tactics To Prevent DDoS Attacks & Keep Your Website Safe, Seen on 4/28/2021 at: https://phoenixnap.com/blog/prevent-ddos-attacks

88- How to prevent SQL injection attacks, Seen on 4/29/2021 at: https://www.ptsecurity.com/ww-en/analytics/knowledge-base/how-to-prevent-sql-injection-attacks/

89- Online dictionary Dictionary.com : Biometrics, Seen on 4/30/2021, link: https://www.dictionary.com/browse/biometrics#

90- Mara Karlin, **How to read the 2018 National Defense Strategy**, January 21, 2018, Direct link: https://www.brookings.edu/blog/order-from-chaos/2018/01/21/how-to-read-the-2018-national-defense-strategy/

91- U.S. Cyber Command History, Direct link: https://www.cybercom.mil/About/History/

92- What We Do: Article. Direct link: https://www.nsa.gov/what-we-do/

93- About us. Seen at 5/18/2021. Direct link: https://www.darktrace.com/en/

94- Products, Solutions, and Services, Direct link: https://www.cisco.com/c/en_dz/products/index.html

95- CrowdStire Services, Direct link: https://www.crowdstrike.com/services/

96- Company informations from Palo Alto Networks: Direct link: https://www.paloaltonetworks.com/

97- Top Ransomware Attacks of 2020, Article, Direct link: https://usa.kaspersky.com/resource-center/threats/top-ransomware-2020

98- Mary-Ann Russon, **US fuel pipeline hackers 'didn't mean to create problems**, Direct link: https://www.bbc.com/news/business-57050690

99- Michael D. Shear, Nicole Perlroth and Clifford Krauss, **Colonial Pipeline Paid Roughly $5 Million in Ransom to Hackers**, Direct link: https://www.nytimes.com/

100- SOLARWINDS COMPANY HISTORY TIMELINE, Seen on: https://www.zippia.com/solarwinds-careers-38741/history/

101- Thank you for growing with us. Direct link: https://www.solarwinds.com/20th-anniversary

102- SolarWinds Product Overview Guide, Simple, powerful, and affordable monitoring software IT pros love, Direct link: https://www.solarwinds.com/-/media/solarwinds/swresources/datasheet/swi-ov-brochure-print.ashx?rev=04da25ab90ce4b08ae6e4e07d962f036

103- Russell Brandom, **SolarWinds hides list of high-profile customers after devastating hack**, Article from THE VERGE website: posted on: Dec 15, 2020 , Direct link: https://www.theverge.com/2020/12/15/22176053/solarwinds-hack-client-list-russia-orion-it-compromised

104- SolarWinds' Customers, Original link: https://www.solarwinds.com/company/customers

Back link from Wayback Machine: https://web.archive.org/web/20201214065921/https://www.solarwinds.com/company/customers

105- **SolarWinds Security Advisory**, Information about SUNBURST, Direct link: https://www.solarwinds.com/sa-overview/securityadvisory

106- Senators Request Information from FBI, CISA on Reports of Russian Cyberattack Against the U.S. Government, Dec 15 2020, Direct link: https://www.moran.senate.gov/public/index.cfm/2020/12/senators-request-information-from-fbi-cisa-on-reports-of-russian-cyberattack-against-the-u-s-government

107- Drew Harwell, Douglas MacMillan, **Investors in breached software firm SolarWinds traded $280 million in stock days before hack was revealed**, Seen on 5/23/2021. Direct link: https://www.washingtonpost.com/technology/2020/12/15/solarwinds-russia-breach-stock-trades/

108- TTP Table for Detecting APT Activity Related to SolarWinds and Active Directory/M365 Compromise, https://us-cert.cisa.gov/ncas/current-activity/2021/03/17/ttp-table-detecting-apt-activity-related-solarwinds-and-active

109- Jeremiah Talamantes, **What is Red Teaming And Why Do I Need It?,** https://www.redteamsecure.com/blog/what-is-red-teaming-and-why-do-i-need-it-2

110- SUNBURST,Article, Seen on 5/23/2021, https://attack.mitre.org/software/S0559/

111- **Tracking UNC2452-Related Reporting**, Seen on5/23/2021, Direct link: https://github.com/center-for-threat-informed-defense/public-resources/blob/master/solorigate/README.md

112- **SUNBURST: How it Happened and How to Minimize the Risk of Future Nation-State Attacks**, 12/23/2020, Direct link: https://securityboulevard.com/2020/12/sunburst-how-it-happened-and-how-to-minimize-the-risk-of-future-nation-state-attacks/

113- Forge Web Credentials: SAML Tokens, https://attack.mitre.org/techniques/T1606/002/

114- Patrick Orzechowski, Greg Genung, Threat Report: **SolarWinds Attack - Part II - Is MITRE ATT&CK Falken's Maze?**, Published date: 02.18.21, Seen on 5/23/2021. Direct link: https://www.deepwatch.com/blog/solarwinds-mitre-attck-falkens-maze/

115- MORGAN CHALFANT AND MAGGIE MILLER, **Biden vows to make cybersecurity 'imperative' following massive hack**, 12/17/20. Seen on 5/23/2021. Direct link: https://thehill.com/policy/cybersecurity/530706-biden-vows-to-make-cybersecurity-imperative-following-massive-hack

116- MAGGIE MILLER, **US intel agencies blame Russia for massive SolarWinds hack**, Seen on 5/23/2021. Direct link: https://thehill.com/policy/cybersecurity/532756-us-intel-agencies-blame-russia-for-massive-solarwinds-hack

117- Christopher Bing, Joseph Menn, **After big hack of U.S. government, Biden enlists 'world class' cybersecurity team**, Seen on 5/23/2021. Direct link: https://www.reuters.com/article/us-usa-biden-cyber/after-big-hack-of-u-s-government-biden-enlists-world-class-cybersecurity-team-idUSKBN29R18I

118- Christopher Bing, Jack Stubbs, Raphael Satter, Joseph Menn, **Exclusive: Suspected Chinese hackers used SolarWinds bug to spy on U.S. payroll agency – sources**, https://www.reuters.com/article/us-cyber-solarwinds-china-exclusive/exclusive-suspected-chinese-hackers-used-solarwinds-bug-to-spy-on-u-s-payroll-agency-sources-idUSKBN2A22K8

119- Biden administration preparing to sanction Russia for SolarWinds hacks and the poisoning of an opposition leader. Seen on 5/23/2021. Direct link: https://www.nationthailand.com/news/30402990

120- **Threat Group Cards: A Threat Actor Encyclopedia**, Thailand Computer Emergency Response Team (ThaiCERT) Electronic Transactions Development Agency, Direct link: https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=UNC2452%2C%20Dark%20Halo%2C%20SolarStorm

121- Cozy Bear, From Wikipedia; seen on 5/23/2021, Direct link: https://en.wikipedia.org/wiki/Cozy_Bear

ملخص الدراسة

ملخص الدراسة

الملخص:

تهدف هذه الدراسة إلى تقييم والبحث في فعالية أنظمة والسياسات الأمنية الأمريكية في المجال الأمن السيبراني و فعاليته في مواجهة التهديدات السيبرانية من خلال دراسة حالة اختراق شركة SolarWinds ، وهو حادث بارز في مجال الأمن السيبراني كشف عن نقاط ضعف في شبكات القطاعين العام والخاص. تحلل الدراسة بشكل نقدي التدابير الأمنية المطبقة قبل الاختراق وأثنائه وبعده لتحديد أوجه النقائص التي أدت الى هذا الاختراق وكذا اقتراح تحسينات التي يمكن العمل وفقها لتجنيب تكرار مثل هذه الحوادث . تم التطرق للسياسات والإستراتجيات التي عملت عليها إدارة الرئيس باراك أوباما في الفترة الممتدة بين 2009-2017 في جانب حماية و تعزيز الأمن السيبراني في الجانب المدني و الدفاعي العسكري للولايات المتحدة الأمريكية ، و كذا الرئيس الذي خلفه دونالد ترامب بين فترة 2017-2021.

أصبح الأمن السيبراني ركيزة أساسية للأمن القومي، حيث تشكل الهجمات الإلكترونية المدعومة من الدول تحديات كبيرة حتى لأكثر الأنظمة تطورًا. يُعزى اختراق SolarWinds إلى مجموعة APT29 المدعومة من الدولة الروسية، واستهدف البنية التحتية الحيوية من خلال استغلال الثغرات في منصة Orion البرمجية واسعة الاستخدام. كشف هذا الحادث عن محدودية أطر الأمن السيبراني في الولايات المتحدة ، برغم من السياسات المنتهجة من طرف رؤساء الولايات المتحدة الأمريكية " باراك أوباما و دونالد ترامب " خلال فترة 2009-2021 في استراتجياتهم لدفاع و الأمن السيبراني، مما أبرز الحاجة إلى إعادة تقييم استراتيجيات الدفاع الوطني ضد التهديدات السيبرانية المتطورة.

الكلمات المفتاحية:

الأمن السيبراني ، الهجومات السيبرانية ، سولارويندز ، الولايات المتحدة ، التهديدات السيبرانية ، الإختراق ، الإختراق السيبراني ، الهجمات الإلكترونية ، الهجمات الإلكترونية ، استراتيجيات الدفاع السيبراني ، إدارة المخاطر السيبرانية.

Summary:

This study aims to evaluate and investigate the effectiveness of American security systems and policies in the field of cybersecurity and their efficiency in confronting cyber threats, through the case study of the SolarWinds breach. This prominent cybersecurity incident revealed vulnerabilities in the networks of both the public and private sectors. The study critically analyzes the security measures implemented before, during, and after the breach to identify the shortcomings that led to this incident, as well as to propose improvements that could help prevent similar occurrences in the future.

The study also addresses the policies and strategies pursued by President Barack Obama's administration during the period from 2009 to 2017 to protect and enhance cybersecurity in both the civilian and military defense sectors of the United States, as well as the subsequent measures taken by President Donald Trump during his term from 2017 to 2021.

Cybersecurity has become a cornerstone of national security, with state-sponsored cyberattacks posing substantial challenges even to the most advanced systems. The SolarWinds breach is attributed to APT29, a state-backed group from Russia, which targeted critical infrastructure by exploiting vulnerabilities in the widely used Orion software platform. This incident revealed the limitations of U.S. cybersecurity frameworks, despite the policies implemented by U.S. Presidents Barack Obama and Donald Trump during 2009–2021 in their cybersecurity defense strategies. It highlighted the need to reassess national defense strategies against evolving cyber threats.

Key words: Cyber Security, Cyber Attacks, United States, Cyber Threats, SolarWinds. Cyber Risk Management, National Security, Cyber Defense Strategies, Hacking.

Résumé:

Cette étude vise à évaluer et examiner l'efficacité des systèmes et politiques de sécurité américains dans le domaine de la cybersécurité, ainsi que leur capacité à faire face aux cybermenaces, à travers l'étude de cas de la violation SolarWinds. Cet incident majeur de cybersécurité a révélé des vulnérabilités dans les réseaux des secteurs public et privé. L'étude analyse de manière critique les mesures de sécurité mises en œuvre avant, pendant et après la violation, afin d'identifier les lacunes ayant conduit à cet incident, ainsi que de proposer des améliorations susceptibles de prévenir des occurrences similaires à l'avenir.

Elle aborde également les politiques et stratégies adoptées par l'administration du président Barack Obama durant la période 2009-2017 pour protéger et renforcer la cybersécurité dans les secteurs de la défense civile et militaire des États-Unis, ainsi que les mesures ultérieures prises par le président Donald Trump pendant son mandat de 2017 à 2021.

La cybersécurité est devenue une pierre angulaire de la sécurité nationale, les cyberattaques parrainées par des États représentant des défis majeurs même pour les systèmes les plus avancés. La faille SolarWinds est attribuée à APT29, un groupe soutenu par l'État russe, qui a ciblé des infrastructures critiques en exploitant des vulnérabilités dans la plateforme logicielle Orion, largement utilisée. Cet incident a révélé les limites des cadres de cybersécurité des États-Unis, malgré les politiques mises en œuvre par les présidents Barack Obama et Donald Trump entre 2009 et 2021 dans leurs stratégies de défense en cybersécurité. Il a souligné la nécessité de réévaluer les stratégies de défense nationale face à l'évolution des menaces informatiques.

Mots clés: Cybersécurité, Cyberattaque, SolarWinds, États-Unis, Menaces Cybernétiques, Piratage, Gestion Des Risques Cybersécurité, Cyberstratégie.