PISSN : 2571-9904 - EISSN : 2602-7763

الهجمات السيبرانية بين الواقع وسبل المواجهة.

Cyber attacks between reality and ways of confrontation

محمد الصغير كاوجة.

جامعة قاصدي مرباح ورقلة (الجزائر)، kaoudja@gmail.com

تاريخ الاستلام: 18/ 07/ 2022 تاريخ القبول: 16/ 09/ 2022 تاريخ النشر: 30/ 09/ 2022

ملخص:

باتت الهجمات السيبرانية في الآونة الأخيرة سلاح فتاك استخدمته قوى مختلفة سعيا منها لتحقيق غايات محددة، هذا السلاح الذي يعتمد على فكرة الهجوم التكنولوجي الافتراضي أضحى اليوم أكثر خطورة يهدد أمن و سرية و خصوصية البيانات، فقد مس بأمن العديد من الدول و أسرارها حيث تعرضت العديد من الدول إلى اختراقات و قرصنة الكترونية خطيرة تم الفضح من خلالها على أهم البيانات و الخصوصيات التي تهدد أمنها، فالأمر أصبح أكثر صعوبة مما كان عليه سابقا إذ أضحت الكثير من المنظومات و المؤسسات في خطر فهي معرضة للاختراق من قبل هذه الجهات الخطيرة التي تسعى إلى فضح أسرار و خصوصيات كبرى من شأنها الإطاحة بمنظومة معينة أو حتى دولة، وعليه تهدف هذه الورقة العلمية إلى التعرف على ماهية هذه الهجمات السيبرانية، بالإضافة إلى التطرق إلى أبرز أنواعها، كما تسعى الدراسة إلى تقديم سبل مواجهة هذه الهجمات و أهم طرق الوقاية منها لتجنب مثل هذه المخاطر الالكترونية و الوصول إلى البيانات.

الكلمات المفتاحية: الفضاء الالكتروني، الأمن السيبراني، الهجمات السيبرانية، حروب الجيل الجديد.

Abstract:

Cyber attacks have recently become a lethal weapon used by various forces in an effort to achieve specific goals This weapon, which depends on the idea of virtual technological attack, has become more dangerous that threatens the security, secret and privacy of data, He touched the security of many countries and their secrets, as many countries have been subjected to dangerous electronic piracy and piracy through which the most important data and privacy that threatens their security.

The matter has become more difficult than it was previously, as many systems and institutions have become in danger, as they are subject to penetration by these dangerous bodies that seek to expose major secrets and specifics that would overthrow a specific system or even a state, accordingly, this scientific paper aims to identify what these cyber attacks are, in addition to addressing the most prominent types, and the study seeks to provide ways to confront these attacks and the most important ways to prevent them to avoid such electronic risks and access to data.

Keywords: *Electronic space, cybersecurity, cyber attacks, new generation wars.*

I. مقدمة

منذ انتشار تكنولوجيا الإعلام و الاتصال الحديثة زاد اعتماد الأفراد و المجتمعات على استخدامها، مما جعل فكرة الاستغناء عن خدماتها أمرا مستحيلا، فق أضحى الفضاء السيبراني مرتبطا بجميع المجالات و الميادين في كافة أنحاء العالم، فالمقصود بالفضاء السيبراني هو تلك البيئة الافتراضية التي تعمل من خلال الاتصال بشبكة الانترنت و الذي يشمل أجهزة الكمبيوتر و أنظمة الشبكات و البرمجيات، فبالنظر إلى الخدمات و التسهيلات التي وفرتها هته الأخيرة لمستخدميها، و كذا التطورات الهائلة التي شملت جميع الميادين سواء السياسية أو الاقتصادية أو الاجتماعية، إلا أنها في الوقت ذاته أصبحت بمثابة التهديد المباشر و السلاح القوي للكثير من الهيئات و الجمعيات البشرية التي كرست هذه التكنولوجيات لنشر الذعر و الهلع في نفوس البش، و كذا في تحقيق غاياتها الشنيعة، هذه الأخيرة التي تستهدف أنظمة المعلومات و الشبكات العنكبوتية و التي تعرف بالهجمات السيبرانية، و التي شكلت مخاطر كبرى و مست بأمن العديد من الأفراد و الجماعات.

الهجمات السيبرانية الخطر الذي يهدد البشر و يلحق الأذى بهم على مختلف الأصعدة ، هذه الهجمات التي قد تكون من قبل دول ذات سيادة أو من قبل منظمات و عصابات و قد تكون أيضا ذات مصادر مجهولة، و ذلك لتحقيق أهدافها المختلفة و التي قد تكمن في كشف أسرار دولة ما أو هيئة أو حتى منظمة بهدف سرقة بيانات أو تعطيلها ، كما أن لهذه الهجمات أنواع و أصناف تختلف عن بعضها البعض، و بالتالي لهذه الهجمات أهداف محددة تسعى لتحقيقها بشتى الوسائل و الطرق ، كما أنها في الوقت ذاته تواجه تحديات و صعوبات تعثر نجاحها. و من خلال هذه الورقة العلمية سنسلط الضوء على ماهية هذه الهجمات السيبرانية، و ما هي أبرز أنواعها، و كذا محاولة معرفة سبل مواجهتها.

تسعى هذه الدراسة إلى تسليط الضوء على ظاهرة الهجمات السيبرانية التي أصبحت من أخطر القضايا الدولية في عصرنا الحاضر بالنظر إلى اتساع نطاق استخدام التكنولوجيا الحديثة في العالم، لذا من الأهمية بمكان معرفة أسبابه لمعرفة كيفية مكافحته في ظل قلة الدراسات والبحوث حولها، كما تنبع أهمية الدراسة من كونها تعد دراسة تسعى إلى التطرق إلى أبرز سبل مواجهة هذه الهجمات السيبرانية ، و كذا أبرز الطرق و الوسائل و الجهود المبذولة لمكافحتها.

بالإضافة إلى كون هذه الدراسة تهدف إلى محاولة الوقوف على أهم سبل و طرق مواجهة هذه الهجمات الخطرة، و كذا الإشارة إلى مدى خطورة هذه الهجمات على الأمن القومي، كما نسعى أيضا من خلال هذه الورقة العلمية إلى إلقاء الضوء على أبرز أنواع الهجمات السيبرانية و طرق تطبيقها.

أما فيما يخص الدراسات السابقة التي تناولت موضوع الهجمات السيبرانية و أولته أهمية و التي تم الاستعانة بها في هذه الدراسة أغلبها جاءت مشابهة، فمن بين الدراسات السابقة نذكر دراسة للدكتور علم الدين بانفا المعنونة بـ مخاطر الهجمات الالكترونية (السيبرانية) و آثارها الاقتصادية: دراسة حالة دول مجلس التعاون الخليجي.

1. إشكالية الدراسة:

أصبحت الهجمات السيبرانية تشكل خطرا كبيرا يهدد الدول و المنظمات و مختلف المؤسسات، هذه الأخيرة التي تشن عبر فضاء افتراضي من قبل جهات مجهولة بغية الوصول إلى أهدافها المرجوة و الاستيلاء على خصوصيات المؤسسات و الشركات، فهي بمثابة وسيلة قتالية حربية حديثة ظهرت نتيجة التطورات التكنولوجية، هذه الهجمات التي لها أنواع عديدة تختلف عن بعضها البعض، كما توجد طرق و سبل وقاية لتفادي مثل هذه الهجمات. الأمر الذي دفع بنا إلى طرح التساؤل التالي: ما هي الهجمات السيبرانية، و ما هي أبرز أنواعها، و ما هي أهم سبل الوقاية منها؟

من هذا التساؤل الرئيسي تثار مجموعة من التساؤلات الفرعية وهي كالتالي:

1- ما المقصود بالهجمات السيبرانية؟
2- ما هي أبرز أنواع هذه الهجمات؟
3- ما هي مقومات هذه الهجمات السيبرانية؟
4- ما هي أخطر الهجمات التي شهدها العالم؟
5- ما هي أبرز الاستراتجيات و السبل لمواجهتها؟

و للإجابة على هذا الإشكال نعتمد على المحاور التالية:

- المحور الأول: مدخل مفاهيمي.
- المحور الثاني: أنواع الهجمات السيبرانية.
- المحور الثالث: نماذج عن الهجمات السيبرانية.

2. مفهوم الهجمات السيبرانية:

إن مصطلح الهجمات السيبرانية مكون من لفظين الهجمات و السيبراني، فللوصول إلى مفهوم كلي لابد من التطرق إلى كلا اللفظين.

2.1 الهجوم:

يقصد بالهجوم عادة عملية عسكرية تهدف إلى احتلال بلاد أو مدينة معينة أو تحقيق غرض معين. الهجوم في حقيقة الأمر هو الغزو الذي يتم لتحقيق أهداف عسكرية خلال الاستراتجيات و العمليات والتكتيكات العسكرية، كما يعتبر الهجوم من أشهر الطرق التي تستعملها الجيوش لتحقيق النصر، فضلا عن اشتمال وسيلة الهجوم على جانب أساسي يعتمد على الدفاع لنجاح العملية الهجومية. (مجدي، 2020)

2.2 السيبراني:

لغة: إن كلمة سايبر أو سيبراني تعتبر ترجمة حرفية لكلمة (Cyber) و المشتقة من كلمة (Cybernetice).

كما يعرفها قاموس Oxfordالانجليزي على أنها "دراسة فاعلية العمل البشري بمقارنتها بفاعلية الالات الحاسبة تتصل بسمات و خصائص الحواسيب و تكنولوجيا المعلومات و الواقع الافتراضي" (عطية)

كما تعني كلمة سايبر "ترابط البنيات التحتية لشبكات تكنولوجيا المعلومات، و تضم أدوات أو وسائل التكنولوجيا مثل الانترنت".(بانفا، 2019، صفحة 12)

اصطلاحا: معنى مصطلح سيبراني وهي تعني الإلكترونية، وقد أُصطلح على أن تُطلق كلمة "سيبراني" على كل ما يتعلق بالشبكات الإلكترونية الحاسوبية، وشبكة الإنترنت، ومثلًا عندما نقول الفضاء السيبراني، فهذا يعني الفضاء الإلكتروني(Cyberspace)، فهذا يعني كل ما يتعلق من قريب أو بعيد بشبكات الحاسوب، والإنترنت، والتطبيقات المختلفة (كالوتسآب، والفيس بوك، وغيرها من مئات التطبيقات)، وكل الخدمات التي تقوم بتنفيذها (كتحويل الأموال عبر النت، والشراء أون لاين،) وغيرها من آلاف الخدمات في جميع مجالات الحياة على مستوى العالم.(ملكاوي، 2019).

2.3 الهجوم السيبراني: تعرف بأنها: "أعمال تقوم بها دولة تحاول من خلالها اختراق أجهزة الكومبيوتر والشبكات التابعة لدولة أخرى بهدف تحقيق أضرار بالغة أو تعطيلها" (زروقة، 2019)

كما عرفها (Michael N.Schmitt) بأنها "تلك الإجراءات التي تتخذها الدولة من أجل الهجوم على نظم المعلومات للعدو بهدف التأثير و الأضرار فيها، والدفاع عن نظم المعلومات الخاصة بالدولة المهاجمة." (Schmitt, 1998-1999, p. 890)

و عرفها عبد القادر محمد فهمي بأنها: "هجمات تستخدم فيها المنظومة الشبكية و الأجهزة الحاسوبية للدولة، أو الفاعلين من غير الدول، لتعطيل كفاءة السيطرة و القدرة على التحكم في منظومة أجهزة أو شبكات الحاسوب و ما تتضمنه من بيانات و معلومات للفاعلين الآخرين من الدول و غير الدول، أو تقليلها، أو حتى تدميرها، سواء كان ذلك على مستوى منظومات قوتها العسكرية، و بالشكل الذي يعرض الأمن القومي للدولة إلى تهديد جسيم.' (عبد الواحد، 2021، صفحة 22)

كما تتميز الحرب السيبرانية عن الحرب التقليدية في أن المفهوم التقليدي للحرب ينطوي على استخدام الجيوش النظامية و يسبقها إعلان واضح لحالة الحرب و ميدان قتال محدد، بينما تبدو هجمات الفضاء الالكتروني غير محددة المجال و غامضة الأهداف، كونها تتحرك عبر شبكات المعلومات و الاتصالات المتعدية للحدود الدولية. (زروقة، 2019، صفحة 1026)

3. أنواع الهجمات السيبرانية:

إن الهجمات السيبرانية تبدأ عندما يتمكن المجرم الإلكتروني من إيقاع ضحيته في المصيدة بعد إقناعه أن المصدر أو الملف المرسل موثوق به، إذ يتم إرسالها على شكل بريد إلكتروني أو رسالة نصية ، وحينما يتم استقبال المتلقي للرسالة وينقر على الرابط يتم تثبيت برامج ضارة على جهازه أو تجميد النظام كجزء من هجوم برامج الفدية أو اختراق الخصوصية الخاصة به. كما تكمن طبيعة الهجمات السيبرانية في مجموعة من العمليات و التي "تشمل عمليات التسلل إلى أنظمة الحاسب الآلي، أو تصديرها، أو إتلافها، أو تغيرها،أو تشفيرها، كما تشمل عمليات زرع برمجيات ضارة للتجسس.

ويرى محمد فهمي بأن الهجمات الالكترونية تشمل أشكال كثيرة، من سرقة المعلومات، و التجسس، و نشر معلومات سرية و فضح الأنظمة السياسية لأغراض التحريض، و نشر أفكار مضادة، و خلق تيارات معارضة، و إثارة احتجاجات . (عبد الواحد، 2021، صفحة 23)

و عليه تأتي هذه الهجمات على الأشكال التالية:

1.3 الاختراق: يعد الاختراق القدرة على الوصول للبيانات و المعلومات الخاصة بشخص ما، فالهجمات هدفها الأساسي تغير المعطيات أو محو معلومات، أو هجمات الحرمان من الخدمة هذا النوع عموما سهل التنفيذ وعادة لا يسبب إلا القليل من الضرر.

2.3 التجسس: يقصد بالتجسس تلك الطرق لاختراق المواقع الالكترونية ومن ثم سرقة بعض المعلومات والتي قد تكون في قائمة الأهمية والخطورة للطرف المتلقي والمسروق منه، و ذلك باستخدام أحصنة طروادة وبرامج التجسس بهدف سرقة المعلومات السرية التي لم يتم تأمينها بشكل صحيح يمكن أن يتم اعتراضها أيضا وقرصنتها.

3.3 وقف المعدات أو تخريبها: يستهدف هذا النوع من الهجوم على الأنشطة العسكرية التي تستخدم أجهزة الكمبيوتر والأقمار الصناعية لتنسيق وسائل الدفاع. يمكن اعتراض الأوامر والاتصالات أو تغييرها، مما يعرض القوات للخطر.

4.3 الهجمات السيبرانية على البنية التحتية الحساسة: تهدف هذه الهجمات السيبرانية لتعطيل محطات الطاقة وتوزيع المياه وأنابيب النفط والاتصالات ووسائل النقل والمستشفيات وغيرها من البنى التحتية الحساسة للدول.

4. نماذج عن الهجمات السيبرانية:

إن تاريخ الهجمات والجرائم الإلكترونية تاريخ طويل فهو يعود لأواخر الثمانينيات، وتحديداً عام 1988، عندما أراد روبرت تابان موريس، ابن عالم التشفير الشهير روبرت موريس، أن يعرف عدد الأجهزة المتصلة بالإنترنت، كما أسس موريس برنامجا ينتقل من حاسوب إلى آخر بطلب إشارة من الجهاز المرسل له، هذا الأخير الذي شكل أخطر الهجمات الالكترونية و الذي يدعى بـ"الحرمان الموزع للخدمة"و الذي تسبب بإيقاف النظام أو حظر اتصالات الشبكات المتصلة بالأجهزة. هذه الأخيرة التي اتسعت رقعتها و انتشرت و تطورت مع التغيرات الحاصلة جراء التكنولوجيات الحديثة، و التي يمكن أن نذكر أخطرها و أكثرها ضررا على العالم:

1.4 الهجمات السيبرانية على مختلف دول العالم:

إن العالم أكثر ترابطا على الصعيد الرقمي اليوم منه في أيّ وقت مضى. ويستغل المجرمون هذا التحول الإلكتروني لاستهداف نقاط الضعف في المنظومات والشبكات والبنى التحتية عبر الإنترنت. ويخلّف هذا الوضع تبعات اقتصادية واجتماعية هائلة على الحكومات والشركات والأفراد في العالم أجمع.

وما التصيد الاحتيالي وبرمجيات انتزاع الفدية وانتهاكات البيانات سوى أمثلة قليلة على التهديدات السيبرية الراهنة، بينما تظهر على الدوام أشكال جديدة من الجريمة السيبرية. ومرتكبو الجرائم السيبرية هم أكثر فأكثر مرونة وتنظيما، ويستغلون التكنولوجيا الجديدة ويكيفون اعتداءاتهم ويتعاونون فيما بينهم بطرق مبتكرة.

والجرائم السيبرية لا تعرف الحدود. فالجناة والضحايا والبنى التحتية التقنية ينتمون إلى اختصاصات قضائية متعددة، مما يضيف على التحقيقات والملاحقات القضائية العديد من التحديات.

والتعاون بين الشركاء من القطاعين العام والخاص هو بالتالي بالغ الأهمية. والإنتربول، بحضوره العالمي، يضطلع بدور أساسي في إقامة الشراكات بين القطاعات والتعاون الدولي بين أجهزة إنفاذ القانون.

نحن في الإنتربول ننسق عمليات إنفاذ القانون، ونوفر منصات مأمونة لتبادل البيانات، ونقدم التحليل والتدريب لتقليص التهديدات السيبرية. ومن خلال تعزيز قدرة بلداننا الأعضاء على منع الجرائم السيبرية وكشفها والتحقيق فيها وتقويضها، يمكننا المساعدة على حماية المجتمعات لجعل العالم أكثر أمان.

أنواع الجرائم الإلكترونية:

قد تنقسم الجرائم الالكترونية الى ثلاثة أقسام وهي: جرائم نقوم بالحديث عن الجرائم ضد الأفراد: وقد سميت الجرائم الالكترونية الشخصية وقد تتمثل في سرقة الهوية ومنها الايميل الالكتروني وانتحال شخصية أخرى بطريقة غير شرعية عبر الإنترنت بهدف الاستفادة من هذه أو لإخفاء هوية المجرم لتسهيل عملية الإجرام.
الجرائم ضد الملكية: تتمثل في ارسال مواقع أو روابط ضارة المضمنة في بعض البرامج التطبيقية والخدمية أو غيرها، والتي تهدف الى تدمير الأجهزة أو البرامج المملوكة للشركات أو الأجهزة الحكومية أو البنوك أو حتى الممتلكات الشخصية.
الجرائم ضد الحكومات: مهاجمة مواقع الحكومات الرسمية وأنظمة الشبكات الحكومية والتي تستخدم تلك التطبيقات على المستوى المحلي والدولي كالهجمات الإرهابية على شبكة الإنترنت، وهي تهدف الى تدمير البنى التحتية ومهاجمة شبكات الكمبيوتر وغالبا ما يكون هدفها سياسي وتستخدم غالبا في الحروب.
هذه بعض أنواع الجرائم الالكترونية والتي مازالت الى اليوم تتطور وبشكل سريع، ونظراً لتعدد أنواع الجرائم الالكترونية وتطورها برزت الحاجة لدى دول العالم لسن قوانين وتشريعات تنظم استخدام الانترنت وفرض عقوبات لمن يسيء استخدامه بأي صورة كانت..

الجرائم الالكترونية واسبابها:

التحضر: فهي تعتبر من أكثر الأسباب شهرة أمام مرتكبو الجرائم الإلكترونية، فإنَّ الانتقال من الريف إلى المدينة مفضّل لدى فئة وشريحة كبيرة من الشباب، خاصة الذين لا يمتلكون مبالغ يلبّون ويغطّون فيها احتياجاتهم وهو سبب رئيسي في ارتكابهم للجرائم بشتى أشكالها، التي لا تتطلب منهم مبالغ مالية لممارستها.
البطالة: حيث تعتبر البطالة والظروف الاقتصادية الصعبة، سبب يدفع فيه الكثير من الشباب للاستثمار في القيام بالجرائم الإلكترونية.
الضغوط العامة: ويقصد بها الضغوط أو الظروف التي يتعرّض لها المجتمع، سواء كانت هذه الضغوط الفقر، الأميّة، البطالة وعوامل أخرى ضاغطة على عامة المجتمع وعلى فئة الشباب خاصة. وتقوم هذه

الضغوط بدفع المجتمع إلى التأقلم بشكل سلبي وهو ما يساهم في المتاجرة بالبشر والجنس بشكل إلكتروني وغيرها.

البحث عن الثراء: ويقصد بذلك قيام المجتمع بسلوك يجعلهم يحصلون على متعة، بعيداً عن الآلام مستخدماً بذلك وسائل وطرق غير مقبولة؛ بهدف الوصول إلى أهدافهم والتي من الصعب الحصول عليها. وبالتالي يلجأ المجتمع إلى الجرائم الإلكترونية والتي تكون أكثر سهولة وسرعة في التنفيذ وتكون ذات مخاطر قليلة.

- **هجوم برامج الفدية:** برامج الفدية هي نوع من البرمجيات الضارة (البرمجيات الخبيثة) التي يستخدمها المجرمون الإلكترونيون،يعمل ذلك الفيروس على حجب الوصول إلى النظام أو يقوم بتشفير البيانات الموجودة، إذ يطلب المجرمون الإلكترونيون مبلغ فدية من ضحاياهم مقابل فك التشفير عن البيانات.

كما يعد"أحد الأمثلة الأكثر شهرة لهجمات برامج الفدية التي ضربت الشركات في جميع أنحاء العالم في عام 2017 الذي أصاب أكثر من200 ألف جهاز كومبيوتر في أكثر من 150 دولة. كما كلفت هذه الهجمة المملكة المتحدة حوالي 120مليون دولار ، بالإضافة إلى تكاليف عالمية تجاوزت 7 مليار دولار".(تريسي، 2021)

و بعد محاولات كثيرة، تم إيقاف الهجوم الإلكتروني عن طريق مفتاح إيقاف عرضي اكتشفه الباحث في أمن الكمبيوتر، ماركوس هتشينز.

- **هجوم شمعون:** شمعون هو نوع من فيروسات الكمبيوتر الذي يؤدي إلى إصابة أنظمة الكمبيوتر والتجسس على أجهزة الكمبيوتر في قطاع الطاقة. وقد تم استخدامه من قبل مجموعة من المتسللين المعروفة باسم "Cut Swords of Justice" في 15 أغسطس/آب 2012 لزعزعة استقرار أنظمة الكمبيوتر في شركة الطاقة السعودية العملاقة. (تريسي، 2021)

هذا الهجوم الذي أدى إلى شلل أكثر من 30ألف محطة طاقة، أدى الى ضرر كبير بالغ على كافة المعدات و الوسائل المتوفرة بهذه الشركة، و قد "وأعلنت المجموعة مسؤوليتها عن الهجوم الذي طالت العمليات في 30 ألف محطة عمل تابعة للشركة، و من الشركات المتضررة من فيروس الكومبيوتر شركة رأس غاز القطرية وشركة الغاز الطبيعي، حيث تعطلت أنظمة الكمبيوتر مؤقتاً بسبب الفيروس ما تسبب في تعطل نظام الشركة التشغيلي. وتم وصفه لاحقاً بأنه "أكبر اختراق في التاريخ". (تريسي، 2021)

- **هجوم تيتان على وزارة الدفاع الأمريكية:** تيتان هو الاسم الرمزي الذي أُطلق على سلسلة من الهجمات الإلكترونية على أنظمة الكمبيوتر الأمريكية، والتي حدثت في أوائل العقد الأول من القرن الحادي والعشرين عام 2003 واستمرت حوالي ثلاث سنوات، ركزت الهجمات على المقاولين الرئيسيين لوزارة الدفاع التي تم استهدافها بسبب معلوماتها الحساسة، بما في ذلك تلك الموجودة في شركة لوكهيد مارتن، ومختبرات ساندیا الوطنية وريدستون أرسنال ووكالة ناسا. كانت الهجمات الإلكترونية على شكل تجسس إلكتروني، حيث تمكن المهاجمون من الحصول على معلومات حساسة من أنظمة الكمبيوتر. على الرغم من عدم الإبلاغ عن سرقة أي معلومات سرية، إلا أن المتسللين تمكنوا من سرقة معلومات غير سرية (على سبيل المثال معلومات من جهاز كمبيوتر منزلي) يمكن أن تكشف عن نقاط القوة والضعف في الولايات المتحدة. (تريسي، 2021)

- **الهجوم على الوزارات السيادية الأمريكية:** هذا الهجوم السيبراني وصف بالأخطر و الذي ضرب وكالات أمريكية غاية في الأهمية منها وزارة الخارجية و وزارة الأمن الداخلي و عناصر من وزارة الدفاع في هجوم من

أكثر هجمات القرصنة انتشارا، استمرت تداعيات هذا الهجوم 8ساعة من إصدار الحكومة الأمريكية تحذيرا تلزم فيه المستخدمين الأمريكيين بقطع الاتصال ببرنامج إدارة الشبكة الذي تم اختراقه "سولر وينس". (تفاصيل أخطر هجوم سيبراني على الوزارات السيادية الأمريكية، 2020)

- **هجوم Wannacry:** والذي يعد من أشهر الهجومات الالكترونية و أكثرها ضررا و الذي حصل في عام2017 الهجمة المسماة Wannacry "و هي برمجة خبيثة تطالب الضحية بالفدية الكالية و قد أثرت على 300.000 جهاز حاسوب في 150 دولة في العالم. و هجماتPetraو Not Petra و التي تسببت في الحاق خسائر فادحة في بعض الشركات العالمية. فعلى سبيل المثال أعلنت شركات MerckFedex, Maersk خسائر تقدر بحوالي 300مليةن دولار بسبب هذه الهجمات".(بانفا، 2019، صفحة 16)

2.4 الهجمات السيبرانية على الجزائر:

تعرضت الجزائر في السنوات الأخيرة إلى حوالي 95 ألف هجمة الكترونية، و قد سبق و أن تم تصنيفها بأكثر الدول المهددة سيبرانيا حول العالم، و من أخطر هذه الهجمات نذكر:

- **الهجوم السيبراني الإسرائيلي المغربي ضد الجزائر:** أوضح الوزير عمار بلحيمر أن مجموعة إسرائيلية أسسها عام 2010 كل من عمري لافي وشاليفهوليو، وهما من خريجي ما يعرف بوحدة الجوسسة الإسرائيلية العسكرية 8200"، قامت في تنفيذ اختراقاتها باستخدام برنامج التجسس المسمى"Pegasus"الذي استخدم بالمناسبة (ضد المدافعين عن حقوق الإنسان والمحامين والزعماء الدينيين والصحفيين وعمال الإغاثة)، كما "منحت المجموعة رخصة استخدام هذا البرنامج لعشرات الحكومات، لاسيما منها الأنظمة التي لا تتمتع بسمعة طيبة في مجال احترام حقوق الإنسان، مثل المغرب"، حسب قول الوزير بلحمير. وأشار في السياق إلى قضية "واتس آب" التي رفعتها شركة "فيسبوك" أمام محكمة كاليفورنيا ضد مجموعة(NSO) ، كما أوضح أيضا وبموجب هذه الدعوى فإن "WhatsApp"يتهم (NSO) بتنفيذ هجمات سيبراينية استهدفت الهواتف المحمولة لأكثر من 1400 مستخدم في 20 دولة.

وتظل بعض التكنولوجيات الأكثر سرية التي أنتجها مطورون في الكيان الإسرائيلي أكثر قربا بنسخها العسكرية الأصلية، وهذا هو حال أحد البرمجيات الهجومية التي يتم بيعها للدول التي ترغب في التجسس على مواطنيها وكذا للدول المتنازعة، وللشركات الخاصة التي تأمل في الحصول على ميزة أو تفوق على منافسيها أو ضمان حسن استغلال زبائنها والتأثير عليهم وتوجيه خياراتهم التجارية. (الحرب السيبرانية الاسرائلية المغربية ضد الجزائر، 2021)

5. سبل مواجهة الهجمات السيبرانية:

تتعدد سبل مواجهة الهجمات السيبرانية، و التي من شأنها تفادي مثل هذه الهجمات التي تنجر عنها مخاطر عديدة لا حصر لها و التي يمكن أن تلخص على النحو التالي:

1.5 جدران الحماية: تعد من أقوى السبل الوقائية لمثل هذه الهجمات الحادة و الخطرة التي تمس أنظمة الكومبيوتر و الشبكات، و التي تعرف أيضا بتسمية "الجدران النارية" Firewall ، أما عن بداية هذه التقنية فقد" ظهرت في أواخر عقد الثمانينات من القرن الماضي، و ذلك استجابة لعدد من الاختراقات لشبكة الانترنت المستجدة حينذاك، و قد ظهر منها عدة أجيال: الجيل الأول يعرف بـ "مرشحات العبوة" (Packet Filters) ، و

يقوم مبدأ عمله على فلترة (ترشيح) العبوة و التي تمثل الوحدة الأساسية المخصصة لنقل البيانات بين الحواسيب على الانترنت. فإذا كانت العبوة تطابق مجموعة شروط الجدار، فإنه يسمح بمرور العبوة، أو يرفضها و يتخلص منها و يقوم بإرسال إشارة خطأ (Error) للمصدر، في حال لم تكن مطابقة. (عبد الواحد، 2021، صفحة 59)

2.5 التطبيقات المضادة للفيروسات: و مضاد الفيروسات هو برنامج يتم استخدامه لاكتشاف البرمجيات الضارة و منعها من إلحاق الضرر بالحاسوب أو سرقة البيانات الشخصية، و ذلك عن طريق إزالتها أو إجراء التعديلات عليها و إصلاحها، بحيث يمكن لهذا البرنامج أن يتصدى لبرنامج التجسس، و برامج أحصنة طروادة، و التي هي عبارة عن شيفرات صغيرة تقوم ببعض المهام الخفية و غالبا ما تتركز على إضعاف قوى الدفاع و اختراق جهاز الحاسوب و سرقة بياناته، و كذلك تتصدى مضادات الفيروسات لـ"الديدان الحاسوبية" (عبد الواحد، 2021، صفحة 60)

3.5 أنظمة كشف التسلل: كما" تتألف أنظمة التسلل من عدة مكونات هي: جهاز استشعار ينبه على وقوع الأحداث، و لوحة تحكم لمراقبة الأحداث و التنبيهات و التحكم بأجهزة الاستشعار، و محرك يقوم بسجيل إدخالات الأحداث المتلقاة من خلال أجهزة الاستشعار في قاعدة البيانات. و تكون أنظمة كشف التسلل مصنفة بالاعتماد على نوع و موقع أجهزة الاستشعار و المنهجيات المستخدمة على المحرك" (عبد الواحد، 2021، صفحة 61)

II. الخاتمة:

إن الهجمات السيبرانية بتنوع أساليبها و وسائلها المتبعة تبقى من أخطر الهجمات المتبعة من قبل المجرمين الالكترونيين، و قد تم تسليط الضوء في هذا المقال على أبرز أنواعها ، كما تم ذكر أهم و أخطر الهجمات التي شنها المجرمون على مختلف شركات و وزارات العالم ، و كذا تم التطرق إلى أخطر هجوم سيبراني تعرضت له الجزائر، و تم الاستنتاج أنه لابد على كل دولة أو منظمة أو شركة بمختلف القطاعات العمل على حماية أنظمتها و شبكاتها من خلال تعزيز عمليات الأمن السيبراني، بالإضافة إلى أنه يجب على كل منظمة توعية موظفيها بأهم الأساليب الوقائية السبرانية التي من شأنها حماية النظام الداخلي لها دون التعرض لأية هجمات، كل هذا يعمل على تعزيز الأمن و حماية الخصوصيات. كما تم التوصل من خلال هذه الورقة العلمية إلى جملة من المقترحات الهامة بخصوص موضوع الهجمات السيبرانية أبرزها:

- الاستعانة بجدار حماية قوي بإمكانه التصدي لهذا النوع من الهجمات الخطرة.
- الاستمرار في تحديث البرامج و التطبيقات الخاصة بمكافحة الفيروسات.
- استخدام شبكة افتراضية خاصة.
- الاعتماد على كلمات مرور قوية و غير المألوفة.
- عدم فتح المرفقات و الروابط الصادرة من جهات غير الموثوقة أو عن جهات مجهولة.
- تجنب استخدام أو تنزيل البرامج و الملفات في جهاز الكومبيوتر الخاص بك دون التأكد من مصداقيتها.

الإحالات والمراجع:

الكتب العربية:

- إدريس عطية، مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري، (الجزائر، بدون تاريخ)، ص

- علم الدين بانفا، مخاطر الهجمات الالكترونية (السيبرانية) وآثارها الاقتصادية: دراسة حالة دول مجلس التعاون الخليجي سلسلة دراسات تنموية، المعهد العربي للتخطيط بالكويت، (الكويت، 2019)، ص12.

الرسائل الجامعية:

- صلاح حيدر عبد الواحد، حروب الفضاء الالكتروني:دراسة في مفهومها وخصائصها وسبل مواجهتها، رسالة مقدمة للحصول على درجة الماجستير في العلوم السياسية، قسم العلوم السياسية، كلية الآداب والعلوم، (جامعة الشرق الأوسط، 2021)، ص ص23-61.

المقالات العربية:

- إسماعيل زروقة، الفضاء السيبراني والتحول في مفاهيم القوة والصراع، مجلة العلوم القانونية والسياسية ، المجلد 10، أفريل 2019، ص ص1016-1031.

المقالات الاجنبية:

- Schmitt, M. N, Computer network attack and the use of force in international law, Thoghts on a normalive framework. Columbia: Journal of transnational law,37 , (1998-1999), 890.

مواقع الانترنيت:

- إسراء تريسي، (2021/09/25)، أسوء الهجمات الالكترونية، تاريخ الزيارة 2022/02/21، من عربي بوست: https://arabicpost.net/

- يارا مجدي، (2020/04/22)، الهجوم الدفاعي، تاريخ الزيارة 2022/02/15، من المرسال: https://www.almrsal.com/post/906349

- الحرب السيبرانية الاسرائلية المغربية ضد الجزائر ,16 02 ,2021) from قناة العالم، 2021/02/16، Retrieved 22/02/2022:

https://www.alalam.ir/news/5444098/%D9%85%D8%A7%D8%B0%D8%A7-%D9%88%D8%B1%D8%A7%D8%A1-%D8%A7%D9%84%D8%AD%D8%B1%D8%A8-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D8%A7%D9%84%D8%A5%D8%B3%D8%B1%D8%A7%D8%A6%D9%8A%D9%84%D9%8A%D8%A9-%D8%A7%D9%8

- تفاصيل أخطر هجوم سيبراني على الوزارات السيادية الأمريكية، 17 /12/ 2020، تاريخ الزيارة 2022/02/12، العربية نت.

- فراس ملكاوي، (2019/10/07)، الأمن السيبراني. تاريخ الزيارة 2022/02/20، من الحقيقة الدولية الأقرب إليكم: http://factjo.com/Articles.aspx?Id=1615